folkehelseinstituttet

Godkjent av: GUKN Gyldig fra: 11.12.2020	Rapport Risikovurdering informasjonssikkerhet	Versjon 1.0

FHI

Risikovurdering

Av ny løsning for Smittestopp

Desember 2020

Gun Peggy Strømstad Knudsen, 11.12.2020
Prosjekteier

Innholdsfortegnelse

Innholdsfortegnelse 2
1 Bakgrunn 3
2 Sammendrag 4
3 Trusselvurdering 7
3.1 Trusselaktører 7
3.2 Motiv for digitale operasjoner 7
3.3 Angrepsvektorer 8
3.4 Diskusjon og konklusjon 8
4 Verdivurdering 10
5 Avgrensning av risikovurdering 11
6 Metode for risikoforståelse 12
6.1 Risikometodikk 12
6.2 Workshopserie med eksternt fagmiljø 12
6.3 Usikkerhet i forståelse av risiko over tid 13
6.4 Risikobehandling 13
6.5 Kommunikasjon og lederforankring 13
6.6 Revidering og oppdatering av RoS 13
6.7 Tabell for vurdering av sannsynlighet 13
6.8 Tabell for vurdering av konsekvens 15
7 Risiko 17
7.1 Risikoscenarioer og tiltak 17
7.2 Risikomatrise før ytterligere tiltak 18
7.1.1 Vurdering av risiko - Hele løsningen 20
7.1.2 Vurdering av risiko – Backend 24
7.1.3 Vurdering av risiko – Applikasjon 27
7.1.4 Vurdering av risiko – Mobiltelefon 32
7.1.5 Vurdering av risiko – MSIS 33
7.1.6 Vurdering av risiko – ID-porten 35
7.1.7 Vurdering av risiko – Verifiseringsløsningen 36
7.1.8 Vurdering av risiko – Utviklingsteam 39
8 Bidragsytere 41
9 Intervjuobjekter 42
10 Tester benyttet inn i RoS-analysen 43
11 Akronymer 44

1 Bakgrunn

«Nye» Smittestopp er en løsning for digital smittesporing, basert på Google og Apples Exposure Notification System (heretter ENS) rammeverk. Digital smittesporing kan være et effektivt virkemiddel som et supplement til manuell smittesporing, særlig i situasjoner med utbredt smitte hvor det har vært mange nærkontakter eller mange ukjente nærkontakter. Dette vil skje hurtig og vil dermed kunne supplere mye av det manuelle arbeidet som både tar lang tid og tar mye personellkapasitet.

Smittestopp skal være en sikker og personvernvennlig løsning som er frivillig å ta i bruk, hvor brukeren klart opplyses om hva løsningen innebærer og hvilke rettigheter man innehar. Uansett valg av sporingsteknologi, vil alle løsninger for digital smittesporing eller registrering av nærkontakter gjøre inngrep i personvernet. Personverninngrep må alltid kunne forsvares med en nytteverdi for den enkelte og for samfunnet som helhet. Det betyr at alle slike smittesporingsløsninger vil være svært problematiske hvis man ikke er i en alvorlig situasjon som krever ekstraordinære tiltak, som i en pandemi. En løsning basert på ENS-rammeverket skal holde inngrepet i personvernet på et lavest mulig nivå.

Nytteverdien er avhengig av flere forhold:

- Teknologien må være treffsikker. Applikasjonen må effektivt kunne måle graden av nærkontakt, med få falske positive og falske negative.
- Smittestopp må ha tilstrekkelig oppslutning. Nytteverdien vil avhenge av hvor mange som tar den i bruk.
- Utbredelse av smitte i samfunnet. Jo flere av de smittede og deres nærkontakter som laster ned og bruker applikasjonen, jo flere kan få riktige varsler om at de er nærkontakter.

Videre må testkapasiteten for Covid-19 være tilstrekkelig høy. Først og fremst er det viktig at smittede blir registrert, slik at også nærkontakter kan fanges opp. Videre er det viktig at de som registreres som nærkontakter enkelt kan teste seg, og eventuelt «friskmeldes» dersom det viser seg å være falsk alarm. Risiko knyttet til testkapasitet er ikke belyst i denne rapporten, men spiller likevel en stor rolle for den totale nytteverdien.

Løsningen som utvikles er basert på lokal og desentralisert lagring i den enkelte telefon. Diagnosenøkler lastes kun opp etter at en person har fått påvist smitte, og etter å ha eksplisitt samtykket i å dele disse opplysningene med andre. Diagnosenøklene er laget slik at det er svært vanskelig å finne ut hvem som har lastet dem opp og identifisere smittede personer. Samtidig vil det i visse situasjoner være mulig å avdekke identiteten deres, eksempelvis dersom man blir registrert som nærkontakt og kun har vært i nærheten av én eller få andre personer.

Diagnosenøkler og noen andre opplysninger, som beskrevet nærmere i DPIA, behandles derfor som personopplysninger, og lagres i 14 dager. Verifiseringsløsningen lagrer pseudonymiserte fødselsnummer i en tidsavgrenset periode (24 timer) for å unngå misbruk av varsler. Løsningen er i tråd med anbefalingene fra European Data Protection Board Guidelines 04/2020 (heretter EDPB) om at en desentralisert løsning og dataminimering bør være på plass for å ivareta personvern i størst mulig grad. Det rettslige grunnlag for behandling av personopplysninger i løsningen er basert på samtykke.

Denne risiko- og sårbarhetsanalysen (heretter RoS-analyse) belyser informasjonssikkerheten og personvernet i Folkehelseinstituttets (heretter FHI) valgte løsning for digital smittesporing, Smittestopp. Den vektlegger spesielt risiko for personvernet til den enkelte bruker av applikasjonen, samt at bruken er frivillig og basert på et opplyst og informert samtykke. Risiko rundt personvern er ytterligere og mer utfyllende håndtert i personvernkonsekvensutredningen (Data Protection Impact Assessment, heretter DPIA). Videre går RoS-analysen også inn på tekniske forhold knyttet til utvikling, drift og forvaltning av løsningen, inkludert bakenforliggende systemer. Store deler av løsningen er basert på en tilsvarende løsning i Danmark (Smittestop), men deler av løsningen, som verifiseringsløsningen, er utviklet fra grunnen av i Norge. Behandling av opplysninger om påvist smitte, som gjøres i verifiseringsløsningen, faller inn under begrepet «særlige kategorier av personopplysninger» og krever ekstra aktsomhet.

RoS-analysen skal gi et oversiktlig bilde av gjenværende risiko i løsningen, slik at den kan benyttes som et beslutningsunderlag før en ny løsning om digital smittesporing tas i bruk. Av praktiske grunner er Norsk Helsenetts metodikk for risikovurdering og akseptansekriterier benyttet i denne analysen, men det er ingen vesentlige forskjeller fra det som normalt benyttes i FHI.

2 Sammendrag

Det antas at Smittestopp får stor utbredelse, og bruken kan påvirke store deler av befolkningen gjennom varsler om at man har vært i nærkontakt med Covid-19-smitted. Risikoen for samfunnets innbygger ved å ta i bruk løsningen er totalt sett vurdert som akseptabel. Likevel er det viktig at arbeidet med personvern og informasjonssikkerhet fortsetter i hele løsningens levetid, samt at tiltak iverksettes for å holde risikoen på et akseptabelt nivå. Endringer i trusselbildet kan forekomme, og det er viktig at dette fanges opp og håndteres fortløpende. Videre kan det senere gjøres endringer i løsningen, og disse endringene må også risikovurderes før de settes i produksjon. Både tekniske løsninger og prosesser knyttet til utvikling og drift er vurdert. Vurdering av personvern er en del av analysen, og dette er mer utfyllende håndtert i DPIA-en. I forbindelse med RoS-arbeidet har det også blitt avholdt flere workshops med eksterne deltagere fra norske fagmiljøer, hvor løsningsarkitektur, risikoscenarier og risikoreduserende tiltak har blitt belyst og diskutert.

Oppsummert er risikoen for brudd på konfidensialitet vurdert som svært liten, i og med at det lagres få sensitive opplysninger i løsningen, og det er ingen sentral lagring før noen velger å dele at de har påvist smitte. Risikoen for brudd på integritet er også liten da det er svært vanskelig for utenforstående å manipulere data i løsningen. Tilgangen til dataen er begrenset til noen få, betrodde medarbeidere, og selv de har begrensede muligheter til å sabotere løsningen. Risiko for brudd på tilgjengelighet er derimot til stede, da det er flere «single-point-of-failure» i løsningen, spesielt ved verifisering av påvist smitte. Nedetid i denne delen av løsningen kan medføre at noen ikke klarer å registrere seg som smittet, og effektiviteten av løsningen blir dermed dårligere. Slike tekniske problemer kan også være skadelig for løsningens omdømme og oppslutning. Tiltak bør iverksettes for å ytterligere sikre oppetid for verifiseringsløsningen.

Dette dokumentet er en offentlig versjon av risiko- og sårbarhetsanalysen hvor enkelte detaljer knyttet til sikringstiltak er fjernet.

Nytteverdi av Smittestopp – hele løsningen

Det er en stor grad av usikkerhet knyttet til treffsikkerheten til Smittestopp. Det er flere feilkilder ved bruk av mobiltelefoner og bluetooth-teknologi til sporing av nærkontakter, og basis-teknologien er heller ikke utviklet for dette formålet. Likevel kan digital sporing av nærkontakter være et nyttig supplement til manuell smittesporing.

Nytteverdien er avhengig av at antall falske positive og falske negative er på et akseptabelt nivå, og det kan være vanskelig å måle dette. FHI samler ikke inn informasjon om bruken av løsningen, utover antall nedlastninger av appen og antall som melder fra at de har påvist smitte. Relevante opplysninger er i stor grad lagret desentralt, og FHI har ingen tilgang til innholdet på hver enkelt brukers mobiltelefon. Det er derfor en utfordring å måle nytteverdien av løsningen, noe som igjen kan gjøre det vanskelig å vurdere om personverninngrepet er berettiget. Disse utfordringene er ikke unike for digital smittesporing, og manuell smittesporing har også mange av de samme utfordringene. Erfaringer fra land som har tatt tilsvarende løsninger i bruk tilsier likevel at løsningen har effekt, og at den er et nyttig supplement til manuell smittesporing. FHI har dratt nytte av disse erfaringene og har aktivt testet ulike scenarier hvor mennesker møtes, for å sikre at konfigurasjonsinnstillinger (vurdering av målt signalstyrke fra mobiltelefoner og tid) er så treffsikker som mulig. FHI har for eksempel gjennomført tester for å simulere kø i supermarked og hvordan folk møtes i en buss.

Nytteverdien avhenger også som nevnt av graden av oppslutning rund bruken av applikasjonen - jo flere som bruker den, desto bedre effekt. Høy oppslutning krever at innbygger har god kjennskap til applikasjonen og dens bruksområde, samt at det foreligger en etablert tillit til at myndighetene forvalter løsningen og personopplysninger på en god måte. Smittestopp er bygget på retningslinjer fra EDPB for å sikre godt personvern. Desentral lagring og ingen bruk av GPS er viktig i denne sammenheng. Videre er det viktig at bruken er basert på reell frivillighet, og at samtykket er spesifisert, informert, utvetydig og gitt gjennom en aktiv handling. God og lett forståelig informasjon i appen og i annet informasjonsmateriell, på flere språk, har også vært viktig.

Verdivurdering

Løsningen lagrer informasjon som kan benyttes til å spore nærkontakter, selv om denne sporingen krever fysisk nærhet (innenfor Bluetooth-rekkevidde) til mobiltelefonen som spores. Prinsippet om dataminimering er benyttet, og GAEN-rammeverket er også laget for å være minst mulig personverninngripende. Alle data ligger lagret desentralt, på brukerens egen mobiltelefon, inntil et positivt prøvesvar foreligger. Diagnosenøklene som da lastes opp, etter eksplisitt samtykke, er også laget slik at de ikke skal kunne spores tilbake til brukeren. Verifiseringsløsningen ber brukeren identifisere seg med fødselsnummer, men dette blir ikke lagret i klartekst. Et pseudonym, som i tillegg har gått gjennom en hash-funksjon, blir lagret i 24 timer for å unngå misbruk.

Google og Apple lagrer noe informasjon om bruken av Smittestopp-appen, men ikke diagnosenøkler eller andre helseopplysninger. Dette gjøres i henhold til selskapenes personvernpolicy.

Backend

Backend for GAEN-løsningen er plassert i to datasentre utenfor København. Disse er fysisk godt sikret, og de er bygd opp med geografisk redundans. Diagnosenøklene som lagres her er laget for å deles med andre brukere av Smittestopp, noe som innebærer at integritet og tilgjengelighet er viktigere enn konfidensialitet. Muligheten for utro medarbeidere til å manipulere diagnosenøkler (risiko for integritet) anses

som liten siden det kun er et begrenset antall betrodde medarbeidere som har tilgang. Tilgjengelighet er godt sikret gjennom bruk av to datasentre, og løsningen er også bygget slik at kort nedetid (noen timer) har liten konsekvens.

Applikasjon

Det er egentlig to Smittestopp-apper, en for Apple iOS-mobiler og en for Android-mobiler. Utviklingsverktøyene som er benyttet støtter begge plattformer, så risikovurderingen er i stor grad felles. Appene lastes ned gjennom Apple Store (IOS) eller Google Play (Android), og Apple og Google samler selv inn informasjon om denne bruken. Dette er en konsekvens av å ta i bruk disse plattformene, og har ingen direkte sammenheng med GAEN-rammeverket eller Smittestopp-appen. Bruk av Smittestopp og GAEN medfører ikke at helseopplysninger samles inn, som informasjon om påvist smitte.

Mobiltelefon

GAEN-rammeverket inneholder funksjonalitet for å måle signalstyrke og tid når to mobiltelefoner er i kontakt med hverandre, men overlater til myndighetsaktører, som FHI, å bestemme hvordan disse opplysningene resulterer i smitterisiko. Dette er ingen eksakt vitenskap, og er en kilde til usikkerhet om appens effektivitet. Erfaringsutveksling mellom land (for Norges del, spesielt fra Danmark), og egen testing har vært viktig i å sette mest mulig effektive konfigurasjonsinnstillinger i appen.

Meldingssystem for smittsomme sykdommer (MSIS)

MSIS inneholder informasjon om positive prøvesvar for covid-19, og verifiseringsløsningen gjør et oppslag mot MSIS før en bruker får lov til å dele sine diagnosenøkler. Selve MSIS er ikke omfattet av denne risikovurderingen, kun grensesnittet mot verifiseringsløsningen.

Grensesnittet, API-et, mot MSIS er godt sikret, og slik API-et er bygget opp, er sannsynligheten for å manipulere innholdet i MSIS vurdert som svært lav. Dette grensesnittet er ikke åpent tilgjengelig fra Internett, kun fra verifiseringsløsningen i helsenettet.

ID-porten

ID-porten er en portal for sikker identifisering mot offentlige tjenester i Norge. Ansvaret for ID-porten ligger hos Digitaliseringsdirektoratet, og de er også ansvarlige for den totale sikkerheten i tjenesten. Vi har lagt til grunn at ID-porten sikkert identifiserer brukere, og at drift og forvaltning er trygt ivaretatt.

Bruk av ID-porten logges, og loggene vil kunne vise identifiseringer fra Smittestopp. Vi vurderer at dette ikke innebærer noen betydelig tilleggsrisiko for at disse opplysningene kommer på avveie, siden vi anser ID-porten for å ha gode generelle sikringstiltak.

Verifiseringsløsningen

Det er gjort flere tiltak i verifiseringsløsningen for å ivareta personvern. Fødselsnummer, som er nødvendig for å identifisere seg mot ID-porten, lagres ikke permanent. Når sesjonen mot ID-porten er terminert, slettes denne informasjonen umiddelbart. For å hindre misbruk av løsningen, ved at en bruker med påvist smitte registrerer seg fra mange forskjellige enheter, lagres det en hash av et pseudonym, utstedt av ID-porten, i 24 timer. Det betyr at en person med påvist smitte kan registrere seg opp til tre ganger i løpet av en 24-timers periode. Årsaken til at noen kan ønske å registrere seg flere ganger, er at en person kan ha benyttet flere mobiltelefoner mens vedkommende har vært smittet. Begrensningen på 24 timer er gjort av hensyn til dataminimering, men sannsynligheten for å identifisere en person på bakgrunn av den lagrede hashen er uansett svært liten, og krever administrativ tilgang til ID-porten.

Utviklingsteam

Det er to utviklingsteam som har utviklet løsningen:

- Innleid fra NetCompany, som har utviklet app og GAEN-backend
- Ett hos FHI, som har utviklet verifiseringsløsningen.

Begge utviklingsteam er intervjuet, og metodikk og kode er gjennomgått. Begge miljøer viser god modenhet, høy bevissthet for innebygd personvern, og tar aktivt i bruk rammeverk for sikker utvikling, som OWASP og BSIMM. All kildekode er åpen og tilgjengelig for alle, noe som gir økt tillit til at koden gjør det den skal, og ikke noe annet. Eventuelle feil og svakheter kan oppdages av alle interesserte, og innspill fra «open source community» tas på alvor.

Resultat av sikkerhetstester

BDO har gjennomført sikkerhetstester av Smittestopp app, backend og verifikasjonsløsning, og detaljer om disse testene finnes i en egen rapport. Det ble ikke avslørt noen alvorlige svakheter, og noen mindre alvorlige funn har allerede blitt rettet opp, eller rettes opp før produksjonssetting.

Anbefalte tiltak

Risikoen i løsningen anses som akseptabel, og det er ikke identifisert ytterligere nødvendige tiltak.

3 Trusselvurdering[1]

I dette kapittelet dokumenterer vi trusselaktører, eksempler på motiver for å gjennomføre digitale operasjoner og angrepsvektorer som brukes mye i dag. Informasjonen er basert på norske myndigheters årlige åpne trusselrapporter, eksempelvis fra Nasjonal Sikkerhetsmyndighet (heretter NSM), Politiets Sikkerhetstjeneste (heretter PST) og Etterretningstjenesten. Denne innsikten er verdifull for å forstå hvorfor vi må beskytte tjenestene som utvikles, samt hvem og hva vi skal beskytte oss mot.

Videre har Mnemonic på oppdrag fra FHI utført en trusselvurdering spesielt rettet mot angrep på applikasjoner basert på Google/Apple ENS.

3.1 Trusselaktører

Lysneutvalget gir en god oversikt over mangfoldet av trusselaktører. De beskriver alt fra innsidetrusselen fra utro tjenere, til aktører i det digitale rom med økende kompetanse og ressurser. Generelt ser vi følgende kategorier av trusselaktører som opererer via internett:

- Script kiddies (gutte- og jenteromshackere)
- Politisk motiverte enkeltpersoner
- Hacktivister
- Cyberterrorister
- Profesjonelle, organiserte cyberkriminelle
- Sofistikerte statsstøttede aktører

I norske sikkerhetsmyndigheters rapporter peker NSM, PST og Etterretningstjenesten særlig mot fremmede staters etterretningsmiljøer og internasjonale kriminelle miljøer, og deres aktiviteter mot norske interesser i det digitale rom, som reelle trusler mot Norge.

Trusselvurdering for smittesporingsløsningen:

Ut fra egenarten til smittesporingsløsningen, og særlig med innsikten fra Etterretningstjenestens Fokus 2020, vil det være nærliggende å tro at **etterretningsmiljøer** i Russland og Kina vil være spesielt opptatt av hvordan de kan benytte Smittestopp til å påvirke og analysere bevegelsesmønsteret til norske innbyggere. Selv om det mest sannsynlig ikke kan hentes ut større mengder persondata gjennom den nye Smittestopp-løsningen, vil det gjennom sofistikerte digitale og fysiske angrep, være mulig å påvirke den norske befolkningens bevegelsesmønster og aktivitetsnivå etter ønsket utfall. Ved en gjennomgang av tilgjengelig informasjon er det ikke funnet indikatorer som bekrefter at liknende applikasjoner i andre land har vært offer for angrep. Denne informasjonen understøtter sannsynlighetsgradene satt i denne vurderingen.

3.2 Motiv for digitale operasjoner

Lysneutvalget, NSM, PST og Etterretningstjenesten gir i sum en god oversikt over trusselaktørenes motivasjon for å gjennomføre cyberoperasjoner:

- **Økonomisk vinning** kan eksempelvis oppnås gjennom løsepengekampanjer ved bruk av kryptovirus, tyveri av datakraft for kryptovalutautvinning, eller tilbud om "crime as a service" der bakmennene selger tjenester slik som tjenestenektangrep eller utleie av (stjålet) datakraft via botnets som tjeneste.
- **Etterretnings- og kartleggingsaktivitet** for å innhente mest mulig informasjon om norske verdier. Både virksomheter og enkeltpersoner kan være i søkelyset.
- **Påvirkningsoperasjoner** for å påvirke beslutninger eller demokratiske prosesser, i virksomheter og/eller på nasjonalt nivå.
- **Industrispionasje** kan gjennomføres for økonomisk vinning, og/eller som middel for å avansere egen forskning og utvikling gjennom tyveri av intellektuelle verdier.
- **Digital sabotasje** kan brukes som ledd i hybrid krigføring og/eller benytte kapabiliteten som et pressmiddel i en påvirkningsoperasjon.

De Nasjonale sikkerhetsmyndighetene påpeker at det er en høy aktivitet mot norske interesser i det digitale rom. Det er nærliggende å anta at mindre avanserte og ressurssvake trusselaktører er motivert av økonomisk vinning. De organiserte statlige aktørene vil kunne drives av både økonomiske motiver og mål om å drive etterretning, spionasje og påvirkningsoperasjoner, i tillegg til å bygge kapabiliteter for sabotasje og hybrid krigføring.

FHIs trusselvurdering for smittesporingsløsningen:

Ut fra egenarten til smittesporingsløsningen vil det være sannsynlig at den fanger interessen til eksterne **etterretningstjenester** og profesjonelle **cyberkriminelle.**

[1] Kilder:
Lysneutvalget, NSM, Etterretningstjenesten, PST, Europol, Trussel rapport Mnemonic, Erfaringer fra Smittestopp 1.0

Løsningen lagrer ikke data på vegne av norske innbyggere, men vil potensielt kunne styre mobilitetsmønsteret til en større mengde norske borgere. Dette er en angrepsvektor som kan benyttes i påvirkningsoperasjoner med mål om å påvirke demokratiske prosesser, eller som del av hybrid krigføring. Mennesker i maktposisjoner i offentlig og privat sektor vil være særlig attraktive mål. Gjennom falsk smittespredning vil trusselaktører kunne påvirke flere deler av samfunnet og samtidig styre norske myndigheters beslutningsgrunnlag slik at beslutninger er gunstige for trusselaktørens måloppnåelse.
Slike operasjoner vil kunne bidra til å svekke tilliten til norske myndigheter, og dermed påvirke demokratiet.

3.3 Angrepsvektorer

NSM, PST og Etterretningstjenesten peker i sum på angrepsvektorer som benyttes for å gjennomføre digitale operasjoner.

- **E-post som angrepsvektor:** PST og NSM beskriver at den vanligste måten for en trusselaktør å komme seg på innsiden av et nettverk på er ved å sende skadevare via målrettede e-poster. Et slikt angrep utnytter både digitale og personellmessige sårbarheter.
- **Sårbare internettjenester som angrepsvektor:** PST og NSM peker på at servere som er koblet mot internett brukes som inngangsport til virksomheters nettverk. Et slikt angrep utnytter digitale sårbarheter.
- **Personell som angrepsvektor:** PST beskriver hendelser der trusselaktører bryter seg inn i datanettverk ved å få ansatte bevisst eller ubevisst til å plassere skadevare via for eksempel minnepinner. Etterretningstjenesten og PST peker særlig på faren for innsidetrusler ved at sentrale personer i virksomheter og hos myndigheter kultiveres og rekrutteres til etterretningsformål. Et slik angrep utnytter personellmessige sårbarheter
- **Digitale verdikjeder som angrepsvektor:** NSM, PST og Etterretningstjenesten peker alle på utfordringen med lange digitale verdikjeder. Trusselaktører angriper virksomheter som ikke er mål i seg selv, men som vil fungere som brohode for videre tilgang til andre mål. Et slikt angrep utnytter både digitale og personellmessige sårbarheter, samt sårbarheter i virksomheters sikkerhetsstyring.
- **Svakheter i sikkerhetsstyringen:** NSM peker på at svak sikkerhetsstyring fører til ubalanse mellom håndteringen av digitale, personellmessige, virksomhetsmessige og fysiske sikringstiltak. Denne ubalansen leder til sårbarheter som kan utnyttes som angrepsvektorer.
- Alle disse angrepsvektorene kan brukes for å gjennomføre nettverksoperasjoner med sabotasjeformål (hybrid krigføring), kryptovirus til økonomisk utpressing, og/eller til etterretnings- og spionasjeformål.

Trusselvurdering for smittesporingsløsningen:

Smittesporingsløsningen utvikles hurtig, med en estimert lanseringsdato som ble satt før organisasjonen hadde et klart bilde av omfanget rundt utvikling og produksjon av en ny tjeneste. Fra ide til realisering og operasjonalisering vil det gå ca. 8 uker. Det var ikke planlagt, eller satt som et krav, at leverandøren som fikk oppdraget med å utvikle en norsk smittesporingsapplikasjon skal ha gjennomført liknende utvikling i andre land.

- Hvis leverandøren opplever at rammene for leveransen er satt uten at det er rom for å spille inn divergerende behov underveis, kan det føre til at leverandøren tar snarveier som kan påvirke sikkerheten i løsningen, for å holde seg innenfor de forhåndsgitte rammer.
- Løsningen bygges av konsortier av samarbeidspartnere som ikke tidligere har jobbet sammen. En trusselaktører vil kunne utnytte denne situasjonen, der ukjente mennesker jobber sammen under tidspress, til å tilegne seg informasjon som senere vil kunne brukes for å skaffe seg urettmessig tilgang gjennom manipulering av mennesker. Dette kan handle om alt fra å få tilgang til brukernavn og passord, til kodebiblioteker og til sertifikater.
- Løsningen består av flere komponenter, og integrerer flere løsninger. Det er integrasjon av både nye og gamle systemer (Google play/App store, applikasjon, sky, MSIS). Hvis det ikke gjennomføres tilstrekkelig sikring av hele verdikjeden basert på analyse og sikkerhetstesting, kan det med denne hastigheten i utvikling være mulighetsrom for å angripe det svakeste ledd i verdikjeden.
- De foregående sårbarhetene vil potensielt forsterkes gjennom at dette er en relativt ny løsning som etableres raskt på tvers av flere selskaper. Operasjonsmønster og styringsmodeller, inkludert sikkerhetsstyring, er ikke etablert. Med mindre slike prosesser er på plass vil dette kunne medføre svakheter både i teknologi, organisasjon og menneskelige faktorer.
- I kjølvannet av løsningen vil cyberkriminelle også kunne utnytte Covid-19 pandemien og innsikt om løsningen til å sende skreddersydde smittevarsler per e-post, både som målrettede- eller generelle kampanjer. De vil kunne utnytte folks manglende innsikt i at det kun vil være varsler gjennom applikasjonen og at det kun er faktisk smittede som vil få muligheten til å varsle.

MERK: : Denne trusselvurderingen er skrevet 08.11.20 og sikkerhetsteamet er ikke presentert en tredjepartsvurdering av NetCompany som leverandør. Dette i seg selv utgjør en risiko da vi ikke har mulighet til å kontrollere utviklingsmetodikken og sørge for at sikkerheten blir ivaretatt gjennom alle ledd i utviklingen. Det foreligger heller ingen integrity due diligence rapport av NetCompany eller deres underleverandører, så risiko forbundet med selve leverandøren er vanskelig å vurdere.

3.4 Diskusjon og konklusjon

I denne trusselvurderingen har vi sett på de overordnede egenskapene til FHIs nye smittesporingssystem, og vi har gjort en betraktning av hva slags type data som vil bli forvaltet i løsningen. Ut fra norske sikkerhetsmyndigheters åpne trusselvurderinger har vi analysert hvordan smittesporingsløsningen og dens effekt på bevegelsesmønsteret til norske borgere kan være av interesse for eksterne trusselaktører. Særskilt fremmede staters etterretningstjenester og profesjonelle cyberkriminelle vil kunne ha interesse av løsningen.

Fra Etterretningstjenestens Fokus 2020 vet vi at navngitte nasjonalstater har vist en særlig interesse for Norge i det digitale rom. En nylig utgitt rapport fra ENISA3 dokumenterer at Russland allerede har begynt å utføre påvirkningsoperasjoner i vestlige land ved å utnytte Covid-19 situasjonen. Videre varsler Europol om økt kriminell aktivitet, og i Norge varsler Telenor om rekordhøy svindeltrafikk i kjølvannet av Covid-19 pandemien.

Fra dette utleder vi som følger:

Trusselvurdering for smittesporingsløsningen:

Med en antakelse om stor utbredelse av Smittestopp vurderer vi følgende:

- Det er like **sannsynlig som usannsynlig** at Smittestopp kan bli et angrepsmål. Potensielle sårbarheter i applikasjonen kan benyttes til å villede den norske befolkningen.
- Det er like **sannsynlig som usannsynlig** at MSIS kan bli angrepet for å utnytte varslingsmulighetene som ligger i applikasjonen for å påvirke/kontrollere bevegelsesmønsteret til store deler av den norske befolkningen.
- Det er **sannsynlig** at aktører kan benytte falske utsendelser av SMS eller e-post (Smishing/Phishing) for å utnytte folks uvitenhet om varslingsmetodikken for Smittestopp. Enten med formål om å påvirke demokratiet gjennom å skape usikkerhet i befolkningen og redusere tilliten til myndighetene eller økonomisk profitt ved at trusselaktøren kan tilegne seg informasjon som kan benyttes til utpressing, eller omsettes ved salg.
- Det er **sannsynlig** at kriminelle aktører vil benytte seg av Smittestopp som plattform for kriminell økonomisk vinning.
- Det er like **sannsynlig som usannsynlig** at aktører vil forsøke å utvikle lignende applikasjoner for å utnytte folks tillit til den nye applikasjonen og gjennom dette installere skadevare på enheter, som igjen kan gi tilgang til sensitive personopplysninger eller geo-lokaliserende informasjon.
- Det er **lite sannsynlig** at et Bluetooth-basert angrep som knytter persondata til bevegelsesmønstre vil ramme Smittestopp siden gjennomføringen vil kreve betydelige ressurser og kapasiteter hos trusselaktør og at det er få aktører som besitter denne type kapasiteter.

4 Verdivurdering

I verdivurderingskapitlet presenteres et sammendrag som redegjør for lagring og innsamling av personopplysninger i Smittestopp-løsningen. Oversikten er basert på DPIA-en, og det henvises til DPIA-en for en fullstendig og grundig gjennomgang og vurdering av personopplysninger og data som lagres i ulike komponenter av løsningen.

Google Play/App Store

Når Smittestopp-appen lastes ned fra Google Play eller App Center, får Google og Apple automatisk tilgang på bruksmønster og feilsituasjoner. Informasjonen kan ikke knyttes opp til personopplysninger som telefonnummer, posisjonsdata eller smittekontakter.

Opplysningene slettes etter 90 dager.

Backend

Backend inneholder kun diagnosenøkler fra den smittede. Alle nøkler er pseudonymiserte og lagres i 14 dager for å kunne varsle nærkontakter opp til 14 dager tilbake i tid. I motsetning til den tidligere Smittestopp Versjon 1, samles det ikke GPS data.

Følgende opplysninger behandles i backend løsningen:

- Diagnosenøkkel (helseopplysning).

Opplysninger i backend eldre enn 14 dager slettes fortløpende.

Applikasjonen

Applikasjonen inneholder opplysninger om vedvarende kontakter med uavbrutt Bluetooth kontakt over en kort periode. Det samles inn mer informasjon enn nødvendig, da alle vedvarende kontakter ikke nødvendigvis er reelle nærkontakter. I tillegg vil kun dataen benyttes dersom positiv smitte registreres, men det er umulig å forutse hvem som faktisk blir smittet så ytterligere dataminimering er utfordrende. Omfanget av potensielle kontakter avgrenses ved å sette krav til avstand/signalstyrke og tid/varighet på kontakt.

Følgende personopplysninger innsamles og lagres på brukerens mobiltelefon når brukeren har lastet ned og aktivert appen (også beskrevet i DPIA):

- Rullerende "Temporary Exposure Key" (heretter TEK) på brukerens telefon.
- Rullerende systemgenerert ID på brukers telefon som utledes fra TEK nøklene.
- Det rullerende systemgenerert ID på andre telefoner, som brukeren har vært i nærheten av.
- Signalstyrke.
- Diagnosenøkler, det vil si TEK som er knyttet til en diagnose (helseopplysning, samles kun inn ved verifisert smitte).
- Opplysninger om dato for eventuelle symptomer (helseopplysning, samles kun inn ved verifisert smitte).

Opplysninger i appen eldre enn 14 dager slettes fortløpende.

Verifiseringsløsningen

Verifiseringsløsningen brukes til å verifisere positiv smitteprøve via ID-porten og meldingssystem for smittsomme sykdommer (heretter MSIS). Informasjonen som lagres er pseudonymisert. Mellomlagring av brukerens ID mellom ID-porten og svar fra MSIS foregår i en kryptert informasjonskapsel, der nøkkelen ligger hos verifiseringsløsningen. Mellomlagringen avsluttes med en gang brukeren avslutter «sesjonen».

Når brukeren benytter verifiseringsløsningen og samtykker til notifikasjon av nærkontakter behandles følgende personopplysninger:

- ID-opplysninger i form av fødselsnummer.
- Pseudonym som er unik for kombinasjonen av fødselsnummer og verifiseringsløsning.

Opplysninger i verifiseringsløsningen slettes etter 24 timer.

5 Avgrensning av risikovurdering

I arbeidet med risiko- og sårbarhetsanalysen av Smittestopp-applikasjonen er det gjort avgrensninger for å fokusere innsatsen mot de mest kritiske komponentene. Samtidig har det vært essensielt at avgrensningen ikke går på bekostning av norske innbyggeres sikkerhet og personvern. Avgrensning av omfang er derfor gjort i dialog med FHI.

Risikoer knyttet til personvern er mer ufyllende håndtert i DPIA-en som dekker dette området. Tett samarbeid mellom prosjektgruppene som har utarbeidet DPIA-en og RoS-en har sikret at de mest fremtredende risikoene knyttet til personvern er dekket på alle områder.

I risikovurderingen av sikker utvikling hos leverandøren av selve applikasjonen og backend til Smittestopp, er analysen avgrenset til å omfatte intervjuer og beskrivelser fra utviklerne. Intervjuene og vurderingene er basert på ledende internasjonale sikkerhetsstandarder, som f.eks. NIST, ISO 27001 og OWASP. Risikovurderingen er hovedsakelig basert på tillit og samtaler med flere av utviklerne hos leverandøren. Det er ikke gjort risikovurderinger av eventuelle underleverandører til utviklerleverandøren av Smittestopp.

Det er gjort avgrensninger slik at denne RoS-en ikke omfatter vurdering av økt risiko for angrep mot MSIS, eller FHI sin motstandsdyktighet mot angrep. Denne RoS-en omhandler ikke risiko knyttet til effekt og måloppnåelse av Smittestopp som tjeneste og heller ikke omdømmerisiko utover kriterier gitt i konsekvensmatrisen.

6 Metode for risikoforståelse

Dette kapitlet redegjør for risikometodikken som er benyttet i risikoanalysen og definerer kriterier for sannsynlighet og konsekvens som danner grunnlaget for risikovurderingen av Smittestopp. En beskrivelse av hvordan det norske sikkerhetsmiljøet er inkludert gjennom en workshopserie, og tilstedeværelsen og bruken av usikkerhet i risikovurderingene er også inkludert.

6.1 Risikometodikk

Denne risikoanalysen er gjennomført i henhold til risikovurderingsmetodikken som benyttes i det norske helsedomenet, basert på ISO 31000 og andre relevante underliggende standarder. Risikoanalysen skal bidra til at FHI på en systematisk måte kan forutse, forebygge og redusere sannsynligheten for, og konsekvensen av, uønskede hendelser relatert til informasjonsbehandlingen i smittevernapplikasjonen. Risikoanalysen er en iterativ prosess med formål å sikre at usikkerhet knyttet til identifiserte risikoer reduseres over tid, at risikonivåer for eksisterende risikoer er oppdatert, samt at oppdukkende risiko kan vurderes. Tre viktige komponenter finnes i en risikovurdering:

- **Verdier:** Informasjon som forvaltes av løsningen, den tekniske løsningen og verdikjeden, for eksempel helseopplysninger, en applikasjon eller sikkerhetsgradert informasjon.
- **Trusler:** Noen eller noe som kan utnytte eller skade verdiene, for eksempel en hacker eller et strømbrudd.
- **Sårbarheter:** Mangel på, eller svakheter i, sikkerhetstiltak som trusselaktørene kan utnytte, for eksempel svak tilgangskontroll eller manglende nødstrøm.

Risiko kan manifestere seg i ulik form og ulik grad av konsekvens. Typiske konsekvenser inkluderer:

- **Liv og helse**, alt fra ubetydelig personskade til dødsfall.
- **Personvern**, alt fra ubetydelig tap av personlig integritet til langvarige konsekvenser for den enkeltes personlig integritet eller anseelse.
- **Regelverk**, alt fra ubetydelig brudd til brudd som medfører vedtak, bøter eller straff.
- **Tjenesteytelse**, alt fra redusert drift til langvarig utilgjengelighet av tjenesten.
- **Omdømme**, alt fra negative oppslag til vesentlig tap av tillit hos brukere og samfunnet.
- **Økonomi**, alt fra ubetydelig økonomisk konsekvens til uopprettelig økonomisk tap.
- **Politikk**, alt fra ubetydelig politisk påvirkning til omfattende politisk påvirkning.

Risikoanalysen har blitt gjennomført som beskrevet under:

1. **Kartlegging av verdier**. Komponentene i smittesporingssystemet og informasjonsverdiene som forvaltes av systemet har blitt identifisert og klassifisert. Identifiseringen av informasjonsverdiene danner grunnlag for identifisering av trusselaktører som potensielt kan skade disse.
2. **Kartlegging av trusler**. Trusselaktørene og deres motiv har blitt kartlagt, samt angrepsvektorene som kan benyttes.
3. **Kartlegging av sårbarheter**. Komponentene og verdikjeden har blitt vurdert.
4. **Etablering av risikoscenarier**. En oversikt over mulige scenarier har blitt etablert. Et risikoscenario skal bestå av en trusselaktør, en uønsket hendelse knyttet til informasjonsverdi(er) som kan få noen konsekvenser.
5. **Vurdering av sannsynlighet, konsekvens og usikkerhet**. Ved bruk av standardene for vurdering av sannsynlighet, konsekvens og usikkerhet i helsedomenet (kapittel 4) har de ulike faktorene blitt vurdert for hvert risikoscenario.
6. **Gruppering og rapportering**. Risikoscenariene har blitt gruppert slik at det blir lettere å få oversikt over de scenariene som har felles faktorer.

6.2 Workshopserie med eksternt fagmiljø

FHI har holdt en workshopserie i forbindelse med RoS-arbeidet for nye Smittestopp som en del av metodikken. Formålet med workshopserien har vært å involvere fagmiljøet utenfor FHI i diskusjon rundt risikoscenariene og tiltak. FHI har fått konkrete innspill på scenarier, og tiltak forbundet med disse, fra fagmiljøet.

Workshopserien har fulgt følgende tematikk:

- Workshop 1 innledet arbeidet med en innføring i arbeidsmetode og veien så langt.
- Workshop 2 tilspisset arbeidet med fokus på "personvern".
- Workshop 3 fokuserer på tematikken "sikkerhet».
- Workshop 4 tok for seg "eksterne aktører."
- Den femte og avsluttende workshopen la frem ferdig risiko- og sårbarhetsvurdering av Smittestopp.

I forkant av hver workshop mottok deltagerne en spørreundersøkelse med beskrivelse av aktuelle scenarioer per tema. Deltagerne ble bedt om å rangere risiko per scenario, samt skrive kommentarer og forslag til tiltak. Disse scenarioene ble så beskrevet i detalj i tilhørende workshop, hvor deltagernes innspill ble diskutert i plenum.

Innspillene fra fagmiljøet ha vært med på å prioritere og forme RoS-arbeidet, slik at vi sikrer helhetlig dekning. Med åpenhet og innsikt fra flere hold har vi hatt muligheten til å bedre bevare helhetlig sikkerhet i den nye Smittestopp appen.

Presentasjonene fra workshopserien er publisert på FHI.no.

6.3 Usikkerhet i forståelse av risiko over tid

Løsningen består av mange komponenter og leverandører med gjensidige avhengigheter. Analyseresultatene i denne rapporten baserer seg på beste praksis og vurderinger etter godt faglig skjønn. Samtidig er det viktig å poengtere at dette er en løsning i en aktiv utviklingsfase, og vurderingene vil derfor inneholde varierende grad av sikkerhet basert på graden av innsikt i hvordan tiltak er implementert i løsningen som settes i produksjon. Denne risikoanalysen tar høyde for graden av usikkerhet i forståelsen av risiko. Den sanne eller objektive risikoen er det ingen som kjenner. Det er derfor tatt høyde for at vurdering av etterlevelse i henhold til beste praksis kan utføres periodisk slik at grad av usikkerhet i risikoforståelsen kan reduseres. Dette gjøres ved å tallfeste grad av etterlevelse av tiltak hvor beste praksis benyttes for å dekke løsningens behov for risikoreduserende tiltak.

6.4 Risikobehandling

Identifiserte risikoer er behandlet gjennom iverksettelse av risikoreduserende tiltak.

Behandlingen og iverksettelse av tiltak er dokumentert i en risikobehandlingsplan. Risikobehandlingsplanen inneholder:

- Beskrivelse av oppfølgingspunkter for hver risiko.
- Beskrivelse av behandlingsalternativ og ytterligere tiltak.
- Tiltakseier. Alle tiltak skal ha en ansvarlig tiltakseier med frist for iverksettelse.

Det er utarbeidet akseptansekriterier for risiko og usikkerhet som en del av prosessen for å behandle risiko. NHN sine etablerte matriser benyttes til dette.

6.5 Kommunikasjon og lederforankring

Risikoeier er FHI. FHI skal sørge for at risiko rapporteres regelmessig for å ivareta lederforankring. Disse skal også ivareta kommunikasjon mot andre relevante interessenter.

6.6 Revidering og oppdatering av RoS

Risikovurderinger skal oppdateres ved endringer som kan påvirke risikobildet.

6.7 Tabell for vurdering av sannsynlighet

Kriterier for valg av sannsynlighet			
Verdi	Beskrivelse	Erfaring/Trend?	Beskrivelse letthet
4	Meget sannsynlig	Har skjedd hos oss og andre.	• Sikkerhet er ikke etablert. • Krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes. • Ikke nødvendig med kjennskap til tiltakene. • Sikkerhetstiltak er sterkt avhengig av at en eller flere manuelle rutiner/policyer følges
3	Sannsynlig	Har hørt om hos andre, kunne like gjerne vært hos oss.	• Sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet. • Sikkerhetstiltak fungerer ikke etter hensikten. • Egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene.

			• Eksterne trenger små/normale ressurser og normal kjennskap til tiltakene for å bryte disse.
2	Mindre sannsynlig	Har hørt om, men aldri hos oss.	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet. • Sikkerhetstiltak fungerer etter hensikten. • Egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse. • Eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse.
1	Lite sannsynlig	Har aldri hørt om.	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet. • Sikkerhetstiltak fungerer etter hensikten. • Krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes. • Eksterne kan ikke omgå tiltakene.

6.8 Tabell for vurdering av konsekvens

Kriterier for valg av konsekvens							
Verdi	Beskrivelse	Personvern (Berører hvor mange?)	Liv og helse (Berører hvor mange?)	Regelverk	Tjeneste- ytelse og tidsaspekt i forhold til tjeneste-kritikalitet Ute av drift /redusert kvalitet	Omdømme	Økonomi
4	Meget stor	Langvarig tap av anseelse eller personlig integritet.	Dødsfall eller alvorlige personskader (flere personer) på grunn av mangel eller feil hos Norsk Helsenett (heretter NHN) eller underleverandører.	Regelverksbrudd som medfører vedtak, foretaksstraff/bøter og/eller fengselsstraff.	Hendelse som fører til at system som benyttes av alle virksomheter og/eller har stor betydning er midlertidig ute av drift eller redusert. Stopp/reduksjon som omhandler alle brukere. Personsensitiv informasjon kan ha gått tapt eller kan ikke stoles på.	Vesentlig tap av tillit hos brukere/ kunder, eier og andre viktige interessenter. Omfattende og svært negative oppslag i media (redaksjonelle medier og sosiale medier).	Uopprettelig økonomisk konsekvens.
3	Stor	Tap av anseelse eller personlig integritet som er krenkende.	Alvorlig person-skade (én person) på grunn av mangel eller feil hos NHN eller underleverandører.	Regelverks-brudd som medfører advarsel eller vedtak, samt mulig foretaksstraff/bøter.	Hendelse som fører til at system av stor utbredelse/ betydning er midlertidig ute av drift eller redusert. Stopp/ reduksjon som omhandler de fleste brukerne. Virksomhets-kritisk informasjon kan ha gått tapt eller kan ikke stoles på.	Tap av tillit hos brukere/ kunder, eier og andre viktige interessenter. Negative oppslag i media over flere dager.	Alvorlig økonomisk konsekvens.

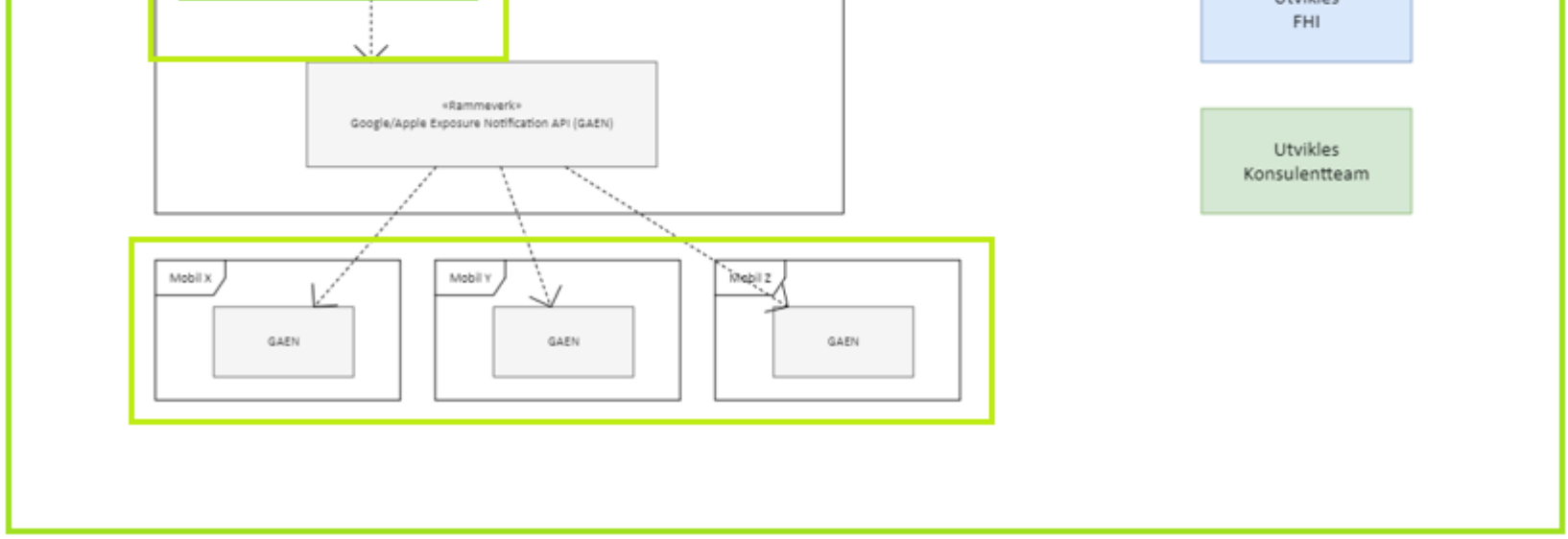
2	Mindre	Tap av anseelse eller personlig integritet som kan oppfattes som krenkende.	Mindre alvorlig person-skade på grunn av mangel eller feil hos NHN eller underleverandører.	Regelverks-brudd som kan medføre advarsel eller vedtak.	Hendelse som fører til at system av større utbredelse/ betydning er midlertidig ute av drift eller redusert. Stopp/ reduksjon som omhandler noen brukere. Informasjon unntatt offentlighet-loven kan ha gått tapt eller kan ikke stoles på.	Mindre eller kortvarige oppslag i media som kan ved gjentatte tilfeller føre til tap av tillit.	Mindre alvorlig økonomisk konsekvens
1	Liten	Ubetydelig tap av anseelse eller personlig integritet.	Ubetydelig personskade på grunn av mangel eller feil hos NHN eller underleverandører.	Ubetydelig regelverks-brudd.	Hendelse som fører til at system av mindre utbredelse/ betydning er midlertidig ute av drift er midlertidig ute av drift eller redusert. Stopp/ reduksjon som omhandler få brukere. Åpen/ tilgjengelig informasjon kan ha gått tapt eller kan ikke stoles på.	Henvendelse fra media uten negative oppslag.	Ubetydelig økonomisk konsekvens.

7 Risiko

Dette kapitlet beskriver risikoscenarier og tiltak knyttet til ulike komponenter av smittestoppløsningen. Scenarienes sannsynlighet, konsekvens og usikkerhet vurderes, i tillegg til at etterlevelse av foreslåtte tiltak gjennomgås. For å illustrere viktigheten av risikoene totalt og for hver komponent, er risikoene kategorisert i risikomatriser.

7.1 Risikoscenarioer og tiltak

Skissering av løsning:



Gjennomsnitt score	Høyeste score		Risikoskala
		Vurdering av risiko for hele løsningen	16
		Vurdering av risiko for backend	15
		Vurdering av risiko for applikasjon	14
		Vurdering av risiko for mobiltelefon	13
		Vurdering av risiko for MSIS	12
		Vurdering av risiko for ID-porten	11
		Vurdering av risiko for verifiseringsløsningen	10
		Vurdering av risiko for utviklingsteam (applikasjon og backend)	9
			8
			7
			6
			5
			4
			3
			2
			1
			0

7.2 Risikomatrise før ytterligere tiltak

Risikomatrisen viser risikoscenarioene som har risikonivå tilsvarende gult eller rødt.

Konsekvens					
	4	R-2-2 R-3-7 R-5-1 R-7-5	R-2-1 R-3-1 R-3-12		
	3		R-1-3 R-3-10 R-1-8 R-7-3 R-2-4 R-8-1 R-3-4 R-8-2 R-3-5 R-8-3		
	2			R-1-4 R-4-1 R-4-2 R-7-2	
	1				R-3-3
		1	2	3	4
		Sannsynlighet			

Oversikt over risikoscenarioer

R-1-3: Mistillit til smittesporings applikasjoner resulterer i at en stor andel av befolkningen ikke tar i bruk appen.
R-1-4: Bruk av appen oppfattes som obligatorisk og mange føler seg presset til å ta appen i bruk.
R-1-8: DDoS-angrep fører til at hele Smittestopp-løsningen er utilgjengelig.
R-2-1: Trusselaktører korrumperer diagnosenøkler ved å kompromittere backendløsningen til Smittestopp appen.
R-2-2: Person med tilgang til backendløsningen utnytter sin rolle og korrumperer data i backend.
R-2-4: En ukjent trusselaktør gjennomfører en ondsinnet villet handling mot datasenteret som lagrer backend til Smittestopp.
R-3-1: Trusselaktør misbruker Smittestopp appen til å påvirke arrangement gjennom å tvinge en gruppe nordmenn i karantene/testing for å påvirke f.eks. et arrangement.
R-3-3: Apple og Google samler inn og behandler statistikk som kan inneholde personopplysninger for alle apper, inkludert Smittestopp. Dette kan stride mot brukerens rettigheter.
R-3-4: Det er uklart for brukeren hvordan man skal utøve sine personvernrettigheter i Smittestopp.
R-3-5: Misbruk av mulighet for repetert utsendelse av smittevarsel fra flere mobiltelefoner.
R-3-7: Trusselaktører korrumperer diagnosenøkler ved å kompromittere Smittestopp-appen.
R-3-10: Tekniske problemer ved Smittestopp reduserer dens funksjon og/eller reduserer mobilens andre funksjoner.
R-3-12: Falsk versjon av Smittestopp applikasjon.
R-4-1: Bluetooth ikke laget for avstandsberegning, dette gjør at nærkontakt registreres feilaktig og fører til falske positive. Eksempelvis i tilfeller der det i realiteten var vegg/glass mellom enhetene.
R-4-2: Bluetooth er ikke laget for avstandsberegning, noe som gjør at nærkontakt registreres feilaktig (mangel på registrering) og fører til falske negative.
R-5-1: Angrep mot MSIS for å korrumpere smittedata.
R-7-2: Brann bryter ut inne på datasenteret der verifiseringsløsningen er lagret.
R-7-3: En ukjent trusselaktør gjennomfører en ondsinnet villet handling mot datasenteret i Norge som lagrer verifiseringsløsningen.
R-7-5: Person med tilgang til verifiseringsløsningen utnytter sin rolle og korrumperer data i verifiseringsløsningen.
R-8-1: Lav kodekvalitet på grunn av mangelfull kontinuerlig forbedring av sikker utviklingsmetodikk, styring og kompetanse.
R-8-2: Mangelfull forståelse av sikker koding fører til ustabile applikasjoner og datalekkasje.
R-8-3: Sårbarheter i kildekode på grunn av manglende analysemetoder for avdekking.

7.1.1 Vurdering av risiko - Hele løsningen

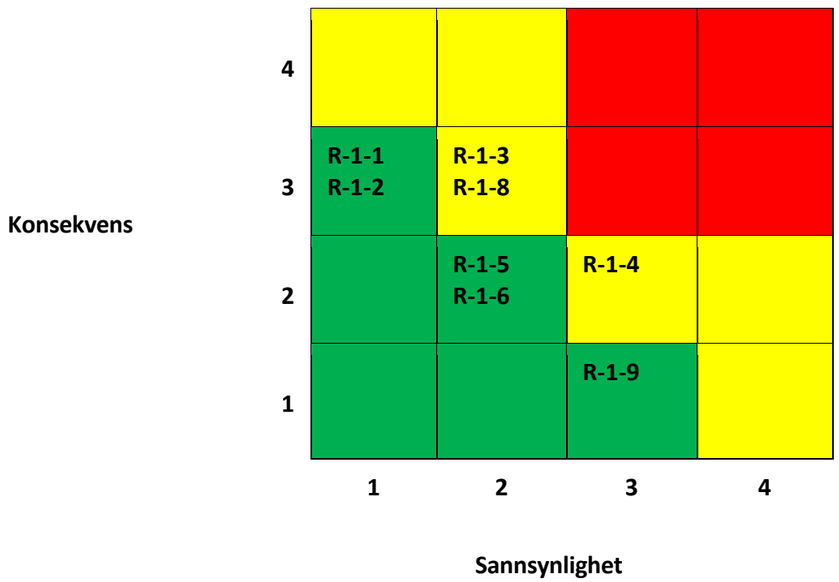
	Tittel	Trussel	Beste praksis		
ID#	Scenario	Scenario	Tiltak	S	K
R-1-1	Misbruk av formålet med Smittestopp.	Smittestopp er en applikasjon som er designet for å bistå FHI og norske myndigheter, som en del av det totale smittesporings arbeidet. Dette for å kunne håndtere den nåværende pandemien, men også fremtidige pandemier. Smittestopp viser seg å fungere svært godt og sporingen av kontakter ansees som svært effektivt. På tross av effektiv smittesporing fortsetter Covid-19 pandemien å herje i Norge, men holdes delvis under kontroll. Covid-19 er nå den "nye normalen" og befolkningen er vant med varierende grad av tiltak. Det er blitt helt naturlig at brorparten av befolkningen til enhver tid har aktivert Smittestopp på telefonene sine. Flere sterke krefter innen diverse norske myndighetsorgan ser mulighetene Smittestopp gir når det kommer til kartlegging av nettverkene til enkeltindivider. Uten befolkningens viten lanseres oppdateringer i Smittestopp som tillater applikasjonen å sende identifikatornøkler til en sentral server som lagrer disse nøklene utover de gitte 14 dagene. Ved å sammenstille disse dataene vil det være mulig å kartlegge nærkontaktene til enkeltindivider.	A) Implementering av dataminimeringsprosesser for å redusere lagring av personopplysninger. B) Sikre innebygget personvern i applikasjonen og gode prosesser for oppdatering og endringer i appen. C) Sikker forvaltning av nøkkel benyttet for å lansere nye versjoner av applikasjonen. D) Etablere ansvar og prosesser for at løsningen settes i dvale umiddelbart etter at myndighetene erklærer Covid-19-krisen som over. E) Monitorere og vurdere oppdateringer av Smittestopp for å detektere mulig misbruk av primærformålet. F) Etablere jevnlig revisjon av DPIA og RoS for å påse korrekt behandling av personopplysninger og akseptabelt risikonivå.	1	3
R-1-2	Formålets omfang øker til å inkludere eksempelvis andre offentlige organers bruk som ikke er i tråd med det originale formålet.	Smittestopps formål er å bidra til kontakt- og smittesporing i Norge og styrke FHIs responsinnsats. Det er en risiko for at formålet til applikasjonen endres eller at omfanget øker, slik at det ikke lenger er i tråd med det originale formålet. Det kan være gjennom at flere offentlige organer ønsker å benytte applikasjonen til ulike formål, eksempelvis håndhevingsformål. Det medfører en risiko for at færre vil benytte Smittestopp, i frykt for at dataen samlet inn via applikasjonen kan brukes mot deres favør i senere anledning. Det vil føre til mistillit mot norske myndigheter og skape uro i befolkningen.	A) Etablere vilkår for Produktstyret som inkluderer formålet med applikasjonen og pålegger komiteen ansvar for å sikre at data prosesseres i tråd med formålet. I tillegg må vilkårene sikre at alle endringer blir nøye vurdert, er lovlige og reflektert i DPIA-en. B) Løpende vurdering av applikasjonen og dataen som prosesseres, spesielt fra et etisk, data- og personvernsperspektiv.	1	3
R-1-3	Mistillit til smittesporings applikasjoner resulterer i at en stor andel av befolkningen ikke tar i bruk appen.	Versjon én av Smittestopp ble stoppet av Datatilsynet, og appen ble av Amnesty International trukket fram som en svært personverninngripende applikasjon. I analysen skriver Amnesty International at appen gikk hardt utover innbyggeres personvernrettigheter, og at den gikk langt ut over hva som var berettiget med tanke på applikasjonens formål. Etter å ha lest medieomtale og diskutert med venner og bekjente, er innbyggerne	A) Trygge befolkning og skape tillit til ny versjon gjennom omfattende og målrettet kommunikasjon. Det er viktig at myndigheter har et samordnet budskap.	2	3

		svært skeptiske til å ta i bruk en ny versjon av Smittestopp. Innbygger har gjort seg opp meninger basert på tidligere informasjon, og er ikke villig til å sette seg inn i endringer i ny applikasjon. Innbyggere er også skeptiske til å dele egen smitteinformasjon og å rapportere sine nærkontakter. Regjeringen kommer med stadig strengere tiltak, og disse tiltakene øker motviljen til innbygger. Dette fører til at Smittestopp 2.0 bringer med seg flere negative assosiasjoner. En stor andel av Norges befolkning velger å ikke laste ned versjon to av Smittestopp, og appen vil derfor ikke ha noen klinisk eller effektiv nytteverdi.	B) Åpenhet om hvilken type informasjon som samles inn, hva informasjonen brukes til og hvor den lagres. Kommunikasjonen må være oppriktig, lett å forstå og korrekt. C) Grundig gjennomgang av GDPR-implikasjoner før utrulling. D) Advare folk mot å tro på alt som spres i sosiale medier om Covid-19, og be folk tenke seg om før de sprer ubekreftet informasjon videre. E) Opprette enhet med formål om å tilbakevise falske påstander. F) Etablere jevnlig revisjon av DPIA og RoS for å påse korrekt behandling av personopplysninger og akseptabelt risikonivå.		
R-1-4	Bruk av appen oppfattes som obligatorisk og mange føler seg presset til å ta appen i bruk.	Norske myndigheter oppfordrer til nedlastning og bruk av appen, men presiserer at det er på frivillig basis. Andre offentlige organer, serveringssteder, butikker o.l., innfører krav og bevis på bruk av appen for å gi adgang/servering eller lignende, på lik linje med at det tidligere har vært krav om registrering før servering på enkelte plasser. Dette fører til at brukeren ikke opplever reell frivillighet, da det kontinuerlig kreves bevis på bruk av appen for å komme gjennom hverdagen, eksempelvis handle på butikken, delta på aktiviteter eller møte på arbeidsplassen. Konsekvensen av dette er misnøye blant brukerne og negative medieoppslag. Videre vil det oppstå en splittelse i befolkningen der noen nekter å bruke Smittestopp-appen, utbredelsen av appen vil reduseres, slik at virkningen av Smittestopp i sporingsarbeidet også reduseres. Da reduseres også nytten ved digital smittesporing og tillit til norske myndigheter vil svekkes.	A) Tydelig kommunikasjonsplan som fokuserer på frivillighetsaspektet ved applikasjonen og at den ikke skal benyttes som adgangskort til aktiviteter/steder.	3	2
R-1-5	Person med bekreftet smitte melder ikke fra fordi MSIS ikke kan bekrefte positivt prøvesvar.	Personer som har symptomer, får beskjed om at de har vært nærkontakt til en smittet eller på andre grunnlag mistenker smitte, tar en Koronatest. Personen tester positivt, men det foreligger en forsinkelse fra positivt prøvesvar til resultatet ligger klart i MSIS, og personen er informert. Når personen da prøver å varsle via Smittestopp-appen, men det ikke samsvarer med resultatet i MSIS, vil det ikke være mulig å varsle. Personen gir til slutt opp fordi prøvesvaret ikke bekreftes og det ikke lar seg gjøre. Det fører til at den digitale smittesporingen fra den smittede personen ikke foretas, og alle nærkontaktene som bør ha fått et varsel ikke får det. Man støtter seg dermed kun på den manuelle smittesporingen og dermed er nytten og virkningen av Smittestopp-appen redusert.	A) Informere gjennom markedsføring om at det kan ta tid før prøvesvar foreligger i MSIS og man kan varsle. Tydeliggjøre at man må forsøke flere ganger etter en viss tid. B) Integrere informasjon om at forsinkelse fra prøvesvar i MSIS kan være årsak til at man ikke får svar, i Smittestopp-appen.	2	2

R-1-6	Lav smittesporing og økt smitte blant innvandrere.	Norske myndigheter har fått kritikk for å ikke nå ut med viktig informasjon om smitte og smittevernstiltak til innvandringsgrupper, noe som har ført til langvarig og økende Covid-19 smitte mange steder. Personer født utenfor Norge er overrepresentert blant de med påvist smitte og sykehusinnleggelser relatert til Covid-19. Mennesker som bor i Norge, men som i liten grad benytter seg av norske media, vil ikke få tilstrekkelig informasjon om Smittestopp. Dette gjelder både personer som bor fast i Norge, og personer som er i Norge for en periode. Disse gruppene vil ikke laste ned Smittestopp fordi de ikke har fått informasjon om hvordan eller hvorfor dette skal gjøres. Dette fører til lav smittesporing og økt smitte blant visse grupper i samfunnet, og vil ha en negativ påvirkning på smittespredningen og smittesporingen i samfunnet generelt.	A) Tilpasset kommunikasjon ved bruk av tolk og oversatt informasjonsmateriell. B) Økt samarbeid med frivillige organisasjoner og ressurspersoner som kan bidra med informasjonsspredning lokalt. C) Smittestopp og informasjon om prosessen må være tilgjengelig på flere språk.	2	2
R-1-7	Kontaktsporing er utilstrekkelig i grenseområder der personer jobber og bor på tvers av landegrenser, da den ikke fungerer på tvers av land.	I områder mot grensen til Sverige, der mange nordmenn bor, jobber og handler på tvers av grensen, kan smittesporingsapplikasjonen være utilstrekkelig. Dersom Smittestopp ikke fungerer på tvers av landegrenser kan man risikere at personer som har testet positivt for Covid-19 og har vært i nærkontakt med andre på grenseområder, ikke får gitt beskjed til nærkontakter på tvers av grensen. Konsekvensen av dette er at Smittestopp ikke er like virkningsfull i grenseområder som igjen kan føre til at færre vil benytte applikasjonen. Om personer i grenseområder frastår fra å benytte Smittestopp, men samtidig reiser rundt i Norge, risikerer man å ta med seg smitte fra nabolandene uten å være klar over det.	A) Samarbeide med kontaktsporingsaktiviteter på tvers av landegrenser, særlig med Sverige og Danmark. B) Benytte det felles datainnsamlingspunktet som tilbys i EU, slik at FHI kan få informasjon om smitte på tvers av landegrenser. Dette kan brukerne selv se gjennom og godta hvilke land som skal ha tilgang på sin data, dersom man har vært i utlandet eller befinner seg i nærheten av grensen.		
R-1-8	DDoS-angrep fører til at hele Smittestopp-løsningen er utilgjengelig.	Nettaktivister ønsker å hemme den digitale smittesporingen i Norge. De gjennomfører et storskala DDoS-angrep (Distributed Denial of Service Attack) for å gjøre Smittestopp utilgjengelig over en lengre tid. Dette kan gjøres ved å angripe backendløsningen, verifiseringsløsningen eller MSIS. Konsekvensen av et angrepet er nedetid for applikasjonen. Dersom dette varer over lengre tid, eller skjer ved flere tilfeller, kan dette føre til mistillit til FHI og den digitale smittesporingen. Det kan medføre nedgang i antall brukere av appen. Videre vil utilgjengelighet av digital smittesporing potensielt føre til at nærkontakter ikke blir varslet, og at nordmenn ferdes i samfunnet, uvitende om at de har vært nærkontakter og potensielt er smittet av Covid-19.	A) Sikkert design. Sørge for at nettverks- og sikkerhetstiltak er på plass for å hindre storskalaangrep. B) Etablere sikker konfigurasjon og herding av samtlige miljøer. C) Sikker drift og vedlikehold. Tydelig ansvarsfordeling og interne øvelser. D) Kontrollert testing og verifikasjon av tåleevnen til eksponerte komponenter i infrastrukturen. E) Gjennomføre trusselmodellering på ulike komponenter som applikasjonen består av.	2	3
R-1-9	Ansatte i FHI kan sjekke hvem som bruker appen til	Oppslag mot MSIS logges i MSIS-databasen, inkludert opplysninger om at appen er benyttet til dette.	A) Redusere antall brukere i FHI med tilgang til MSIS-logger.	3	1

	å melde fra om positivt prøvesvar, og brukere kan derfor føle seg presset til å gjøre dette.	Hvis ansatte i FHI kan følge med på hvem som melder fra når de har fått påvist smitte, kan noen oppleve det som et press, og samtykket til å dele denne informasjon er ikke helt frivillig, basert på en ubalanse i maktforholdet mellom myndigheter og bruker.	B) Hindre at FHI kan spore brukere som ikke har registrert positivt prøvesvar i appen, men som har testet positivt.		

Risikomatrise tilknyttet risikoscenarioer for hele løsningen



R-1-1: Misbruk av Smittestopps primærformål.
R-1-2: Formålets omfang øker til å inkludere eksempelvis, andre offentlige organers bruk som ikke er i tråd med det originale formålet.
R-1-3: Mistillit til smittesporings applikasjoner resulterer i at en stor andel av befolkningen ikke tar i bruk appen.
R-1-4: Bruk av appen oppfattes som obligatorisk og mange føler seg presset til å ta appen i bruk.
R-1-5: Person med bekreftet smitte melder ikke fra fordi MSIS ikke kan bekrefte positivt prøvesvar.
R-1-6: Lav smittesporing og økt smitte blant innvandrere.
R-1-8: DDoS-angrep fører til at hele Smittestopp-løsningen er utilgjengelig.
R-1-9: FHI kan sjekke hvem som bruker appen til å melde fra om positivt prøvesvar.

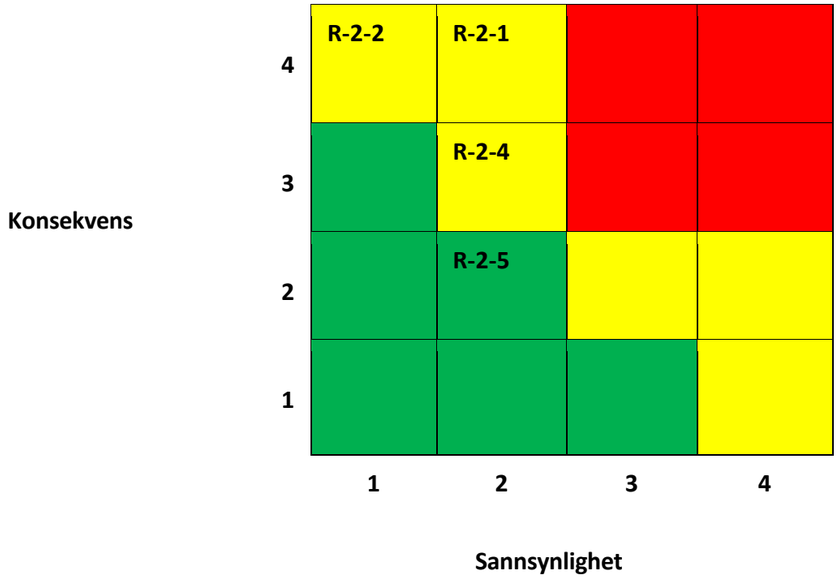
7.1.2 Vurdering av risiko – Backend

	Tittel	Trussel	Beste praksis		
ID#	**Scenario**	**Scenario**	**Tiltak**	**S**	**K**
R-2-1	Trusselaktører korrumperer diagnosenøkler ved å kompromittere backendløsningen til Smittestopp appen.	En trusselaktør kompromitterer backendløsningen til Smittestopp-appen og innfører dårlige data i diagnosenøkkelregisteret for å forringe databasen. Dette vil kunne føre til en undergravelse av resultatene ved at mange mottar meldinger som viser seg å være falske, og brukere vil begynne å mistro informasjonen Smittestopp sender ut. Brukere vil deaktivere applikasjonen eller ikke lengre ta meldingene den sender ut på alvor, og applikasjonen vil ikke lengre ha noen nytteverdi.	A) Autentisering av innbygger før diagnosedata lastes inn i appen. Dermed skal all data som sendes fra appen og til databasen være autentisert. B) Sørge for at nettverks- og sikkerhetstiltak er på plass for å hindre storskalaangrep. C) Begrense antall apper som kan sende data til backend. D) Etablere kontinuerlig monitorering av backend. E) Etablere mulighet for å ta ned hele Smittestopp-løsningen dersom man oppdager at backend er kompromittert.	2	4
R-2-2	Person med tilgang til backendløsningen utnytter sin rolle og korrumperer data i backend.	Person med tilgang til backendløsningen utnytter sin rolle og tilgang til å korrumpere data. Den ansatte gjør dette ved å overstyre tilgangskontrollen og godkjenne økt tilgang til seg selv slik at vedkommende får tilgang til deler av backend han/hun i utgangspunktet ikke hadde. Backendløsningen inneholder diagnosenøkler til personer med påvist Korona. Korrumpering av data kan medføre at nærkontakter ikke blir varslet ved at diagnosenøkler slettes. I tillegg kan trafikkanalyse av opplastede diagnosenøkler benyttes til å avsløre smittede personer fordi deres mobiltelefoner vil generere mye trafikk.	A) Sikre gode prosesser for tilgangsstyring og jevnlig gjennomgang av tilganger. Etablere tekniske, menneskelige og organisatoriske barrierer. B) Prosedyrer for sikker utvikling og gjennomgang og jevnlig revidering av at prosedyrene følges. C) Logge hendelser og innlogginger for å detektere indikatorer på ikke-normal aktivitet. D) Etablere mulighet for å ta ned hele Smittestopp-løsningen dersom man oppdager at backend er kompromittert. E) Sørge for at man ikke direkte kan benytte trafikkanalyse til å identifisere Covid-19-smittede personer.	1	4
R-2-3	Tilsiktet eller utilsiktet overføring av personopplysninger lagret i backend, ut av EU/EØS uten ytterligere tiltak,	Personopplysninger som er samlet inn i backend blir overført til USA. USA er ikke underlagt GDPR eller tilsvarende regelverk, noe som gjør at verken FHI eller innbygger har kontroll over hvordan personopplysninger som overføres ut av EU/EØS blir håndtert. Informasjonen blir lekket og innbygger som har positivt prøvesvar blir hengt ut i sosiale medier, og sterk kritikk rettes mot FHI og	A) Kryptere data, både i transitt og lagring. B) Anonymisering av personopplysninger. C) Etterleve GDPR, og flytte backendløsningen fra sky til on-premise på datasenter i EU.	0	4

	fører til datalekkasje til utenlandske myndigheter.	Smittestopp. Innbygger var ikke kjent med at data ble overført til USA og føler seg lurt. Mange innbyggere velger å deaktivere applikasjonen, og den vil ikke lengre fungere etter tiltenkt hensikt. Tilliten til FHI synker, og det er vanskelig for FHI å oppnå gjennomslag i befolkningen i lang tid framover. FHI har brutt sin forpliktelse til å sikre opplysningene Smittestopp samler inn.	D) Gjennomføre risikovurdering og opprette tiltaksliste mot kompromittering av datasenter i Danmark.		
R-2-4	En ukjent trusselaktør gjennomfører en ondsinnet villet handling mot datasenteret som lagrer backend til Smittestopp.	Rekognoseringen gjennomføres over lengre tid og i flere steg for å unngå oppmerksomhet. Aktøren kjører forbi datasenteret på ulike tider av døgnet og bruker for å kartlegge bemanning og få en god oversikt over området og rutiner. Aktøren tar samtidig bilde av ansatte som har tilgang til datasentrene og gjennom å kjøre reverserte bildesøk på google/eller ved å overvåke den enkelte finner de fram til identiteten deres. Aktøren benytter sosial manipulering til å komme seg på innsiden av datasenteret. Aktøren ønsker først å teste beredskapen og responstiden til politi, nødetater og vektertjeneste og gjennomfører et enkelt innbrudd mot en av inngangene til datasenteret. Aktøren avbryter innbruddet etter at alarmen er satt av og trekker seg tilbake i posisjon til å observere responstid. Etter å ha dokumentert responstid legger aktøren en omfattende plan der det skisseres flere mulige framgangsmåter. Aktøren kan nå fritt ta seg inn eller true ansatte på bakgrunn av informasjon man har om vedkommende til å igangsette flere mulige utfall: • Aktør får tilgang direkte inn i backend til Smittestopp og laster ned personopplysninger og forlater stedet uberørt. Potensielt tap av data med diagnosenøkler. • Aktøren plasserer ondsinnet skadevare i backend til Smittestopp og forlater stedet uberørt. Omdømme, tap av data og driftskonsekvenser er konsekvensen for Smittestopp. • Aktøren saboterer datasenteret ved hjelp av brann, eksplosjon eller liknende. Omdømme, tap av data og driftskonsekvenser for Smittestopp og FHI. Aktøren gjennomfører ingen ondsinnede handlinger, men legger igjen bevis på inntrengning, legger ut hele operasjonen på nett og forårsaker enorm skade i form av at befolkningen mister tillit til FHI sin evne til å håndtere personopplysninger.	A) Gjennomføre risikovurdering av datasenteret som lagrer verifiseringsløsningen. B) Sikre at Smittestopp vil være i kontinuerlig drift, selv om en hendelse inntreffer. C) Etablere prosesser for bruk av trussemodellering og trusseletterretning for å forutse angrep. D) Etablere monitorering av diskusjonsforum.	2	3

R-2-5	Brann bryter ut inne på datasenteret der backendløsningen er lagret.	Det bryter ut brann inne på serverfarmen på datasenteret der backendløsningen er lagret. Alarmsystemet varsler, og nødetatene rykker ut. Brannen har utviklet seg og de ansatte har flyktet ut. Brannen er for kraftig til at det interne brannslukkingssystemet fungerer effektivt og brannen sprer seg utover flere rom. Grunnet den intense brannen blir det høye temperaturer inne på de forskjellige rommene på datasenteret, som fører til at adgangssystemene svikter og brannpersonale kommer hindres i å slukke brannen lokalt. Brannen brer seg gjennom ventilasjonskanaler og kjølekanaler. Nødetatene har ingen annen mulighet enn å la brannen brenne ut og begynne slukning av små branner som oppstår i kjølvannet av den initiale brannen. Serverfarmen til datasenteret som lagrer backendløsningen er totalskadet og umulig å gjenopprette. Smittestoppapplikasjonen er derfor ute av drift og det tar lang tid å gjenopprette. Dette får store konsekvenser for FHIs omdømme, smittesporingen i Norge og redusert tillit til norske myndigheter.	A) Gjennomføre risikovurdering av datasenteret som lagrer verifiseringsløsningen. B) Sikre at Smittestopp vil være i kontinuerlig drift, selv om en hendelse inntreffer.	2	2

Risikomatrise tilknyttet risikoscenarioer for backend



R-2-1 Trusselaktører korrumperer diagnosenøkler ved å kompromittere backendløsningen til Smittestopp appen.
R-2-2 Person med tilgang til backendløsningen utnytter sin rolle og korrumperer data i backend.
R-2-4 En ukjent trusselaktør gjennomfører en ondsinnet villet handling mot datasenteret som lagrer backend til Smittestopp.
R-2-5 Brann bryter ut inne på datasenteret der backendløsningen er lagret.

7.1.3 Vurdering av risiko – Applikasjon

	Tittel	Trussel	Beste praksis		
ID#	**Scenario**	**Scenario**	**Tiltak**	**S**	**K**
R-3-1	Trusselaktør misbruker Smittestopp appen til å påvirke arrangement gjennom å tvinge en gruppe nordmenn i karantene/testing for å påvirke f.eks. et arrangement.	Trusselaktør ønsker å påvirke en kategori av nordmenns bevegelsesmønster for å videre påvirke utfallet av et arrangement. Over tid kartlegger trusselaktøren en gruppe mennesker som skal påvirkes til et ondsinnet formål. Gjennom diverse sosiale medier, åpne forum eller andre tilgjengelige kilder søker trusselaktøren informasjon som vil sette den i stand til å identifisere menneskene som skal påvirkes og metoder for å kompromittere løsningen. Aktøren sørger så for å bli smittet, tester seg og får positivt resultat eller oppsøker testsenter for COVID-19 hvor aktøren benytter utstyr til å plukke opp nøkler fra smittede personer. Aktøren sørger deretter for å påtvinge nærkontakt med de i målgruppen sin og nærkontaktene blir varslet om at de har vært i kontakt med en smittet og må teste/gå i karantene. Aktøren kan dermed påvirke f.eks.: • Planlagte demonstrasjoner • Valg • Viktige møter • Forsamlinger • Konkurrenter innen forskjellige bransjer • Befolkningens tillit til myndighetens tiltak og deres effekt	A) Autentisering av bruker for å laste opp diagnosenøkler. B) Kontinuerlig trusselmonitorering for å identifisere nye trusselaktører og detektere mulige angrep. C) Monitorering etter ikke-normale mønstre i brukeratferd og bevegelser. D) Blokkere enkeltindivider som misbruker Smittestopp-appen. For å muliggjøre dette må man kunne detektere mønstre for å identifisere og stenge ute misbrukende enkeltbrukere. Det kan gjøres gjennom bruk og lagring av logger i en kort periode (14 dager), slik at mønstre kan detekteres. En avveining mellom dataminimering og håndteringsmulighet av misbruk må gjøres i forkant av denne beslutningen.	2	4
R-3-2	Subjektive oppfatninger og/eller manglende forståelse av symptomer fører til feilrapportering.	Myndighetene anbefaler alle som har alvorlige symptomer på Covid-19 å kontakte lege. Dersom man har milde symptomer skal man holde seg hjemme. Feilrapportering av symptomer reduserer kvaliteten på analysene Smittestopp genererer, noe som igjen har innvirkning på tiltak som implementeres og gjennomføres. Subjektive oppfatninger av egne symptomer fører til feilrapportering, som for eksempel underrapportering eller overrapportering. Basert på disse feilrapporteringene blir symptomer som ikke tidligere var forbundet med Covid-19 trukket fram som symptomer som gjør at personer må holde seg hjemme. Dette legger bånd på samfunnet og får store ringvirkninger.	A) Standardisere prosessen for varsling av symptomer slik at det blir enklest mulig for innbyggeren å forstå og vedlikeholde symptomdata. Gjennomføre brukertesting for å sikre at best mulig metode blir benyttet for å oppgi symptomer slik at påliteligheten og styrken til dataen økes. B) Kreve at smittetest må godkjennes i MSIS. C) Tydelig informasjon på nettsider og i applikasjon om symptomdataen som inkluderer: hva som menes med symptomer, hvilke symptomer som bør registreres og til hvilket tidspunkt symptomer skal registreres.	3	1

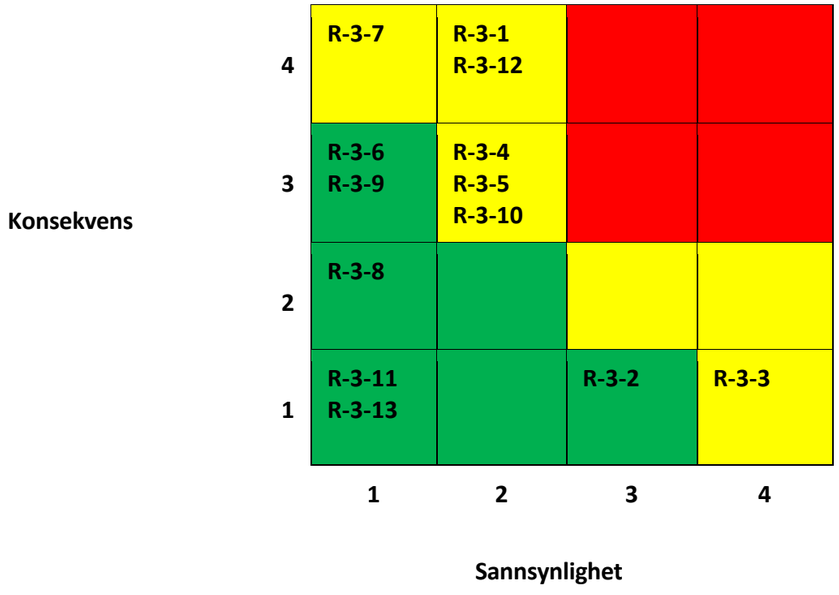
			D) Informere brukere om hvilke konsekvenser feilrapportering kan føre til.		
R-3-3	Apple og Google samler inn og behandler statistikk som kan inneholde personopplysninger for alle apper, inkludert Smittestopp. Dette kan stride mot brukerens rettigheter.	Norske innbyggere laster ned Smittestopp-applikasjonen i Google Play Services eller Apples App Store. Alle apper som lastes ned via Google Play eller App Store gjør at telefonen sender statistikk og data tilbake til Google og Apple. På denne måten kan det samles inn brukerstatistikk eller lokasjonsdata. Bruk av Smittestopp vil derfor føre til at Google og Apple får personopplysninger om store deler av den norske befolkningen. Lokasjonsdataen kan brukes til å beskrive og forutse bevegelsesmønsteret til den norske befolkningen og dermed brukes i målrettede angrep for å ramme flest mulig. Dataen kan også brukes til å drive målrettet markedsføring uten at brukerne er klar over det og ikke får utøvd sine personvernsrettigheter. Dersom dette ikke kommuniseres på riktig måte, er konsekvensen at den norske befolkningen føler seg ført bak lyset og avstår fra å laste ned applikasjonen på tross av anbefalinger fra norske myndigheter.	A) Tydelig informasjon og kommunikasjon om Google og Apples innsamling av data, slik at innbyggere føler seg informert og opplyst. Det må bygges på tilgjengelig informasjon fra Google/Android/Apple. B) Eksplisitt presisere i markedsføring og kommunikasjon at Smittestopp og FHI verken samler inn eller lagrer lokasjonsdata.	4	1
R-3-4	Det er uklart for brukeren hvordan man skal utøve sine personvernrettigheter i Smittestopp.	Etter at personvernforordningen (GDPR) trådde i kraft for et par år siden har personvern og brukers rettigheter blitt stadig viktigere for både tilbydere og brukere. Brukeren oppfatter at Smittestopp ikke tar hensyn til personvern, og det er uklart for brukeren hvordan hen kan utøve sine rettigheter. Dette fører til at brukeren ikke ønsker å ta i bruk Smittestopp, og dens formål og virkning svekkes.	A) Tydeliggjøre samtykkefunksjonen gjennom brukergrensesnittet i applikasjonen, både for å synliggjøre at samtykke kreves for bruk av Smittestopp, og at samtykke når som helst kan trekkes tilbake. B) Det må være tydelig for brukeren hva man gir samtykke til, samt hvordan samtykke kan trekkes tilbake, gjennom samtykkefunksjonen og generell markedsføring og kommunikasjon av Smittestopp. C) Tydelig kommunikasjon og markedsføring rundt hvordan data behandles. D) Lansere ny markedsføringskampanje for å øke bruken av Smittestopp og tilliten til applikasjonen noen uker/måneder etter lansering.	2	3
R-3-5	Misbruk av mulighet for repetert utsendelse av smittevarsel fra flere mobiltelefoner.	Smittestopp blir lansert og har tilsynelatende god effekt. Varslingsmekanismen fungerer effektivt og befolkningen ser umiddelbar effekt av å varsle om positiv smitte ved hjelp av tjenesten. Folk følger smittevernreglene og rådene og befolkningen begynner etter hvert å få overskuddet i hverdagen tilbake. Flere begynner å se muligheten for å manipulere utsendelsen av smittevarsel gjennom Smittestopp for å fremme egen agenda. Ved å benytte innlogging på flere ulike telefoner eller andre enheter sender en aktør varsel på enheter som har vært på ulike geo-lokasjoner, men ikke nødvendigvis der den personen som har fått	A) Begrense antall tillate enheter en innbygger har lov til å være innlogget på. B) Utestenge enkeltindivider som misbruker Smittestopp-appen. For å muliggjøre dette må man kunne detektere mønstre for å identifisere og stenge ute misbrukende enkeltbrukere. Det kan gjøres gjennom bruk og lagring av logger i en kort periode (14 dager), slik at mønstre kan detekteres. En avveining mellom dataminimering og håndteringsmulighet av misbruk må gjøres i forkant av denne beslutningen.	2	3

		bekreftet smitte har vært. Dette fører til en mengde falske positive varsler til grupper eller deler av befolkningen som en aktør ønsker å påvirke. Dette kan eksempelvis påvirke: • Demonstrasjoner eller andre folkesamlinger • Nedstengning av skoler, arbeidsplasser osv. • Påvirkning av industri, konkurranser osv. • Påtvingning av karantene hos ulike befolkningsgrupper i den hensikt å skape polarisering	C) Monitorering av diskusjonsforumer/trusseletterretning.		
R-3-6	Dataoverføring gjøres gjennom usikrede metoder, som åpner tilgang til data idet den sendes mellom brukeren og FHI, eksempelvis symptomer.	Dataoverføringen fra Smittestopp til FHI gjøres gjennom utilstrekkelig sikrede metoder som gjør at trusselaktører får tak i informasjonen. Hver gang applikasjonen brukes sendes data fra applikasjonen til FHI. Dataen omfatter eksempelvis symptomer som er personlig informasjon, og som dermed risikeres å kompromitteres. Konsekvensen av dette er data på avveie eller upålitelig data fra Smittestopp dersom trusselaktøren gjør endringer i symptomdata på vei til FHI.	A) Kryptere all data i ro og i transitt mellom innbyggerne og FHI. B) Sørge for hashing av data slik at det ikke er mulig for trusselaktører å koble hvilke enkeltindivider som har blitt smittet og hvilke symptomer de har hatt. C) Etablere en responsplan med mitigerende tiltak for hendelser som blant annet datalekkasje, for å hindre økning i negative ringvirkninger etter denne type hendelser.	1	3
R-3-7	Trusselaktører korrumperer diagnosenøkler ved å kompromittere Smittestopp-appen.	En trusselaktør korrumperer Smittestopp-appen og innfører dårlige data i diagnosenøkkelregisteret for å forringe og kompromittere databasen. Dette fører til en undergravelse av resultatene ved at mange brukere mottar meldinger som viser seg å være falske. Brukerne begynner derfor å mistro informasjonen Smittestopp sender ut, og ender opp med å deaktivere applikasjonen eller ikke lengre ta meldingene den genererer på alvor. Statistikken applikasjonen genererer er falske, og Smittestopp har ikke lengre har samme nytteverdi.	A) Integritetssjekk av enheter gjøres av applikasjonen i løpet av «onboarding» av enheten. Det må sørges for at all trafikk til backend i Smittestopp er beskyttet via dette. B) Autentisering av innbygger før diagnosedata lastes inn i appen og sendes til backend. C) Sørge for at nettverks- og sikkerhetstiltak er på plass for å hindre storskalaangrep. D) Begrense antall apper som kan sende data til backend.	1	4
R-3-8	Innbyggers IP-adresser lagres i backend.	Applikasjoner utvikles ofte til å kunne lagre informasjon om enhetene som benytter applikasjonene, som for eksempel IP adresser. Dette gjør at brukere vil kunne gjenidentifiseres, og tilbyder av applikasjonen vil sitte på mye informasjon om mange brukere som samlet sett kan misbrukes direkte eller selges til ukjente trusselaktører. Dersom IP-adresser til brukerne lagres i backend er dette en risiko.	A) Sørge for at IP-adresser ikke lagres i applikasjonen.	1	2
R-3-9	Statistikk om bruk av Smittestopp samles inn og er ikke anonymisert.	For å kartlegge bruken av Smittestopp samler applikasjonen inn data for analyse. Denne dataen omfatter blant annet hvordan brukerne interagerer med applikasjonen, deres daglige bruk, raten av slettinger, kontaktsporing, eksponeringshendelser og lignende. Denne dataen er ikke anonymisert og det er en risiko for at brukerne	A) Implementere dataminimeringsprosesser og sørge for at denne type data ikke samles inn.	1	3

		ikke er klar over dette og forventer at dataen er anonymisert. Dersom Smittestopp og helsenorge.no kobles sammen kan man identifisere enkeltpersoners kontaktnett og bruke dette til andre formål enn Smittestopps primærformål.	B) Hashing og salting av data for å sikre at det ikke er mulig å koble innlogging hos helsenorge.no med en opplasting til Smittestopp ved hjelp av opplastet token. Dette kan gjøres ved bruk av Privacy Pass.		
R-3-10	Tekniske problemer ved Smittestopp reduserer dens funksjon og/eller reduserer mobilens andre funksjoner.	Tekniske problemer fører til at brukeren ønsker å skru av eller deaktivere Smittestopp. Dette skjer fordi brukeren tenker at applikasjonen bruker for mye batteri, at andre funksjoner på mobilen blir negativt påvirket, eller fordi brukeren mener at periferiutstyr som kobles til via Bluetooth får redusert kapasitet. Dette fører igjen til at Smittestopp blir mindre effektiv til sitt formål.	A) Teste hvordan applikasjonen påvirker mobilens andre funksjoner som eksempelvis batteritid og bruk/tilgjengelighet av andre applikasjoner. B) Teste hvordan applikasjonen påvirker periferiutstyr som kobles til mobiltelefonen via Bluetooth, eksempelvis headset eller høyttalere. C) Tydeliggjøre eventuelle påvirkninger Smittestopp-appen kan ha for andre applikasjoner på enheten, slik at brukeren ikke har en feiloppfatning av dette som fører til misnøye og avinstallasjon. D) Bruke Apple og Google ENS til å dra nytte av deres evne til å optimalisere funksjonalitet av ENS utover hva andre app-utviklere er i stand til.	2	3
R-3-11	Nedlastning av diagnosenøkler tømmer brukerens mobildatakvote.	Mengden mobildata personer har tilgjengelig avhenger av brukerens mobilabonnement. Dersom man bruker opp mobildataen som er inkludert i abonnementet må man vanligvis enten kjøpe en ny mobildatapakke eller betale per MB man bruker utover kvoten. Brukeren opplever at Smittestopp bruker mye mobildata og velger derfor å skru av Bluetooth eller deaktivere appen. Dette fører til at Smittestopp blir mindre effektiv til sitt formål i kontaktsporingen ved at nærkontakter ikke registreres.	A) Benytt et design som begrenser applikasjonens bruk av mobildata. B) Inkludere et estimat som tydeliggjør for brukeren hvor mye(lite) mobildata applikasjonen bruker i snitt (for eksempel i løpet av en uke). Dette må tydelig kommuniseres i appen og i generell markedsføring og informasjon i forbindelse med utrulling av appen. C) Sikre at trafikk til og fra enheten ikke bruker mer mobildata enn absolutt nødvendig. D) Informere brukeren om at dersom applikasjonen bruker mer mobildata i en periode så vil det gjerne skyldes en økning i antall smittede, og at det derfor er ekstra viktig at applikasjonen fungerer.	1	1
R-3-12	Falsk versjon av Smittestopp applikasjon.	Trusselaktør lager falsk versjon av Smittestopp applikasjon og innbygger laster ned denne ved en feil. Applikasjonen ekstraherer informasjon om innbygger som igjen brukes til å presse vedkommende for penger, eller er designet slik at innbygger må betale før applikasjonen kan tas i bruk. Disse forfalskede applikasjonene fører til mistillit til Smittestopp og FHI, samt at en stor andel av befolkningen avinstallerer applikasjonen.	A) Må sikre at falske apper ikke blir tilgjengelige i app-store. B) Utbredt og kontinuerlig markedsføring som gjør det tydelig for brukeren nøyaktig hvilken smittestoppapplikasjon som er utviklet av myndighetene og hvilken funksjonalitet denne har. C) Kontinuerlig trusseletterretning for å identifisere planlegging eller lansering av falske versjoner av Smittestopp.	2	4

R-3-13	Smittestopp brukes til å vise en persons Covid-19 status.	Bruker blir smittet av Covid-19 og laster opp denne informasjonen i Smittestopp via en diagnosenøkkel. Det registreres at vedkommende er smittet. På denne måten vil man kunne se om en person er registrert smittet eller ikke. Aktør får tilgang til denne informasjonen og bruker dette til å ta avgjørelser, eller gjøre seg opp meninger om den registrerte. Brukerens Covid-19 status kan da tas i bruk av andre, for eksempel til å ta avgjørelser om den registrerte.	A) Applikasjonen designes en måte slik at man ikke kan se Covid-19 statusen til personer. B) Applikasjonen skal kun prosessere data i tråd med formålet og DPIA-en. C) Randomisering av tokens for å hindre mulighet til å koble identitet til smittenøkler og dermed avgjøre Covid-19 statusen til personer.	1	1
R-3-14	Appen er ikke laget for å motstå Reverse Engineering.	Det er ikke tatt høyde for Reverse Engineering i appen slik at forfalskede apper kan kompromittere innbyggernes mobile enheter. Brukerne opplever dermed at enhetene sine kompromitteres, noe som fører til mistillit til appen og FHI, samt at en stor andel av befolkningen avinstallerer appen.	A) Vurdere sårbarheter i henhold til anbefalinger under Resilience against Reverse Engineering – Android fra standarden OWASP Mobile Application Security. B) Endre kildekoden fra å være lukket til åpen. C) Implementere tiltak som forhindrer falske apper i å bli tilgjengelig.	0	3

Risikomatrise tilknyttet risikoscenarioer for applikasjon

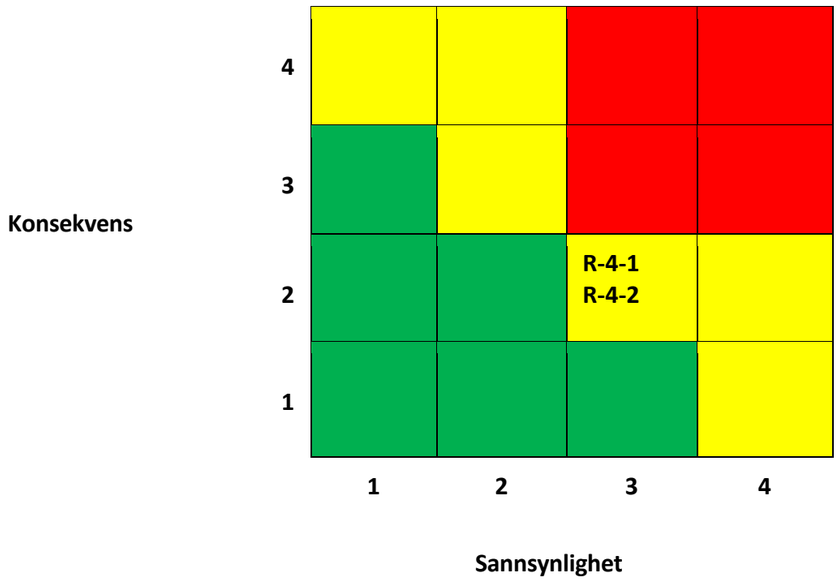


R-3-1: Trusselaktør misbruker Smittestopp appen til å påvirke arrangement gjennom å tvinge en gruppe nordmenn i karantene/testing for å påvirke f.eks. et arrangement.
R-3-2: Subjektive oppfatninger og/eller manglende forståelse av symptomer fører til feilrapportering.
R-3-3: Apple og Google samler inn og behandler statistikk som kan inneholde personopplysninger for alle apper, inkludert Smittestopp. Dette kan stride mot brukerens rettigheter.
R-3-4: Det er uklart for brukeren hvordan man skal utøve sine personvernrettigheter i Smittestopp.
R-3-5: Misbruk av mulighet for repetert utsendelse av smittevarsel fra flere mobiltelefoner.
R-3-6: Dataoverføring gjøres gjennom usikrede metoder, som åpner tilgang til data idet den sendes mellom brukeren og FHI, eksempelvis symptomer.
R-3-7: Trusselaktører korrumperer diagnosenøkler ved å kompromittere Smittestopp-appen.
R-3-8: Innbyggers IP-adresser lagres i backend.
R-3-9: Statistikk om bruk av Smittestopp samles inn og er ikke anonymisert.
R-3-10: Tekniske problemer ved Smittestopp reduserer dens funksjon og/eller reduserer mobilens andre funksjoner.
R-3-11: Nedlastning av diagnosenøkler tømmer brukerens mobildatakvote.
R-3-12: Falsk versjon av Smittestopp applikasjon.
R-3-13: Smittestopp brukes til å vise en persons Covid-19 status.

7.1.4 Vurdering av risiko – Mobiltelefon

	Tittel	Trussel	Beste praksis		
ID#	**Scenario**	**Scenario**	**Tiltak**	**S**	**K**
R-4-1	Bluetooth ikke laget for avstandsberegning, dette gjør at nærkontakt registreres feilaktig og fører til falske positive. Eksempelvis i tilfeller der det i realiteten var vegg/glass mellom enhetene.	Smittestopp baserer sin kontaktsporing på å registrere møter med andre mobiltelefoner over Bluetooth. Det krever at Bluetooth til enhver tid er slått på, ellers vil ikke kontaktsporingen fungere. Bluetooth kapabiliteten til mobiltelefoner varierer i kraft/styrke og i mottagelighet fra andre enheter. Dette vil påvirke Bluetooth-målerens avstands- og styrkeregistrering, som igjen kan påvirke om møtet mellom enhetene registreres som kontakt, nærkontakt eller ikke i det hele tatt. Konfigurasjonen er satt opp på en måte som gjør at den registrerer for mange møter som nærkontakt. Dette fører til økning i feilaktige positive tilfeller. Dette inntreffer fordi applikasjonen registrerer nærkontakt på tross av at brukere har vært på hver side av en vegg eller pleksiglass som i mange tilfeller er satt opp i restauranter og butikker.	A) Grundig testing av ulike scenarioer i forkant av lansering på forskjellige enheter med varierende Bluetooth-intensitet. Informasjon og kunnskap fra Apple og Google ENS kan brukes til å gjennomføre omfattende testing. B) Utarbeid en kommunikasjonsplan for å sikre at de som er spesielt utsatt for dette får beskjed om å skru av Bluetooth i visse situasjoner (for eksempel trikkeførere og bussjåfører på arbeid). Inkluder informasjon om at løsningen ikke er 100% sikker. C) Sikre at Smittestopp brukes til å forsterke den allerede eksisterende kontaktsporingsoperasjonen.	3	2
R-4-2	Bluetooth er ikke laget for avstandsberegning, noe som gjør at nærkontakt registreres feilaktig (mangel på registrering) og fører til falske negative.	Smittestopp baserer sin kontaktsporing på å registrere møter med andre mobiltelefoner over Bluetooth. Det krever at Bluetooth til enhver tid er slått på, ellers vil ikke kontaktsporingen fungere. Bluetooth kapabiliteten til mobiltelefoner varierer i kraft/styrke og i mottagelighet fra andre enheter. Dette vil påvirke Bluetooth-målerens avstands og styrke-registrering, noe som igjen kan påvirke om møtet mellom enhetene registreres som kontakt, nærkontakt eller ikke i det hele tatt. Konfigurasjonen av Bluetooth-måleren er satt opp på en måte som gjør at den registrerer for få møter som nærkontakt, og dette fører til falske negative. Dette gir igjen en økt risiko for at personer som har vært i nærkontakt med personer som har testet positivt for Covid-19 ikke får beskjed om dette, og er uvitende om sin mulige smitte. For få settes derfor i karantene fordi nærkontakten ikke er registrert, og smitten i samfunnet fortsetter å øke. Brukere opplever at personer de har vært i nærkontakt med får påvist smitte uten at de selv har fått beskjed via Smittestopp. Tilliten til applikasjonen reduseres og brukere velger å deaktiverer den.	A) Grundig testing i forkant av lansering på ulike enheter med ulik Bluetooth-intensitet. Informasjon og kunnskap fra Apple og Google ENS kan brukes til å gjennomføre omfattende testing. B) Utarbeid en kommunikasjonsplan for å sikre at de som er spesielt utsatt for dette får beskjed om å skru av Bluetooth i visse situasjoner (for eksempel trikkeførere og bussjåfører på arbeid). C) Introdusere anonyme beregninger for å måle raten av antall applikasjonsbaserte nærkontakter mot antall applikasjonsbaserte positive diagnoser for å overvåke overrapportering av nærkontakter. D) Sikre at Smittestopp brukes til å forsterke den allerede eksisterende kontaktsporingsoperasjonen.	3	2

Risikomatrise tilknyttet risikoscenarioer for mobiltelefon



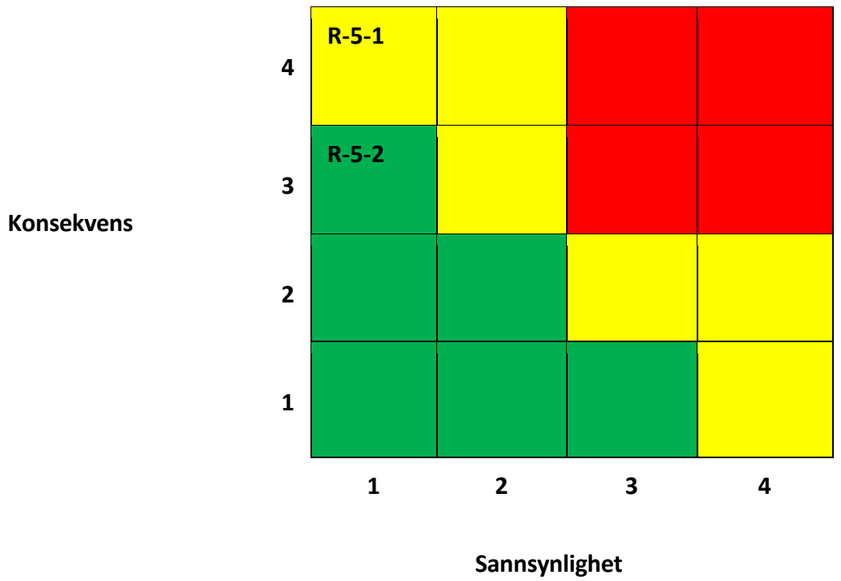
R-4-1: Bluetooth ikke laget for avstandsberegning, dette gjør at nærkontakt registreres feilaktig og fører til falske positive. Eksempelvis i tilfeller der det i realiteten var vegg/glass mellom enhetene.
R-4-2: Bluetooth e**r** ikke laget for avstandsberegning, noe som gjør at nærkontakt registreres feilaktig (mangel på registrering) og fører til falske negative.

7.1.5 Vurdering av risiko – MSIS

	Tittel	Trussel	Beste praksis		
ID#	Scenario	Scenario	Tiltak	S	K
R-5-1	Angrep mot MSIS for å korrumpere smittedata.	En avansert statlig aktør ønsker å påvirke Norges økonomi. Gjennom langsiktige påvirkningsoperasjoner på flere nivå ønsker en statlig aktør å hindre økonomisk vekst i Norge for å svekke Norges posisjon i verdenssamfunnet og samtidig skape interne uroligheter. En av disse påvirkningsoperasjonen har som mål å angripe MSIS for å korrumpere data slik at smittetallet i Norge blir kritisk høyt og tvinger fram full lockdown. Norske myndigheter har siden første lockdown ikke vist motivasjon til å føre landet inn i en ny lockdown periode. Dette grunnet de store sosioøkonomiske utfordringene det skapte. Norge håndterer de utbruddene som oppstår på en god måte og smittetrykket er stabilt lavt. Aktøren får tak i den private nøkkelen til grensesnittet og igangsetter målrettede angrep mot det eksponerte MSIS API grensesnittet ved å benytte metoder for	A) Sikker håndtering av nøkler til grensesnittet gjennom beste praksis på området, eksempelvis ISFs Crypto Key Management. B) Herding av integrasjonsgrensesnitt (MSIS API). C) Gjennomføre penetrasjonstester av eksponerte grensesnitt for å kartlegge sårbarheter og mulige angrepsmønstre fra trusselaktører.	1	4

		kodeinjisering. Dette resulterer i at aktøren klarer å hente ut data fra grensesnittet gjennom returmeldingen til grensesnittet. Etter at aktøren har tilegnet seg tilgang sørger den for at smittetrykket gradvis øker slik at det ikke fattes mistanke til utviklingen. Tiden går og norske myndigheter foreslår stadig kraftigere og mer inngripende tiltak, men nekter å sette landet i lockdown. Ved å øke smittetrykket eksponentielt etter lang tid med moderat oppgang, tvinges myndighetene til å gjeninnføre lockdown i en tidsbegrenset periode. Aktøren sørger for at smittetallet synker, men at det til enhver tid holder seg rett over og under nivået norske myndigheter setter som grense for å oppheve lockdown. Dette fører til at Norge over en lang periode stenger ned landet og de sosioøkonomiske konsekvensene er fatale for norsk økonomi. Norge opplever en kraftig resesjon over lengre tid.			
R-5-2	Angrep på MSIS gjør at persondata til personer med kode 6/7 blir tilgjengeliggjort.	Kode 6/7 personer har behov for særlig skjerming av persondata og geolokaliserende informasjon. Ved et angrep mot MSIS eller andre deler av informasjonskjeden kan informasjon komme på avveie som senere kan benyttes til ondsinnede handlinger.	A) Vurdere om Smittestopp skal anbefales for personer med kode 6/7.	1	3

Risikomatrise tilknyttet risikoscenarioer for MSIS

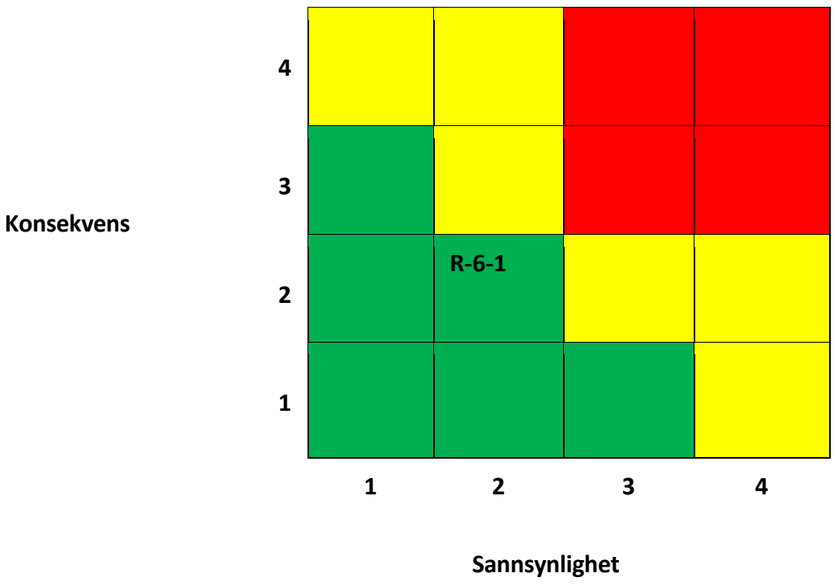


R-5-1: Angrep mot MSIS for å korrumpere smittedata.
R-5-2: Angrep på MSIS gjør at persondata til personer med kode 6/7 blir tilgjengeliggjort.

7.1.6 Vurdering av risiko – ID-porten

	Tittel	Trussel	Beste praksis		
ID#	**Scenario**	**Scenario**	**Tiltak**	**S**	**K**
R-6-1	Leverandør av SMS-tjenester identifiserer enkeltperson og bruker meldingene personen mottar til å tolke seg fram til at vedkommende er smittet av Covid-19.	Leverandøren av SMS-tjenesten som benyttes til å sende flash meldinger i Smittestopp greier å identifisere enkeltpersoner. Ved å sammenstille dette med informasjon om hvilke meldinger personen har mottatt greier leverandøren å tolke seg fram til at brukeren har testet positivt for Covid-19.	A) Tokens blir autorisert for å hindre at API-et blir spammet ned av informasjon og settes ut av spill. B) Unngå at SMS-melding inneholder informasjon som gjør at SMS-leverandøren kan identifisere at brukeren laster opp nøkler knyttet til Smittestopp/FHI. C) Randomisering av tokens for å hindre mulighet til å koble identitet til smittenøkler.	2	2

Risikomatrise tilknyttet risikoscenarioer for ID-porten



R-6-1: Leverandør av SMS-tjenester identifiserer enkeltperson og bruker meldingene personen mottar til å tolke seg fram til at vedkommende er smittet av Covid-19.

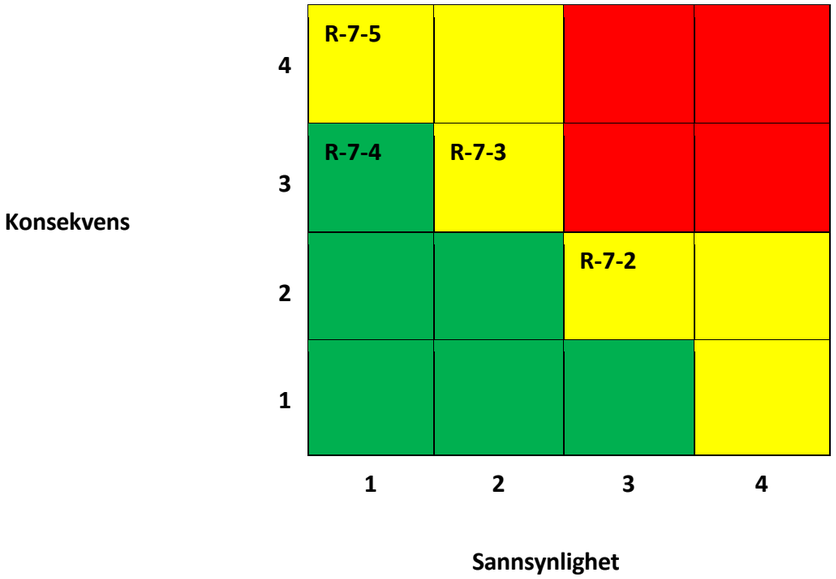
7.1.7 Vurdering av risiko – Verifiseringsløsningen

	Tittel	Trussel	Beste praksis		
ID#	**Scenario**	**Scenario**	**Tiltak**	**S**	**K**
R-7-1	Tilsiktet/ utilsiktet overføring av personopplysninger ut av EU/EØS, uten ytterligere tiltak fører til datalekkasje til utenlandske myndigheter.	Personopplysninger som er samlet inn i verifiseringsløsningen blir overført til USA. USA er ikke underlagt GDPR eller tilsvarende regelverk, noe som gjør at verken FHI eller innbygger har kontroll over hvordan personopplysninger som overføres ut av EU/EØS blir håndtert. ID-porten og servere blir kompromittert, og lister over personer med positivt prøvesvar blir lekket. Informasjonen blir lekket og innbygger som har positivt prøvesvar blir hengt ut i sosiale medier, og sterk kritikk rettes mot FHI og Smittestopp. Innbygger var ikke kjent med at data ble overført til USA og føler seg lurt. Mange innbyggere velger å deaktivere applikasjonen, og den vil ikke lengre fungere etter tiltenkt hensikt. Tilliten til FHI synker, og det er vanskelig for FHI å oppnå gjennomslag i befolkningen i lang tid framover. FHI har brutt sin forpliktelse til å sikre opplysningene Smittestopp samler inn.	A) Kryptere data, både i transitt og lagring. B) Anonymisering og pseudomynisering av personopplysninger. C) Lagre verifiseringsløsningen på europeisk jord for å holde data i EU og være underlagt GDPR. D) Gjennomføre risikovurdering av datasenteret som lagrer verifiseringsløsningen.	0	4
R-7-2	Brann bryter ut inne på datasenteret der verifiseringsløsningen er lagret.	Det bryter ut brann inne på serverfarmen i datasenteret. Alarmsystemet varsler og nødetatene rykker ut. Selv om responstiden er rask, tar det 15 minutter (7 min unna) før de er på stedet. Brannen har utviklet seg og de ansatte inne på datasenteret har flyktet ut. Brannen er for kraftig til at det interne brannslukkingssystemet fungerer effektivt og brannen sprer seg utover flere rom inne på datasenteret. Grunnet den intense brannen blir det enorme temperaturer inne på de forskjellige rommene på datasenteret fører til at adgangssystemene svikter og brannpersonale kommer seg ikke inn for å slukke brannen lokalt. Brannen brer seg gjennom ventilasjonskanaler og kjølekanaler og til slutt eksploderer diesel-tanken på utsiden av datasenteret. Nødetatene har ingen annen mulighet enn å la brannen brenne ut og begynne slukning av små branner som oppstår i kjølvannet av den initiale brannen. Serverfarmen til NHN er totalskadet og umulig å gjenopprette. Smittestoppapplikasjonen er derfor ute av drift og det tar lang tid å gjenopprette. Dette for store konsekvenser for FHIs omdømme, smittesporingen i Norge og redusert tillit til norske myndigheter.	A) Gjennomføre risikovurdering av datasenteret som lagrer verifiseringsløsningen. B) Utarbeidelse- og kontinuerlig gjennomføring av scenariotrening og forbedring av respons- og beredskapsplaner for å sikre effektiv håndtering av hendelser som brann på datasenteret. C) Sikre at Smittestopp vil være i kontinuerlig drift, selv om en hendelse inntreffer.	3	2

R-7-3	En ukjent trusselaktør gjennomfører en ondsinnet villet handling mot datasenteret i Norge som lagrer verifiseringsløsningen.	Rekognoseringen gjennomføres over lengre tid og i flere steg for å unngå oppmerksomhet. Aktøren kjører forbi datasenteret på ulike tider av døgnet og bruker for å kartlegge bemanning og få en god oversikt over området og rutiner. Aktøren tar samtidig bilde av ansatte som har tilgang til datasentrene og gjennom å kjøre reverserte bildesøk på google/eller ved å overvåke den enkelte finner de fram til identiteten deres. Aktøren benytter sosial manipulering til å komme seg på innsiden av datasenteret. Aktøren ønsker først å teste beredskapen og responstiden til politi, nødetater og vektertjeneste og gjennomfører et enkelt innbrudd mot en av inngangene til datasenteret. Aktøren avbryter innbruddet etter at alarmen er satt av og trekker seg tilbake i posisjon til å observere responstid. Etter å ha dokumentert responstid legger aktøren en omfattende plan der det skisseres flere mulige framgangsmåter. Aktøren kan nå fritt ta seg inn eller true ansatte på bakgrunn av informasjon man har om vedkommende til å igangsette flere mulige utfall: • Aktør får tilgang direkte inn i verifiseringsløsningen til Smittestopp og laster ned en større mengde persondata og forlater stedet uberørt. Potensielt tap av enorme mengder data med diagnosenøkler eller annen persondata. • Aktøren plasserer ondsinnet skadevare i verifiseringsløsningen til Smittestopp og forlater stedet uberørt. Omdømme, tap av data og driftskonsekvenser er konsekvensen for Smittestopp. • Aktøren saboterer serverfarmen ved hjelp av brann, eksplosjon eller liknende. Omdømme, tap av data og driftskonsekvenser for Smittestopp og FHI. Aktøren gjennomfører ingen ondsinnede handlinger, men legger igjen bevis på inntrengning, legger ut hele operasjonen på nett og forårsaker enorm skade i form av at befolkningen mister tillit til FHI sin evne til å håndtere personopplysninger.	A) Gjennomføre risikovurdering av datasenteret som lagrer verifiseringsløsningen. B) Utarbeidelse- og kontinuerlig gjennomføring av scenariotrening og forbedring av respons- og beredskapsplaner for å sikre effektiv håndtering av hendelser som brann på datasenteret. C) Etablere prosesser for bruk av trussemodellering og trusseletterretning for å forutse angrep. D) Etablere monitorering av diskusjonsforum.	2	3
R-7-4	Trusselaktør kan identifisere person som varsler om smitte gjennom bruk av pseudonym i verifiseringsløsningen.	Trusselaktøren har tilgang til pseudonym generert av ID-porten og kan ved hjelp av dette identifisere personen som har varslet om positivt prøvesvar gjennom Smittestopp-appen.	A) Sikre at fødselsnummeret er pseudonymisert i verifiseringsløsningen for å sikre dataminimering. B) Nøkkelseparasjon for å hindre trusselaktør i å få tilgang til positivt prøvesvar og ID-porten.	1	3

R-7-5	Person med tilgang til verifiseringsløsningen utnytter sin rolle og korrumperer data i verifiseringsløsningen.	Person med tilgang til verifiseringsløsningen utnytter sin rolle og tilgang til å korrumpere data. Den ansatte gjør dette ved å overstyre tilgangskontrollen og godkjenne økt tilgang til seg selv slik at vedkommende får tilgang til deler av verifiseringsløsningen han/hun i utgangspunktet ikke hadde. Verifiseringsløsningen inneholder persondata som fødselsnummer og personen med tilgang kan dermed stjele ID-er og bruke det til å handle, oppta lån eller autentisere seg. Dette vil skape mistro til Smittestopps og FHIs evne til å håndtere persondata. Det vil få konsekvenser for FHIs omdømme og at folk avinstallerer appen. Det medfører at effekten og virkningen av den digitale smittesporingen reduseres.	A) Sikre gode prosesser for tilgangsstyring og jevnlig gjennomgang av tilganger. B) Prosedyrer for sikker utvikling og gjennomgang og jevnlig revidering av at prosedyrene følges. C) Logge hendelser og innlogginger for å detektere indikatorer på ikke-normal aktivitet. D) Etablere mulighet for å ta ned hele Smittestopp-løsningen dersom man oppdager at verifiseringsløsningen er kompromittert.	1	4

Risikomatrise tilknyttet risikoscenarioer for verifiseringsløsningen



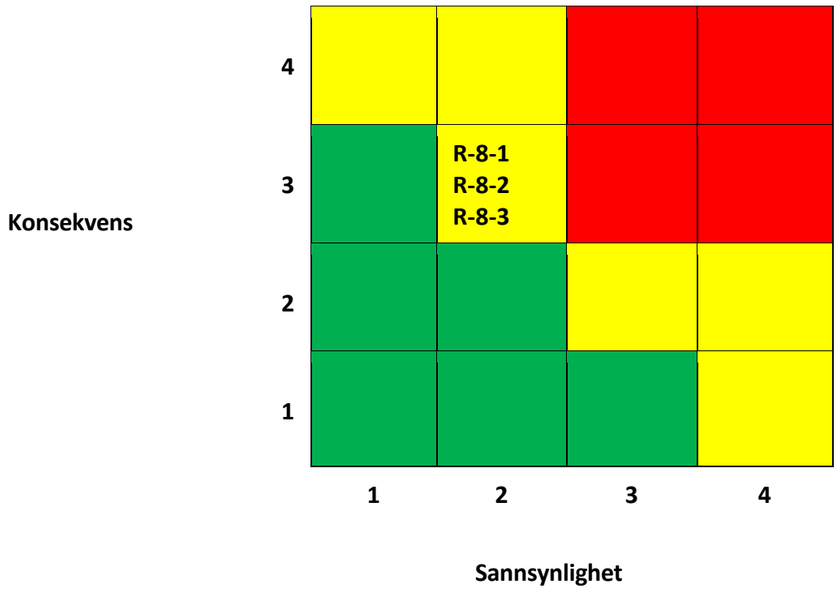
R-7-2: Brann bryter ut inne på datasenteret der verifiseringsløsningen er lagret.
R-7-3: En ukjent trusselaktør gjennomfører en ondsinnet villet handling mot datasenteret i Norge som lagrer verifiseringsløsningen.
R-7-4: Trusselaktør kan identifisere person som varsler om smitte gjennom bruk av pseudonym i verifiseringsløsningen.
R-7-5: Person med tilgang til verifiseringsløsningen utnytter sin rolle og korrumperer data i verifiseringsløsningen.

7.1.8 Vurdering av risiko – Utviklingsteam

	Tittel	Trussel	Beste praksis		
ID#	**Scenario**	**Scenario**	**Tiltak**	**S**	**K**
R-8-1	Lav kodekvalitet på grunn av mangelfull kontinuerlig forbedring av sikker utviklingsmetodikk, styring og kompetanse.	Mangelfull kontinuerlig forbedring av sikker utviklingsmetodikk, styring og kompetanse fører til lav kodekvalitet. Dette fører til at kvaliteten på Smittestopp blir dårligere. Brukere blir misfornøyde og Smittestopp blir mindre virkningsfull i forhold til sitt formål. Lav kodekvalitet gjør det også vanskeligere tilføre nye oppdateringer i Smittestopp.	A) Fokus på kontinuerlig utvikling og implementering av kodemetodikk for å styrke applikasjonen. B) Dra nytte av samarbeid med andre lands oppdateringer i tilsvarende applikasjoner, eksempelvis Danmark. C) Dra nytte av Google og Apples kompetanse og informasjon på området. D) Ivareta personvern og sikker utvikling.	2	3
R-8-2	Mangelfull forståelse av sikker koding fører til ustabile applikasjoner og datalekkasje.	Mangelfull institusjonell forståelse av sikker koding benyttet til overgripende sikkerhetsaktiviteter integrert inn i utviklingsprosessene. Eksempler på dette er angrepsmodeller, sikker design og standardiseringsarbeid. Dette fører til ustabile applikasjoner eller datalekkasje, som gjør at FHI opplever en mediestorm uten sidestykke. Resultatet er at FHI blir tvunget til å gjennomføre en ekstern revisjon/evaluering av hele utviklingsløpet. Evalueringen konkluderer med at det ikke er gjennomført en vurdering av utviklerselskapet og deres metodikk for sikker utvikling, samt at flere feil er begått i utviklingsløpet. Dette blir både kostbart og tidkrevende, samtidig som det svekker omdømme og tilliten den norske befolkning har til både FHI og Smittestopp. Mediene går ut med en anbefaling til befolkningen om å slette applikasjonen og FHI/norske myndigheter har nå spolert alle muligheter for å benytte digitale verktøy i forbindelse med smittesporing og pandemihåndtering.	A) Gjennomføre trening og øvelser på viktige sikkerhetsområder som omfatter sikker koding. B) Bruke sikkerhetseksperter til å sørge for at sikkerhetsaktiviteter blir integrert i utviklingsprosessen. C) Kontinuerlig vurdere sikkerhetsarbeidet og diskutere mulige angrepsmodeller underveis i utviklingsarbeidet. D) Kontinuerlig monitorere og vurdere utviklingsprosessen for å detektere mangler knyttet til sikker koding.	2	3
R-8-3	Sårbarheter i kildekode på grunn av manglende analysemetoder for avdekking.	Risiko for mangel på analysemetoder for å avdekke sårbarheter i kildekode; herunder arkitekturanalyse, koderevisjon og sikkerhetstesting. Dette fører til at sårbarheter eksisterer uten at utviklingsteamet og FHI er klar over det, og kan utnyttes av trusselaktører. Sårbarheter kan gi hackere tilgang på personlig data og sette FHI i en svært uheldig situasjon der data er korrumpert, fjernet eller på avveie.	A) Implementere standardiserte prosesser for arkitekturanalyse, koderevisjon og sikkerhetstesting. B) Utnevne ansvarlige i utviklingsteamet til å overse at sårbarheter i kildekode avdekkes. C) Gjennomføre rutinemessige automatiske og manuelle koderevisjoner og sikkerhetstestinger gjennom hele utviklingsløpet.	2	3

			D) Benytte åpne kildekode og oppfordre innbyggere til å finne feil. E) Utarbeide en responsplan som dekker prosesser rundt gjennomføring av tiltak og kommunikasjon utad dersom sårbarheter i kildekoden avdekkes.		

Risikomatrise tilknyttet risikoscenarioer for utviklingsteam



R-8-1: Lav kodekvalitet på grunn av mangelfull kontinuerlig forbedring av sikker utviklingsmetodikk, styring og kompetanse.
R-8-2: Mangelfull forståelse av sikker koding fører til ustabile applikasjoner og datalekkasje.
R-8-3: Sårbarheter i kildekode på grunn av manglende analysemetoder for avdekking.

8 Bidragsytere

Gjennom RoS-arbeidet av Smittestopp 2.0 har nøkkelpersoner og fageksperter bidratt gjennom prosjektmøter og workshops med det norske sikkerhetsmiljøet. Oversikten viser bidragsytere og deres funksjoner i RoS-arbeidet.

Navn	**Funksjon**
Pål Jakob Solerød	Informasjonssikkerhetsleder FHI
Tor Gaute Indstøy	Sikkerhetsleder NHN
Stian Ervik	Senior Sikkerhetsrådgvider NHN
Sindre Solem	Infrastruktur/drift
Sindre Alvær	Infrastruktur
Agnieszka Zachariassen	Jurist, FHI
Erlend Bakken	Personvernombud FHI
Sindre M. Braaten	Arkitekt
Deltagere i workshopserien, blant annet: - Harald Wesenberg (Tekna) - Torgeir Andrew Waterhouse - Lise Lyngsnes Randeberg (Tekna) - Frode Strisland (SINTEF) - Thomas Gøytil (Klaveness Digital) - Maria Bartnes (SINTEF)	Eksternt fagmiljø utenfor FHI

9 Intervjuobjekter

RoS-arbeidet omfatter blant annet intervjuer med sentrale personer i NetCompany, Norsk Helsenett og FHI. En oversikt over intervjuobjekter og områder for dekning følger.

Navn	Område for dekning
Netcompany	Utviklingsmetodikk, monitorering, forvaltning, arkitektur
NHN	Utviklingsmetodikk, monitorering, forvaltning
FHI (teknisk)	Arkitektur, utviklingsmetodikk
FHI (juridisk)	Personvern, rettslig grunnlag
FHI/Dinamo	Kommunikasjonsstrategi/-plan

10 Tester benyttet inn i RoS-analysen

Flere tester har blitt gjennomført i løpet av RoS-arbeidet, og danner grunnlaget for deler av RoS-analysen.

Oversikt tester	**Ansvarlig for test**
Penetrasjonstester	BDO
Ytelsestest	NHN/Netcompany

11 Akronymer

Akronym	Beskrivelse
DDoS	Distributed Denial of Service Attack
DPIA	Data Protection Impact Assessment
EDPB	European Data Protection Board
ENS	Exposure Notification System
GAEN	Google Apple Exposure Notification
GDPR	General Data Protection Regulation
ISO	International Standards Organization
MSIS	Meldingssystem for smittsomme sykdommer
NHN	Norsk Helsenett
NIST	National Institute of Standards and Technology
NSM	Nasjonal Sikkerhetsmyndighet
OWASP	Open Web Application Security Project
PST	Politiets Sikkerhetstjeneste
RoS	Risiko- og Sårbarhetsanalyse