DPIA smittesporing

Om behandlingsansvarlig

Behandlingsansvarlig	Folkehelseinstituttet
Navn på prosjektet	Smittestopp
Kontaktpersoner hos behandlingsansvarlig	Camilla Stoltenberg, Geir Bukholm, Gun Peggy S. Knudsen, PVO Erlend Bakken

Trinn 1: Vurdering av om det er behov for å gjennomføre en DPIA

Forklar hva formålet med prosjektet er og hva slags behandling som utføres. Oppsummer om det er behov for å gjennomføre en DPIA.

Utbruddet av Covid-19 er erklært som et alvorlig utbrudd av smittsom sykdom som kan få alvorlige helsekonsekvenser for mange mennesker. Sykdommen er av Verdens helseorganisasjon erklært som en pandemi og en alvorlig hendelse av betydning for internasjonal folkehelse.

Covid-19 har i dag ulik utbredelse i Norge. Fra 10. mars 2020 har Helsedirektoratet registrert at sykdommen har gått over i en ny fase hvor en ikke har klart å identifisere smittekjeden for alle som blir syke.

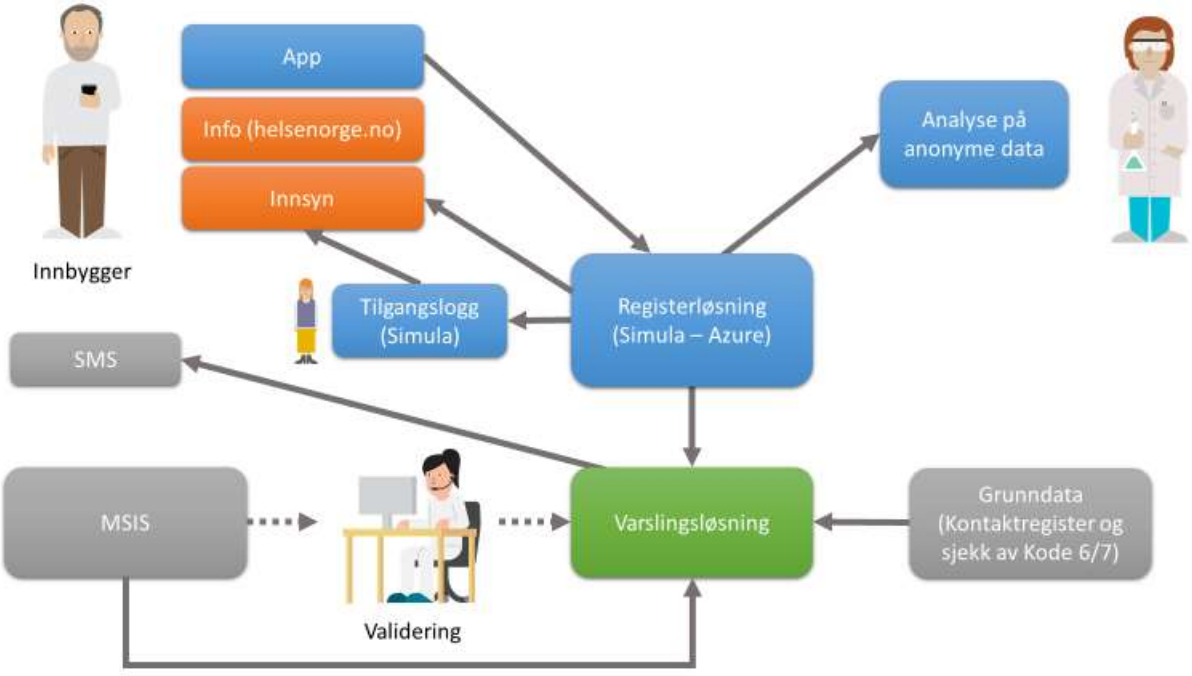
En rekke land har den senere tid innført svært strenge restriksjoner av ulik art. I den nåværende situasjonen er det nødvendig å forebygge og motvirke overføring av SARS CoV-2 virus og Covid-19, og det er avgjørende å få satt i verk tiltak raskt for hele landet.

Folkehelseinstituttet har fått i oppdrag fra Helse- og omsorgsdepartementet å etablere et system for digital og automatisert sporing av nærkontakter til personer som er smittet av koronaviruset SARS CoV-2 og informasjon til nærkontaktene (sporingssystemet).

Hensikten med sporingssystemet er å bidra til rask oppsporing av og formidling av råd til personer som kan være smittet av koronaviruset SARS CoV-2. Videre skal sporingssystemet, gjennom overvåkning på befolkningsnivå, også bidra til å følge smitteutbredelse og vurdere effekt av smitteverntiltak.

Kontaktsporing er rekonstruksjon av en persons bevegelseshistorie for å identifisere personer de kan ha smittet, og blir vanligvis gjort manuelt basert på intervjuer fra et infisert individ. Denne manuelle prosessen er tidkrevende og usikker. Med automatisert kontaktsporing vil man få tilnærmet øyeblikkelig informasjon om personer som kan ha vært utsatt for smitte når en person har blitt bekreftet å være smittet av COVID-19. Sporingssystemet vil dermed kunne supplere og erstatte mye av det manuelle arbeidet som både tar lang tid og tar mye personellkapasitet. Tiltaket vil også gjøre det mulig å lempe på allmenne og brede samfunnsmessige restriksjoner på et tidligere tidspunkt, fordi det er mer målrettet.

Sporingssystemet består av ulike elementer som vist i tegningene nedenfor. Tegningene vil bli endret når man får en helautomatisert varslingsløsning.



Smittestopp medfører behandling av personopplysninger som faller inn under Datatilsynets liste over behandlingsaktiviteter som krever vurdering av personvernkonsekvenser, jf. GDPR art. 35 nr. 4. Sporingssystemet i appen forutsetter bruk av algoritmer knyttet til lokasjonsdata og vil omfatte behandling av personopplysninger i stor skala hensyntatt antall personer inkludert, detaljeringsgrad av personopplysninger som vil behandles, appens planlagte varighet og geografiske omfang. I tillegg faller behandlingen av personopplysningene inn under flere av de øvrige kriteriene Artikkel 29-gruppen har fastsatt for å få oversikt over behandlinger som krever en vurdering av personvernkonsekvenser på grunn av deres iboende høye risiko. Smittestopp medfører behandling av særlige kategorier av personopplysninger etter GDPR art. 9 idet helseopplysninger om påvist smitte hos brukerne av appen vil inngå. Behandlingen medfører også sammenstilling av ulike datasett. Det vil blant annet gjøres koblinger mellom MSIS-databasen og mobiltelefonnummer som hentes fra det sentrale Kontakt- og reservasjonsregisteret. Bruk av slike data, sammen med lokasjonsdata, til å kartlegge smittespredning og varsle befolkningen på nye måter er nytt og innovativt både i nasjonal og internasjonal sammenheng. På denne bakgrunn er det vurdert å være sannsynlig at behandlingen av personopplysninger i løsningen vil medføre en høy risiko for fysiske personers rettigheter og frihet og lagt til grunn at en personvernkonsekvensvurdering er nødvendig, jf. GDPR art. 35 nr. 1.

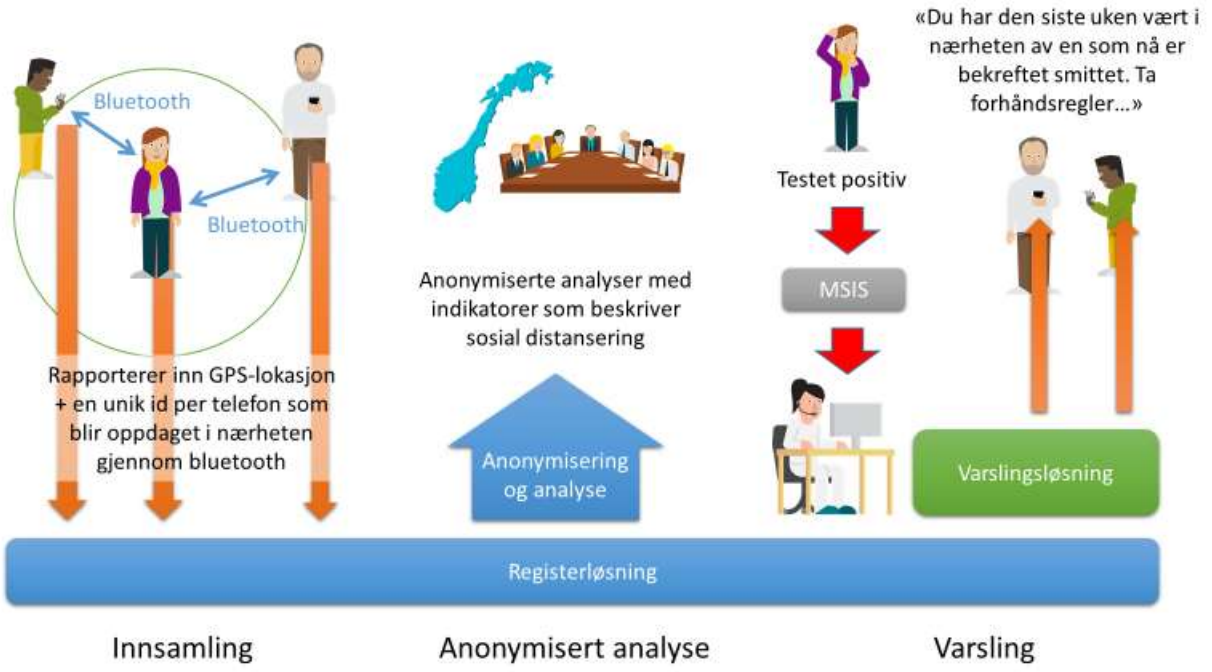
Alle elementene ved løsningen er ikke ferdige på nåværende tidspunkt. Dette gjelder for eksempel analysesystemet og innsynsløsningen. Det legges derfor opp til at DPIA utvides etter hvert, gjennom nye versjoner av DPIA.

Trinn 2: Beskrivelse av behandlingsaktivitetene

Beskriv behandlingsaktivitetene: *Hvordan skal du samle inn, behandle og slette personopplysninger? Hva er kildene? Hvem vil du dele personopplysningene med?*

Hvordan skal du samle inn, behandle og slette personopplysninger? Hva er kildene?

Gjennom sporingssystemet vil FHI innsamle, lagre, analysere (personopplysninger vil analyseres i varslingsløsningen, og i tillegg vil anonyme data analyseres i analyseløsningen), sammenstille, og slette personopplysninger. Den nærmere behandlingen av personopplysninger i de ulike elementene er beskrevet nedenfor.



Innsamling av data om brukernes bevegelsesmønster, samt kontakt med andre mobiltelefoner (Smittestopp-appen)

Lokasjonsdata samles inn fra brukere som har lastet ned og aktivert appen Smittestopp. Applikasjonen benytter telefonnummer som identifikator ved at brukeren taster inn telefonnummeret sitt og mottar autorisasjon via SMS.

Mellom telefoner som utveksler kontaktinformasjon over Bluetooth benyttes en unik id heller enn telefonnummer, og koblingen mellom denne id-en og telefonnummer er lagret separat i registerløsningen. Ved et innbrudd på en enkelt app på en telefon vil det derfor ikke være mulig å hente ut telefonnummer til andre personer som denne telefonen har vært i kontakt med over bluetooth.

Det er frivillig å laste ned og å bruke Smittestopp. Bruker vil motta informasjon om Smittestopp (brukervilkår) og personvernpolicy og må akseptere disse før brukeren laster ned Smittestopp.

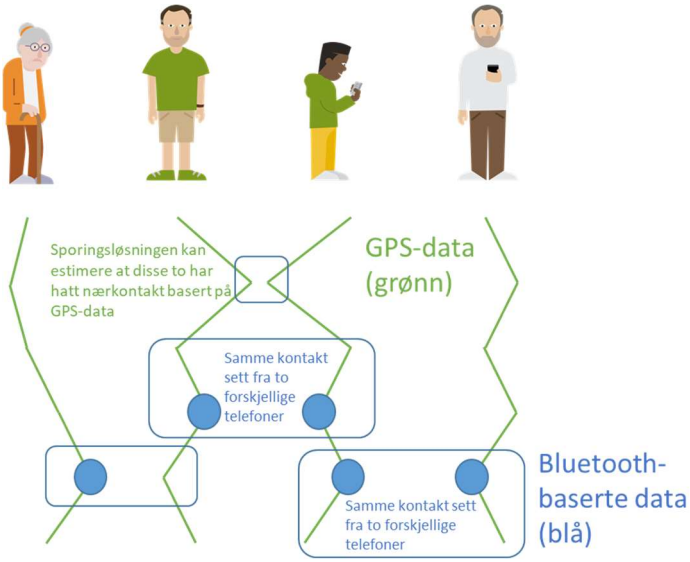
Applikasjonene samler automatisk inn data om brukernes bevegelsesmønster fra GPS, samt kontakt med andre mobiltelefoner i nærheten som har lastet ned appen via Bluetooth sensorene på telefonene. Brukeren må aktivere Bluetooth funksjonen, og kan enkelt slå av og på lokasjon- og bluetoothrapportering midlertidig i en innstilling i applikasjonen. Applikasjonen mellomlagrer dataene fra GPS og Bluetooth og laster opp data til sporingsløsningen hver time når mobilen har mobildata eller Wifi-tilkobling. Utenfor dekning venter appen på å laste ned data til den får internett, men data vil også slettes på telefonen innen 30 dager hvis disse ikke blir lastet opp før. Data lastes opp til en database i skyen i den sentrale lagringsplassen («sporingssystemet») for lagring og analyse.

Gjennom appen samles det inn og lagres data om kontakter med andre telefoner som har installert appen, innenfor bluetooth-rekkevidden. Avhengig av type telefon, hva man har på seg, om telefonen er i en veske osv, vil rekkevidden kunne variere mye. I en normalsituasjon vil rekkevidden være på 10 meter eller mindre. Beregningen av hvilken avstand telefonene reelt sett har til hverandre skjer sentralt, basert på data fra begge telefonene. Det skjer ved å sammenligne målt signalstyrke, og sammenholde det med hvilken telefonmodell de har, om de var utendørs eller innendørs. etc. Antall bluetooth kontakter som lagres i sporingsløsningen vil være større enn antallet kontakter som vurderes å være «nærkontakt» i smittefaglig sammenheng. Dette er også synliggjort i personvernerklæringen. Valget om en kontakten utgjør en «nærkontakt» i smittefaglig perspektiv gjøres senere i en algoritme i sporingsløsning og ikke i telefonen.

Definisjonen av «nærkontakt» er ved lansering satt til 2 meter i mer enn 15 minutter. Definisjonen vil kunne endre seg basert på en smittefaglig vurdering. Dette vil for eksempel være aktuelt dersom man ser at det er noen kontakter som ikke fanges opp av den nåværende definisjonen, men som burde være det. Dersom man sletter kontakter hvor avstanden har vært lengre enn 2 meter, vil man være låst til dagens definisjon av «nærkontakt». Videre vil informasjon om kontakter være viktig for matematiske modeller, som brukes i beredskapsarbeid til å følge smitteutbredelse og vurdere effekt av smitteverntiltak.

Det kan på sikt bli implementert en mulighet for å lagre data lengre i telefonen (lengre enn mellomlagring i 1 time slik det skjer nå, men aldri mer enn 30 dager ref. forskrift), både for å kunne vise data til brukeren selv eller slik at brukeren kan holde tilbake data for rapportering i en periode. Noen andre land som har implementert lignende løsninger har i større grad basert seg på lagring av data på telefonen.

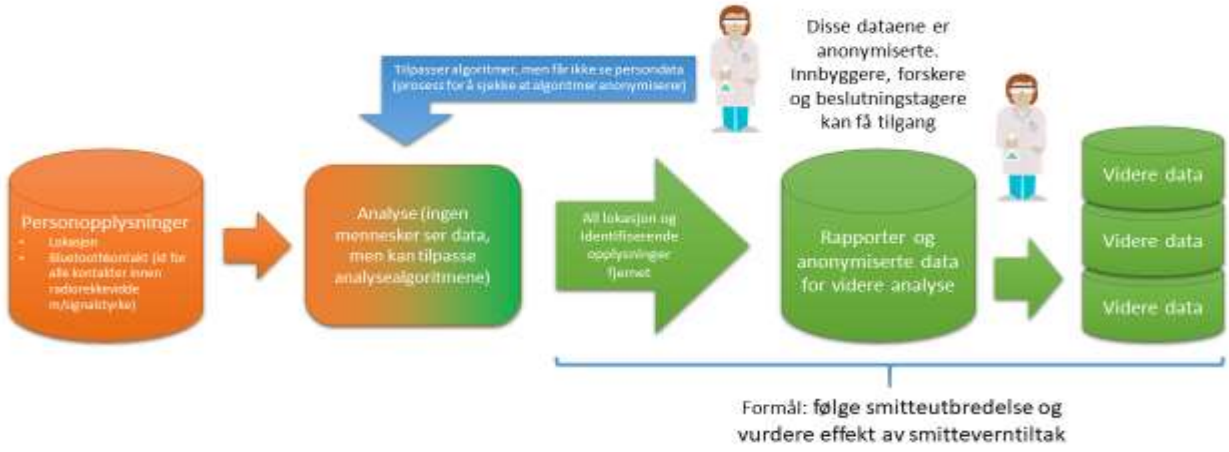
Apper eller den delen av sporingsløsningen som ligger i skyløsningen Microsoft Azure vil ikke ha informasjon om hvilke personer som er smittede, men det kan være mulighet å utlede informasjon om slike smittede basert på hvilke kall varslingsløsningen gjør inn mot sporingsløsningen i Azure. Tilgang og bruk av logger i Azure må derfor vurderes opp mot risiko for å implisitt peke på hvem som er smittet. Informasjonen som eksplisitt beskriver at en person er smittet vil kun behandles og lagres i varslingsløsningen og MSIS. Tiltak for å maskere søk på smittede er under utredning, slik at det ikke skal være mulig å avdekke informasjon om smittede fra logger.



Ettersom apper ser informasjon om andres brukere identifikator gjennom bluetooth, vil en bruker laste opp data om kontakt med andre brukere gjennom sin informasjon. Brukeren av appen har enkel mulighet for å slette data om seg i sporingsløsningen ved å trykke på en knapp i appen og re-autentisere seg med en SMS-bekreftelsesprosess tilsvarende første innlogging. Sletting av data inkluderer ikke bare de data som brukerens app har lastet opp, men også identifiserbare data som andre har lastet opp om brukeren som følge av bluetooth-kontakt med brukerens app.

Uttrekk av anonymiserte data for analyse (Analysesystemet)

I den sentrale lagringsplassen legges det til rette for søk på- og analyse basert på de lagrede lokasjonsdataene. Formålet for søk- og analyser er, gjennom overvåkning på befolkningsnivå, å følge smitteutbredelse og vurdere effekt av smitteverntiltak. FHI vil også kunne bruke de anonyme subdatasettene til forskningsformål.



Et analysesystem vil forenklet sett bestå av uttrekk av aggregerte bevegelsesmønster-data og nettverk av kontakter fra sporingssystemet (inklusiv aldersgrupper og kommune eller fylke).

Disse subdatasettene skal være anonyme. Det det skal dermed ikke være mulig å reversere denne prosessen for å finne tilbake til de faktiske brukernes identitet, heller ikke ved å bruke for eksempel lokasjon på bosted eller på annen måte bakveisidentifiseres. Slike data skal kunne frigis uten at noen kunne klare å opprette en relasjon tilbake til de opprinnelige brukerne av apper.

De anonyme subdatasett lagres i skyen og vil kunne gjøres tilgjengelig for FHI, helsemyndigheter og andre forskningsinstitusjoner. Subdatasettene vil lagres i minst 6 måneder.

Disse anonyme subdatasettene vil kunne brukes til modellering av epidemien (prediksjoner). De kan også benyttes for å vurdere hvilken effekt politiske tiltak og pålegg, som for eksempel karantene og skolestenging, har på epidemien. Man vil for eksempel kunne lage en social-distancing indikator for hver kommune. Slike data vil også bidra til å kunne forstå befolkningens bevegelsesmønster og hvordan folk møtes. Slik informasjon vil kunne brukes til å vurdere om det er spesielle områder, aldersgrupper eller aktiviteter som er mer utsatt for å genere smitte («hotspots»).

Hvordan anonymiseringsprosessen vil skje er ikke ferdigstilt på nåværende tidspunkt. Simula vil jobbe med analysesystemet og anonymiseringsprosessen sammen med teknologer og personvernjurister. Analysesystemet vil ikke innføres før det foreligger en oppdatert DPIA/tillegg til DPIA som beskriver nærmere prinsippene for anonymisering.

Varslingsløsning

Varslingen av personer som har vært i nærkontakt (iht. gjeldende definisjon det vil si mindre enn 2 meter i min. 15 minutter) med en smittet, starter ved at Varslingsløsningen kaller et MSIS API, med til og fra dato. I retur sender MSIS fnr., bostedskommune og dato for positivt prøvesvar tilbake til Varslingsløsningen. Fnr. legges i en tabell.

Denne etterfølgende prosessen følges for hvert av fnr. i tabellen:

1. Varslingsløsningen gjør et kall mot Folkeregisteret (PREG) med fnr. for å kontrollere om den smittede er registrert som kode 6 eller 7. I disse tilfellene vil hele prosessen stoppes. Hvis den smittede ikke er registrert som kode 6 og 7 fortsetter behandlingen videre
2. Varslingsløsningen gjør et API-kall til Kontakt- og reservasjonsregisteret (KRR) med fødselsnummer til den smittede som parameter og får tilbake mobiltelefonnummer til den smittede
3. Med mobiltelefonnummer til den smittede, gjøres det et API-kall til SmitteStopp registerløsning, som ligger i skyen. Hvis mobiltelefonnummeret til den smittede finnes i SmitteStopp registerløsning, returneres en liste med mobiltelefonnumre og dag på alle som har vært i nærkontakt med den

smittede. I de tilfeller den smittedes mobiltelefonnummer ikke finnes i Smittestopp appen, eller man ikke finner noen som har vært i nærkontakt med den smittede, avsluttes prosessen. I dette API-kallet returneres også utfyllende informasjon om kontakten mellom den smittede og nærkontakten, slik som antall kontaktpunkter, et tall som beskriver vurdert risikograd (risk score), lengde i tid på kontakten, lokasjon for kontaktene og en automatisk vurdering om hvor kontaktene fant sted (innendørs, utendørs, offentlig transport osv). Varslingsløsningen vil ikke lagre mer enn nødvendig av denne informasjonen.

I beta versjonen av Varslingsløsningen, kommer Varslingsløsningen til å produsere en oversikt antall smittede og antall nærkontakter knyttet til hver smittet.

For å validere listen over nærkontakter og bidra til rask oppsporing av og formidling av råd til personer som kan være smittet vil en definert brukergruppe med tjenstlig behov hos FHI og FHIs databehandlere få tilgang til opplysninger som er tilgjengelig i disse API-kallene samt informasjon om antall tidligere varsler, også inkludert personopplysninger. Lokasjonsinformasjon om kontaktpunktene kan bli presentert på en kartløsning eller lignende grafisk fremstilling. Tilgangens formål skal være begrenset til oppsporing og råd til personer som kan være smittet. Slik tilgang vil da logges i tilgangsloggen til registerløsningen slik at innbygger kan få innsyn i at personell hos FHI eller databehandler har hatt tilgang til deres opplysninger.

FHI tar kontakt (pr. telefon) med kommunelegen når oversikten foreligger. Kommunelegen får vite hvor mange som er smittet i kommunen og hvor mange som skal motta varsel. Kommunelegen får ikke vite hvilke telefonnumre det gjelder. Kommunelegen gjør en vurdering av antallet SMS varsler som skal sendes ut og gir en aksept eller avviser at SMS-varsler skal sendes ut.

Noen kommuner kommer til å bli valgt som pilot brukere, og kun disse vil bli kontaktet av FHI. Oversikten for de andre kommunene vil bli produsert, men FHI kommer ikke til å ta kontakt med disse og det vil ikke bli sendt ut noen SMS-varsler for disse kommunene.

Etter at varslingsløsningen har vært i en testfase i en periode, kommer løsningen til å automatiseres og SMS-varsler sendes ut uten at det er noen manuell prosess eller vurdering før varslene sendes ut. Også i denne fasen vil det være mulig for en definert brukergruppe å kunne få tilgang til opplysninger på samme måte som i test-fasen, med samme formål og begrensing som angitt i forskriften.

I beta versjonen vil SMS-varslene kan meldingen inneholde noe informasjon som er knyttet til kommunen (f.eks. kontakttelefonnummer til kommunelegen), samt dag for når man var i nærkontakt med en smittet. På den måten kan den som får varseletberegne når man kan gå ut av karantene igjen (14 dager)

Varslingsløsningen kommer til å lagre data om den smittede og av dem som har fått tilsendt varsel i 30 dager. Dette er gjort av hensyn til validering av løsningen.

Dersom det viser seg at data ikke trenger å være lagret så lenge, vil lagringstiden reduseres.

Hele varslingsløsningen kommer til å ligge i FHI sin sikker sone.

Innsynsløsning

Innsynsløsningen er en separat webløsning som kan linkes til fra appen og andre websider som for eksempel Helsenorge og FHI.

Innsynsløsningen vil benytte seg av en kjede av autentiseringstiltak for å sikre at brukeren er den hun utgir seg for:

1) Autentisering ved bruk av ID-Porten, som gir et personnummer
2) Brukeren blir så bedt om å taste inn sitt telefonnummer. Dette sjekkes opp mot telefonnummeret som er registrert på personnummeret i Digitaliseringsdirektoratets Kontakt- og reservasjonsregister
3) Telefonnummeret bekreftes ved å sende en SMS til telefonnummeret, og brukeren legger inn koden på websiden.

Innsynsløsningen gir tilgang til informasjon om lokasjonshistorie på en brukervennlig måte. Det vil ikke bli gitt innsyn i opplysninger om lagrede kontakter via bluetooth ettersom dette er opplysninger om andre personer. Innsynsløsningen gir også en oversikt over hvem som hatt tilgang til data om brukeren, inkludert brukeren selv (fra innsynsloggen i sporingsløsningen).

Sletteløsning

Lokasjonsdata som er sendt inn fra appen lagres i sporingsløsningen i maksimum 30 dager, og slettes så automatisk. Appen har en knapp som gjør det mulig for brukeren etter en ny bekreftelse av telefonnummer å slette alle personopplysninger relatert til denne brukeren i sporingsløsningen. Sletting av appen vil ikke automatisk slette personopplysninger knyttet til brukeren i sporingsløsningen, men sporingsløsningen vil automatisk slette disse dersom appen ikke rapporterer inn data innen 7 dager.

Hvem vil du dele personopplysningene med?

Som hovedregel vil behandling av personopplysninger skje gjennom automatiserte løsninger og ikke behandles av mennesker. Likevel kan det oppstå behov for at autorisert personell kan gis tilgang til identifiserende opplysninger i registeret. Dette vil for eksempel være at smittesporere ved FHI går gjennom listen med telefonnummeret til de som skal motta varsel manuelt for å kvalitetssikre listen (se nærmere beskrivelse av varslingssystemet). Det føres en logg over hvem som har slått opp på hvilke personopplysninger og når dette skjedde. Relevante deler av denne loggen vil være tilgjengelig for innbygger gjennom innsynsløsningen.

Ved varsling av andre personer om at de har vært i nærheten av en smittet, vil ingen kjennetegn ved den smittede formidles. Nærkontaktene vil få vite hvilken dag kontakten skjedde (innenfor 24 timer), slik at tiden for karantene kan beregnes. I

situasjoner der få har kontakt med andre, kan det likevel ikke utelukke at noen av de varslede kan forstå hvem den smittede er. Brukere er informert om dette gjennom brukervilkår og personvernpolicy.

FHI bruker databehandlere til å samle inn, lagre eller på annen måte behandle personopplysninger på FHIs vegne. FHI benytter seg av følgende databehandlere per i dag:

- Simula Research Laboratory AS, Simula Metropolitan Center for Digital Engineering AS (Simula Met) og Simula Consulting AS for utvikling av tjenesten
- Microsoft Ireland Operations Ltd for lagring av personopplysningene i MS Azure
- Norsk Helsenett for å gi innbyggere innsyn i egne data

All behandling av personopplysninger vil skje innenfor EU/EØS-området.

Hva med sensorer?

Andre sensorer som akselerometer, kompass og gyroskop brukes og logges ikke av appen.

Beskrivelse av personopplysningene: *Hvilke kategorier personopplysninger behandles og inkluderer dette særlige kategorier av personopplysninger? Hvor mange personopplysninger vil bli innsamlet og behandlet? Hvor ofte? Hvor lenge skal disse lagres? Hvem er brukere?*

Hvilke kategorier av personopplysninger behandles og inkluderer dette særlige kategorier av personopplysninger? Hvor mange personopplysninger vil bli innsamlet og behandlet? Hvor ofte? Hvor lenge skal disse lagres?

Innsamling av data om brukernes bevegelsesmønster, samt kontakt med andre mobiltelefoner (Smittestopp-appen)

Følgende personopplysninger samles inn gjennom Smittestopp-appen:

- Mobiltelefonnummer
- Alder
- GPS posisjon slik at nærkontakt med andre personer/mobiltelefoner kan spores, det vil si at det registreres bevegelsesmønster kontinuerlig (lengdegrad, breddegrad, hastighet, høyde over havet, tid på ulike lokasjoner) når Smittestopp er aktivert og mobiltelefonen er påslått
- Generert UUID fra Smittestopp (unik ID som følger telefonnummeret)
- Operativsystem, versjonsnummer, mobiloperatør, og telefonmodell – dette brukes til å øke kvaliteten på innsamlede data da ulike telefoner og operativsystem forskjellig presisjon på posisjonsdata. Videre vil denne informasjonen forenkle feilsøking og feilretting.
- Bluetooth data om smittestopp-apper på andre telefoner som er innen rekkevidde av telefonen (startidspunkt for kontakt, sluttidspunkt for kontakt, generert UUID for telefoner i nærheten, vektor med signalstyrke for telefoner i nærheten) logges kontinuerlig
- Skjermstørrelse og mobiloperatør

Registrering av enheter som er nære hverandre i tilstrekkelig tid til at smittefare kan oppstå, vil skje automatisk. Hva som anses å være «nære» og «tilstrekkelig tid» vil vurderes ut fra utbruddsituasjonen og vil kunne endres ettersom vår kunnskap om epidemien blir bedre. Ved lansering av Smittestopp, er kontakt nærmere enn 2 meter i mer enn 15 minutter, definert som nærkontakt. Data som rapporteres inn fra apper og lagres i sporingsløsningen inkluderer også telefoner utover denne 2-metersgrensen, da utregning av avstand skjer i sporingsløsningen heller enn i telefonen. Dersom dette endres, vil brukere få informasjon om dette.

Applikasjonen vil lagre informasjon lokalt og så sende den til en database i skyen en gang i timen. Informasjonen slettes da på telefonen, men det kan tenkes at det på sikt vil bli implementert lagring utover dette i telefonen for å gi bedre innsyn til brukeren om historiske data.

Så lenge app'en er aktivert vil GPS-data, opplysninger om hvor brukeren har vært og hvilke andre mobiltelefoner brukeren har vært i nærheten av, registreres, lagres og slettes automatisk etter 30 dager.

Faste opplysninger som mobiltelefonnummer, UUID og versjonsnummer på mobiltelefonens operativsystem lagres så lenge man bruker Smittestopp.

Personopplysningene i appen kan når som helst slettes ved at brukeren benytter slettefunksjonaliteten i Smittestopp, og deretter sletter Smittestopp. Ved å bare slette Smittestopp fra mobiltelefonen, slettes personopplysninger ikke før etter en ukes inaktivitet.

Alle innsamlede personopplysninger skal slettes når forskriften opphører å gjelde den 1. desember 2020.

Uttrekk av anonymiserte data for analyse (Analysesystemet)

Et analysesystem vil forenklet sett bestå av uttrekk av aggregerte bevegelsesmønster-data og nettverk av kontakter fra sporingssystemet (inklusiv aldersgrupper og kommune/fylke). Disse subdatasettene vil være anonyme. De anonyme subdatasett lagres i skyen og vil kunne gjøres tilgjengelig for FHI, helsemyndigheter og andre forskningsinstitusjoner. Subdatasettene vil lagres i minst 6 måneder.

Varslingsløsning

Gjennom varslingsløsningen vil FHI behandle opplysninger som fødselsnummer, bostedskommune og prøvesvardato fra MSIS registeret. Gjennom kontaktregisteret vil man også få tilgang til den smittedes mobiltelefonnummer. Ved å kalle opp Smittestopp appen med den smittedes mobiltelefonnummer (kun det) vil FHI få tilgang til et subdatasett av mobiltelefonnumre som ligger lagret i Smittestopp systemet. Subdatasettet vil bestå av mobiltelefonnummer og dag for nærkontakt, til alle som har vært i nærkontakt med den smittede.

FHI vil lagre informasjon om den smittede, samt mobiltelefonnummer til de som blir varslet, i 30 dager. FHI vil vurdere behov for denne lagringen og vil gi beskjed til brukere om denne tidsperioden endres eller om slik lagring utelates.

Fødselsnummer, som er mottatt fra MSIS, men som ikke gir noen treff i Smittestopp app`en, vil bli slettet fra Varslingsløsningen og vil ikke bli lagret.

Alle dataene vil bli behandlet og lagret i sikker sone.

Hvem er brukere?

Det er frivillig å delta. Hele Norges befolkning (over 16 år) er potensielle brukere av appen.

Det er på nåværende tidspunkt ikke avklart om appen skal kunne benyttes av helsepersonell.

Beskriv behandlingen i en kontekst: *Hva er forholdet til brukere? Hvor mye kontroll vil brukerne ha? Ville de forvente at personopplysningene brukes på denne måten? Omfatter dette barn eller sårbare grupper? Er det tidligere risikomomenter eller sikkerhetsfeil forbundet med denne behandlingen? Er dette nytt? Hva er nåværende teknologi standard innenfor dette området? Er det noen aktuelle spørsmål av offentlig interesse som bør drøftes?*

Hva er forholdet til brukere? Hvor mye kontroll vil brukerne ha? Ville de forvente at personopplysningene brukes på denne måten? Omfatter dette barn eller sårbare grupper?

Det vil være frivillig for den enkelte å laste ned appen. Dette innebærer at både smittede og andre har godtatt å bli registrert og bli sporet. Det skal innarbeides en funksjonalitet i applikasjonen der man aktivt gir en form for godkjennelse av behandling av personopplysninger. Det skal gis god informasjon om hva det innebærer. Godkjennelsen vil gjelde all behandling av personopplysninger, og det blir ikke mulig å gi delvis godkjennelse, for eksempel sporing i et bestemt område. Alle brukere av applikasjonen vil bli gitt informasjon om ovennevnte før de laster ned appen (brukervilkår) og det vil foreligge informasjon tilgjengelig på en nettside (helsenorge.no).

Konsekvensen av at den enkelte ikke laster ned appen, er at vedkommende ikke vil få tilgang til tjenesten, men det har ingen direkte negative konsekvenser for den som velger å ikke delta.

Hver bruker kan slette allerede registrerte data ved å bruke slettefunksjonen i appen og deretter slette appen.

Varsel/SMS

Brukeren vil motta varsling om karantene eller annen relevant informasjon via SMS, med henvisning til hvor de kan søke råd og veiledning (helsenorge.no). Dette er et råd om å gå i karantene, ikke et pålegg.

Varslingen vil ikke gi detaljert informasjon om når og hvor kontakt med en smittet har skjedd, men vil gi eller henvise til informasjon og råd om hvordan man skal opptre. For å oppfylle formålet må imidlertid varslingen angi hvilken dag kontakten har vært, slik at nærkontakten kan vite hvor lenge han eller hun skal være i karantene. Det finnes flere eksempler på hvordan smittede man har vært i kontakt med kan identifiseres. For eksempel, dersom man har kun vært i kontakt med 1 person den dagen, vil dette kunne innebære at man identifiserer den smittede. Brukere vil informeres (brukervilkår) om at det ikke kan utelukkes at andre personer blir gjort kjent med 1) at du er smittet og 2) at du har utsatt dem for smitte.

Omfatter dette barn eller sårbare grupper?

Aldersgrense er foreslått til å være 16 år. Eventuell endring av aldersgrense vil kreve en forskriftsendring og dette vil måtte vurderes i et tillegg/ny versjon til denne DPIAen.

Er det tidligere risikomomenter eller sikkerhetsfeil forbundet med denne behandlingen? Er dette nytt? Hva er nåværende teknologi standard innenfor dette området? Er det noen aktuelle spørsmål av offentlig interesse som bør drøftes?

Pandemisituasjonen er krevende og det oppstår behov for å benytte tiltak som ikke tidligere er benyttet. Flere EU medlemsland har brukt lokasjonsdata fra mobiltelefoner i et forsøk på å hindre spredning. Det Europeiske Personvernrådet (EDPB) har publisert en erklæring hvor de sier at bruk av persondata for å bekjempe Korona-smitte ikke bryter med EUs databeskyttelsesregelverk. Nasjonal lovgivning for bruk av ikke-anonyme data kan innføres med hjemmel i ePrivacy-direktivet. https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/EU-EOS-informasjon/EU-EOS-nytt/2020/eueos-nytt---23.-mars-2020/korona-tiltak-bryter-ikke-personvernregler/

Sporingssystemer på mobil der innbygger får beskjed dersom man er i nærheten av en smittet, har blitt benyttet i Kina, Sør-Korea og Israel. I motsetning til disse systemene, skal ikke denne sporingsappen benyttes til å kontrollere om brukere overholder pålegg om karantene eller varsles når bruker er i umiddelbar nærhet av en smittet.

Beskriv formålet med behandlingen?: *Hva ønsker man å oppnå? Hva er ønsket effekt for brukere? Hva er fordelene med behandlingen?*
Hensikten med systemet er å gjøre automatisk kontaktsporing for å begrense spredningen av COVID-19. Kontaktsporing er rekonstruksjon av en persons bevegelseshistorie for å identifisere personer de kan ha smittet, og blir vanligvis gjort manuelt basert på intervjuer fra et infisert individ. Denne manuelle prosessen er tidkrevende og usikker. Med automatisert kontaktsporing vil FHI få tilnærmet øyeblikkelig informasjon om personer som kan ha vært utsatt for smitte når en person har blitt bekreftet å ha en smittsom sykdom. Videre skal sporingssystemet, gjennom overvåkning på befolkningsnivå, også bidra til å følge smitteutbredelse og vurdere effekt av smitteverntiltak. Rimeligheten og samfunnsnytten er vurdert av Helse- og omsorgsdepartementet i forskriftsprosessen for dette systemet, ref. kgl.res. 27. mars 2020 med hjemmel i lov 5. august 1994 nr. 55 om vern mot smittsomme sykdommer § 7-12, jf. § 1-2 tredje ledd. Fremmet av Helse- og omsorgsdepartementet.

Trinn 3: Involvering

Involvering av relevante interessenter: *Beskriv når og hvordan man vil involvere brukergrupper eller begrunnelse for hvorfor dette ikke gjøres. Hvem andre vil bli involvert? Er det behov for å involvere databehandlere? Er det planer om å konsultere sikkerhetseksperter eller andre eksperter?*
På grunn av tidsaspektet er det ikke mulig å innhente synspunkter fra de registrerte/brukergruppen. Helse- og omsorgsdepartementet er involvert gjennom utforming av forskriften. Helse- og omsorgsdepartementet har forespurt råd fra Datatilsynet. Det er innhentet innspill fra Sekretariatet for forskningsetiske komiteer. Utkast til DPIA er gjennomgått av Simula, Norsk helsenett, Direktoratet for e-helse. Personvernombudet er kontaktet, har gitt innspill underveis og vil komme med en tilrådning. Helse- og omsorgsdepartementet har oppnevnt en ekspertgruppe som skal levere en overordnet vurdering av om sikkerhet og personvern er forsvarlig ivaretatt.

Trinn 4: Vurdering av nødvendighet og proporsjonalitet

Beskriv overholdelse av regelverket (compliance) og proporsjonalitets tiltak, særlig: *Hva er det rettslige grunnlaget for behandlingen av personopplysninger? Oppnås det faktiske formålet med behandlingen? Kunne formålet ha blitt oppnådd på en annen måte? Hvordan vil man sikre «function creep»? Hvordan vil man sikre dataminimering og kvalitet? Hvilken informasjon vil man gi til brukere? Hvordan vil man ivareta deres interesser? Hvordan er de registrertes friheter tatt hensyn til med tanke på Den europeiske menneskerettskonvensjonen (EMK). Hvilke tiltak er tatt i forhold til databehandlere? Hvordan vil man sikre internasjonale overføringer?*

Hva er det rettslige grunnlaget for behandlingen av personopplysninger?

Det rettslige grunnlaget for behandling av personopplysninger vil være personvernforordningen artikkel 6 nr. 1 bokstav e og artikkel 9 nr. 2 bokstav i, jfr forskrift om Forskrift om digital smittesporing og epidemikontroll i anledning utbrudd av Covid-19, fastsatt ved kgl.res. 27. Mars 2020. mars 2020 med hjemmel i lov 5. august 1994 nr. 55 om vern mot smittsomme sykdommer § 7-12, jf. § 1-2 tredje ledd. Det vil være frivillig å installere appen. Det skal innarbeides en funksjonalitet i applikasjonen der man aktivt gir en form for godkjennelse av behandling av personopplysninger.

Oppnås det faktiske formålet med behandlingen?

Formålet med tiltaket er rask oppsporing og formidling av råd til personer som kan være smittet av koronaviruset SARS CoV-2. Gjennom overvåkning på befolkningsnivå skal tiltaket også bidra til å følge smitteutbredelse og vurdere effekt av smitteverntiltak. Dataene vil ikke bli brukt til å følge med på om enkeltpersoner overholder råd eller pålegg, men vil kunne utnyttes til å undersøke grad av etterlevelse på befolkningsnivå for dermed overordnet å kunne følge og vurdere epidemiens utvikling inkludert effekt av tiltak.

Nytten av tiltaket øker jo flere deltar. Appen vil ha nytteeffekt, selv om en mindre andel enn den ønskede 60 % av befolkningen i Norge vil ta appen i bruk. Lokasjonsdata kan brukes i et aggregert og anonymisert format til å avdekke generelle trender om atferd i befolkningen. Dette gir helsemyndighetene er ny mulighet for å kartlegge hvor og når folk samles og kan risikere å spre smitte. For eksempel, så kan man følge med i utviklingen av antall kontakter og varighet av kontakter i ulike områder, så som barnehager, skoler, kontorbygninger, restauranter etc. Denne type av data fra ulike aldersgrupper og lokaliteter, så som kommune eller fylker, vil kunne danne basis for målrettede tiltak. Bedre kunnskap om kontakter i befolkningen er viktig for å tilpasse matematiske modeller, som brukes i beredskapsarbeid til å simulere effekter av tiltak.

Kunne formålet ha blitt oppnådd på en annen måte?

Smitteoppsporing er en lovpålagt oppgave etter smittevernloven § 3-6. Manuelle smittesporing gjøres allerede i dag. Denne manuelle prosessen er tidkrevende og usikker. Med automatisert kontaktsporing vil man få rask informasjon om personer som kan ha vært utsatt for smitte når en person har blitt bekreftet å ha en smittsom sykdom. Tiltaket vil dermed supplere den manuelle smittesporingen som gjøres i dag.

Smittesporingssystemet har to formål:

- rask oppsporing og formidling av råd til personer som kan være smittet av koronaviruset SARS CoV-2,
- gjennom overvåkning på befolkningsnivå, bidra til å følge smitteutbredelse og vurdere effekt av smitteverntiltak.

Sentral lagring av personopplysninger knyttet til smittesporing kan anses som et større inngrep enn å lagre disse dataene lokalt på hver enkelt mobiltelefon. Et valg av sentral løsning må derfor begrunnes ved at ett eller begge formål vanskelig kan oppnås på annen måte.

En av grunnene er at appen skal hjelpe helsemyndighetene med å vurdere effekten av smitteverntiltak ved anonyme data om hvordan vi beveger oss. Dette vil være et verktøy for å analysere befolkningens bevegelsesmønstre. Slik blir det mulig å følge med på om tiltakene Norge innfører virker, og hva som skjer med antallet nærkontakter til smittede når samfunnet åpner opp de svært strenge restriksjonene litt etter litt. Dette krever at opplysningene lagres samlet sentralt, slik at data kan sammenstilles.

En annen grunn til sentral lagring av lokasjons- og kontaktinfo er nøyaktighet og hastighet. Tester har vist at appen kan gi høyere nøyaktighet på sporingen hvis data kan lagres og behandles sentralt. Dette er fordi data fra begge telefonene som «møtes» kan sammenlignes for å gi en mer nøyaktig vurdering av nærkontakt. Slik kan det unngå at appen varsler om at en innbygger har hatt nærkontakt til en smittet, uten at det stemmer.

Sentral lagring gjør det raskere å få sendt ut beskjeder til de som har vært nærkontakt til en smittet person. Ved sentral lagring unngås forsinkelser ved å først kontakte den smittede, som så må laste opp sine data.

Vurderingen er at begge formålene best oppnås ved sentral lagring, og at denne nytten oppveier ulempen med sentral lagring.

Hvordan vil man sikre «function creep»?

De personopplysningene som samles inn kan kun brukes til det formålet som er angitt i forskriften. Formålet med tiltaket er rask oppsporing og formidling av råd til personer som kan være smittet av koronaviruset SARS CoV-2. Gjennom overvåkning på befolkningsnivå skal tiltaket også bidra til å følge smitteutbredelse og vurdere effekt av smitteverntiltak. Personopplysningene kan ikke benyttes for å kontrollere om enkeltpersoner overholder råd eller pålegg. Helseopplysninger eller lokasjonsdata kan ikke gjøres tilgjengelig for politi eller påtalemyndighet eller

brukes i forsikringsøyemed eller av arbeidsgivere selv om den registrerte samtykker. Personopplysningene kan ikke utnyttes kommersielt.

Hvordan vil man sikre dataminimering og kvalitet?

Smittespredning skjer gjennom nærkontakt og nærkontakt med en person som er smittet kan identifiseres hvis man har bevegelseshistorien til den smittede og alle andre personer i samme område. Det vil kun bli innsamlet personopplysninger som er definert i forskriften og som nødvendig for gjennomføring av tiltaket. Et annet dataminimeringstiltak er fortløpende sletting av lokasjonsdata etter 30 dager.

Data vil ikke deles i app, eller mellom app/mobiltelefoner. Mobiltelefonnummer og andre direkte personidentifiserende kjennetegn skal separeres og lagres adskilt fra andre registeropplysninger.

Risiko for lekkasje av en vesentlig mengde informasjon ved hacking av en stjålet telefon er liten ettersom data vanligvis ikke lagres på telefonen mer enn time. I noen situasjoner som for eksempel dårlig mobildekning, vil noe mer data lagres, men det vil fremdeles være vanskelig å få tak i denne informasjonen. Flere andre land har basert sine løsninger på mer utstrakt lagring av data på telefonen, og det kan være at denne løsningen også vil legge opp til mer lagring på telefonen etterhvert, men da må innsyn i denne informasjonen sikres på en god måte.

Appen krever kun innlogging via en SMS-bekreftelse første gang man starter den, men dette gir ikke tilgang til lokasjonsinformasjon. Innsyn i data vil ha ekstra autentisering, inkludert både innlogging via ID-porten og ny bekreftelse av telefonnummer via SMS, og denne kombinasjonen anses som en sikker nok autentisering før innsyn.

Hvilken informasjon vil man gi til brukere?

Brukerne vil motta informasjon om sporingssystemet før de laster ned appen. Brukerne av tjenesten vil gis informasjon om formål, hvilke opplysninger som brukes til hva og hvordan, innsyn og sletting, og hva behandlingen innebærer (brukervilkår). Brukervilkår/personvernpolicy er vedlagt.
Brukervilkår/personvernpolicy vil kunne oppdateres. Brukeren får da beskjed via sms om oppdateringer med lenke til nettsiden med de oppdaterte brukervilkårene/personvernpolicy.

Videre vil den enkelte bruker av appen ha rett til å vite hvem som har tilgang til informasjon om vedkommende og hva informasjonen brukes til. Dette gjelder også lokasjonsdata. Brukeren vil kunne få innsyn i egne lokasjonsdata, og i loggen som viser hvem som har hatt tilgang til vedkommendes personopplysninger, når og for hvilket formål, samt vil kunne få informasjon om antall kontakter.

Hvordan vil man ivareta deres interesser? Hvordan er de registrertes friheter tatt hensyn til med tanke på Den europeiske menneskerettskonvensjonen (EMK)?

Brukere vil kunne utøve sine rettigheter til innsyn, retting og sletting

Når det gjelder forholdet til den Europeiske menneskerettighetskonvensjon (EMK) vil de samfunnsmessige fordelene veie opp for de negative konsekvensene mht rett til privatliv. Sporingssystemet vil kunne supplere det manuelle sporingsarbeidet, gjøre at sporingen av smittede skjer raskere og mer presist. Tiltaket vil også gjøre det mulig å lempe på de andre inngripende samfunnsmessige restriksjonene på et tidligere tidspunkt, fordi det er mer målrettet. Det er helt frivillig å ta appen i bruk og brukerne kan når som helst slette sine personopplysninger.

Kjernen i EMKs forbud mot diskriminering er at det ikke skal foregå forskjellsbehandling basert på eksempelvis kjønn, etnisitet, seksuell legning mv, uten en saklig og god begrunnelse. Alle brukere over 16 år kan installere appen, men gruppen med adressesperre (kode 6 og 7) frarådes å gjøre det. Dette kan virke diskriminerende da denne gruppen hovedsakelig omfatter kvinner, men sikkerhetsaspektet på nåværende tidspunkt vil oppveie de negative konsekvensene. De registrertes tanke, tros- og religionsfrihet er ikke påvirket av behandlingsaktivitetene. Det samme gjelder for de registrertes rett til å gi uttrykk for de meninger man ønsker å dele med andre (ytringsfrihet) – og til å la seg informere om andres tanker og ideer (informasjonsfrihet).

Hvilke tiltak er tatt i forhold til databehandlere?

FHI bruker databehandlere til å samle inn, lagre eller på annen måte behandle personopplysninger på våre vegne. I slike tilfeller har FHI inngått avtaler for å ivareta informasjonssikkerheten i alle ledd av behandlingen. FHI benytter seg av følgende databehandlere per i dag:

- Simula Research Laboratory AS, Simula Metropolitan Center for Digital Engingeering AS (Simula Met) og Simula Consulting AS for utvikling av tjenesten
- Microsoft Ireland Operations Ltd for lagring av personopplysningene i MS Azure
- Norsk Helsenett for innsynsløsningen

Hvordan vil man sikre internasjonale overføringer?

All behandling av personopplysninger vil skje innenfor EU/EØS-området, slik at personvernforordningen gjelder fullt ut. Databehandlere kan ikke benytte underdatabehandlere uten FHIs forhåndsgodkjenning.

Trinn 5: Identifisere og vurdere risiko

Det er identifiserte flere trusler mot løsningen:

- Smittesporingsappen kan bli et angrepsmål. Potensielle sårbarheter i app'en, eller dens oppdateringsfunksjon, kan utnyttes til uautorisert innsamling av geolokasjonsinformasjon om Norges befolkning.
- Skyløsningen/analyseløsningen kan være et attraktivt angrepsmål. Potensielle sårbarheter i teknologien eller styringssystemene (f.eks tilgangsstyringen) kan utnyttes til å hente ut data om Norges befolkning.
- SMS-varslingen kan misbrukes ved å sende ut SMS til norske innbyggere med forfalsket avsendernummer.
- Geolokaliserende datasett som trekkes ut til forskningsøyemed kan benyttes til re-identifisering og profilering av enkeltindivider.

Vurdering av personvernrisiko, juridiske betraktninger, etikk og moral

Tabellen oppsummerer en vurdering av risiko knyttet til ivaretagelse av personvern. Scenariene er nærmere beskrevet i risiko- og sårbarhetsanalysen.

Risiko ID	Scenario	Sannsyn-lighet	Konse-kvens	Usikker-het	Risiko nivå
R-2-1	Innbygger tror at det er samtykke som reguler bruken av opplysningene	Moderat	Liten	Lav	Lav
R-2-2	Manglende etterlevelse av kommunikasjonsverndirektivet fører til regelbrudd	Liten	Stor	Lav	Lav
R-2-3	Det sammenstilles data med kilder det ikke er opplyst om til den registrerte	Liten	Stor	Lav	Lav
R-2-4	Myndighetene overvåker innbygger uten en granulert vurdering av nødvendighetskravet for de forskjellige formålene	Liten	Stor	Lav	Lav
R-2-5	Formålene slik de er definert i forskrift om digital smittesporing synes å gi myndighetene anledning til vid bruk av innsamlede opplysninger, uten at dette oppgis til innbyggere	Moderat	Stor	Middels	Middels
R-2-6	Innbygger får for lite eller for vanskelig informasjon slik at dataansvarlig ikke tilfredsstiller plikten til å informere	Moderat	Stor	Lav	Middels

Risiko ID	Scenario	Sannsyn-lighet	Konse-kvens	Usikker-het	Risiko nivå
R-2-7	Appen bryter taushetsplikt som fører til brudd på regelverk	Moderat	Stor	Middels	Middels
R-2-8	Myndighetene vedtar tiltak som ikke er godt nok vurdert mot grunnleggende menneskerettigheter som fører til svekket tillit til myndighetene.	Moderat	Meget stor	Lav	Middels
R-2-9	En person som er under 16 år tar i bruk appen	Svært høy	Liten	Lav	Middels
R-2-10	Det utgis informasjon om trusselutsatte personer som fører til fare for liv og helse	Moderat	Meget stor	Middels	Middels
R-2-11	Innbygger får ikke brukt sin rett til innsyn	Liten	Stor	Lav	Lav
R-2-12	Nytteverdien står ikke i forhold til inngrepet smittesporing utgjør, spesielt ved liten oppslutning om appen, under 60%.	Moderat	Stor	Middels	Middels
R-2-13	Det samles inn og lagres informasjon som ikke er nødvendig for å oppnå formålet med løsningen.	Liten	Stor	Lav	Lav
R-2-14	Formålet med løsningen kunne vært oppnådd med lavere risiko for personvern gjennom lokal lagring av sporingsdata.	Moderat	Stor	Middels	Middels

Flere andre, tekniske risikoer er listet opp med tiltak i neste kapittel.

Trinn 6: Identifisere tiltak for å redusere risiko

Risiko og tiltak for å redusere risiko er beskrevet detaljert i risiko- og sårbarhetsanalysen, og er oppsummert her.

Personvernrisiko

Sporing av individers bevegelser og kontakter utgjør et vesentlig personverninngrep. Den samfunnsmessige nytten av digital smittesporing må derfor stå i forhold til dette inngrepet. Innsamlede opplysninger skal kun benyttes til de definerte formålene: rask varsling til personer som kan være smittet og oppfølging av smitteutbredelse for å vurdere effekt av smitteverntiltak. Individer skal informeres om sine rettigheter, og de innsamlede opplysningene skal beskyttes slik at de ikke misbrukes eller kommer på avveie.

Det er gjennomført en rekke tiltak for å sikre at informasjonen brukes i henhold til de juridiske føringene i forskrift om digital smittesporing og personvern-forordningen. Teknisk arkitektur, implementasjon, drift og forvaltning er vurdert opp mot personvern og beste praksis. Ekstern kompetanse er benyttet for kvalitetssikring, som f.eks. ekspertgruppens gjennomgang av kildekode, og sikkerhetstesting gjennomført av anerkjente sikkerhetsfirmaer. Tilbakemeldinger er fulgt opp og svakheter utbedret. Gjennomgangen har ikke avslørt noen alvorlige gjenværende sikkerhetsrisikoer i løsningen

En totalvurdering av forholdsmessighet og nødvendighet tilsier derfor at samfunnsnytten av sporingssystemet overgår de mulige ulempene for personer som frivillig velger å benytte løsningen.

Arkitektur app
Flere initiativ har revidert app og appens arkitektur, eksempler på dette er ekspertutvalget som har revidert app både for Android og iOS. Grensesnitt mellom app og backend har også blitt gjennomgått i detalj. To separate penetreringstester har blitt utført, en for selve appen og en for app og grensesnitt mot backend. Det er identifisert en sårbarhet hvor lokalt lagret data er ikke kryptert som gjør mulig å manipulere data i den mobile enheten. Appen har også blitt vurdert i henhold til beste praksis for app utvikling.

Sikker utvikling
Det er identifisert noe mangelfulle prosesser i utviklingsmetodikken til Simula. Som en del av beste praksis for sikker koding skal sikkerhetsaktiviteter være integrert i utviklingsprosessene, eksempler på dette er angrepsmodeller, sikker design og standardiseringsarbeid. Mangel på dette kan føre til ustabile applikasjoner eller datalekkasje. Som et kompenserende tiltak er det nedsatt et ekspertutvalg som har vurdert kildekoden i løsningene slik at det nå er lavere usikkerhet knyttet til kildekoden til løsningen. Det er også iverksatt tiltak med dedikert 24/7 monitorering i et SOC (Security Operations Center) og etablert en prosess for kontinuerlig trusselmonitorering.

Eksponerte API-er
De eksponerte API-ene er delt i to hovedområder, de som er innbyggerrettede og de som er rettet mot integrasjonene via FHI (varsling) og NHN/Helsenorge (innsyn).

De innbyggerrettede, for innsending av data, registrering og sletting, er betydelig mer eksponert og krever atskillige tiltak og lag av sikkerhetsbarrierer. Man må anta at de blir gjenstand for både inntrenging- og tjenestenektangrep, og det er etablert tiltak i proporsjon med dette (DDoS Protection, Web Application Firewall, API

Management). Utover truslene om angrep er risikoen for overbelastning av spesielt API for registrering til stede, siden man ikke har mulighet for en kontrollert utrulling av mobilapplikasjonen. Det er ingen grensesnitt for uthenting av data som er eksponert mot innbygger, alt innsyn går gjennom Helsenorge. Dette reduserer risikoen for datalekkasje. En styrt prosess for å identifisere svakheter, inkludert inntrengingstesting, har bidratt til å lukke vesentlige funn.

API-ene som er eksponert mot FHI/Helsenorge er mye mindre synlig og er sikret mye sterkere (IP-filter og gjensidig sertifikatautentisering), slik at det er veldig liten risiko for at disse blir rammet av angrep.

Skytjenester (Microsoft Azure backend)
Bruken av Azure som plattform for å lage tjenester som behandler persondata er vurdert flere ganger av NHN som akseptabel. Disse vurderingene dekker kravene på plattformnivå, inkludert krav på juridisk, merkantilt og teknisk område.

All administrativ tilgang til løsningen er styrt via Azure AD, hvor det er satt krav om multifaktorautentisering for de berørte brukerne, og Azure AD Identity Protection automatisk flagger og varsler om mistenkelige aktiviteter/påloggingsforsøk.
Den tekniske løsningen er etablert av ressurser fra Simula, Microsoft og NHN, hvor hver komponent, bruk av disse og koblingen mellom dem i løsningen er dokumentert og vurdert ut fra beste praksis. Azure Security Center benyttes for å automatisk skanne etter potensielt sårbare konfigurasjoner. Dette gjøres og følges opp kontinuerlig, siden miljøet er i stadig endring. Dette sørger for liten risiko på det som brukes av komponenter fra skyplattformen.

Programvaren for de tjenestene som bygges er utviklet av Simula, hvor koden for disse er vurdert av flere uavhengige sikkerhetsleverandører, samt en ekspertgruppe samlet av HOD. Så langt har funnene vært knyttet til trusler om tilgjengelighet/skalerbarhet, noe man også har bekreftet og utbedret ved hjelp av volumtesting.

Forvaltning og drift
Folkehelseinstituttet har dataansvaret og det overordnede ansvaret for at de tekniske løsningene etableres innen forsvarlige rammer og lovverket.
Varslingsløsningen etableres i FHIs infrastruktur, hvor infrastruktur og andre driftstjenester leveres av Norsk Helsenett, og modellen for drift og forvaltning er allerede godt innarbeidet.

Innsynsløsningen leveres som utvidelse av eksisterende innsynsdel i Helsenorge, hvor den er utviklet, driftet og forvaltet av Norsk Helsenett. Dette er også en godt innarbeidet modell, hvor det allerede er innsyn i andre FHI-systemer via samme plattform.

FHI har valgt å bruke Simula for å sørge for drift av skyløsningen i første fase, siden kompetansen fra utviklingen av løsningen er nødvendig å benytte for å sikre tryggest mulig drift. Det beskrives i avtale mellom Simula og FHI hvilke roller man trenger i forvaltning, med videreutvikling og drift. NHN leverer støtte på noen punkter hvor det finnes kompetanse og kapasitet, og det har blitt inngått samarbeid med Mnemonic for overvåkning og hendelseshåndtering på sikkerhetsområdet. Det er veldig kort tid å avklare roller og oppgaver i detalj, men det vil kompenseres for ved spesielt tett oppfølging og samarbeid ved oppstarten.

Innsynsløsning
Innsynsløsningen skal sikre innbyggere innsyn i egne data som er samlet inn og lagret. Vurderte risikoer inkluderer:

- Bruk av mobilnummer som identifikator har svakheter, og kan gjøre det mulig for at en innbygger skaffer seg tilgang til en annen innbyggers sporingsinformasjon. Endring av registreringsprosessen vil kunne redusere risiko, men da på bekostning av tungvint registrering og lavere oppslutning om appen.
- Når et telefonnummer bytter eier, så vil ny eier kunne se informasjonen lagret for forrige eier. Spesielt trusselutsatte personer bør være oppmerksomme på dette.
- Kjente svakheter ved bruk av SMS-baserte engangskoder, vil personer i sikkerhetsmiljøer vil publisere kunne publisere informasjon om dette, noe som kan påvirke omdømmet til FHI, NHN og påvirke bruk av helsenorge.

Bruk av innsynsløsningen krever sterk autentisering til Helsenorge, og alt innsyn logges.

Anbefalte overordnede tiltak

- Jevnlig vurdering av nytteverdi. Løsningen er personverninngripende og kan bare forsvares hvis samfunnsnytten står i forhold, og formålene i forskriften oppnås. Etter hvert som man får bedre kunnskap om oppslutning og effekt, bør det gjøres nye vurderinger av forholdsmessighet og nødvendighet.

- Etablering av organisasjon og rutiner for drift og forvaltning. Når prosjektaktivitetene trappes ned, er det viktig at ansvarsforhold, prosesser og rutiner for samhandling blir innarbeidet i alle involverte virksomheter for å sikre prosesser som hendelseshåndtering og endringskontroll.

- Fortsatt overvåkning og sikkerhetstesting av løsningen. Lansering av nye versjoner og endringer i løsningen kan introdusere nye sårbarheter, og gjentagende testing vil redusere risikoen.

Samlet vurdering av personvernet og informasjonssikkerheten

Utbruddet av covid-19 er en alvorlig hendelse som truer liv og helse. Utbruddet medfører at det er behov for å ta i bruk tiltak som ikke har vært benyttet før. Sporingssystemet innebærer behandling av personopplysninger med potensielt alvorlige personvernmessige konsekvenser for personen selv og andre. Sporingssystemet omfatter behandling av personopplysninger i stor skala hensyntatt antall personer inkludert, detaljeringsgrad av personopplysninger som vil behandles, sporingssystemets planlagte varighet og dets geografiske omfang. Behandlingen omfatter også helseopplysninger om påvist smitte hos brukerne av appen.

I tråd med vurderinger av forholdsmessighet og nødvendighet gjort av Helse- og omsorgsdepartementet i forskriftsprosessen, er det etter en totalvurdering FHIs oppfatning at samfunnsnytten av sporingssystemet i vesentlig overgår de mulige ulempene for personene som velger å benytte Smittestopp.

Smittestopp vil supplere det manuelle sporingsarbeidet som gjøres i dag, og bidra til at sporingen av smittede skjer raskere og mer presist. Nytten av tiltaket øker jo flere som deltar. Men appen vil ha nytteeffekt, selv om en mindre andel av befolkningen i Norge enn ønsket vil ta appen i bruk. Gjennom overvåkning på befolkningsnivå vil Smittestopp bidra til å følge smitteutbredelse og gjøre det mulig å lempe på de andre inngripende samfunnsmessige restriksjonene på et tidligere tidspunkt enn hva som ellers ville være tilfellet, fordi det er mer målrettet.

Nedlasting og bruk av Smittestopp er frivillig. Det skal gis god informasjon om tiltaket i personvernerklæringen og gjennom andre kommunikasjonstiltak. Personopplysningene kan ikke benyttes til andre formål enn de som er angitt i forskriften. Personopplysningene lagres kun i begrenset periode og forskriften har en begrenset varighet. Brukere kan når som helst slette sine personopplysninger.

Det er gjennomført en rekke tiltak for å sikre at informasjonen brukes i henhold til de juridiske føringene i forskrift om digital smittesporing og personvernforordningen. Teknisk arkitektur, implementasjon, drift og forvaltning er vurdert opp mot personvern og beste praksis. Ekstern kompetanse er benyttet for kvalitetssikring, som f.eks. ekspertgruppens gjennomgang av kildekode, og sikkerhetstesting gjennomført av anerkjente sikkerhetsfirmaer. Tilbakemeldinger er fulgt opp og svakheter utbedret. Gjennomgangen har ikke avslørt noen alvorlige gjenværende sikkerhetsrisikoer i løsningen.

Det er en risiko for lagring av overskuddsinformasjon, siden informasjon tilsynelatende kan bli liggende «ubrukt» for personer som ikke varsles. Dette er vurdert, og for å oppnå formålet om oppsporing og varsling av de som kan ha vært utsatt for smitte, forutsetter det at informasjon om nærkontakter lagres en periode, siden det kan ta tid før smitte blir påvist og varsling mulig. I tillegg krever

det andre formålet, følge smitteutbredelse og vurdere effekt av smitteverntiltak, at alle innsamlede data benyttes. Det kan være vanskelig å på forhånd si nøyaktig hvilke data som har størst verdi, siden dette vil avdekkes gjennom analyse. En ny vurdering av nytteverdi av konkrete innsamlede data bør likevel gjøres når økt kunnskap og erfaring tilsier det.

Det vil iverksettes tiltak for å begrense tilgang til personopplysninger, i form av både tekniske og personalmessige restriksjoner. Behandling av personopplysninger skjer i stor grad gjennom tekniske løsninger. Alle lokasjonsdata ligger kryptert i skyen. Helseopplysninger behandles separat i varslingsløsningen. Varslingsløsningen ligger i sikker sone. Kun et begrenset antall utpekte medarbeidere hos FHI eller deres databehandlere vil få tilgang til personopplysninger og det vil bli ført logg over hvem som har hatt tilgang. Opplæring av medarbeidere og internkontroll har høyt fokus for at krav og forventninger skal være kjent. Det vil bli utarbeidet rutiner for arbeidsprosessene som bygger på de som allerede benyttes i FHI for håndtering av liknende data.

Trinn 7: Godkjenning og endringer

	Navn/stilling/dato	**Kommentarer**
Tiltak akseptert av:	Gun Peggy Knudsen, fungerende assisterende direktør, 13.04.2020	Oppfølging og tiltak følges opp i prosjektplan.
Restrisiko akseptert av:	Gun Peggy Knudsen, fungerende assisterende direktør, 13.04.2020	Behandlingen medfører ikke høy risiko for de registrertes rettigheter og friheter tatt i betraktning tiltakene. Forhåndsdrøftelser med Datatilsynet anses ikke nødvendig.
PVOs råd er innhentet:	Erlend Bakken, PVO, 13.04.2020	PVOs råd er implementert i DPIA.
Oppsummering av PVOs råd: Se tilrådning.		
PVOs råd akseptert av:	Gun Peggy Knudsen, fungerende assisterende direktør, 13.04.2020	Hvis overprøvd, skal begrunnes.
Kommentarer: Ikke overprøvd.		
Innhentede eksterne vurderinger gjennomgått av:	Ikke aktuelt.	Dersom overprøvd, skal begrunnes.
Kommentarer: Nedsatt ekspertgruppe gir råd om teknisk løsning, men vurderer ikke innhold i DPIA.		

Denne DPIA vil revideres og kontrolleres av:	Gun Peggy Knudsen, fungerende assisterende direktør og Geir Bukholm, områdedirektør	PVO bør også vurdere overholdelse av DPIA