I. Prosjektopplysninger

System/registernavn: Digital smittesporing

Systemeier/dataansvarlig: Gun Peggy Knudsen

Fagansvarlig/Produkteier: Gun Peggy Knudsen

Systemforvalter:

Systemets tilhørighet:

Arkivnummer (P-360): 20/14482-1

Innhold

II. Rettslig grunnlag

A. Rettslig grunnlag for behandling av personopplysninger

Det må finnes et rettslig grunnlag for behandling av personopplysninger i registeret (som kan bestå av flere systemer) eller for et gitt system. Alle behandlingsgrunnlagene er angitt i personvernforordningen artikkel 6. Fyll ut med fritekst og henvisning til riktig alternativ i artikkel 6, eller bruk avkrysningen nedenfor hvor de grunnlagene som antas mest aktuelle for systemer er angitt som alternativer.

Behandlingen er nødvendig for:

☐ å **oppfylle en avtale som den registrerte er parti** i, eller for å **gjennomføre tiltak på den registrertes anmodning** før en avtaleinngåelse, jf. personvernforordningen artikkel 6 nr. 1 bokstav b),

☐ at Folkehelseinstituttet skal kunne oppfylle en **rettslig forpliktelse**, jf. personvernforordningen artikkel 6 nr. 1 bokstav c), på grunnlag av:

☐ Lov- eller forskriftshjemmel må angis og eventuelt begrunnes nærmere:

☐å utføre en **oppgave i allmennhetens interesse** eller å **utøve offentlig myndighet** som Folkehelseinstituttet **er pålagt**, jf. personvernforordningen artikkel 6 nr. 1 bokstav e), på grunnlag av:

☐ Lov- eller forskriftshjemmel må angis og eventuelt begrunnes nærmere:

☒ Den registrerte har **samtykket** til behandling av sine personopplysninger for ett eller flere spesifikke formål, jf. personvernforordningen artikkel 6 nr. 1 bokstav a).

B. Rettslig grunnlag for behandling av særlige kategorier av personopplysninger

Ved bruk av særlige kategorier av personopplysninger for eksempel helseopplysninger, må det i tillegg foreligge et særskilt grunnlag for å behandle denne typen opplysninger, jf. unntakene i personvernforordningen artikkel 9.

Behandlingen er nødvendig:

☐ for at den behandlingsansvarlige eller den registrerte skal kunne **oppfylle sine forpliktelser** og **utøve sine særlige rettigheter** på **området arbeidsrett, trygderett og sosialrett**, jf. personvernforordningen artikkel 9 nr. 2 bokstav b**,** på grunnlag av:

☐ Lov- eller forskriftshjemmel må angis og eventuelt begrunnes nærmere:

☐ av hensyn til **viktige allmenne interesser**, jf. personvernforordningen artikkel 9 nr. 2 bokstav g**),** på grunnlag av:

☐ Lov- eller forskriftshjemmel må angis og eventuelt begrunnes nærmere:

☐ i forbindelse med **forebyggende medisin** eller **arbeidsmedisin for å vurdere en arbeidstakers arbeidskapasitet**, i forbindelse med **medisinsk diagnostikk**, **yting av helse- eller sosialtjenester**, **behandling eller forvaltning av helse- eller sosialtjenester og –systemer**, jf. personvernforordningen artikkel 9 nr. 2 bokstav h**),** på grunnlag av:

☐ Lov- eller forskriftshjemmel må angis og eventuelt begrunnes nærmere:

☐ av allmenne **folkehelsehensyn**, f.eks. vern mot alvorlige grenseoverskridende helsetrusler eller for å sikre høye kvalitets- og sikkerhetsstandarder for helsetjenester og legemidler eller medisinsk utstyr, jf. personvernforordningen artikkel 9 nr. 2 bokstav i**),** på grunnlag av:

☐ Lov- eller forskriftshjemmel må angis og eventuelt begrunnes nærmere:

☐ for **arkivformål** i allmennhetens interesse, for formål knyttet til **vitenskapelig eller historisk forskning** eller **for statistiske formål, jf.** personvernforordningen artikkel 9 nr. 2 bokstav j) på grunnlag av

☐ Lov- eller forskriftshjemmel må angis og eventuelt begrunnes nærmere:

☒ Den registrerte har gitt uttrykkelig **samtykke** til behandlingen av særlige kategorier av personopplysninger, jf. personvernforordningen artikkel 9 nr. 2 bokstav a**).**

III. Er det behov for personvernkonsekvensvurdering?

Før behandlingen av personopplysninger i systemer starter skal man vurdere om det er nødvendig med en personvernkonsekvensvurdering, ved bruk av følgende kriterier:

☒ Involverer systemet **særlige kategorier personopplysninger** som («rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold) (se definisjon punkt 4 i retningslinjen).
Av personvernforordningen artikkel 35 nr. 1 følger:

> «*Dersom det er* sannsynlig *at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre* en høy risiko *for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige* før behandlingen *foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger.*»

☒ Dreier det seg om en behandling av personopplysninger **i stor skala**, som f.eks registre, med i form av:

- antallet personer inkludert i systemet (mer enn 5 000 personer),
- volumet av personopplysningene som vil behandles (antall variabler, detaljeringsgrad),
- systemets varighet (kort, tidsavgrenset, permanent) og
- geografisk omfang (lokalt, regionalt, nasjonalt, internasjonalt)?

☐ Vil **to eller flere datasett**, herunder personopplysninger fra ulike registre, **sammenstilles**? (for mange av systemene på FHI svarer en nei her, men det kan være aktuelt for systemer for statistikk/helseanalyse, helseregistre og forskningsprosjekter)

☐ Er behandlingen en **evaluering eller poengvurdering**, inkludert profilering og forutsigelse, blant annet av aspekter som helse, personlige preferanser eller interesser, pålitelighet eller adferd, plassering eller bevegelser av enkeltindivider? For de fleste systemer på FHI er svaret nei.

☐ Omfatter systemet personopplysninger om **personer med særskilt beskyttelsesbehov**, f.eks. barn?

☐ Vil konteksten for behandlingen **begrense muligheten de registrerte har til å utøve sine rettigheter**, f.eks. vil det være vanskelig å gi god informasjon? For de fleste systemer på FHI er svaret nei, men dette er relevant i systemer som er indirekte identifiserbare.

☒ Vil systemet ta i bruk **ny teknologi** eller brukes eksisterende teknologi til nye formål?

☐ Omfatter systemet noen form for **automatiserte avgjørelser** for enkeltindivider? For de fleste systemer på FHI er svaret nei.

☐ Innebærer systemet en **systematisk overvåking** av enkeltindivider? For de fleste systemer på FHI er svaret nei.

☒ **Det er vurdert å være behov for personvernkonsekvensvurdering**.

Fyll ut resten av malen.

Navn på leder som har vurdert behandlingsgrunnlaget for personopplysninger i systemet (punkt II), samt behovet for personvernkonsekvensvurdering (punkt III).

Skriv inn navn på leder som har gjort vurderingen: Gun Peggy Knudsen

IV. Beskrivelse av personopplysninger og behandling av disse

1. Beskrivelse av personopplysninger i systemet

1.1 Formålet med behandlingen av personopplysninger

Hensikten med digitalt sporingssystem er å bidra til å forebygge og stoppe utbredelse av covid-19 gjennom rask oppsporing av personer som kan være smittet av koronaviruset og formidling av råd til disse.

Ved enhver form for kontaktsporing vil behandling av personopplysninger som bekrefter identitet, smittestatus, bevegelsesmønster og nærkontakt med andre personer være nødvendig. Det gjøres en

rekonstruksjon av en persons bevegelseshistorie for å identifisere personer de kan ha smittet, og dette blir i utgangspunktet gjort manuelt. Med automatisert digital kontaktsporing vil brukeren ha mulighet til å gi beskjed til personer som brukeren har vært i kontakt med, dersom brukeren blir smittet av koronaviruset. Tilsvarende vil brukeren kunne få beskjed dersom brukeren har vært i kontakt med en som er smittet. Dette vil skje hurtig og vil dermed kunne supplere mye av det manuelle arbeidet som både tar lang tid og tar mye personellkapasitet. Digital smittesporing gjør det mulig å notifisere kontakter som en bruker ikke kjenner eller som brukeren ikke husker. Brukere vil raskt kunne ta nødvendige forholdsregler, som testing, karantene eller isolasjon, og dermed hjelpe med å minske smittespredningen og bryte smittekjedene.

1.2 De registrerte i systemet

☐ **Systemer med egen datafangst**

Gi en generell beskrivelse av hvem som er registrert i systemet (de registrerte);

Det er frivillig å ta i bruk appen og verifisere seg selv som smittet. Den digitale smittesporingsappen blir gjort tilgjengelig gjennom App Store og Google Play. Hele Norges befolkning over 16 år er potensielle brukere av appen. Appen vil ha aldersgrense på 16 år.

Nærmere om alder

Det er ikke mulig å verifisere alder for nedlastning av denne appen på App Store og Google Play. Det vil derfor ikke være mulig for FHI å vite hvilke deler av befolkningen som laster ned appen, herunder om barn laster ned appen. I og med at FHI ikke vet hvem som laster ned appen vil det heller ikke være mulig å forhindre at barn og unge mottar notifikasjoner om nærkontakt med en smittet. Det har vært vurdert om en bruker skal logge seg inn med ID-porten for å aktivere selve appen og kontakteregistreringen. Det har også vært vurdert om en bruker selv skal oppgi alder før de kan aktivere appen og kontaktsporingen. Dette vil imidlertid medføre betydelig større behandling av personopplysninger og er vanskelig å få til i en desentralisert løsning. Det er derfor ikke iverksatt. Det vil imidlertid følge av samtykketeksten der man samtykker til aktivering av appen at appen har en aldersgrense på 16 år.

For å kunne varsle andre brukere om sin smittestatus vil brukeren verifisere seg gjennom ID-porten. Dette medfører at kun brukere over en viss alder kan logge seg inn og anvende denne funksjonen. Både MinId og BankId vil være gyldig innloggingsmetode. MinID utstedes av Digitaliseringsdirektoratet, og kan bestilles fra det året man fyller 13 år. BankID utstedes av banker, og kan bli utsendt til personer som er fylt 13 år. Flere banker utsteder ikke før fylte 15 år. Videre vil det foreligge en filtrering i MSIS som vil hindre at informasjon for personer under 16 år skal kunne leveres ut. Verifisering gjennom ID-porten og filtrering mot MSIS vil følgelig hindre at barn og yngre enn 16 år kan aktivere varslingsfunksjonen og hindre dem i å notifisere deres nærkontakter. Dersom en 14-åring forsøker å varsle sine nærkontakter vil vedkommende få beskjed at slik varsling ikke kan gjennomføres på grunn av manglende verifisert smittestatus eller for lav alder.

Kryss deretter av for hvilke kategorier av registrerte det behandles opplysninger om (du kan krysse av for flere hvis det er relevant);

☐ Elever/studenter

☐ Pasienter/klienter/brukere

☐ Barn, spesifiser aldersgrupper

- ☐ 0-12
- ☐ 13-15
- ☐ 16-18

☐ Pårørende

☐ Etniske minoriteter

☐ Avdøde

☒ Annet (som spesifisert i beskrivelsen over)

Anslå omfanget av de registrerte (f.eks geografiske omfang (lokalt/institusjon, regionalt, nasjonalt, internasjonalt) eller karakteristika) og når systemet ble etablert (utvalget):

☐ **Systemer basert på sammenstilling av andre datakilder**

☒ Sentrale helseregistre; MSIS

☐ Helseundersøkelser (eksisterende);

☐ Kvalitetsregistre; … *[Angi hvilke]*

☐ Pasientjournal; … *[Angi hvilke institusjoner]*

☐ Folkeregisteret

☐ SSB; … *[Angi hvilke registre]*

☐ Internett

☒ Annet

Spesifiser datakildene og beskriv kobling dersom dette er relevant:

I tillegg til kobling mot MSIS vil det gjøres en kobling mot ID-porten.

1.3 Kategorier av personopplysninger

Personidentifiserbare personopplysninger

☐ Navn

☐ Adresse

☐ Fødselsdato

☒ Fødselsnummer, D-nummer, DUF-nummer (11 siffer)

☒ Andre identifiserbare opplysninger, for eksempel telefonnummer, e-postadresse, IP-adresse

☐ Andre beskrivende opplysninger, for eksempel demografiske variabler, sosioøkonomiske forhold (utdanning, inntekt, yrke), familiestatus.

Særlige kategorier av personopplysninger (tidligere kalt sensitive opplysninger)

☐ Rasemessig eller etnisk bakgrunn

☐ Politisk, filosofisk eller religiøs oppfatning

☐ At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling

☐ Seksuelle forhold

☐ Medlemskap i fagforeninger

☐ Biometri

☐ Helseopplysninger:

- ☒ Diagnoser
- ☐ Legemiddelbruk
- ☐ Kognitive evner

☐ Genetikk

☐ Annet, spesifiser under

Spesifiser hvilke opplysninger og nivå på variabler:

Positiv/negativ Covid-19 test, selvrapporterte symptomer

Nedenfor følger en nærmere beskrivelse av hvilke opplysninger som behandles i tilknytning til løsningen**.**

Innsamling av data til Google Play/App Store

Når digital smittesporingsapp tas i bruk vil appen automatisk sende informasjon om bruksmønster (f.eks. start og stopp av appen) og feilsituasjoner (f.eks. at appen krasjer) til App Store og Google Play. Denne informasjonen lagres i inntil 90 dager og brukes til feilretting og til å forstå hvordan appen brukes, men uten at dette kan knyttes opp mot personopplysninger som telefonnummer, posisjonsdata eller smittekontakter. Dette er ikke en behandling som gjøres spesielt for den digitale smittesporingsappen, men gjelder for mange apper som lastes ned fra App Store og Google Play. Tilbakemelding fra Google er at beregningene og telemetrien disse rapportene dekker, beskriver en bransjepraksis for mobile operativsystemer (ikke bare på Android) som hjelper med å sikre at enheter forblir oppdatert, holder mennesker og systemer sikre mot angrep og tillater pålitelig drift av økosystemet til enheter som kjører Android. Det er ingen sammenheng mellom de generelle observasjonene om Android-telemetri i rapporten og bruk av Exposure Notification APIs.» https://support.google.com/android/answer/9021432?hl=en.
https://developers.google.com/android/exposure-notifications/telemetry-design

Google og Apple kan også samle inn andre opplysninger fra mobiltelefonen uavhengig av Smittestopp, i henhold til selskapenes personvernpolicy, https://www.apple.com/uk/privacy/
https://policies.google.com/privacy?hl=en

Opplysninger som behandles i appen på telefonen

Når brukeren har lastet ned og gitt sitt samtykke til å aktivere appen, anvendes Bluetooth-forbindelse på brukerens telefon til å registrere og lagre signaler (kontaktnøkkel, Rotating Proximity Identifiers, RPI) fra andre telefoner, som brukeren er i nærheten av og som har installert og aktivert Smittestopp. Den lagringsteknologi som anvendes i appen er Apple/Google- teknologien. Disse opplysningene behandles kun på brukeres telefon. Verken FHI eller andre har adgang til disse opplysningene.

Det er stilt spørsmål om flere av de opplysningene som registreres og lagres på mobiltelefonen er å anse som personopplysninger eller anonyme opplysninger. Det er en teoretisk mulighet til å knytte opplysninger til enkeltpersoner ved at en brukers RPI kringkastes til alle som ønsker å lytte på den via Bluetooth, og dermed kan bruke denne uten å være hindret av GAEN. Hvis du starter med å være i kontakt med én kjent person, og registrerer deres RPI, har du mulighet til å følge denne personens bevegelser i 10-20 min med et stort nok nettverk av Bluetooth-scannere i det relevante geografiske området. Hvis denne personen også er alene når RPI-er byttes ut, kan man fortsette sporingen på neste RPI osv. Ved flere til stede kan man likevel gjøre kvalifisert gjetning på hvilke RPI-er som tilhører samme person ved å se på når RPI-er forsvant og dukket opp. For ordens skyld legger vi derfor til grunn at dette er personopplysninger.

Følgende personopplysninger innsamles og lagres på brukerens mobiltelefon når brukeren har lastet ned og arkivert appen:

- Rullerende Temporary Exposure Key, “TEK” på brukers 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

Når en bruker har blitt verifisert som smittet og appen har fått utdelt en tilgangstoken (se nedenfor om verifiseringsløsning), hentes Temporary Exposure Keys (TEKs) for de siste 14 dagene ut fra den smittede brukers telefon. TEK knyttet til en verifisert diagnose av covid-19 omtales som en diagnosenøkkel. Bruker blir forespurt om å oppgi dato der første symptomer oppstod (helseopplysning). Dette skjer på brukerens mobil. Ut fra dette blir hver diagnosenøkkel tildelt informasjon om smittsomhet ut fra hvilken dag den var i bruk. Hva denne verdien er, avhenger av versjon av rammeverket og potensielle beslutninger gjort per land, men er vanligvis en «riskscore» basert på dato diagnosenøkkelen gjelder for relativt til dato for symptomer hos den som har lastet opp nøkkelen, basert på selvrapportering. Deretter blir så diagnosenøklene med tilhørende smittsomhetsinformasjon lastet opp til en backend (se nedenfor om backend).

Opplysninger som behandles i verifiseringsløsningen

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

Når en bruker har verifisert seg via ID-porten gjøres et oppslag i MSIS for å se om det finnes opplysninger om positiv/negativ prøve for covid-19 for oppgitt fødselsnummer innenfor siste 14 dager, og at tilknyttet person er over 16 år. MSIS svarer verifiseringsløsningen med en Ja/Nei-verdi for om det fantes en slik prøve. Hvis «Ja», følger også prøvedato med. Basert på denne informasjonen utsteder verifiseringsløsningen en tilgangstoken til appen. For tilfeller hvor smitte ikke kunne bli verifisert inneholder disse tokene kun informasjon om at verifisering ikke kunne gjennomføres, og at tilgang til varsling ikke er gitt. Hvis smitte ble verifisert vil en slik token inneholde tilfeldig generert ID for den aktuelle verifiseringen, bekreftelse om at smitte er verifisert, prøvedato for avlagt positiv test samt informasjon om brukeren er blokkert fra varsling eller ikke. Brukere blir blokkert fra varsling hvis det er registrert mer enn 3 gjennomførte verifiseringer for de siste 24 timene. Hver gang en bruker har blitt verifisert smittet vil det lagres en oppføring for tidspunkt og pseudonym (ID-porten pseudonym kjørt gjennom en egen enveisfunksjon) som slettes etter 24 timer. Verifiseringsløsningen vil også ha behov for å mellomlagre ID til bruker fra ID-porten, og eventuelt svar fra MSIS, så lenge brukeren har en aktiv tilkobling til løsningen, men vil ikke lagre denne informasjonen etter at brukers «sesjon» er avsluttet. Denne informasjonen lagres i en kryptert informasjonskapsel som utveksles mellom brukers nettleser og verifiseringsløsningen så lenge det er en aktiv «sesjon», hvor nøkkelen ligger hos verifiseringsløsningen.

Følgende personopplysninger behandles ved oppslag mot MSIS:

- Fødselsnummer
- Opplysninger om positivt/negativt smitte med Covid-19 (helseopplysning)
- Tidspunkt for positiv Covid-19 prøve (helseopplysning)

Opplysninger som behandles i backend

Diagnosenøklene med tilhørende smittsomhetsinformasjon for en bruker som er verifisert smittet lastes opp til sentral backend. Diagnosenøkler som lastes opp på denne måten blir så periodisk lastet ned av alle aktive apper i systemet. Deretter sammenlignes disse diagnosenøklene med kontaktnøkler registrert via Bluetooth. Ved å kombinere «smittsomhetsinformasjon» fra hver diagnosenøkkel som har treff, tidspunkter disse er registrert kontakt på, signalstyrke ved kontakt, og valgt GAEN-konfigurasjon, vil eventuelle kontakter som skal varsles beregnes. Appen vil, ut fra denne informasjonen, varsle nærkontaktene til brukeren som er verifisert som smittet.

Følgende opplysninger behandles i backend løsningen:

Diagnosenøkkel (helseopplysning)

I motsetning til den tidligere Smittestopp Versjon 1, samles det ikke GPS data.

2. Behandling av personopplysninger

Med «behandling» menes enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger. Kryss av for hva som skal gjøres med personopplysningene i systemet og eventuelt spesifiser. Behandlingene må være i samsvar med det oppgitte formål.

- ☒ Innsamling
- ☒ Lagring
- ☐ Helseanalyse/sammenstilling for kvalitetssikring og statistikkproduksjon
- ☐ Gjenfinning
- ☐ Tilgjengeliggjøring av individdata
- ☒ Sletting
- ☒ Annen

2.1 Innsamling

Nr	Spørsmål	Svar
1	Hvordan samles personopplysningene inn? Samles personopplysningene inn direkte fra de registrerte selv eller fra andre kilder som f.eks via helsetjenesten? Hvor ofte samles dataene inn?	Personopplysningene som behandles i appen samles direkte inn fra brukeren og deres nærkontakter fortløpende. Brukeren som er verifisert som smittet blir forespurt om å oppgi dato for når første symptomer oppstod (hvis aktuelt). Dette skjer på brukerens mobil. For øvrig skjer det oppslag mot MSIS og ID-porten. Se for øvrig pkt 1.3.
2	Er det noe som er særlig inngripende ved måten personopplysningene samles inn (for eksempel ved hjelp av fingeravtrykk, kamera- eller	Nei

Nr	Spørsmål	Svar
	lydopptak, eller sporing av en persons lokasjon, biometri)?	
3	Samles det inn flere opplysninger enn det som er nødvendig ut fra formålet? Kommer det f.eks inn dokumenter eller fritekst som må kodes og som kan inneholde overskuddsinformasjon som bør slettes?	**Opplysninger i appen:** Registrering av elektroniske kontakter skjer i henhold til API utviklet av Google og Apple. Alle vedvarende kontakter med uavbrutt Bluetooth kontakt over en kort periode registreres. Det er en del av funksjonaliteten til Apple/Google API, og det er ikke mulig å endre på dette. Det at det samles opplysninger om alle kontakter innebærer at det registreres potensielle nærkontakter, men alle vil ikke være reelle nærkontakter med smittede. Dermed registreres flere kontakter enn det som er nødvendig for å notifisere om nærkontakt og smitte. Det er på forhånd ikke mulig å si hvem som faktisk blir smittet, og da ikke mulig å avgrense hvilke kontakter som bør lagres for å gjøre det mulig å varsle. Alle disse kan utgjøre potensiell smittekilde og det er derfor nødvendig at appen registrerer alle disse elektroniske kontaktene. Omfang av potensielle kontakter avgrenses ved å sette krav til avstand/signalstyrke og tid/varighet på kontakt. **Opplysninger i verifiseringsløsningen:** Det samles ikke andre opplysninger enn ID i verifiseringsløsningen. Det gjøres et oppslag mot MSIS for å bekrefte covid-19-positivt svar samt dato for den positive testen. Oppslaget mot MSIS, som i realiteten er en utlevering fra MSIS, er hjemlet i MSIS-forskriften § 4-5. Det er Folkehelseinstituttet som er behandlingsansvarlig for MSIS-registeret og behandling av opplysninger i MSIS er regulert i MSIS-forskriften. **Opplysninger i backend:** I backend lastes kun diagnosenøkler fra den smittede opp. Ingen andre opplysninger innhentes. Sentral backend med diagnosenøkler er nødvendig for løsningen fordi det er eneste måten som kan sikre at brukere av appen får notifikasjoner om påvist smitte.
4	Hvilken relasjon har den behandlingsansvarlige med de registrerte? Beskriv maktforholdet mellom dem. Har den registrerte anledning til å nekte f. eks. gjennom reservasjon, sperring eller sletting?	Selv om behandlingsansvarlig er en offentlig myndighet (FHI), vil ikke appen anvendes i offentlig myndighetsutøvelse. Appen er ikke ment som et verktøy for helsemyndighetenes smittesporingsarbeid eller til f.eks. smittespredningsanalyse, men som et verktøy for den enkelte bruker for egen digital smittesporing – som supplement til manuell smittesporing. Det vil være frivillig for den enkelte å laste ned appen. Brukeren må videre samtykke til notifisering av nærkontakter. Det skal innarbeides en funksjonalitet i applikasjonen der man aktivt gir

Nr	Spørsmål	Svar
		en form for godkjennelse av behandling av personopplysninger (skyveknapp). Det skal gis god informasjon om hva det innebærer. Det vil bli lenket fra Google Play og App Store til personvernerklæringen og det vil foreligge informasjon tilgjengelig på en nettside (fhi.no og/eller helsenorge.no). Konsekvensen av at den enkelte ikke laster ned appen, er at vedkommende ikke vil få tilgang til tjenesten, men det har ingen direkte negative konsekvenser for den som velger å ikke delta. Hver bruker kan slette allerede registrerte data på den enkeltes telefon. En bruker kan imidlertid ikke slette «sine» kontaktnøkler som allerede er registrert på andres mobiltelefoner. Det er heller ikke tenkt noe funksjon for å tilbakekalle diagnosenøkler som er lastet opp ifm varsling. Selv om det blir oppfordret til å ta appen i bruk, må de som ønsker det aktivt, velge å gå inn i Google Play og App Store, deretter laste den ned, lese informasjon og samtykke til aktivering før de faktisk kan ta den i bruk. Brukere av appen vil til enhver tid ha mulighet til å trekke samtykket tilbake, og ved eventuelt påvist smitte vil brukere selv ha anledning til å velge om man vil varsle personer som man har hatt nærkontakt med og som kan være utsatt for smitte. Både plikter og rettigheter etter smittevernregelverket er upåvirket av nedlastning eller bruk av appen. Det er altså ikke tale om en medbestemmelsesrett eller valgfrihet som knytter seg til faktisk myndighetsutøvelse. For nærmere drøftelse knyttet til samtykke som rettslig grunnlag, se punkt 5.1.

2.2 Lagring

Nr	Spørsmål	Svar
1|	Beskriv behandling av data fra de registreres til de er kommet inn i systemet/registeret, og eventuelt ulike steder dataene lagres på veien inn (papir, ulike soner, bruk av TSD, skanning, … etc)	Se vedlegg om teknisk beskrivelse.
2	Hvor og hvor lenge lagres personopplysningene? Brukes det ulike kriterier for lagringstid og i så	**Opplysninger i appen:** Opplysninger lagres på telefonen til brukeren inntil de blir slettet fortløpende etter 14 dager.

Nr	Spørsmål	Svar
	fall hvilke for ulike typer personopplysninger? Lagringstiden skal beskrives og begrunnes (ev. henvise til hjemmel for dette).	Sletting på telefonen er styrt av API-et, og det er ikke mulig å endre dette. **Opplysninger i verifiseringsløsningen:** ID-opplysninger som samles inn når en bruker identifiserer seg via ID-porten lagres kun i en begrenset periode. Fødselsnummer fra ID-porten behandles kun i verifiseringsløsningen så lenge bruker har en aktiv tilkobling til løsningen. Så fort verifisering er gjennomført slettes denne informasjonen. Pseudonym fra ID-porten og tidspunkt for verifisering blir lagret i 24 timer. Lagring av pseudonym i 24 timer gjøres for å hindre at en enkel bruker usteder mange notifikasjoner fra telefoner som ikke tilhører brukeren og følgelig sender falske notifikasjoner. Opplastning av nye diagnosenøkler for et pseudonym som allerede er registrert 3 ganger de siste 24 timene vil avvises av backend. Opplysninger om brukere som har testet positivt for covid-19 oppbevares og lagres i MSIS i henhold til MSIS-forskriften. **Opplysninger i backend** Opplysninger om diagnosenøkler lagres i backend i 14 dager for å kunne varsle kontakter 14 dager bakover i tid. Opplysninger i backend eldre enn 14 dager slettes fortløpende. Se mer om lagringssted i punkt 2.7
3	Hvor lenge lagres personopplysningene før de slettes, etter at formålet ved behandlingen er oppnådd? Er det en er tidsbegrensning men uten fastsatt dato? Er det angitt forhåndsfastsatte slettedato eller dato for anonymisering? Henvis eventuelt til hjemmel for dette.	Se ovenfor, samt punkt 2.7. Appen legges ned, herunder registrering av nøkler, deaktiveres og alle data i backend slettes når appen ikke lengere er aktuell å bruke i forbindelse med covid-19.
4	Er det utarbeidet rutiner for sletting?	Nei, sletting er innarbeidet i systemene.

2.3 Helseanalyse/sammenstilling for kvalitetssikring og statistikkproduksjon

Nr	Spørsmål	Svar
1	Brukes systemet/registeret for å ta ut data om delpopulasjoner i registeret som deretter skal sammenstilles med andre datakilder for å gjøre helseanalyse eller håndtere beredskapssituasjoner (f.eks. utbrudd av smittsomme sykdommer)?	Nei
2	Beskriv hvilke andre datakilder som systemet vaskes/valideres/berikes med mot på jevnlig basis (Folkeregisteret, andre helseregistre, SSB data, DIFI Kontakt og reservasjonsregister mm)…	Ikke aktuelt
3	Beskriv hvilke retningslinjer og praksis systemet har for publisering av statistikk og for å unngå tilbakeveisindentifisering (refr. kotyme om prikking av celler med 5 eller færre når nevner er liten)	Ikke aktuelt
4	Hvilke andre kilder kobles systemet/registeret med på periodisk basis for kvalitetssikring/validering og hva slags mekanismer har en for å unngå «skyggeregistre», dvs at en sletter kopi av data fra andre registre etter kvalitetssikring ?	Ikke aktuelt
5	Beskriv retningslinjer og praksis knyttet til uttak og tilgjengeliggjøring av data for gjensidig kvalitetssikring med andre systemer/registre og institusjoner, og hva slags mekanismer en har for å unngå skyggeregistre.	Ikke aktuelt

2.4 Gjenfinning

Nr	Spørsmål	Svar
1	Brukes registeret eller sammenstilte data for å ta kontakt med denne populasjonen (se spørsmål 1 i kapittel 2.3).	Nei

2.5 Tilgjengeliggjøring av individdata

Nr	Spørsmål	Svar
1	Tilgjengeliggjøres det personopplysninger til andre i eller utenfor virksomheten? Dette samt spørsmål 2,	Nei

Nr	Spørsmål	Svar
	3 er relevant for helseregistre og helseundersøkelser.	
2	Hvordan tilgjengeliggjøres personopplysningene – beskriv dataflyten?	Ikke aktuelt
3	Hvordan er mottakere av personopplysninger identifisert og dokumentert (for eksempel ansatte, databehandlere, tredjeparter, eksterne virksomheter osv.)?	Ikke aktuelt
4	Hvordan deles personopplysningene mellom avdelinger internt i virksomheten? Dette samt spørsmål 4, 5 og 6 er relevant for blant annet administrative systemer, smittevernberedskap og lab.	Ikke aktuelt
5	Hvilke personopplysninger deles med hvilke avdelinger og hva er formålet med hver av disse delingene?	Ikke aktuelt
6	Hvilke eksterne virksomheter deles personopplysningene med (private, offentlige myndigheter osv)? Se tilsvarende spørsmål i kapittel 2.3	Ikke aktuelt.
7	Hvilke personopplysninger deles eksternt, for hvilket formål og med hvilke rettslige grunnlag? Se tilsvarende spørsmål i kapittel 2.3	Ikke aktuelt.
8	Beskriv retningslinjer og praksis for tilgjengeliggjøring og kobling av data, samt eventuell mottak av data for kobling og hvordan en unngå skyggeregistre. Angi navn og nummer på relevante rutiner.	Ikke aktuelt.

2.6 Sletting

Det forutsettes at systemet har etablert rutiner for å kvalitetssikre dataene i systemet/registeret. Spørsmålene under gjelder sletting av innholdet i registre på bakgrunn av henvendelser fra den registrerte.

Nr	Spørsmål	Svar
1	Har FHI mulighet til å slette den registrerte i systemet eller er en avhengig av oppdateringer fra annet sted?	**Opplysninger i appen:** • TEK-nøkler og RPI-nøkler som er registrert på brukers mobiltelefon slettes automatisk fortløpende etter 14 dager. • Alle opplysninger registrert i appen på mobiltelefonen slettes når brukeren har slettet appen. Sletting skjer på brukerens telefon og bestemmes av API. FHI har ingen tilgang til opplysninger på telefonen. **Opplysninger i verifiseringsløsningen:** • Fødselsnummeret slettes så fort bruker har gjennomført eller avsluttet verifiseringsprosessen. • Pseudonymet slettes automatisk etter 24 timer. **Opplysninger i backend:** • Diagnosenøkler slettes automatisk etter 14 dager. Det er ikke mulig for FHI å fjerne nøklene på server som ble sendt av appen fordi det ikke er mulig å binde nøklene til enhet som sendte dem. Alle nøklene fjernes av server etter 14 dager etter de ble submittet.
2	Dersom den registrerte ikke selv kan slette egne personopplysninger, finnes det andre måter å gjøre det på? Finnes det dokumenterte rutiner for sletting av helseopplysninger i hht henvendelser fra den registrerte?	Ref. punktet overfor. Sletting av opplysninger i MSIS reguleres av helseregisterloven § 25 og personvernforordningen artikkel 17, ref. https://www.fhi.no/div/personvern/til-allmennheten/rett-til-informasjon-om-innsyn-i-og/ Brukeren vil gis informasjon om muligheter/begrensinger når det gjelder sletting av personopplysninger i løsningen.
3	Finnes det rettsgrunnlag i lov eller forskrift som gir grunnlag for å nekte sletting?	Se overfor.

2.7 Lagringssted

Angi hvor og hvordan personopplysninger skal lagres og håndteres.

☐ Ordinær sone FHI

☐ Sikker sone FHI

☐ Ekstern databehandler utenom NHN

☒ Annet, spesifiser under

Opplysninger i appen: Alle personopplysninger lagres på den enkelte brukers telefon via GAEN.

Opplysninger i verifiseringsløsningen: Oppslag i MSIS lagres i MSIS sin innsynslogg i henhold til MSIS sine eksisterende retningslinjer og tilganger. Informasjon om fødselsnummer fra ID-porten og resultat fra MSIS lagres i en kryptert informasjonskapsel som utveksles mellom brukers nettleser og verifiseringsløsningen så lenge det er en aktiv tilkobling. Pseudonymet lagres hos NHN (on premises)

Opplysninger i backend: Opplysninger i backend blir lagret på en server i Danmark. Netcompany Norway AS er databehandler, og Netcompany A/S i Danmark er deres underdatabehandler.

2.8 Annen

Kommenter eventuell annen databehandling. Er det noen punkter som ikke er behandlet overfor eller som kan gi allmenn bekymring, så kan du beskrive dette nedenfor i fritekst. Kommenter også dersom behandlingen er så kompleks at den registrerte har begrenset kontroll over sine opplysninger.

Nedlastninger: Folkehelseinstituttet kan, på aggregert og anonymisert nivå, ta ut statistikk som forteller hvor mange som har lastet ned appen.

Verifiseringsløsning: Det eneste som er planlagt lagret i verifiseringsløsningen er en systemlogg med informasjon om hendelser i løsningen. Dette gjelder loggen i løsningen som brukes for å overvåke status og belastning på systemet. Eksempel: «Forsøk på innlogging ble avbrutt», «Token fra ID-porten kunne ikke tolkes», «Oppslag mot MSIS feilet», «Verifiseringsflyt gjennomført med resultat: Verifisert positiv», «Verifiseringsflyt gjennomført med resultat: Kunne ikke verifisere smitte». Ingen av disse loggene vil inneholde informasjon som kan knyttes til bruker, bare hva som har skjedd i løsningen. Denne systemloggen vil følgelig ikke inneholde noen personopplysninger. Drift og utviklere vil ha tilgang til loggen i produksjonsfasen.

Backend: Her vil mye det samme som verifiseringsløsningen gjelde, men i tillegg så vil drift ha tilgang til databasene med diagnosenøkler for de siste 14 dagene. Det vil også sannsynligvis være behov for å ta ut data om antallet opplastninger av diagnosenøkler per dag fra løsningen, og hvor mange som i appen velger å varsle om smitte til nære kontakter. Dette vil sannsynligvis håndteres via drift. eHealth-network etterspør disse tallene fra alle medlemsland som har en covid-19-app, så det forventes at Norge også kan stille med dette. Kun aggregerte tall skal tas ut og eventuelt deles med eHealth-network (totalt antall nedlastninger, totalt antall varslingsopplastninger/diagnosenøkler). Siden vi kun lagrer data i 14 dager må vi jevnlig hente ut disse tallene og oppdatere «totalen» av antallet opplastninger/diagnosenøkler.

3. Dataansvarlig, datatilgang og databehandlere

3.1 Datatilganger til systemet

Beskrivelse av tilganger til systemet, herunder funksjon/rolle og type personopplysninger er angitt i ROS-analysen. Beskrivelse av hvem som kan tildele tilganger, hvilke rutine som følges og hvor ofte tilgangsgruppene skal gjennomgås beskrives også i ROS analysen.

3.2 Databehandler

Norsk helsenett (NHN) drifter FHI sin IKT-infrastruktur og leverer arkivtjenester til instituttet. Driften av IKT skjer i Norge. Det er gitt tilstrekkelige garantier for at behandlingen oppfyller kravene i forordning og vern av den registrertes rettigheter, ref. den til enhver tid gjeldende databehandleravtalen mellom FHI og NHN.

☐ Systemet benytter kun NHN og har ingen andre databehandlere– gå videre til neste kapittel.

Dersom det benyttes databehandler(e), fyll inn informasjon:

Følgende andre virksomheter vil fungere som databehandlere i systemet. Fjern det som ikke passer.

Virksomhet	Rolle/funksjon	Land
Netcompany Norway AS (med Netcompany A/S som underdatabehandler)	Leverandør av server for backend og support.	Danmark
Mnemonic	Overvåkning og hendelseshåndtering på sikkerhetsområdet	Norge

For hver databehandler skal det godtgjøres at de gir tilstrekkelige garantier for at behandlingen oppfyller kravene i forordning og vern av den registrertes rettigheter. Dersom en har brukt FHI sin standard databehandler avtale vil dette være ok og en kan krysse av punktene under. Hvis ikke, må en kontakte Jusskasse/juridisk avdeling for å få avklart svaret status her.

For databehandler(e) er følgende aktuelt og vil være oppfylt før behandling finner sted:

☒ Databehandler avtale som oppfyller forordningens krav

☐ Mottatt og gjennomgått ROS (Risiko- og sårbarhetsanalysen vedlegges)

☐ Mottatt beskrivelse av tekniske og organisatoriske tiltak

☐ Mottatt oversikt over underleverandører

Hvis man benytter databehandlere, er det viktig at disse selv bidrar med informasjon om blant annet personopplysningsvern/informasjonssikkerhet, og kontakten med dem bør beskrives. Dersom databehandlere har vært involvert i personvernkonsekvensvurderingen, beskriv hvordan.

Innleide konsulenter som jobber i FHIs infrastruktur under FHI sin ledelse behandles som vanlig ansatte og ikke som databehandlere.

3.3 Overføring av personopplysninger til andre land og/eller internasjonale organisasjoner

☒ Ikke aktuelt – Gå videre til neste kapittel

☐ Personer/institusjoner i EU/EØS

☐ Tredjeland (utenfor EU/EØS)

☐ Internasjonale organisasjoner

Overføringene vil skje på følgende grunnlag:

☐ Beslutning om at det aktuelle land har et tilstrekkelig beskyttelsesnivå

☐ Overføringen er omfattet av nødvendige garantier, slik som EUs standardavtaler, beskriv under:

☐ Overføringen er underlagt bindende virksomhetsregler, slik som registrering under Privacy Shield, beskriv under:

☐ Unntak for særlige situasjoner, beskriv under:

Hva er rettslig grunnlag for overføring utenfor EØS?

Redegjør for hvordan personopplysningene overføres og lagres ut av Norge:

3.4 Atferdsnormer

I den grad det finnes atferdsnormer/bransjenormer for den aktuelle behandling, som f.eks. Normen (for informasjonssikkerhet i helsesektoren) for blant annet helseregistrene eller BBMRI Code of Conduct (biobank), skal disse angis og det skal opplyses om de vil følges i behandlingen av personopplysninger i prosjektet. Det er foreløpig ikke etablert godkjente atferdsnormer, og dette punktet er derfor foreløpig **ikke obligatorisk**.

Oppgi atferdsnorm dersom dette skal følges i behandlingen av personopplysninger:

Løsningen er i tråd med retningslinjene fra Det Europeiske Databeskyttelsesråd (EDPB) vedrørende bruk av apper til bekjempelse av COVID-19
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_da.pdf

samt EU Kommisjonens veiledning om apper til støtte for bekjempelse av COVID-19-pandemien

https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)

V. Vurdering av personvern og registrertes rettigheter

4. Formålsbegrensning, dataminimering og lagringsbegrensning

4.1 Rimelighet

Behandlingen skal vurderes i forhold til personvernprinsippene og ivaretakelsen av den registrertes rettigheter. Formålet med behandlingen er oppgitt i kapittel 1.1. Personopplysningene skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål.

Nr	Spørsmål	Svar
1	Vurder rimeligheten av behandlingen: Hva er forventede fordeler ved behandlingen? For virksomheten, den registrerte, samfunnet for øvrig osv.	Smittestopp og behandling av personopplysninger i løsningen tjener aktuelle og tungtveiende samfunnsmessige hensyn som befolkingens liv og helse og bekjempelse av covid-19. Disse hensyn finner klar støtte i forordningen og i smittevernloven. Bruk av data og teknologi i form av apper er anerkjent både av Det Europeiske Databeskyttelsesråd og EU-kommisjonen i kampen mot viruset. Også studie fra Oxford University støtter digital smittesporing som middel til å bremse spredning av covid-19. Flere land i Europa og i verden har utviklet apper for digital smittesporing. Med automatisert kontaktsporing vil personer få rask informasjon om at de kan ha vært utsatt for smitte når en bruker har blitt bekreftet å være smittet av koronaviruset. Digital smittesporing gjør det mulig å notifisere kontakter som en bruker ikke kjenner eller som brukeren ikke husker. Tiltaket vil dermed supplere den manuelle smittesporingen som gjøres i dag. Brukere vil raskt kunne ta nødvendige forholdsregler, som karantene, testing og isolasjon, og dermed hjelpe med å minske smittespredningen og bryte smittekjedene. Nytten av tiltaket øker jo flere deltar. Appen vil ha nytteeffekt, selv om en mindre andel enn av befolkningen i Norge vil ta appen i bruk. Selv ved lav oppslutning vil appens smittesporingsdel kunne ha en nytteeffekt innenfor et mindre lokalt nettverk/cluster. Dette er også omtalt i ECDCs retningslinjer, https://www.ecdc.europa.eu/sites/default/files/documents/covid-19-mobile-applications-contact-tracing.pdf

Nr	Spørsmål	Svar
2	Hva vil konsekvensene være dersom behandlingene ikke gjennomføres?	Smitteoppsporing er en lovpålagt oppgave etter smittevernloven § 3-6. Manuelle smittesporing gjøres allerede i dag. Denne manuelle prosessen er tidkrevende og usikker. Med automatisert kontaktsporing vil man få rask informasjon om personer som kan ha vært utsatt for smitte når en person har blitt bekreftet å være smittet av koronaviruset. Tiltaket vil dermed supplere den manuelle smittesporingen som gjøres i dag.

4.2 Formålsbegrensning og dataminimering

Personopplysningene som behandles skal være adekvate, relevante, nødvendige og begrenset til det som er nødvendig for formålene (Formålsbegrensning). Prinsippet om dataminimering innebærer å begrense mengden personopplysninger til det som er nødvendig for å realisere formålet.

Nr	Spørsmål	Svar
1	Gi en kort vurdering av om formålet med systemet eller registeret er i samsvar med behandlingsgrunnlaget. Det er uansett nyttig å vurdere om det er behov eller bruk av systemet som er utenfor behandlingsgrunnlaget, om det er noe i andre forskrifter eller lover som begrenser formålet, eller om det er noe som er utfordrende sett opp mot rettsgrunnlaget. Angi også om rettslig grunnlag gjelder utlevering i tillegg til egne formål, hvilket er tilfelle for helseregistrene.	Som nærmere beskrevet overfor er Smittestopp-appens formål å bidra til å forebygge og stoppe utbredelse av covid-19 gjennom rask oppsporing av personer som kan være smittet av koronaviruset, og formidling av råd til disse. Det rettslige grunnlaget for behandling av personopplysninger er samtykke, ref. personvernforordningen artikkel 6 nr. 1 bokstav a) jfr. Artikkel 9 nr. bokstav a). Samtykke setter dermed rammer for hvilken behandling av personopplysninger som kan gjøres. Dersom behandlingen endres, vil nytt samtykke måtte innhentes. Videre vil MSIS forskriften sette rammer for hva opplysningene fra MSIS kan utleveres til, ref. MSISforskriften § 1-3 og § 4-5. Også utforming av løsningen med løpende sletting vil hindre at opplysninger brukes til andre formål.
2	Er det forholdsmessighet mellom de personopplysningene som samles inn og formålet med systemet?	Bruk av data og teknologi som digitale sporingsapper er anerkjent både av EDPB og EU Kommisjonen som et middel i kamp mot viruset. Mange land i Europa har igangsatt og tatt i bruk slike apper, da de har vurdert at dette er et effektivt verktøy for smittesporing. I vurderingen av forholdsmessighet må det legges vekt på at nedlastning av appen og videre bruk er frivillig. I

Nr	Spørsmål	Svar
		tillegg må brukere samtykke til å aktivere appen og til å utstede notifikasjoner. Den aktuelle løsningen er utviklet slik at det samles inn og lagres kun de absolutt nødvendige opplysningene for digital smittesporing (formålet). Løsningen registrerer ikke brukernes lokasjonsdata. Løsningen er en desentralisert løsning. Lagring og behandling av opplysninger om kontakter skjer kun på brukernes telefoner og ikke i en sentral server. FHI har ikke tilgang til disse opplysningene. Det skjer kun en overførsel av opplysninger fra brukers mobiltelefon dersom brukeren velger å verifisere seg som smittet via verifiseringsløsningen. I verifiseringsløsningen utveksles det kun opplysninger som er nødvendige for å fastslå at brukeren er smittet. Matchingen mellom kontakter og smittede skjer ved at kontakters telefoner gjør oppslag mot en backend som har diagnosenøkler. Heller ikke her skjer en sentralisert behandling av kontaktopplysninger.
3	Hvilke andre alternativer for å oppnå formålet med behandlingen har vært vurdert? Finnes det mindre personverninngripende alternativer for å oppnå det samme formålet? Hvilke alternativer har vært vurdert? Har en vurdert bruken av anonyme eller pseudonyme data?	Andre løsninger for digitale smittesporingsapper har vært vurdert, ref. Smittestopp Versjon 1. Denne løsningen (Smittestopp versjon 2) er det minst personverninngripende alternativet, da den ikke inneholder GPS data og er basert på en desentralisert løsning. I Smittestopp versjon 1 var bruken av GPS-data for smittesporing nødvendig på grunn av «sovende» telefoner. Denne utordringen er løst gjennom Google/Apple-APIet.
4	Beskriv hvilke variable (grupper) som samles inn og som har vært diskutert om er nødvendige og relevante for formålet? Beskriv eventuelle variabler som ikke samles inn og som har vært diskutert og konkludert med at de ikke er nødvendige og relevante for formålet? Beskriv hvorfor en ikke kan oppnå formålet selv om en samler inn mindre detaljerte, fortrolige eller sensitive personopplysninger?	Løsningen samler inn og lagrer kun de absolutt nødvendige opplysninger for digital smittesporing. Registrering av kontakter skjer via Bluetooth og lagres kun på brukers telefon. FHI eller andre har ikke tilgang til disse opplysningene. Registrering av elektroniske kontakter skjer i henhold til API utviklet av Google og Apple. Alle vedvarende kontakter med uavbrutt Bluetooth kontakt over en kort periode registreres. Det er en del av funksjonaliteten til Apple/Google-API og det er ikke mulig å endre på dette. Det at det samles opplysninger om alle kontakter innebærer at det registreres potensielle nærkontakter, men alle vil ikke være reelle nærkontakter med smittede. Dermed

Nr	Spørsmål	Svar
		registreres flere kontakter enn det som er nødvendig for å notifisere om nærkontakt og smitte. Det er på forhånd ikke mulig å si hvem som faktisk blir smittet, og da ikke mulig å avgrense hvilke kontakter som bør lagres for å gjøre det mulig å varsle. Alle disse kan utgjøre potensiell smittekilde og det er derfor nødvendig at appen registrerer alle disse elektroniske kontaktene. Omfang av potensielle kontakter avgrenses ved å sette krav til avstand /signalstyrke og tid/varighet på kontakt. Opplysningene om kontaktene er pseudonymiserte. Telefonene genererer kun en vilkårlig enhets-ID til eksponeringsnotifikasjon. For å sikre at disse vilkårlige ID-ene ikke kan brukes til å identifisere brukeren eller brukerens posisjon, byttes de hvert 10. eller 20. minutt. I utgangspunktet skal derfor ikke den enkelte bruker kunne utlede hvilke fysiske personer som er registrert. Det vil imidlertid i enkelte tilfeller være mulig å utlede identifikasjonen til den bruker som er testet positivt på covid-19 og som har valgt å notifisere sine kontakter. Dette vil gjelde i de tilfellene hvor en bruker, som mottar smittenotifikasjon, har hatt en eller få kontakter og er bevisst på det. Denne risikoen er gjort uttrykkelig kjent gjennom den informasjonen som gis i forbindelse med nedlastning av appen og i appens personvernerklæring. Verifisering gjennom ID-porten og oppslag mot MSIS er nødvendig for å bekrefte at brukeren som ønsker å notifisere sine kontakter faktisk er smittet. Når en bruker samtykker til verifikasjon og notifikasjon av sine kontakter, kan vedkommende samtidig opplyse om dato for symptomer (hvis aktuelt). Dette har betydning for hvilke brukere som skal motta smittenotifikasjon. Denne opplysningen er en del av metadata og krypteres deretter. Når en bruker har gjennomført en smitteverifikasjon lastes brukers diagnosenøkler for de siste dagene opp til backend. Formålet med en backend er å ha en sentralisert sett av diagnosenøkler slik at de øvrige brukeres telefoner kan gjøre oppslag mot disse diagnosenøkler for å finne en eventuell match og etterfølgende notifikasjon. Backend-en med

Nr	Spørsmål	Svar
		diagnosenøkler er nødvendig for at andre brukere/kontaktene kan motta smittenotifikasjoner. Alle nøkler er pseudonyme og det er ikke mulig for FHI eller andre å koble nøklene til en spesifikk bruker etter at nøkkelen er utstedt.
5	Er formålet definert slik at det samsvarer med forventningene til de registrerte?	Ja. Brukerne vil bli gitt informasjon før innhenting av samtykke til å aktivere appen og til å notifisere andre.

4.3 Lagringstid av data

Nr	Spørsmål	Svar
1	Vurder om personopplysninger skal lagres etter at formålet er oppnådd eller om og når opplysningene skal slettes, anonymiseres eller pseudonymiseres etter formålet er oppnådd. Noen av FHI sine løsninger har krav om minst 10 års lagringstid, mens andre (helseregistre) har krav om lagring til evig tid.	Personopplysninger skal ikke lagres etter formålet er oppnådd.
2	Hvor lenge det vil være behov for behandling av personopplysningene. Er det forhåndsfastsatte slettedatoer (spesifiser, og begrunn med tid for analyse, etterfølgende oppbevaring for dokumentasjon/arkivformål) eller tidsbegrenset, men uten fastsatt dato (angi kriterier for fastsetting av varighet).	Det vil være behov for løsningen, herunder behandling av personopplysninger, så lenge pandemien pågår. For å sikre at Smittestopp vedvarende er nødvendig og lever opp til dens formål, vil dataansvarlig ved hjelp av prosjektstyret (eller etterfølgende organisasjon) foreta kvartalsvise løpende evalueringer av appen og dens effekt, funksjonalitet og datakilder/datakvalitet på bakgrunn av utviklingen i smittespredningen i samfunnet, oppslutningen i befolkningen om appen og nasjonale strategier i Norge. Evalueringen bør også inneholde vurderingen av avsnitt 6 i DPIA om risikomomenter og tiltak sett i lys av risikobilde som foreligger på evalueringstidspunktet.
3	Vurder også om graden av tilgang til data kan variere over tid; f.eks at data som er under mottak og kvalitetssikring er mer tilgjengelig enn data som er ferdig kvalitetssikret eller flere år gamle	Ikke aktuelt.

5. De registrertes rettigheter

5.1 Samtykke

Dette punktet gjelder for de systemene hvor det skal innhentes eget samtykke eller benyttes opplysninger fra allerede innsamlede befolkningsbaserte helseundersøkelser.

Dersom det skal innhentes samtykke i for systemet/registeret se Retningslinje FO-JU-RE-005 *Samtykke* i forskningsprosjekter. Spesifiser og vurder prosess for innhenting av samtykke (se veiledning i retningslinjen):

☒ Systemet er basert på samtykke

GDPR artikkel 7 stiller generelle krav til samtykke: uttrykkelig, informert, dokumentert og frivillig. Beskriv prosessen for innhenting av samtykket nedenfor:

Det rettslige grunnlag for behandling av personopplysninger i løsningen er samtykke, ref. GDPR art. 6(1)(a) og art. 9(1)(a).

EDPB omhandler relevante rettslig grunnlag i Guidelines 04/2020 avsnitt 29, hvor det fremgår at: "Furthermore, the EDPB notes that the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent. When public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest, i.e. Art. 6(1)(e) GDPR."

EDPB anser imidlertid at andre rettslige grunnlag, som for eksempel samtykke, kan benyttes, ref. Avsnitt 32:"However, if the data processing is based on another legal basis, such as consent (Art. 6(1)(a))13 for example, the controller will have to ensure that the strict requirements for such legal basis to be valid are met."

Etter fortalepunkt 43 til GDPR bør ikke samtykke utgjøre et gyldig rettslig grunnlag for behandling av personopplysninger dersom det er en klar skjevhet mellom den registrerte og den behandlingsansvarlige, særlig dersom den behandlingsansvarlige er en offentlig myndighet og det derfor er usannsynlig at samtykket er gitt frivillig med hensyn til alle omstendigheter som kjennetegner den bestemte situasjonen. EDPB angir i Guidelines 05/2020 om samtykke, avsnitt 16 og 17, at offentlige myndigheter kan bygge på samtykke som behandlingsgrunnlag innenfor den juridiske rammen av GDPR dersom det etter forholdene vil være maktbalanse mellom den behandlinganansvarlige offentlig myndighet og de registrerte.

Samtykke er definert i GDPR art. 4 (11) som: "«samtykke» fra den registrerte enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende." I tillegg må samtykke oppfylle de vilkår som fremgår av GDPR art. 7.

Frivillig

Med frivillighet menes at brukere må ha en reell mulighet til å velge om de ønsker å samtykke til behandling eller ikke. Samtykke kan ikke benyttes som rettslig grunnlag i de tilfeller der det er ubalanse i styrkeforholdet mellom den behandlingsansvarlige og den registrerte. Dette var en del av vurderingene rundt Smittestopp versjon 1, der det ble trukket frem at «Gitt en uavklart og alvorlig situasjon kan enkelte føle seg presset til å delta, og det kan være vanskelig å sette seg inn i alle konsekvensene av å bli sporet på denne måten. Det vil derfor kunne oppstå en viss tvil om hvorvidt den enkeltes samtykke oppfyller de strenge kravene personvernforordningen for at et samtykke skal være gyldig i forordningens forstand.», ref. Kongelig resolusjon vedrørende Forskrift om digital smittesporing og epidemikontroll i anledning utbrudd av Covid-19 https://www.regjeringen.no/contentassets/116076d9a39b473a97d97474048e1fb0/kgl.-res.- 27.-mars-digital-smittesporing.pdf.

FHI har tatt opp samtykke som rettslig grunnlag i møter med Datatilsynet. I møtereferat fra møtet 14. august 2020 mellom FHI og Datatilsynet fremgår det at «Til det første punktet kommenterte Datatilsynet at samtykke som rettslig grunnlag for en behandling forutsetter at personvernerklæringen gjør det mulig for brukerne å forstå rekkevidden av hva man takker ja til. Dette henger igjen sammen med kompleksiteten i behandlingen, herunder hvilke type data som samles inn og hvor inngripende behandlingen er totalt sett. Datatilsynet presiserte at større inngrep medfører større makt-ubalanse mellom myndighetene og brukerne. Dersom inngrepet er mindre, er også risikoen for en slik makt-ubalanse mindre.» Videre har det vært en åpen debatt rundt Smittestopp versjon 1 og de personvernkonsekvensrettslige vurderingene, slik at borgerne er mer bevisste med hensyn til hva slike apper innebærer. Erfaringen fra Smittestopp versjon 1 viser også at mange valgte å avstå fra laste ned appen eller valgte å slette appen, uten at det fikk noen konsekvenser. Selv om det blir oppfordret til å ta appen i bruk, må de som ønsker det aktivt velge å gå inn i App Sstore, lese informasjon om behandlingen av personopplysninger i appen og deretter laste den ned, før de faktisk kan ta den i bruk. Brukere av appen vil til enhver tid ha mulighet til å trekke samtykket tilbake, og ved eventuelt påvist smitte vil brukere selv ha anledning til å velge om man vil varsle personer som man har hatt nærkontakt med og som kan være utsatt for smitte. Både plikter og rettigheter etter smittevernregelverket er upåvirket av nedlastning eller bruk av appen. Det er altså ikke tale om en medbestemmelsesrett eller valgfrihet som knytter seg til faktisk myndighetsutøvelse. Personer som ikke tar appen i bruk vil ha nøyaktig de samme rettigheter til informasjon og personlig smittevernveiledning, jf. bla. smittevernloven § 2-1, og de vil ha de samme pliktene til bla. å gi informasjon om hvem han eller hun kan ha overført smitten til, jf. smittevernloven § 5- 1, som andre. Tatt i betraktning at den valgte løsningen innebærer en løsning der personverninngrepet er redusert til et minimum samt erfaringene med Smittestopp versjon 1 synes kravet om frivillighet være oppfylt.

<u>Spesifikt</u>
Det følger av forordningen fortalepunkt 32 at samtykke skal omfatte alle deler av en behandling som utføres med henblikk på samme formål. Dersom det er flere formål med behandlingen, bør det gis samtykke til alle. FHI legger opp til samtykke i to trinn; ett samtykke ved nedlasting av app og ett nytt samtykke for å verifisere smittestatus ved å gjøre oppslag i MSIS for å varsle nærkontakter via app. Vi mener et slikt samtykke i to trinn virker som et hensiktsmessig rettslig grunnlag.

Spesifikt samtykke innebærer at det aktuelle samtykke som innhentes setter rammer for hvilken behandling som kan gjøres. Ytterligere behandling av personopplysninger enn det som fremgår av samtykket er ikke mulig. Det kan på lenger sikt være aktuelt med oppkobling mot EUs knutepunkt. I så fall vil nytt samtykke for denne behandlingen innhentes.

Informert og utvetydig
Datatilsynet understreker, ref. møtereferat fra møtet 14. august 2020, at «Før samtykke avgis, må brukeren ha fått utfyllende informasjon om hvilke data som samles inn, lagringstid m.m. Det er viktig å få frem at samtykke avgis idet brukerne laster ned appen. Vi legger til grunn at brukerne vil få dekkende informasjon før den enkelte eksplisitt gir sitt samtykke til den behandlingen av personopplysninger som den digitale smittesporingsløsningen legger opp til».

Et trinnvist samtykke og informasjon som FHI foreslår er en god måte å både forenkle informasjon samtidig som man tilrettelegger for mer detaljert informasjon til de som ønsker det. Vi undersøkte med Google/Apple om det er teknisk mulig å avgi et samtykke før man laster ned appen. Våre undersøkelser av den danske (Smittestop), den irske (TraceCovid) og den østerrikske appen (Stopp Corona) viser at alle appene gir informasjon før bruker velger å laste ned appen, men at selve samtykket med «godkjennerknapp», skjer etter at man har lastet ned appen. Appen blir aktivert (og innhentingen av opplysningene skjer) først når brukeren har trykket på «godkjennerknappen». Våre danske kollegaer bekrefter at det ikke er mulig å implementere (ePrivacy-)samtykket før nedlasting. Deres løsning er at 1) det linkes fra App Store/Google Play til deres privacy-tekst for appens hjemmeside og 2) noe av det første bruker blir møtt med når brukeren åpner appen er samtykke. Vi oppfatter at denne løsningen er innenfor Datatilsynets krav om at «samtykke avgis idet brukerne laster ned appen», og har ikke fått tilbakemelding om at så ikke er tilfelle. Vi har også engasjert advokatfirma Wikborg og Rein til å bistå oss med utforming av informasjons- og samtykketeksten(e). FHI vil også her legge vekt på klarspråk, universell utforming og tilgjengelighet for ulike målgrupper i samfunnet.

Bruker kan selv trekke tilbake samtykke del 1 når som helst ved å velge dette i egen fane i app. Det finnes ingen annen måte å trekke samtykke, siden det ikke er mulig å identifisere bruker uten tilgang til telefonen.

5.2 Informasjon om behandlingen - informasjonsplikten

Det må beskrives hvordan informasjon om behandling av personopplysninger vil gis til de registrerte. Informasjonsplikten gjelder for alle systemer uavhengig om det samtykkebasert eller basert på f.eks. data fra helsetjenesten.

Informasjonen gis på følgende måte(r):

☒ Informasjonsskriv i forbindelse med samtykke hvis relevant (vedlegges)

☒ Informasjon på nett

☐ Nyhetsbrev

☐ Brev

☐ E-post

☐ Individuell informasjon per e-post eller brev

☒ Sosiale medier

☐ Offentlig informasjonskampanje

☐ Annet, spesifiser:

5.3 Rett til innsyn, behandlingsbegrensning, retting, sletting og dataportabilitet

Nr	Spørsmål	Svar
1	Vurder hvordan informasjon til de registrerte gis om rettferdighet og åpenhet i behandlingen, og hvordan dataene om den enkelte behandles, brukes og lagres.	FHI vil gjennom appen (design) gi nødvendig informasjon til brukere om behandling av opplysninger i appen. Det vil bli lenket fra Google Play/Apple Store til nettsiden på helsenorge.no og/eller fhi.no der brukere kan lese mer om behandlingen av personopplysningene. Behandlingsgrunnlaget for behandling av personopplysninger er brukernes samtykke. Det vil bli lagt opp til to-delt samtykke. Første del gjelder behandling av personopplysninger på telefonen i forbindelse med kontaktregistrering. Bruker vil bli forelagt informasjon om den behandlingen og forespurt om samtykke til dette. Brukeren vil også få informasjon om at det vil bli innhentet ytterligere samtykke fra brukeren for verifisering av smitte og notifikasjon av kontaktene (del2). Andre del av samtykke vil bli innhentet før brukeren logger seg på ID-porten. I tillegg til ekstern informasjon på helsenorge.no og/eller fhi.no, vil det ligge desentralisert informasjon om samtykke og lenker på selve appen, slik at brukere alltid kan gjenfinne og lese informasjon, når brukeren ønsker det. Løsningen forutsetter at det gjøres oppslag mot MSIS. I MSIS behandles også personopplysninger om personer som ikke har lastet ned appen. Vi anser at informasjon om behandling av personopplysninger om MSIS som sådan faller utenfor opplysningsplikten knyttet til digital sporingsapp. Men for ordens skyld vil vi på helsenorge.no og/eller fhi.no også ha en lenke til MSIS https://www.fhi.no/hn/helseregistre-og-registre/msis/.
2	Vurder hvordan den registrertes rett til innsyn ivaretas gjennom informasjon,	Slik API fra Google/Apple er utformet er det ikke mulig for FHI å håndtere brukerens eventuelle henvendelser knyttet til innsyn eller sletting i opplysninger lagret på

Nr	Spørsmål	Svar
	manuelle rutiner eller tilgang til elektroniske tjenester for dette	telefonen. API-et er designet på den måten at det er ikke mulig for andre å få adgang til de data som ligger på telefonen. Dette er gjort av hensynet til å beskytte brukerens personvern. Innsyn i opplysninger som behandles i verifiseringsløsningen (ID-porten) er ikke mulig ettersom disse opplysningene lagres kun så lenge bruker har en aktiv tilkobling til løsningen. Så fort verifisering er gjennomført forkastes denne informasjonen. Innsyn i opplysninger som behandles i MSIS som sådan, vil bli ivaretatt på vanlig måte enten gjennom innsyn via helsenorge.no eller ved at den registrerte sender et skjema. https://www.fhi.no/div/personvern/til-allmennheten/rett-til-informasjon-om-innsyn-i-og/. Det er ikke mulig å gi brukere innsyn i deres diagnosenøkler i backend. Diagnosenøkler som finnes i systemet til enhver tid vil være lagret og tilgjengelig (de lastes tross alt ned på alle telefoner som har appen). Disse diagnosenøklene kan imidlertid ikke knyttes til enkeltbrukere. For å få dette til måtte man lagre kobling mellom hver diagnosenøkkel og et pseudonym i backend i 14 dager. Dette ville medføre betydelig større behandling av personopplysninger og er ikke ønskelig.
3	Vurder hvordan den registrertes rett til retting og sletting ivaretas, gjennom informasjon, manuelle rutiner eller tilgang til elektroniske tjenester for dette	Brukeren har selv rett til å slette personopplysninger som ligger på brukerens telefon. Dette gjøres ved at brukeren selv enten trekker tilbake samtykke om lagring av data på telefonen eller sletter appen. Dette kan også gjøres ved at brukeren manuelt sletter nøkler fra telefonen, men dette krever teknisk innsikt. Opplysninger på brukeres telefon slettes i tillegg automatisk fortløpende etter 14 dager. FHI har ikke mulighet til å slette opplysninger på brukerens telefon. Eventuelle anmodning om krav om sletting i MSIS, ref. helseregisterloven § 25 og personvernforordningen artikkel 17 vil bli håndtert på vanlig måte, ref. https://www.fhi.no/div/personvern/til-allmennheten/rett-til-informasjon-om-innsyn-i-og/ Det er ikke mulig å fjerne nøklene på server som ble sendt av appen fordi det ikke er mulig å binde nøklene til enhet som sendte dem. Alle nøklene fjernes fra

Nr	Spørsmål	Svar
		server 14 dager etter de ble sendt inn. Detter innebærer at en bruker som har samtykket til notifisering av sine kontakter (del 2 samtykke) og har gjennomført verifiseringsprosessen, ikke kan angre seg og stoppe at kontakter blir varslet når verifiseringsprosessen er gjennomført.
4	Har FHI mulighet til å rette feil i den registrertes opplysninger i systemet eller er en avhengig av oppdateringer fra annet sted? Refr at noen helseregistre er avhengig av å få oppdaterte opplysning fra andre aktører for å kunne rette opplysningene (f.eks HKR)?	Nei. Pga av utformingen av GAEN generelt er det vanskelig å rette opp i feilregistreringer. GAEN har definert en mekanisme for å sette diagnosenøkler til status «revoked», men dette er vanskelig å benytte seg av uten å samle inn og lagre mer data under verifisering og opplastning. Brukeren vil bli informert om manglende mulighet til retting. Opplysningene i MSIS kan rettes i henhold til egne retningslinjer: https://www.fhi.no/div/personvern/til-allmennheten/rett-til-informasjon-om-innsyn-i-og/
5	Dersom den registrerte ikke selv kan rette feil i egne personopplysninger, finnes det andre måter å gjøre det på (se tilsvarende i kap 2.6) ? Finnes det dokumenterte rutiner for retting av helseopplysninger i hht henvendelser fra den registrerte?	Nei, ref. overfor.
6	For de fleste av FHI sine løsninger er ikke den registrertes rett til dataportabilitet aktuelt, men i tilfelle det er relevant, vurder hvordan det ivaretas, gjennom informasjon, manuelle rutiner eller tilgang til elektroniske tjenester for dette.	Retten til dataportabilitet er ikke aktuelt.
7	For de fleste av FHI sine løsninger er det ikke automatiserte individuelle avgjørelser, herunder profilering aktuelt, men, men i tilfelle det er	Løsningen innebærer ikke at det gjøres automatiserte avgjørelser for den enkelte bruker i forbindelse med at brukeren mottar smittenotifikasjoner. Smittenotifikasjonen vil inneholde informasjon og

Nr	Spørsmål	Svar
	relevant, vurder hvordan forbudet ivaretas, gjennom informasjon, alternative funksjoner, manuelle rutiner eller tilgang til elektroniske tjenester for dette.	veiledning til brukere, ikke pålegg. Den som mottar en notifikasjon vil først bli registrert i MSIS når vedkommende har valgt å ta en covid-19 test.
8	Andre kommentarer	

Det forutsettes at registeret eller systemet har etablert rutiner for å kvalitetssikre dataene i systemet/registeret. Spørsmålene under gjelder retting av innholdet i registre på bakgrunn av henvendelser fra den registrerte.

I systemet er følgende virkemidler etablert:

☐ Kontaktinformasjon for registeret eller systemet– *i informasjonsskriv*

☐ Mal for standardsvar – *dette kan utarbeides ved planlagt tilbakemelding til deltakere eksempelvis om analyseresultat*

☐ Databehandler avtale med klausuler som sikrer de registrertes rettigheter til innsyn, retting og sletting – *kun aktuelt ved bruk av databehandler(e)*

☐ Annet, spesifiser under

5.4 Ivaretakelse av de registrertes friheter

Vurder hvordan de registrertes friheter er tatt hensyn til med tanke på Den europeiske menneskerettskonvensjonen (EMK)

Når det gjelder forholdet til den Europeiske menneskerettighetskonvensjon (EMK) vil de samfunnsmessige fordelene veie opp for de negative konsekvensene mht rett til privatliv. Sporingssystemet vil kunne supplere det manuelle sporingsarbeidet, gjøre at sporingen av smittede skjer raskere og mer presist.

Det er helt frivillig å ta appen i bruk og brukerne kan når som helst slette sine personopplysninger.

Kjernen i EMKs forbud mot diskriminering er at det ikke skal foregå forskjellsbehandling basert på eksempelvis kjønn, etnisitet og seksuell legning mv, uten en saklig og god begrunnelse. Løsningen er gitt en utforming og funksjonalitet som er ment å gjøre den enkel i bruk også for alle brukergrupper, herunder også eldre personer og personer med funksjonsnedsettelser. Alle brukere over 16 år kan installere appen. De registrertes tanke, tros- og religionsfrihet er ikke påvirket av behandlingsaktivitetene. Det samme gjelder for de registrertes rett til

å gi uttrykk for de meninger man ønsker å dele med andre (ytringsfrihet) – og til å la seg informere om andres tanker og ideer (informasjonsfrihet).

6. Personvern; risikoanalyse og tiltak

6.1 Medbestemmelse, åpenhet, forutsigbarhet

[Det skal gjøres en vurdering av risiko for de registrertes rettigheter og friheter. Deler av disse vurderingene er gjort allerede i tidligere kapitler i dette dokumentet, men nå skal en beskrive tiltak en mener bør iverksettes avhengig av alvorlighetsgrad. Vurderingen skal gjøres fra de registrertes perspektiv for hver risiko].

I: Uønsket hendelse/situasjon: Avklar potensielle konsekvenser for den registrertes personopplysningsvern for hvert enkelt risiko. Det er satt inn eksempler i tabellen nedenfor og angitt i hvilke kapitler dette allerede er blitt vurdert i dette dokumentet.

II: Alvorlighetsgrad: Anslå alvorlighetsgrad for hver risiko, særlig avhengig av hvilken inngripen en potensiell virkning har på den registrerte. **Minimal, betydelig eller alvorlig**

III: Vurdering av hvor problematisk denne uønskete hendelsen er for den registrerte.

IV: Tiltak: Legg inn forslag til tiltak, dersom det er behov for det.

Vurdering av potensielle uønskete hendelser/situasjoner knyttet til risikoer sett fra den registrertes perspektiv og identifisering av eventuelle tiltak. Tabellen under har lagt inn forslag til uønskete hendelser og forslag til svar som en kan benytte.

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
Den registrerte får mangelfull informasjon i forbindelse med avgivelse av e-privacy samtykke (se kap 5.2).	Betydelig	Det er klare krav til form og innhold på informasjon som må gis til borgerne før nedlastning og bruk av appen, jf. også krav til informasjon for gyldig samtykke. Kompleksiteten i løsningen gjør imidlertid at den er vanskelig å forklare på en enkel, tydelig og samtidig dekkende måte.	Risiko er forsøkt redusert ved at det gis utførlig og tilpasset informasjon til brukeren i forbindelse med at de avgir samtykke. For øvrig vil informasjon om behandlingen av personopplysninger til enhver tid være tilgjengelig for brukeren i personvernerklæringen som ligger lett tilgjengelig via lenke i appen.

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
Tilsidesettelse av frivilligheten	Betydelig	Det vil kunne oppstå utfordringer i forbindelse med frivillighet dersom arbeidsgivere krever at ansatte laster ned og benytter appen.	Som en del av kommunikasjonsstrategien i forbindelse med appen, bør myndighetene kommunisere at bruk skal baseres på frivillighet og ikke skal kunne pålegges
Den registrerte har manglende evne til å forstå konsekvensene av aksept til å dele informasjon om smittestatus om andre (fare for at noen identifiserer deg som smittet).	Alvorlig	Idet en smittet bruker gis mulighet til å dele opplysninger om smittestatus, og på denne måten varsle de han/hun har hatt kontakt med de siste 14 dagene, ligger en sjanse for at brukeren i noen tilfelle vil kunne identifiseres som smittekilde. Det understrekes at sannsynligheten for slik identifikasjon anses som liten, men det er ikke gitt at en bruker er tilstrekkelig forberedt på og forstår alle konsekvensene at egen smittestatus kan bli kjent.	Risiko er søkt redusert ved at brukeren - både før appen tas i bruk og ved innhenting av samtykke til å varsle kontakter - gjøres oppmerksom på at han/hun kan identifiseres som smittet av andre.
Fare for formålsutglidning – tilsidesettelse av prinsippet for formålsbegrensning i GDPR art. 5	Betydelig	Det er en klar forutsetning for appen at personopplysninger ikke blir brukt på individnivå til å f.eks. pålegge enkelte borgere restriksjoner, smitteverntiltak, eller foreta overvåkning av	Løsningen i smittestopp-appen er designet og utviklet slik at kontaktsregistreringene foregår lokalt på brukernes telefoner. FHI vil ikke ha

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
		enkeltindivider, f.eks. hva gjelder enkeltindividers etterlevelse av regler og pålegg.	tilgang til disse opplysningene. Risikoen for formålsutglidning er også redusert ved bruk av løpende sletting av data og organisatoriske tiltak i form av interne retningslinjer som skal sikre at opplysninger ikke vil behandles i strid med eller utover formålet og de registrertes berettigede forventinger ved det samtykket de har gitt og den informasjonen de har fått.
Fare for tilsidesettelse av prinsippet om dataminimering (mer data enn hva som er nødvendig og hva som er formålet).	Betydelig	Samler appen inn andre eller flere opplysninger enn hva som er nødvendig, vil det utgjøre en risiko for at brukerne ikke har den nødvendig forståelse av, og oversikt over, hvilke opplysninger som samles inn og behandles i løsningen.	Det ligger smittevernfaglige vurderinger bak hvilke opplysninger som er nødvendige for å foreta effektiv smittesporing, herunder også hvilke kriterier som tilsier hvem av brukernes kontakter som vil lagres i løsningen. Det er dessuten en desentralisert løsning. Det skjer kun en overførsel av opplysninger dersom brukeren velger å melde seg smittet via appen. I slike tilfeller utveksles kun opplysninger som er nødvendige for å bekrefte brukers identitet og smittestatus. Løsningen er utviklet slik at det ikke registreres opplysninger om brukeres lokasjon (GPS).

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
Risiko for unøyaktig data	Betydelig	Det kan spres feilaktige opplysninger gjennom løsningen - dels ved falske positiver; dersom det spres opplysninger om smitte feilaktig, og dels ved falske negativer; dersom appen ikke fanger opp at bruker har vært i kontakt med en smittet person.	Det vises til rapporten fra Simula om nøyaktigheten av Bluetooth rapportering, og gjennomført ROS. https://www.simula.no/sites/default/files/sammenligning_alternative_digital_smittesporing.pdf De smittevernfaglige vurderingene ligger bak kriterier for hva som bør utløse smittevarsel. Løsningen legger for øvrig opp til en verifisering av smittestatus ved oppslag i MSIS, og et slikt oppslag kan kun gjøres ved sikker identifisering via ID-porten.
Risiko for manglende oppnåelse av formålet	Betydelig	For at appen skal bidra til å forebygge smittespredning av covid-19, må appen bidra til å smittesporing gjennom kontaktregistrering og varsler til personer som potensielt er utsatt for smitte. Oppnåelsen av formålet forutsetter at en viss andel av befolkningen tar i bruk appen.	Kommunikasjon, markedsføring og informasjon ifm. utrulling av appen er tiltak for å sikre god oppslutning om løsningen.
Risiko for manglende opphør av behandlingen (pandemien er opphørt, men folk har ikke avsluttet appen).	Alvorlig	Det er lagt til grunn at appen skal legges ned og alle data slettes når formålet med Smittestopp-appen ikke lengre er aktuelt.	Det er angitt kriterier for sletting av løsningen i driftsmiljøer i forbindelse med at løsningen legges ned.

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
			Samtidig er det implementert løsning for løpende sletting av opplysninger. For at sikre at Smittestopp-appen vedvarende er nødvendig og lever opp til dens formål, vil dataansvarlig ved hjelp av prosjektstyre (eller etterfølgende organisasjon) foreta jevnlige vurderinger og evalueringer av appen.
Den registrerte får ikke innsyn i opplysningene (kap 5.3)	Alvorlig	Slik API fra Google/Apple og løsningen for øvrig er utformet er det ikke mulig for FHI å håndtere brukerens eventuelle henvendelser knyttet til innsyn.	Brukere blir informert om manglende mulighet til innsyn i opplysningene. Innsyn i opplysninger som behandles i MSIS som sådan, vil bli ivaretatt på vanlig måte enten gjennom innsyn via helsenorge.no eller ved at den registrerte sender et skjema. https://www.fhi.no/div/personvern/til-allmennheten/rett-til-informasjon-om-innsyn-i-og/.
Egnede måter for å trekke tilbake samtykke er ikke spesifikt innebygd i appen. (kap A og B, 1.2, 4.1, 5.1)	Alvorlig	Samtykke fra brukerne av appen må innhentes for å lovlig kunne innhente data. Brukerne har krav på muligheten til å trekke tilbake samtykke i appen, men det er en risiko knyttet til om dette ikke er synliggjort på tilstrekkelig måte. Dette kan føre til at brukere velger å ikke benytte appen eller at	Brukere har til enhver tid mulighet til å trekke tilbake sitt samtykke (del 1) gjennom egen funksjon i appen. Brukere kan ikke trekke tilbake sitt samtykke til å notifisere sine kontakter (del 2) etter at verifiseringsprosessen er

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
		samtykke innhentes uten at brukeren er bevisst på det, noe som kan gi uheldige konsekvenser i forhold til omdømme og det offentliges oppfatning av appen.	gjennomført. Dette vil fremgå av tilgjengelig informasjon.
Behandling av personopplysninger, herunder utsendelse av varsler, om eller til barn under 16 år.	Alvorlig	Se punkt 1.2. Det er ikke mulig å forhindre at også barn (under 16 år) tar appen i bruk, og det er heller ikke mulig å forhindre at mindreårige vil motta notifikasjoner om nærkontakt med en smittet. Det er mulig at det vil kunne forhindres at en mindreårig bruker varsler om sin smittestatus, men det kan ikke utelukkes, jf. redegjørelsen i punkt 1.2 ovenfor.	Informasjon ved nedlastning av appen vil være tydelig på at den har 16 års aldersgrense. Det bør også gjøres særskilt oppmerksom på at mindreårige ikke vil kunne varsle om smittestatus, da slik varsling forutsetter pålogging via ID-porten.

7. Informasjonssikkerhet; risikoanalyse og tiltak

7.1 Risikovurdering av systemets informasjonssikkerhet

Der hvor en bruker ekstern databehandler må en gjøre en vurdering av dennes DPIA og ROS, evt ekstern revisjon av denne.

Der hvor FHI utvikler og forvalter systemene selv, skal en følge retningslinje Metode for risikovurdering av informasjonssikkerhet (AD-UI-AR-008) og fylle ut risikomatrisen og identifisere nødvendige tiltak i hht AD-UI RA-001 Risikovurdering informasjonssikkerhet.

Risikovurderingen av system gjennomføres og vil bli oversendt PVO og lagret i P360 og er listet opp i kapittel 12 over vedlegg.

7.2 Tiltak informasjonssikkerhet

Se oppdatering av tiltak knyttet til informasjonssikkerhet i [rapport basert på AD-UI-RA-001 Risikovurdering informasjonssikkerhet].

Legg ved lenke til Rapporten og list den opp i kapittel 12 over vedlegg.

8. Samlet vurdering av personvernet

Utbruddet av covid-19 er en alvorlig hendelse som truer liv og helse. Utbruddet medfører at det er behov for å ta i bruk tiltak som ikke har vært benyttet før. Løsningen som er valgt for Smittestopp versjon 2 er basert på API utviklet av Google og Apple og har som formål å minimere personverninngrepet. Dette gjøres ved at opplysningene om brukeres kontakter registreres kun på brukers telefon og det er ikke mulig for andre (heller ikke for FHI) å få tilgang til disse opplysningene. Detter er således en desentralisert løsning. Det innhentes heller ikke GPS data.

Den største risikoen i løsningen er at den registrerte ikke forstår konsekvensene av aksept til å dele informasjon om smittestatus om andre (fare for at noen identifiserer deg som smittet). I noen få tilfeller vil brukeren kunne identifiseres som smittekilde. Andre alvorlige risikoer er at de registrerte ikke får utøvd sine rettigheter og at barn under 16 år kan motta notifikasjoner. Videre er det også risikoer forbundet med formålsutgliding, dataminimering og at få brukere laster ned appen.

Det vil imidlertid iverksettes tiltak for å begrense disse risikoene gjennom tekniske og organisatoriske tiltak, slik at restrisikoen knyttet til de registrertes rettigheter ikke blir høy. Brukere vil bli gitt informasjon om appens funksjoner og risikoene. Det vil bli innhentet samtykke fra brukere både før de aktiverer appen og igjen før de velger å notifisere andre. Det understrekes også at alle opplysningene som behandles i løsningen er kryptert og pseudonymest på en måte som gjør det veldig vanskelig å koble opplysningene til enkeltbrukere. Løsningen er videre utarbeidet i tråd med reglene om innebygget personvern (privacy by design og privacy by default) samt i tråd med retningslinjer fra Det europeiske Personvernrådet (EDPB) og EU kommisjonen om apper som benyttes til bekjempelse av covid-19 pandemien. Dokumentasjon for API er offentliggjort og FHI vil offentliggjøre kildekoden. Ytterligere beskrivelse og vurderinger av sikkerhetsmessige tiltak fremgår av ROS.

I tråd med vurderinger av forholdsmessighet og nødvendighet, er det etter en totalvurdering FHIs oppfatning at samfunnsnytten av sporingssystemet i vesentlig overgår de mulige ulempene for personene som velger å benytte Smittestopp versjon 2.

9. Involvering og drøftelser

9.1 De registrerte

Som utgangspunkt skal man innhente synspunkter på behandlingen fra de registrerte eller representanter for de registrerte når det er relevant. Dette kan eksempelvis være pasientforeninger, fokusgrupper, pasientombud, mv.

Synspunkter er innhentet: Ja/nei, begrunnelse:

Det er opprettet et eksternt fagråd for brukere - bestående av representanter fra ulike brukergrupper i befolkningen mtp spesielle behov og alder (20-30 år, eldre, ungdom, blinde og svaksynte, innvandrergrupper). Blant deltakerne er også kommuneoverleger i enkelte kommuner. Brukergruppen vil gi innspill på forhold som påvirker brukervennlighet og adapsjon i befolkning og innspill på utvidet funksjonalitet og forbedringer utover første versjon. Dette gjøres ved at gruppen inviteres til ukentlige demomøter. I tillegg er det opprettet et eksternt fagråd for teknologer, bestående av representanter fra Den norske dataforening (DND) og Tekna. De vil bidra med rådgivning ift teknologiske valg og løsninger underveis og bidra med råd og synspunkter knyttet til sikkerhetsarkitekturen. De vil inviteres til ukentlige arkitektmøter. I tillegg er det avholdt dialogmøter med Datatilsynet og utkast til DPIA/ROS, samt teknisk informasjon vil bli sendt til Datatilsynet for gjennomsyn og innspill.

9.2 Datakilden

Med datakilden menes den institusjon som sender dataene til FHI. Datakilden kan ha synspunkter på behandlingen, og eventuell kontakt med dem og innhentede synspunkter bør beskrives.

Synspunkter er innhentet: Ja/nei, begrunnelse:

Ikke aktuelt

9.3 Personvernombud

Personvernombudet skal involveres ved utarbeidelsen av personvernkonsekvensvurderinger, og synspunkter innarbeides.

Dette punktet skal fylles inn av personvernombudet

Personvernombudets vurdering av registeret eller systemet er følgende:

Personvernombudet tilrår at personvernkonsekvensvurderingen godkjennes. Vurderingen er etter personvernombudets oppfatning gjennomgående god og betryggende. Råd om å godkjenne vurderingen skjer på følgende forutsetninger:

Når det gjelder pkt. II deler personvernombudet synspunktet at samtykke er egnet behandlingsgrunnlag. Likevel vil personvernombudet knytte noen momenter til vurderingen som også gjelder pkt. V, 5.1 og pkt. IV 2.1, 4. Veiledningen fra EDPB forstår personvernombudet dit hen at primært grunnlag bør i utgangspunktet være annet enn samtykke: "When public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest, i.e. Art. 6(1)(e) GDPR".

Danmark har for øvrig valgt forskrift og har vurdert det slik: «For at skabe et solidt hjemmelsgrunnlag for løsning samt sikre en regulering af de øvrige databeskyttelsesretslige rammer for løsningen har Sunheds-og Ældreminersteriet fasat regler om behandlingen af personoplysninger i Smittestop-appen i bekendtgørelse nr. 9896 af 17. juni 2020 om behandling af oplysninger om elektronisk registrerede kontakter medhenblik på at forebygge og inddeæmme udbredelsen af Covid-19».

Både plikter og rettigheter etter smittevernregelverket er i utgangspunktet upåvirket av nedlastning eller bruk av appen. Det har imidlertid vært talt om at dette er en løsning som skal være et supplement til manuell (lovregulert) smittesporing, og det antas at det vil bl.a. fra politisk hold kommuniseres at nedlasting og bruk er svært ønskelig. Dette vil kunne oppfattes som myndighetsutøvelse hos noen brukere og det kan stilles spørsmål ved om det også vil kunne kjennes som om det er en tilknyttet medbestemmelsesrett. Dette igjen forholder seg til frivillighetsvilkåret for samtykke, som er godt beskrevet i vurderingen.
Likevel vil personvernombudet gjenta at samtykke er egnet, og at overnevnte utfordringer langt på vei kan løses med god og dekkende informasjon, kommunikasjon, samtykke og personvernerklæring.

Personvernombudet deler også de vurderinger som er gjort om alder og aldersgrense, se pkt. IV, 1.2, ref. også pkt. V, 5.4, 6.1 og 8. Gitt den to-delte løsning for appen med ett samtykke for å kunne bli varslet, og ett (senere i tid) samtykke for å kunne varsle andre dersom en selv er smittet, bes det likevel vurdert om ikke de under 16 år likevel kan benytte «del 1» og, dersom dette er ønskelig, at dette eventuelt informeres om tydelig.

For pkt. IV, 3.1 og datatilganger er det vist til ROS-en i sin helhet. Det bes vurdert om utdrag av det mest relevante her kan tas inn i vurderingen, av hensyn til at personvernkonsekvensvurderingens helhet og at den dermed kan stå mer på egne ben.

For pkt. V, 4.3 om lagringstid av data kan det på sikt vurderes å sette noen konkrete kriterier for når og hvor ofte en skal ta stilling til videre bruk av løsningen.

Når det gjelder samtykketekst og pkt. V, 5.1 foreligger bare utkast så langt og personvernombudet skriver følgelig ikke noe råd på det nå. Det forutsettes videre dialog om det og at endelig versjon forelegges ved anledning.

I tilknytning til pkt. 9.1 er det positivt at kommunal sektor er representert, jf. rollen som «smittesporer» i smittevernloven § 3-6.

Avslutningsvis minnes det om at saksnummer i P360 må oppgis og at lagring av vurderingen må følge FHIs rutiner for dette.

9.4 Forhåndsdrøfting med Datatilsynet

Skal Datatilsynet kontaktes for forhåndsdrøfting? Dette er aktuelt når registeret eller systemet innebærer høy risiko for personvernet.

Dette punktet skal drøftes med personvernombudet.

Konklusjon: nei.

10. Plan for implementering av tiltak

Oversikt over hvilke tiltak som skal iverksettes etter kapitel 6 og 7, samt andre tiltak (for eksempel utarbeide databehandleravtale):

Tiltak	Tidsfrist	Ansvarlig
Inngå nødvendige databehandleravtaler	Før behandling starter	Roger Schaffer
Ferdigstillelse av samtykketekstene og personvernerklæring	Før oppstart	Agnieszka Anna Zachariassen
Utarbeidelse av annet kommunikasjonsmateriell	Før oppstart	Kjetil Veire

10.1 Organisering av personvernkonsekvensvurderingen og ansvarsforhold

Systemeier og fagansvarlig for systemet (eventuelt med bistand fra fagavdeling, systemforvalter/IT og eventuelt juridiske avdeling) har gjennomført en personvernkonsekvensvurdering.

Følgende personer har deltatt i prosjektgruppen som har gjennomført personvernkonsekvensvurderingen:

Navn	Rolle/funksjon	Virksomhet
Sindre Møgster Braaten	Senioringeniør, utvikler	FHI
Pål Solerød	Informasjonssikkerhetsleder	FHI

Navn	Rolle/funksjon	Virksomhet
Lars Røstad		Netcompany
Agnieszka Anna Zachariassen	Jurist	FHI

11. Endringslogg

Loggen kan brukes til å holde oversikt over godkjente versjoner av DPIA slik at det kommer tydelig fram hva som har endret seg i prosjektet.

Versjon	Dato	Endring

11.1 Godkjenning

Dato	Versjon av DPIA	Godkjent av (henhold til fullmakt)
11.11.2020	Versjon 1	Ole Trygve Stigen

12. Vedlegg

Husk å legge ved dokumentasjon eller oppgi arkivreferanse

☐ Systemdokumentasjon

☐ Risikovurdering av informasjonssikkerhet

☒ Samtykkeerklæring og informasjonsskriv

☒ Personvernerklæring

☐ Informasjonsmateriell (evt link til nettside)