PERSONVERNKONSEKVENSVURDERING KORONASERTIFIKAT

I. Prosjektopplysninger	II.

System/registernavn: Koronasertifikat

Systemeier/dataansvarlig: Gun Peggy Knudsen

Fagansvarlig/Produkteier: *[Refr systemforvaltningsmodellen; dette er operativt ansvarlig for systemet/registeret i fagavdelingen] Roger Schäffer.*

Systemforvalter: *[Refr systemforvaltningsmodellen; det er ikke systemer som har egen systemforvalter] Knut Ellefsen*

Systemets tilhørighet (avdeling/klynge): Team B, Knut Ellefsen

Arkivnummer (P-360): 21/14200

Protokollnummer: 21

Innhold

A. Rettslig grunnlag for behandling av personopplysninger 4

B. Rettslig grunnlag for behandling av særlige kategorier av personopplysninger (for definisjon se retningslinje pkt 4) 6

1. Beskrivelse av personopplysninger i systemet 10

1.1 Formålet med behandlingen av personopplysninger 10

1.2 De registrerte i systemet 10

1.3 Kategorier av personopplysninger 13

2. Behandling av personopplysninger 14

2.1 Innsamling 15

2.2 Lagring 16

2.3 Helseanalyse/sammenstilling for kvalitetssikring og statistikkproduksjon 19

2.4 Gjenfinning 20

2.5 Tilgjengeliggjøring av individdata 21

2.6 Sletting 24

2.7 Lagringssted 24

2.8 Annen 25

3. Dataansvarlig, datatilgang og databehandlere 25

3.1 Datatilganger til systemet 25

3.2 Databehandler 28

3.3 Overføring av personopplysninger til andre land og/eller internasjonale organisasjoner 29

3.4 Adferdsnormer 30

4. Formålsbegrensning, dataminimering og lagringsbegrensning 31

4.1 Rimelighet 31

4.2 Formålsbegrensning og dataminimering 32

4.3 Lagringstid av data 36

5. De registrertes rettigheter 37

5.1 Samtykke 37

5.2 Informasjon om behandlingen - informasjonsplikten 37

5.3 Rett til innsyn, behandlingsbegrensning, retting, sletting og dataportabilitet 38

5.4 Ivaretakelse av de registrertes friheter 41

6. Personvern; risikoanalyse og tiltak 42

6.1 Medbestemmelse, åpenhet, forutsigbarhet 42
6.2 Tiltak personvern 48
7. Informasjonssikkerhet; risikoanalyse og tiltak 49
7.1 Risikovurdering av systemets informasjonssikkerhet 49
7.2 Tiltak informasjonssikkerhet 50
8. Samlet vurdering av personvernet og informasjonssikkerheten 50
9. Involvering og drøftelser 55
9.1 De registrerte 55
9.2 Datakilden 55
9.3 . Personvernombud 56
9.4 Konklusjon: 61
9.5 Forhåndsdrøfting med Datatilsynet 64
10. Plan for implementering av tiltak 64
10.1 Organisering av personvernkonsekvensvurderingen og ansvarsforhold 64
11. Endringslogg 65
11.1 Godkjenning 66
12. Vedlegg 66

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:

Behandling av personopplysninger som er nødvendig for utstedelse og verifikasjon av koronasertifikater for å lette fri bevegelighet i EØS (Europeisk koronasertifikat) er det rettslige grunnlaget smittevernloven § 4A-1 og midlertidig lov 19. juni 2020 nr. 83 om innreiserestriksjoner for utlendinger av hensyn til folkehelsen § 2 fjerde ledd andre punktum jf. GDPR artikkel 6 nr. 1 bokstav c (rettslig forpliktelse) og/eller bokstav e (oppgave i allmennhetens interesse), jf. nr. 3 samt artikkel 9 nr. 2 bokstav g om behandling av særlige kategorier av personopplysninger som er nødvendig av hensyn til viktige allmenne interesser.

For behandlingen av personopplysninger som gjelder nasjonalt koronasertifikat er det rettslige grunnlaget de nærmere reglene som åpner for og regulerer bruk av sertifikatet innenlands, jf. smittevernloven § 4A-2, midlertidig lov 19. juni 2020 nr. 83 om innreiserestriksjoner for utlendinger av hensyn til folkehelsen § 2 fjerde ledd andre punktum, covid-19-forskriften og forskrift om innreiserestriksjoner for utlendinger av hensyn til folkehelsen. Koronasertifikatet skal benyttes til å gi fordeler, ikke for å sette begrensninger. Fordelene vil knytte seg til de ulike smittevernrestriksjonene.

Fra 11. juni vil det bli lettelser i smitterestriksjoner ved fremleggelse av koronasertifikat jf. covid-19 forskriften § 4, § 4a, § 4c, § 4d og endringer i vedlegg D. 20. juni oppdateres bruksområder med kystcruise, jf. § 10a og bruk ved større arrangement, jf. § 13 e, samt mulighet for å forskriftfestebruk av koronasertifikat for særskilte smitteutsatte kommuner, jf. § 18 g og § 19.

I lovgivningsprosessen er det vurdert som nødvendig å trekke data fra MSIS og SYSVAK for å opprette et koronasertifikat. I denne prosessen er det vurdert at dette ikke vil være i strid med andre bestemmelser i helseregisterloven m.v.

EU-forordningene 2021/953 og 2021/954 om EUs digitale koronasertifikat for EU/EØS borgere og for borgere av tredjeland ble vedtatt 14.06.2021 og vil tre i kraft 1. juli og vare til 30. juni 2022, jf. artikkel 17 https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32021R0953&from=EN

Kommunen har ansvar for å utstede koronasertifikat etter anmodning fra innehaveren av et koronasertifikat eller dennes representant, jf. covid-19-forskriften § 5h.

☒ 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:

Se over under bokstav c,

FHI ønsker å tilgjengeliggjøre disse opplysningene via helsenorge.no, i et format som er i tråd med EUs Guidelines for et koronasertifikat. Dette gir borgeren mulighet til å laste ned opplysningene på et papir eller digitalt medium ved behov.

For personer som ikke kan eller vil benytte digitale løsninger, skal det tilbys sertifikat på papir. Tjenesten skal lanseres i flere trinn (hvorav trinn 1A, 1B, trinn 2 og trinn 3 er besluttet p.t.). I trinn 1A vil Helfo besvare telefonhenvendelser fra personer som ønsker koronasertifikat på papir, skrive ut dette ved hjelp av en egen webapplikasjon for formålet, og sende sertifikatet per post til folkeregistrert adresse. I trinn 1B vil Helfo besvare brev fra personer som ønsker koronasertifikat på papir, skrive ut dette ved hjelp av webapplikasjonen, og sende sertifikatet per post til opplyst adresse.

I trinn 2 tilpasses web-applikasjonen som benyttes hos Helfo og tilbys private helseaktører som allerede utfører korona hurtigtest. Det inngås individuell avtale med den enkelte aktør. Gjennom løsningen kan de private aktører skrive ut koronasertifikat til personer med felles hjelpenummer basert på gjennomgått hurtigtest

I trinn 3 utvides web-applikasjonen som brukes av Helfo med mulighet for å etter-registrere vaksiner som er gitt i Norge til personer uten norsk ID-nummer inn i SYSVAK. Aktuelle personer sender brev til Helfo med kopi av gyldig legitimasjon og vaksinasjonsdokumentasjon. Registreringen knyttes til felles hjelpenummer og ID-nummer på vedlagt legitimasjon.

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

Samtykke er nødvendig for at den registrerte skal sammenstille egne data inn i et koronasertifikat og laste dette ned på et papir/elektronisk dokument.

B. Rettslig grunnlag for behandling av særlige kategorier av personopplysninger (for definisjon se retningslinje pkt 4)

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:

[For administrative systemer blir det henvisning til arbeidsmiljøloven, bokføringsloven med videre]

☒ 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:

Se over under artikkel 6 bokstav c.

På bakgrunn av smittesituasjonen er det nødvendig at enkeltindividet skal kunne dokumentere vaksinasjon, immunitet eller negative test på en måte som aksepters nasjonalt og internasjonalt for å unngå smitterestriksjoner.

☒ 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:

Dette kan bli aktuelt dersom f.eks. enkeltindividet trenger opplysningene i et format som verifiserer opplysningene, på en slik måte at de kan benyttes for medisinske formål.

☒ 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:

Se over under artikkel 6 bokstav c. *På bakgrunn av smittesituasjonen er det nødvendig at enkeltindividet skal kunne dokumentere vaksinasjon, immunitet eller negative test på en måte som aksepters nasjonalt og internasjonalt for å unngå smitterestriksjoner.*

☐ 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:

[For administrative systemer blir det henvisning til arkivloven med videre]

☐ Den registrerte har gitt uttrykkelig **samtykke** til behandlingen av særlige kategorier av personopplysninger, jf. personvernforordningen artikkel 9 nr. 2 bokstav a**).**
[*Legg ved kopi av samtykkeerklæring og list den opp i kapittel 12 over vedlegg]*

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**?

☐ 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?

☒ 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?

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

☐ Omfatter systemet noen form **for automatiserte avgjørelser** for enkeltindivider?

☐ Innebærer systemet en **systematisk overvåking** av enkeltindivider?

Hvis **svaret er ja på to eller flere av spørsmålene** om et planlagt prosjekt/system/register er det sannsynlig at dere må gjøre en personvernkonsekvensvurdering. Dersom en behandling oppfyller færre enn to kriterier, kan det hende det ikke er behov for en konsekvensvurdering, men det avhenger også her av en konkret vurdering.

Se retningslinjen for personvernkonsekvensvurderinger FO-JU-RE-013, punkt 6, for mer veiledning.

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

Fyll ut resten av malen.

☐ Det er vurdert at det **ikke** er behov for personvernkonsekvensvurdering. Skriv inn begrunnelsen under. Dersom systemet bruker særlige kategorier av personopplysninger (ref. første avkrysning) skal PVO rådføres. Fyll deretter ut del III eller oppgi det rettslige grunnlag på annen måte, og send til godkjenner i ditt område:

[*F.eks: Systemet inneholder ikke sensitive personopplysninger. Systemet inneholder bestillinger om brukerstøtte/vaksine som ikke ansees som særlig sensitive opplysninger*.]

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 Strømstad Knudsen

IV. Beskrivelse av personopplysninger og behandling av disse

1. Beskrivelse av personopplysninger i systemet

1.1 Formålet med behandlingen av personopplysninger

Formålet med et koronasertifikat er å etablere et system for sikker og verifiserbar dokumentasjon av vaksinasjonsstatus, gjennomgått koronasykdom og testresultat. Formålet med behandlingen av personopplysningene er å kunne tilgjengeliggjøre et koronasertifikat for borgerne, som kan verifiseres av en kontrollør. Innbygger henter selv sitt koronasertifikat på helsenorge.no, ved å gi fullmakt til en annen person som henter dette, ringe saksbehandler ved HELFO for å få det tilsendt i posten eller gjennomføre test og utskrift hos en privat helseaktør. Kommunen skal kunne tilgjengeliggjøre koronasertifikat etter anmodning fra innehaveren eller dennes representant, jf. covid-19-forskriften § 5h.

Sertifikatet skal være i tråd med EUs Guidelines, slik at borgeren kan benytte sertifikatet for ulike behov i Norge og andre EU- og EØS-land, f.eks. krysse grenser uten karanteneplikt eller for å få lettelser i begrensninger på bakgrunn av et koronasertifikat. Det vil være borgeren som beslutter om et koronasertifikat skal opprettes, lastes ned og benyttes.

FHI er ikke dataansvarlig for bruken av et koronasertifikat. Kontrollør vil trenge et eget behandlingsgrunnlag og være behandlingsansvarlig for den behandlingen.

Alle formål et sertifikat skal kunne benyttes til i Norge er ikke endelig klarlagt, men det vil reguleres i lov og forskrift, jf. smittevernloven kapittel 4A og midlertidig lov 19. juni 2020 nr. 83 om innreiserestriksjoner for utlendinger av hensyn til folkehelsen § 2 fjerde ledd andre punktum, jf. covid-19-forskriften og forskrift om innreiserestriksjoner for utlendinger av hensyn til folkehelsen. Et koronasertifikat kan per 21. juni medføre lettelser i innreiserestriksjoner og lettelser i adgangsbegrensninger for større arrangementer og kystcruise.

1.2 De registrerte i systemet

[*Denne malen brukes for personvernkonsekvensvurdering av systemer, helseregistre, FHIs lovpålagte oppgaver innen blant annet smittevern- og beredskap, bistand overfor helsetjenesten og administrative systemer. Forskningsprosjekter har egen mal som denne malen er basert på og som også brukes av helseundersøkelsene.*]

☐ **Systemer med egen datafangst**

[De fleste systemene på FHI har egen datafangst basert på data fra helsetjenesten eller direkte fra den registrerte som i helseregistre. Beskriv utvalget av de registrerte i systemet]

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

Dette vil anslagsvis kunne være hele befolkningen fordi alle som ønsker et koronasertifikat vil kunne etterspørre det. Opplysningene hentes fra MSIS og SYSVAK via et API, etter at borgeren har ønsket et koronasertifikat.

Data fra MSIS for personer som er registrert med et prøvesvar etter en covid-19 prøve, både NAT-test, antigen hurtigtest og antistofftest og data fra SYSVAK for personer som er registrert med covid-19 vaksinasjon ihht. indikasjon og vaksinasjonsanbefalinger på oppslagstidspunktet, vil kunne få utstedt et koronasertifikat i Norge, etter til enhver tid gjeldende forretningsregler.

Det forventes at *ikke digitale brukere,* vil kunne være anslagsvis ca. 100 000 personer.
Løsning for test for personer med fødselsnummer eller d-nummer vil ikke være aktuell i Trinn 1 eller Trinn 2, da denne løsningen baserer seg på å sende sertifikatet i posten og validiteten på en test er begrenset til 24 timer.

Personer som oppholder seg i Norge som ikke har fødselsnummer eller d-nummer kan få gjennomført hurtigtest og få utskrift av koronasertifikat hos private helseaktører basert på felles hjelpenummer
Personer som ikke har fødselsnummer eller d-nummer, men som har mottatt koronavaksine i Norge kan få etter-registrert vaksinen hos SYSVAK og dermed får utskrift av koronasertifikat via Helfos brevløsning.

Alle som har fått utstedt et koronasertifikat i et EU- eller EØS-land vil kunne få koronasertifikatet kontrollert/verifisert i Norge.

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**

[De fleste registrene og enkelte andre systemer produserer helseanalyse og statistikk, og sammenstilles med andre datakilder for kvalitetssikring eller statistikk produksjon. Angi da hvilke datakilder en henter data fra]

☒ Sentrale helseregistre; SYSVAK og MSIS

☐ Helseundersøkelser (eksisterende); … *[Angi hvilke]*

☐ Kvalitetsregistre; … *[Angi hvilke]*

☐ Pasientjournal; … *[Angi hvilke institusjoner]*

☒ Folkeregisteret

☐ SSB; … *[Angi hvilke registre]*

☐ Internett

☐ Annet

Spesifiser datakildene og beskriv kobling dersom dette er relevant:

Data skal hentes ut fra SYSVAK og MSIS for å utstede koronasertifikat. Data utleveres til løsning for utstedelse av koronasertifikat.no via et API. API'et utveksler nødvendige data for å utstede koronasertifikatet og informasjon om status basert på et regelverk. Dette regelverket vil kunne sammenstille informasjon fra både MSIS og SYSVAK relevant for utstedelse av koronasertifikat. Ved ønske om å få tilsendt koronasertifikat hjem vil folkeregistrert adresse bli slått opp via personregisteret (PREG).

Ved ønske om å få tilsendt koronasertifikat til annen adresse vil det opprettes sak og gjort oppslag på innbygger i Helfo Public 360.

1.3 Kategorier av personopplysninger

[Kryss av for hvilke kategorier personopplysninger som vil behandles i systemet]

Personidentifiserbare personopplysninger

☒ Navn

☒ Adresse

☒ Fødselsdato

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

☐ 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:

For å utstede koronasertifikat så behandles følgende personopplysninger:

Fødselsnummer / D-nr / Felles hjelpenummer
Benyttes for å identifisere en person i systemene, hente data og utveksle data på tvers av forskjellige systemer.

Navn / fødselsnummer
Navn og fødselsnummer benyttes for å kunne sammenstille koronasertifikat med annen ID som dokumenterer identiteten til den som viser fram koronasertifikatet. Koronasertifikatet er ikke et ID-bevis, men er avhengig av å bli brukt sammen med annen dokumentasjon – og navn og fødselsnummer er den informasjonen som kan knytte disse to dokumentene sammen.

Navn / folkeregisterregistrert adresse
Vil kunne bli brukt hvis man ønsker koronasertifikat «sendt hjem». Adresse vil ikke vises på utstedt koronasertifikat. Hvis man selv henter koronasertifikat via Helsenorge.no vil ikke navn / adresse bli brukt for utstedelse av koronasertifikat.

Vergeerklæring

Vil kunne bli brukt hvis verge ber om utskrift på vegne av innbygger for å verifisere at verge har denne fullmakten. Fullmakten må være registrert i Helfos Public 360.

Informasjon om vaksinestatus og informasjon om prøvesvar
Det benyttes helseopplysninger for å kunne gi informasjon om vaksinestatus og / eller resultat av prøvesvar på utført covid-19-test. Dette er informasjon som benyttes for å vurdere om det kan utstedes gyldig koronasertifikat.

ID-nummer

Ved etter-registrering av vaksine for personer uten norsk fødselsnummer eller d-nummer som har mottatt koronavaksine i Norge, vil man ved registrering på felles hjelpenummer i SYSVAK legge til ID-nummer fra vedlagt legitimasjon for å styrke identiteten knyttet til felles hjelpenummer.

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?	Dette er strukturerte data som ligger i eksisterende helseregistre, SYSVAK og MSIS. De behandles på bakgrunn av at den registrerte ønsker et koronasertifikat.
2	Er det noe som er særlig inngripende ved måten personopplysningene samles inn (for eksempel ved hjelp av fingeravtrykk, kamera- eller lydopptak, eller sporing av en persons lokasjon, biometri)?	Etableringen av et koronasertifikat, baseres på innbyggers ønske. Opplysningene kommer fra lovbestemte registre, hvor innmelding av opplysningene har skjedd basert på helsepersonell sin lovbestemte meldeplikt, jf. helsepersonelloven § 37. Innmelding av opplysningene til registrene er derfor ikke frivillig.
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?	Data til et koronasertifikat trekkes fra SYSVAK og MSIS via et API. Det er kun data som er nødvendige for å etablere et sertifikat som trekkes ut.
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?	Utstedelse av koronasertifikat gjøres på bakgrunn av et ønske fra borger som ønsker å benytte seg av opplysninger allerede registrert for å ta del i goder som krever at man viser et koronasertifikat. Dersom borger ikke ønsker et koronasertifikat, vil borgeren kunne miste rettigheter i tråd med lov og forskrift.

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)	Et koronasertifikat kan etableres ved at innbygger logger inn på Helsenorge og etablerer et koronasertifikat selv/via fullmaktshaver eller innbygger kan ringe eller sende brev til Helfo for utsendelse av sertifikat via post. Data vil, på forespørsel fra innbygger, trekkes ut fra helseregistrene og via API leveres til løsning for utstedelse av koronasertifikat. Dataene lagres ikke i løsningen men tilgjengeliggjøres for innbygger som kan lagre sertifikatet etter eget ønske. Det finnes 3 løsninger som utsteder koronasertifikat: Helsenorge På Helsenorge.no kan innbygger logge inn, etablere og hente sitt koronasertifikat. Innbygger kan se en utskriftsvisning, som gjør det mulig for innbygger å skrive ut en papirversjon. Innbygger kan også lagre en kopi i sitt dokumentarkiv på Helsenorge. Det er ingen mellomlagring av koronasertifikat på Helsenorge utover det innbygger gjør på egne vegne Det vil ikke finnes en oversikt over hvem som har fått utstedt koronasertifikat. Henvendelse HELFO Innbygger ringer HELFO. Saksbehandler spør om fødselsnummer eller D-nummer. Det sendes spørring fra systemet til folkeregisteret som presenterer adresse på skjermen (lagres ikke) Ved sammenfallende data sendes det spørring til registre etter: Vaksinestatus, status på gjennomgått sykdom og testresultat. Data sammenstilles (lagres ikke i systemet) og tilgengelige sertifikater sendes til «sentral-

Nr	Spørsmål	Svar
		print» som printer, pakker og sender sertifikat til folkeregistrert adresse Innbygger sender brev til Helfo. Brevet skal inneholde fødselsnummer eller D-nummer, navn, kopi av gyldig identifikasjon med signatur (pass, nasjonalt ID-kort, førerkort eller bankkort med bilde), adresse sertifikatet skal sendes til og signatur. Brevet registreres som innkommende brev i public 360. Hvis alle opplysninger foreligger svares det innkomne brevet ut med et utgående brev gjennom Public 360. I forbindelse med utsendelse/lukking av saken lagres en versjon midlertidig i Public 360. Et automatisert slette-script sørger for at alle koronasertifikat eldre enn 30 dager slettes. Ved manglende opplysninger i brevmal eller manglende koronasertifikat besvares brevet med utgående brev fra public 360, uten lagring av helsedata, og saken lukkes. Personer uten fødselsnummer eller d-nummer møter hos privat helseaktør som utfører test og som har avtale med FHI. Personen identifiserer seg med gyldig ID, det opprettes et felles hjelpenummer og utføres hurtigtest. Felles hjelpenummer og testresultat registreres i MSIS. Det gjøres videre oppslag i web-applikasjonen på det opprettede felles hjelpenummeret og testresultatet printes på lokal printer. Testresultat eller koronasertifikatet lagres ikke hos den private helseaktøren. Private helseaktører har bare tilgang til å gjøres oppslag på felles hjelpenummer og vil ikke få svar på eventuelle oppslag på fødselsnummer eller d-nummer Personer uten fødselsnummer eller d-nummer som har mottatt koronavaksine i Norge sender brev til Helfo. Brevet skal inneholde navn, kopi av gyldig identifikasjon med signatur (pass, nasjonalt ID-kort, førerkort eller bankkort med bilde), kopi av vaksinasjonsbevis (må inneholde

Nr	Spørsmål	Svar
		navn, fødselsdato, vaksinedato, type vaksine og batch-nummer og være stemplet og signert av kommunen som har gitt vaksine) adresse sertifikatet skal sendes til og signatur. Brevet registreres som innkommende brev i public 360. Hvis alle opplysninger foreligger svares det innkomne brevet ut med et utgående brev gjennom Public 360. I forbindelse med utsendelse/lukking av saken lagres en versjon midlertidig i Public 360. Et automatisert slette-script sørger for at alle koronasertifikat eldre enn 30 dager slettes. Ved manglende opplysninger i brevmal eller manglende koronasertifikat besvares brevet med utgående brev fra public 360, uten lagring av helsedata, og saken lukkes.
2	Hvor og hvor lenge lagres personopplysningene? Brukes det ulike kriterier for lagringstid og i såfall hvilke for ulike typer personopplysninger? Lagringstiden skal beskrives og begrunnes (evt henvise til hjemmel for dette).	Personopplysningene i SYSVAK, MSIS og PREG lagres iht reglene som gjelder for disse registrene. Det opprettes ingen oversikt over hvem som har fått utstedt koronasertifikat. I forbindelse med utstedelse av koronasertifikat for ikke-digitale innbyggere, vil det skje et manuelt oppslag fra saksbehandler på Helfo på fødselsnummer eller d-nummer og fra private helseaktører på felles hjelpenummer. Dette logges og det lagres oversikt over hvilke fødselsnummer/d-nummer eller felles hjelpnummer operatøren har forespurt på. Ved henvendelse fra ikke-digitale brukere per brev registreres henvendelsen i Helfos public 360 og saksbehandlerens aktivitet i saken logges. Dette for å unngå snoking i registre. jf. helseregisterloven § 24. Ved hjelp av utskriftsløsningen blir koronasertifikat utstedt på papir og sendt til innbygger. Skatteetaten, som utfører print, sletter data automatisk etter 70 dager.

Nr	Spørsmål	Svar
		Innbygger kan selv lagre utstedt koronasertifikat ved å: • Lagre dokument i Helsenorge.no • Lagre utskriftsversjon av koronasertifikat på egen lokal enhet (telefon eller pc) • Ta skjermkopi av koronasertifikat på mobilen • Skrive ut koronasertifikat på papir Lagringstiden for disse koronasertifikatene som innbygger selv lagrer er inntil de blir destruert. På koronasertifikatet oppgis en «gyldig-til» dato.
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.	FHI lagrer ikke Koronasertifikatet, det er innbygger som kan lagre og eventuelt slette koronasertifikatet. For trinn 1B løsning for ikke-digitale brukere per brev, lagrer Helfo koronasertifikat midlertidig i forbindelse med utsendelse av brev til innbyggere per brev. Dette for å kunne gjennomføre rutinen mest mulig automatisert og kunne spore hendelsen på en hensiktsmessig måte i koronasertifikatets levetid på 3 måneder.
4	Er det utarbeidet rutiner for sletting?	Det er opprettet en automatisert sletteprosess. Et automatisert slette-script i Public 360 sletter forløpende alle koronasertifikat eldre enn 3 måneder fra public 360. Aktiviteten utført av operatør vil fremdeles kunne spores.

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	Nei, Koronasertifikatet etableres basert på vaksinasjonsstatus fra SYSVAK eller testresultat fra MSIS, eller ved en kombinasjon (sammenstilling) av informasjon fra SYSVAK og

Nr	Spørsmål	Svar
	helseanalyse eller håndtere beredskapssituasjoner (f.eks utbrudd av smittsomme sykdommer)?	MSIS. Utover etablering vil det ikke skje sammenstillinger
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)…	N/A Løsningen «ikke-digitale innbyggere – koronasertifikat» benytter folkeregisteret for å validere innringer samt hente folkeregistrert adresse som sertifikatet sendes til. Ved henvendelse fra verger brukes public 360 får å verifisere at verge har rettigheter til å be om koronasertifikat på vegne av innbygger SYSVAK og Labdatabasen brukes for å hente innringer koronasertifikat. Se svar 1 under punkt 2.2.1
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)	N/A
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 ?	N/A
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.	N/A

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).	Det finnes ikke et sentralt register over koronasertifikat.

2.5 Tilgjengeliggjøring av individdata

Nr	Spørsmål	Svar
1	Tilgjengeliggjøres det personopplysninger til andre i eller utenfor virksomheten? Dette samt spørsmål 2, 3 er relevant for helseregistre og helseundersøkelser.	Ja, personopplysninger, inkl. helseopplysninger, tilgjengeliggjøres til innbygger selv via Helsenorge.no, via Helfo eller privat helseaktør. Ved kontakt med helfo kan saksbehandler på spørsmål fra innringer velge og åpne sertifikatet i løsningen for å se dette. Ved kontakt med privat helseaktør printes koronasertifikatet ut på lokal printer umiddelbart etter registrering i MSIS og utleveres over disk til person uten fødselsnummer eller d-nummer. Kommunene skal kunne skrive ut et koronasertifikat etter anmodning fra innbygger, jf. covid-19-forskriften § 5h. På anmodning fra innbygger, og med innbygger fysisk til stede, gjør saksbehandler oppslag på personens fødselsnummer, d-nummer eller felles nasjonale hjelpenummer. Personen skal identifisere seg med gyldig ID (pass, nasjonalt identitetskort eller gyldig førerkort). Etter oppslag vil saksbehandler få oversikt over personens navn og fødselsdato, samt tilgjengelige koronasertifikat for utskrift. Detaljer i koronasertifikater vil ikke være synlig ved oppslag. For detaljer, se bilde under vedlegg 12 – Prosessflyt kommuner.
2	Hvordan tilgjengeliggjøres personopplysningene – beskriv fort?	Se systemdokumentasjon og ROS og tegning av dataflyt
3	Hvordan er mottakere av personopplysninger identifisert og dokumentert (for eksempel ansatte, databehandlere, tredjeparter, eksterne virksomheter osv.)?	Innbygger selv identifisert ved innlogging i ID-Porten på sikkerhetstnivå 4. Saksbehandlere i Helfo, kommuner og hos privat helseaktør identifiseres gjennom tilgangsstyring og Whitelist. Helfo og den enkelte helseaktør har egen organisasjonsstyring for å kunne skille hvilken organisasjon den enkelt saksbehandler tilhører.

Nr	Spørsmål	Svar
		Innbyggere som henvender seg til Helfo per telefon identifiserer seg gjennom å opplyse om fødsels- eller d-nummer som bekreftes mot registrerte opplysninger. Innbyggere som henvender seg til Helfo per brev indentifiseres gjennom å opplyse om fødselsnummer eller d-nummer, kopi av gyldig identifikasjon, samt signatur. Innbyggere som henvender seg til privat helseaktører, gjør det med personlig oppmøte og identifiserer seg med gyldig ID. Foreldre som henvender seg på vegne av barnet vil få direkte tilgang til sine barn på Helsenorge, men må identifisere barnet på lik linje som de identifiserer seg ved Helfo eller for helseaktør. For f.eks. turister som kommer og tar test, vil vi ikke kunne sjekke foreldreansvaret. Det må antas tilstrekkelig dokumentasjon på dette at de kommer med barnet på teststasjonen og at de her gyldig ID på barnet. For vurdering av tilgang til barn se gjerne notat om tilgang til koronasertifikat - Helsenorge Innbyggere eller dennes representant som henvender seg til kommunen og anmoder kommunen om å skrive ut et koronasertifikat. Innbygger eller dennes representant skal vise legitimasjon. Kommunens representant skal da via sikkerhetsnivå 4 logge seg på FHIs web-applikasjon. Her ser kommunens representant om det foreligger et koronasertifikat og kan skive dette ut. Det fremkommer ikke ytterligere personopplysninger enn navn, fødselsdato (som kommunens representant skriver inn) og hvilke koronasertifikater som foreligger for personen i web-applikasjonen. Se vedlegg 12, prosessflyt kommuner for detaljert informasjon om innsyn ved oppslag.

Nr	Spørsmål	Svar
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.	Koronasertifikatet opprettes og brukes av innbygger selv. Det er ingen deling av personopplysninger i systemet
5	Hvilke personopplysninger deles med hvilke avdelinger og hva er formålet med hver av disse delingene?	N/A For ikke-digitale innbyggere: HELFO • Fødselsnummer og folkeregistrert navn og adresse deles for å bekrefte innringers identitet • Kopi av gyldig identifikasjon med bilde og signatur deles for å bekrefte henvendelser per brev. Private helseaktører • Gyldig ID fremvises ved oppmøte Skatteetaten • Koronasertifikat sendes via API til sentralprint for automatisk utskrift, pakking og utsendelse av koronasertifikat til folkeregistrert adresse.
6	Hvilke eksterne virksomheter deles personopplysningene med (private, offentlige myndigheter osv)? Se tilsvarende spørsmål i kapittel 2.3	Deles med databehandlere, Helfo, NHN, og private heleaktører, Kommuner se pkt. 3.
7	Hvilke personopplysninger deles eksternt, for hvilket formål og med hvilke rettslige grunnlag? Se tilsvarende spørsmål i kapittel 2.3	Se punk 1.1. Nødvendige data for å tilgjengeliggjøre et sertifikat, basert på databehandleravtale med FHI. I tillegg kan kommunen etter anmodning fra innbygger skrive ut et koronasertifikat, jf. covid-19-forsrkfiten § 5h. Kommunen får tilgang til personopplysninger via en web-applikasjon.
8	Beskriv retningslinjer og praksis for tilgjengeliggjøring og kobling av data, samt eventuell	Ingen nye registre, kun uttrekk til innbygger. Se dataflyt.

Nr	Spørsmål	Svar
	mottak av data for kobling og hvordan en unngå skyggeregistre. Angi navn og nummer på relevante rutiner.	

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?	Innbygger skal slette sitt sertifikat. Sletting av data i MSIS/SYSVAK, må gjøres av primærkilden. Feilregistrerte vaksinemeldinger som er sendt elektronisk til SYSVAK skal korrigeres fra journalsystemet, på samme måte som vaksinen opprinnelig ble meldt. Feilregistrerte opplysninger som er registrert i SYSVAK-nett, kan slettes via SYSVAK-nett. Feilregistrerte opplysninger i MSIS må korrigeres av laboratorium/teststasjon som har sendt svaret, i tråd med eksisterende rutiner.
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?	Se pkt. 1 – endringer og slettinger må gjøres via primærkilden som har lagt inn data i registrene.
3	Finnes det rettsgrunnlag i lov eller forskrift som gir grunnlag for å nekte sletting?	Nei

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

*[Gi kort oppsummering av hvor dataene **lagres** og legg inn lenke til der systemdokumentasjonen er lagret. Dette vil også bli beskrevet i risikovurderingen av informasjonssikkerheten]*

Data om vaksiner og test lagres i Helseregister (Sysvak og MSIS)

Persondata (navn og fødselsdato) hentes fra personregisteret (PREG) og er lagret i PREG.

Koronasertifikatet som viser informasjon om vaksiner, test og persondata lagres ikke i Helsenorge, med mindre innbygger velger å lagre en kopi på eget grunnlag. Denne lagres da i innbyggers dokumentarkiv i Helsenorge.

Brukslogg og tekniske logger i Helsenorge logger/lagrer ikke personidentifiserende informasjon.

For ikke digitale innbyggere vil det foreligge en manuell prosess. Koronasertifikatet som åpnes i PDF format lagres midlertidig på saksbehandlers PC. PDF innehar da data om vaksiner, test og persondata. Det er innført rutiner for at PDF lagres i midlertidig mappe som automatisk slettes en gang i døgnet.

For ikke digitale innbyggere som henvender seg per brev vil det opprettes en sak i Helfos public360 på personen der det innkommende brevet og utgående brev lagres. I det utgående brevet lagres også koronasertifikatet midlertidig. Det er opprettet et automatisk slette-script som setter alle koronasertifikat eldre enn 3 måneder i Public 360.

Kommunene har ikke tilgang til å laste ned sertifikat som pdf, innholdet i koronasertifikatene lagres ikke lokalt på saksbehandlers PC, men de har anledning til å skrive ut koronasertifikatet. Kommunene har et selvstendig ansvar i forhold til sikkerhet knyttet til skrivere, herunder sikkerhet knyttet til skyløsning og sikker print i tilfeller der skriver ikke er i umiddelbar nærhet til saksbehandler som bruker løsningen.

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.

3. Dataansvarlig, datatilgang og databehandlere

3.1 Datatilganger til systemet

Dokumentet *[Navn og som vedlegges denne vurderingen i kapittel 12]* gir en beskrivelse av tilgangene til systemet for de ulike rollene internt og eksternt, hvem som har hvilke roller/tilganger, om tilgangen er

tidsbegrenset og siste gangen tilgangene ble kontrollert. Dette dokumentet er også viktig for å vurdere informasjonssikkerheten til systemet.

[Mal for beskrivelse av tilgangsgrupper(applikasjonsgrupper og roller) finner en på arbeidsrommet Digitalisering og IT (her) og det anbefales at IT bidrar til å fylle ut denne: eventuelt kan en bruke eksempelet under og lagre beskrivelser av tilgangene i eget dokument. Personnavn bør ikke legges inn i DPIA da det vil føre til at DPIA måtte oppdateres unødvendig hyppig..]

MSIS og SYSVAK er kilder for Koronasertifikatet og FHI er dataansvarlig for disse registrene. Datatilganger i SYSVAK og MSIS administreres av dataansvarlig, og er nærmere beskrevet i DPIA for henholdsvis SYSVAK og MSIS.

Funksjon/Virksomhet	Rolle/funksjon	Beskrivelse av tilganger	Type person-opplysninger
FHI	Dataansvarlig/Behandlings ansvarlig	Har ikke tilgang til Koronasertifikatet	[Direkte id/ Indirekte id/ Begge]
FHI	Fagansvarlig/ produktansvarlig	Har ikke tilgang til Koronasertifikatet	
FHI	Utvikler	Har tilgang til SYSVAK og MSIS for utviklingsformål.	Kan dekryptere direkte personidentifiserbare opplysninger, dekryptering logges.
NHN	Utvikler	Har tilgang til API for SYSVAK og MSIS på Helsenettet.	Har ikke tilgang til indirekte eller direkte personid.
HELFO*	Saksbehandler	Har tilgang på forespørsel fra innbygger	Navn, adresse og koronasertifikat
Private helseaktører**	Saksbehandler	Har tilgang til resultat av hurtigtest på forespørsel fra personer uten fødselsnummer eller d-nummer	Navn, fødselsdato, og koronasertifikat basert på test.
Skatteetaten	Forvalter preprint	Har tilgang til printfiler som en del av administrasjon og	Navn, adresse og

Funksjon/Virksomhet	Rolle/funksjon	Beskrivelse av tilganger	Type person-opplysninger
		forvaltningsoppgaven	koronasertifikat
Skatteetaten	Print operatører	Har tilgang til fysisk print under produksjonsprosessen	Navn, adresse og koronasertifikat
NHN	Systemforvalter	Har tilgang til løsninger og data som en del av sitt ansvar som driftsleverandør	Navn, adresse og koronasertifikat
Kommuner***	Behandlingsansvarlig	Har tilgang på forespørsel fra innbygger	Koronasertifikat

Angi hvem som kan tildele tilganger, hvilke rutine som følges og hvor ofte tilgangsgruppene gjennomgås (for eksisterende systemer).

*Tilgang til web-applikasjon tildeles saksbehandlere i HELFO med arbeidsoppgaver som innebefatter utskrift av koronasertifikat på forespørsel fra innbyggere. Tilgang vurderes og gis av nærmeste leder. Ved endrede arbeidsoppgaver eller opphør av arbeidsforholdet slettes tilgang til applikasjonen gjennom eksisterende rutiner ved HELFO.

Tilgang til Helfo public 360 gis til saksbehandlere gjennom eksisterende rutiner ved Helfo. Ved endrede arbeidsoppgaver eller opphør av arbeidsforholdet slettes tilgang til applikasjonen gjennom eksisterende rutiner ved Helfo.

** Tilgang til web-applikasjon for private helseaktører tildeles saksbehandlere tilknyttet den enkelte aktør. Saksbehandler oppretter felles hjelpenummer, gjennomfører hurtigtest og registrerer resultatet i MSIS etter gjeldende rutiner. Gjennom web-applikasjonen gjøres oppslag på felles hjelpenummer og koronasertifikat printes på lokal printer og overleveres over disk.

*** Tilgang til web-applikasjon tildeles koordinator i den enkelte kommune. Saksbehandler vil bare ha tilgang til løsningen via norsk helsenett, etter å ha logget seg på med e-ID på sikkerhetsnivå 4 og etter å ha blitt gitt personlig tilgang til løsningen. Det rettslige grunnlaget er covid-19-forskriften § 5h. Kommunen er pålagt å bistå innbygger i å få et koronasertifikat. Tilgang vurderes og gis av kommunens koordinator etter aksept av brukervilkår. Ved endrede arbeidsoppgaver eller opphør av arbeidsforholdet slettes tilgang til applikasjonen. Kommunen v/ koordinator har et selvstendig ansvar for å tildele tilgang til saksbehandlere med tjenstlig behov. Koordinator har også et selvstendig ansvar for å slette tilganger om det tjenstlige behovet bortfaller eller saksbehandler ikke lengre er ansatt i kommunen. FHI gjennomfører månedlig kontroll med gitte tilganger ved å sende oversikt til koordinator med aktive tilganger og etterspørre bekreftelse på at personer på listen har tjenstlig behov for tilgang. Det vil også utarbeidet logger som kartlegger

tilganger uten aktivitet for å styrke FHI´s tilgangsstyring. FHI´s administratorer av løsningen kan til enhver tid overstyre kommunens koordinatorer.

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
Helfo	*Databehandler utstedelse av koronasertifikat for ikke-digitale innbyggere*	*Norge*
Dr. Dropin	*Databehandler utstedelse av koronasertifikat over disk til personer med felles hjelpenummer*	*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/oppfylt:

☐ 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.

Helfo er databehandler for løsningen av ikke-digitale innbyggere og har bidratt gjennom utarbeidelse av databehandleravtale og tjenesteavtale. Dr. Dropin er databehandler for løsning for ikke-digitale innbyggere/Privat versjon og har bidratt gjennom utarbeidelse av avtale, inkludert databehandleravtale

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

Dette spørsmålet kan være relevant for systemer som også brukes for internasjonalt samarbeid, som f.eks knyttet til smittevernberedskapen. Angi om data som deles er anonyme eller indirekte identifiserbare.

[I utgangspunktet gjelder ikke dette tilgjengeliggjøring av data fra registrene. Registrene har ikke plikt til å tilgjengeliggjøring data til andre land/internasjonale organisasjoner, som ikke er EU organer. Men dersom registrene mener at det er relevant og ønsker at det vil bli vurdert av PVO bør det legges inn fritekstfeltet under]

☒ Ikke aktuelt – Gå videre til neste kapittel

☐ Personer/institusjoner i EU/EØS

☐ Tredjeland (utenfor EU/EØS)

☐ Internasjonale organisasjoner

I den grad personopplysninger skal overføres til **tredjeland** (utenfor EU/EØS) eller **internasjonale organisasjoner**, må det beskrives hvordan pliktene etter kapittel V i personvernforordningen skal oppfylles.

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 Adferdsnormer

I den grad det finnes adferdsnormer/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 adferdsnormer, og dette punktet er derfor foreløpig **ikke obligatorisk**.

Oppgi adferdsnorm dersom dette skal følges i behandlingen av personopplysninger:

Norm for informasjonssikkerhet i Helsesektoren.

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.	Regulering av koronasertifikat kommer i lov og forskrift se beskrivelse i kapittel 1.1. Det er flagget at et koronasertifikat vil medføre privilegier som setter frivilligheten til å anskaffe seg et koronasertifikat under press. Det vil derfor etableres lov og forskrift til 1.0 versjon av et koronasertifikat. Den registrerte er ikke pålagt å skaffe seg et koronasertifikat, men det kan være nødvendig for å vå visse privilegier. Det antas å være en forventing i samfunnet og at borgerne vil kreve koronasertifikat fra myndighetene, for å unngå smittevernrestriksjoner innenlands, ved grensepasseringer og i andre land. Departementet vurderer det som rimelig, og ikke urettferdig, at vaksinerte og personer som har gjennomgått koronasykdom, får visse lettelser i smitterestriksjoner. Lovgiver har sett det nødvendig at FHI tilrettelegger for en løsning der den registrerte kan få dokumentert de opplysninger som allerede eksisterer i sentrale helseregistre, fremlagt som et koronasertifikat. Lovgiver setter visse rammer for hva koronasertifikatet skal kunne brukes til og departementet må forholde seg til disse ved

Nr	Spørsmål	Svar
		etablering av forksrifthjemler som kan gi lettelser i smitterestriksjoner.
2	Hva vil konsekvensene være dersom behandlingene ikke gjennomføres?	Smittevernsrestriksjonene under pandemien er nødvendige, men inngripende for innbyggernes rettigheter. Et koronasertifikat vil kunne lette på disse restriksjonene for dem som ikke utgjør en smitterisiko for seg selv eller andre. Etableres ikke et koronasertifikat som skal kunne dokumentere status på vaksinasjon, immunitet eller negativ test, vil ikke disse opplysningene kunne verifiseres sikkert. Det vil stride mot lovgivers intensjon og mot EU-forordningene som kommer anslagsvis i slutten av juni. Både regjering og Storting har lagt til grunn at det er opplysninger fra MSIS og SYSVAK som skal benyttes til et koronasertifikat. Det er ansett nødvendig for å etablere en sikker og effektiv løsning for etablering av et koronasertifikat. Det kan være utfordrende å etablere et annen system som skal kunne verifisere slike opplysningene for borgeren. Borgeren vil måtte hente opplysninger fra primærkilden, som må kunne gi en tilstrekkelig verifikasjon i tråd med EUs Guidelines.

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.	Formålet med koronasertifikatet er i samsvar med behandlingsgrunnlaget og ble vurdert i lovgivningsprosessen for dette systemet som følger av lov og forskrift som beskrevet i kapittel 1.1.

Nr	Spørsmål	Svar
	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.	FHI skal kunne tilgjengeliggjøre et koronasertifikat til de som har krav på det. Det er eieren av et koronasertifikat, skal kunne bruke og tilgjengeliggjøre sertifikatet. Det er kun de som her et rettslig grunnlag for å be om et koronasertifikat som kan be om et koronasertifikat og verifisere det. Koronasertifikatet skal benyttes for å kunne gi fordeler til enkeltindividet, basert på smitterestriksjoner, ikke for å sette begrensninger. Konkrete krav til når koronasertifikat eller annen gyldig dokumentasjon av koronastatus kan benyttes, skal reguleres i covid-19-forskriften og forskrift om innreiserestriksjoner for utlendinger av hensyn til folkehelsen. Kravene bør knyttes til de ulike smitteverntiltakene. Koronasertifikatet er også nødvendig for å kunne implementere EØS-relevante rettsakter om koronasertifikat. Helseregisterloven § 19 d setter begrensinger for tilgjengeliggjøring av helseopplysninger fra MSIS og SYSVAK. «*Helseopplysningene kan ikke gjøres tilgjengelige for påtalemyndigheten eller til bruk for arbeidsgivere eller forsikringsøyemed selv om den registrerte samtykker*» Departementet bemerker i Prop 203 pkt. 3.3 siste avsnitt *at «denne bestemmelsen gjelder den dataansvarliges adgang til å utlevere opplysninger»*. … videre bemerker departementet at «*bestemmelsen ikke være i veien for at en person bruker utskrift fra for eksempel SYSVAK for å dokumentere overfor sin arbeidsgiver at han/hun er vaksinert. Å vise frem koronasertifikatet må vurderes likt*.»

Nr	Spørsmål	Svar
2	Er det forholdsmessighet mellom de personopplysningene som samles inn og formålet med systemet?	Ja. Forholdsmessigheten mellom personopplysningene og formålet med koronasertifikatet er vurdert i lovgivningsprosessen for dette systemet som følger av lov og forskrift som beskrevet i kapittel 1.1. På bakgrunn av at det for visse formål for bruk av et koronasertifikat ikke trenger å være nødvendig med detaljerte helseopplysninger er det utarbeidet et dataminimert koronasertifikat, som skal benyttes innenlands der det er tilstrekkelig dokumentasjon, f.eks. ved større arrangementer. I den dataminimerte versjonen vil kun deler av navn vises (første bokstav i fornavn og tre første i etternavn), samt vise om sertifikatet er grønt og gyldig eller rødt og ugyldig. Fullt navn og årsaken til gyldigheten, vaksinert, immunitet eller negativ test, vises ikke. Med fullt navn og fødselsdato har vi i praksis identifisert innbygger unikt, og har da person og geografisk plassering på et gitt tidspunkt. Med foreslått bruk mener vi at vi har tilstrekkelig identifisering av person og reduserer mengden persondata på avveie og persondata som behandles. Eksempel: • Kjetil Vam Lund kan det finnes en av • K. Lun* er det antagelig ganske mange av Dataminimeringen sikrer at dersom data skulle kommet på avveie, så ville man ikke kunne identifisert hvem sine data dette er. Legitimasjon må benyttes der det er nødvendig for sikker verifisering

Nr	Spørsmål	Svar
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 alternativer for å oppnå formålet med behandlingen er vurdert i lovgivningsprosessen for dette systemet som følger av lov og forskrift som beskrevet i kapittel 1.1. I tillegg til koronasertifikatet fastsatt i EU, er det opprettet en dataminimert løsning som skal kunne benyttes til innenlands bruk. Ved innenlands bruk er det ikke gitt at man trenger vise detaljerte helseopplysninger og det er laget en dataminimert versjon av koronasertifikatet for slik bruk. Det viser seg et behov for å kunne skille mellom beskyttet (vaksinert og immun) og negativ test til visse formål, f.eks. for å slippe innreisekarantene og kystcruise. Her vil det være behov for å vise EU-versjonen av sertifikatet.
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?	Vi følger de kravene EU har til informasjon i et koronasertifikat. Dette er nødvendig for å kunne fremvise et gyldig sertifikat i EU/EØS-land. For bruk i Norge til f.eks. større arrangementer, har vi etablert en dataminimert løsning, som viser grønn eller rød status. Det er de samme dataene som ligger bak den dataminimerte delen, men detaljerte helseopplysninger vises ikke i sertifikatet. Det fremkommer kun deler av navn, fødselsår, gyldighetsdato og rød/grønn status i den dataminimerte løsningen.
5	Er formålet definert slik at det samsvarer med forventningene til de registrerte?	Formålet med etableringen av et koronasertifikat er klar. Konkrete krav til når koronasertifikat eller annen gyldig dokumentasjon av koronastatus kan benyttes, vil reguleres i covid-19-forskriften og forskrift om innreiserestriksjoner for utlendinger av hensyn til folkehelsen. Kravene

Nr	Spørsmål	Svar
		skal knyttes til de ulike smittevernrestriksjonene, og vil kunne endres. Det er antatt at disse forskriftene kan skje raskt og kanskje uten høring. Endringene må skje innen rammene til smittevernloven og departementet har uttalt at koronasertifikatet bør brukes med klare begrensninger og på en måte som reduserer ulempene knyttet til bruken. Departementet bemerker i Prop. 203 at når samfunnet er gjenåpent, vil det ikke være aktuelt å bruke koronasertifikat utover eventuelle reiser utenlands. Nasjonalt skal koronasertifikat kun brukes for å gi mulighet til en raskere gjenåpning av samfunnet. Det innebærer at koronasertifikatet skal benyttes for å kunne gi fordeler, ikke for å sette begrensninger. Departementet foreslår i Prop. 203 at reglene om koronasertifikat skal gjelde i 6 måneder. Når ulike formål for bruk lanseres oppdateres dette på regjeringen sine sider. FHI vil også informere om dette på sine sider. FHI har en kommunikasjonsplan som er ment å holde de registrerte informert.

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.	Det er innehaver av et koronasertifikat som beslutter hvor lenge det skal lagres. Behovet for et koronasertifikat skal være midlertidig. Utgangspunktet er at den registrerte bestemmer selv om et koronasertifikat skal opprettes og når det skal slettes.

Nr	Spørsmål	Svar
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).	Behovet for et koronasertifikat skal være midlertidig. I prop 203 anslår departementet at regelverket skal gjelde i seks måneder. EU-forordningen har en varighet fra 1. juli til 22. juni 2022.
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 nedfor:

Legg ved kopi av samtykkeerklæring og list den opp i kapittel 12 over vedlegg.

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:

Hovedkanal for koronasertifikatet vil være helsenorge.no/koronasertifikat.no. Klarspråk er overordnet et av de viktigste virkemidlene for å gjøre de registrerte i stand til å få informasjon om koronasertifikatet uavhengig av språkforståelse, kognitive forskjeller og ressurser generelt. Medieomtale vil være viktig i formidlingen av koronasertifikatets formål, bruksområder mm. I tillegg legger vi opp til spørsmål og svar-tjeneste på chatbot på helsenorge.no, brukerstøtte på koronatelefonen 815 55 015, kampanjer om ulike sider ved koronasertifikatet, bruk av sosiale medier, flerspråklig kommunikasjon om viktigste temaer samt å sette grensekontroll og andre kontrollører av koronasertifikatet samt kommunene i stand til å gi riktig informasjon og brukerveiledning ved hhv. kontroll og endring av opplysninger.

Utarbeidet informasjonsmateriell skal vedlegges (eller lenke til informasjon på nett):

- https://www.helsenorge.no/koronasertifikat
- https://www.fhi.no/om/koronasertifikat/personvern/
- Flere ulike virkemidler er under arbeid og vil lenkes opp eller vedlegges etter hvert.

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

Hvilke virkemidler er etablert for å ivareta de registrertes rett til innsyn, innsigelser (behandlingsbegrensning), retting og sletting og (eventuelt) hvordan retten til dataportabilitet oppfylles, samt hvordan eventuelle krav som dataansvarlig mottar vil følges opp overfor databehandlere. Dette er spesielt relevant for helseregistre og andre systemer med helseopplysninger.

Instituttet har følgende retningslinjer og informasjon på nettsiden for å ivareta ta de registrertes rettigheter:

- Retningslinje for behandling av innsynskrav, retting og sletting i forskningsprosjekter (FO-JU-RE-014)
- RF-RD-AR-007 Begjæring om innsyn i eller retting, sletting eller sperring av helseopplysninger i lovbestemte helseregistre ved FHI.
- RF-RD-RE-007 Personvernrettigheter i de sentrale helseregistrene ved Folkehelseinstituttet.
- Kontaktinformasjon for innsynskrav på nettside: https://www.fhi.no/div/personvern/rett-til-informasjon-om-innsyn-i-og/
- *[Legg gjerne inn lenker til rutiner eller informasjon på nettsider for det spesifikke registeret eller systemet]*

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.	Informasjon finnes i personvernerklæringen og via fhi.no. Det er mye mediaoppmerksomhet rundt koronasertifikat og det står daglig om dette i avisen.
2	Vurder hvordan den registrertes rett til innsyn ivaretas gjennom informasjon, manuelle rutiner eller tilgang til elektroniske tjenester for dette	Innbygger kan få innsyn via Helsenorge. Det opprettes også en løsning for utstedelse av koronasertifikat for ikke-digitale brukere på HELFO. Her skjer det en manuell jobb og saksbehandlers navn, hvem hen slår opp på og hva slags informasjon de har tilgang til og tidspunkt logges. Bruker har rett til innsyn i disse dataene, jf helseregisterloven § 24 Innsynsretten i SYSVAK og MSIS reguleres via helseregisterloven og er omhandlet i DPIA for SYSVAK og MSIS og https://www.fhi.no/div/personvern/tilallmennheten/rett-til-informasjon-om-innsyn-i-og/
3	Vurder hvordan den registrertes rett til retting og sletting ivaretas, gjennom informasjon, manuelle rutiner eller tilgang til elektroniske tjenester for dette	Viser til DPIA for SYSVAK og MSIS

Nr	Spørsmål	Svar
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)?	FHI kan slette innholdet om den registrerte i systemet. Ved retting er avhengig av oppdateringer fra primærkilden. Viser til DIPA for SYSVAK og MSIS.
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?	Retting må skje i primærkilden, jf. DPIA for SYSVAK og MSIS, jf. retningslinjer og fhi.no https://www.fhi.no/div/personvern/til-allmennheten/rett-til-informasjon-om-innsyn-i-og/
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.	Dataportabilitet er ikke aktuelt. Uavhengig av dataportabilitet kan den registrerte selv laste ned koronasertifikatet eller skrive dette ut på papir.
7	For de fleste av FHI sine løsninger er det ikke automatiserte individuelle avgjørelser, herunder profilering aktuelt, men, men i tilfelle det er relevant, vurder hvordan forbudet ivaretas, gjennom informasjon, alternative funksjoner, manuelle rutiner eller tilgang til elektroniske tjenester for dette.	Det foreligger forretningsregler bak sammenstillingen av data for å avgjøre om den dataminimerte løsningen av et koronasertifikat er gyldig. Dette er en automatisk behandling av opplysninger, for å utstede en dokumentasjon av faktiske forhold. Av personvern hensyn begrenser man detaljerte helseopplysninger.
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)

Personopplysningene som behandles stammer fra kilder etablert med hjemmel i lover og forskrifter, og forholdet til EMKs bestemmelser om rett til privatliv og kommunikasjonsvern er vurdert og avveid mot samfunnsinteressen av Stortinget og Regjeringen i forbindelse med at lovgrunnlaget ble etablert, jf. Prop. 203 LS (2020-2021).

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. Et gyldig koronasertifikat kan gi enkeltindivider fordeler andre ikke har. Det er likevel slik at ingen skal kunne forskjellsbehandles på grunnlag av at de ikke kan fremvise et koronasertifikat, med mindre bestemmelser i eller i medhold av lov gir adgang til dette, jf. smittevernloven § 4A-2. Diskrimineringsvernet er nøyevurdert i Prop.203 LS (2020-2021), se spesielt pkt. 6.11 Diskrimineringsvernet. Noen grupper vil ha større utfordringer med å anskaffe seg et koronasertifikat enn andre. Det legges et stort arbeid i at alle skal kunne anskaffe seg et koronasertifikat, tross i ulike forutsetninger. Det vil etableres en digital løsning for etablering av koronasertifikat og en ikke digital løsning. Det vil f.eks. finnes unntak for å fremvise koronasertifikat for visse aldersgrupper.

De registrertes tanke, tros- og religionsfrihet er ikke påvirket av FHIs behandlingsaktiviteter. 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). Religionsfriheten er omtalt i høringsrunden til smittevernloven kapittel 4A. Departementet viser til i Prop. 203 at koronasertifikatet kan innebære et visst insitament til å la seg vaksinere, men at det ikke er et hensyn som begrunner sertifikatet. Tvert imot vil departementet fremheve prinsippet om frivillighet, noe som taler for at bruken av koronasertifikatet ikke må være for omfattende eller langvarig.

FHI vil være ansvarlig for etableringen av et koronasertifikat. Bruken skal reguleres i forskrift og det vil være andre aktører, med et eget behandlingsgrunnlag, som skal kontrollere et koronasertifikat. FHI er ikke dataansvarlig for bruken av et koronasertifikat.

Departementet anser hensynet til menneskerettighetene som tungtveiende når bruk av koronasertifikat skal vurderes, jf. siste avsnitt i pkt. 6.1.2. Det vil være Departementet som fastsetter bruken av et koronasertifikat.

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 hver 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**
Risiko: Manglende reell medbestemmelse			
Den registrerte har ikke et reelt valg om deltakelse (se i kap A og B, 1.2, 4.1, 5.1)	Minimal	Koronasertifikatet er regulert i lov og forskrift og ikke på samtykke. Den regististerte kan velge selv om det skal etableres et koronasertifikat, så fremt dataene foreligger. Det kan foreligge et press på å anskaffe seg et koronasertifikat, f.eks for å	God informasjon til innbygger. For de uten f. og d. nummer jobbes det fortsatt med en løsning.

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
		slippe karantenehotell i 10 dager. Etablering kan skje via Helsenorge, eller via Helfo for de ikke-digitale innbyggere eller de uten f. og d. nr. Løsningen for ikke-digitale via HELFO er ikke fullgod, da den ikke åpner for utstedelse av koronasertifikat basert på negativ test. Det er i dag begrenset hvilke lettelser man kan oppnå ved et koronasertifikat basert på test. Dette kan endre seg. Ved større arrangementer vil koronasertifikat basert på test være aktuelt. Her vil testing i regi av arrangør være et alternativ til koronasertifikat.	
Den registrerte får mangelfull informasjon (se kap 5.2)	Minimal	Det er stort fokus på informasjonskampanjer og koronasertifikat dekkes også daglig i mediebildet.	God informasjon til innbygger.
Den registrerte får ikke trukket seg fra prosjektet (kap A og B, 1.2, 4.1, 5.1)	Minimal	Det er den registrerte som selv bestemmer når koronasertifikatet skal destrueres. FHI lagrer ikke koronasertifikatet.	
Den registrerte får ikke vist frem et gyldig koronasertifikat.	Betydelig	Det er flere grunner for at den registrerte ikke får et koronasertifikat: 1.Den registrerte har ikke rett på et gyldig koronasertifikat. Den registrerte skal da heller ikke kunne vise frem gyldig	2.Informasjon til Innbygger om å sjekke status før koronasertifikatet skal benyttes 3.Rutiner for etterregistrering kommuniseres utad og ligger på fhi.no

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
		koronasertifikat. Dette er i tråd med intensjonen. 2. Data fra helsetjenesten har ikke kommet inn til FHIs registre eller er registrert inn feil. Det må estimeres at slike feil kan skje. Såfremt helsepersonell er gode til å registrere riktige opplysninger i rett tid, vil risikoen for at feil skjer være liten. Konsekvensen vil like fult kunne være betydelig for den registrerte. Det er dermed viktig at den registrerte raskt sjekker opplysningene i et koronasertifikat er korrekte og at dette skjer i god tid før f.eks. en grensepassering, slik at det vil være tid til å rette opp sertifikatet før det skal benyttes. 3.Utenlendsk vaksinasjon kan ikke meldes inn via SYSVAK, men kan etterregistreres basert på gitte rutiner, fordi dokumentasjonen ikke er god nok. Det vil etableres rutiner for etterregistrering av vaksiner i SYSVAK. Her tas det en konkret vurdering på hvem som har rett på etterregistrering og ikke. Dette skaper forutberegnelighet og det vil være full åpenhet rundt dette. 4.Verifikasjonsappen fungerer ikke.	4. Foreligger brukerveiledning for kontroll av koronasertifikat, som er testet og følges opp.

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
Behandlingen kan resultere i diskriminering eller tap av omdømme for den registrerte (kap 5.4)	Betydelig / Alvorlig	Dette kan skje ved at koronasertifikat viser ikke gyldig av ulike grunner, nevnt over. Eller fordi borgeren ikke får tilgang til Helsenorge av ulike grunner. Det foreligger en løsning hvor ikke-digitale kan ringe Helfo for å få et koronasertifikat. Det vil på grunn av postgang ikke være aktuelt for testresultater.	Jobber med å utvide løsningen på HELFO.
De uten samtykkekompetanse			
Formålsutglidning	Alvorlig	Personer uten rettslig grunnlag ønsker å ta i bruk koronasertifikat. Dette er ulovlig, men det er ikke utenkelig at det kan skje	Lett tilgjengelig informasjon om hvem som kan kontrollere et koronasertifikat. En god kommunikasjonsplan. Det vil også være mye informasjon om dette i mediabildet så lenge koronasertifikatet varer.
Risiko: Manglende reell åpenhet			
Forklarer ikke tydelig behandlingen eller forventet resultat av sammenstilling med andre datasett (kap 2.3, 2.5 og 2.6)	minimal	Det er informasjon om de tre delene; vaksine, negativ test og immunitet, samt om sertifikatet er «true» eller «false» samt dato for gyldighet, som vises i sertifikatet.	God informasjon til innbygger. Se personvernerklæring på https://www.fhi.no/om/koronasertifikat/personvern/ . Se kommunikasjonsplan på https://www.fhi.no/contentassets/32b6f777d7474486820d339724f3aa5f/vedlegg/dokumenter/aktivitetsplaner-for-kommunikasjon-koronasertifikat.pdf
Regelmotor i verifikasjonsappen	minimal	Regelmotoren virker ikke, gir uriktig resultat Vi må kunne gi meningsfull informasjon om logikken i	FHI må gi informasjon til borgerne og kontrollør.

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
		dataprogrammet. Vi må også informere om betydningen og de forventede konsekvensene av avgjørelsen. Det er den dataminimerte delen av koronasertifikatet som blir påvirket av dette. Den utvidede delen vil fortsatt kunne vises.	FHI må raskt kunne rette opp dersom man oppdager feil i regelmotoren.
Manglende forutsigbarhet			
Behandlingen er utenfor det den registrerte vil forvente (kap 2.1, 4.2,)	betydelig	Det er mange forventinger til et koronasertifikat. Denne DPIAen omhandler etablering av et koronasertifikat. Hvordan et koronasertifikat kan etableres er godt kommunisert på pressekonferanser, i media og tydeliggjøres på fhi sine sider.	God informasjon til innbygger. Se personvernerklæring på https://www.fhi.no/om/koronasertifikat/personvern/ . Se kommunikasjonsplan på https://www.fhi.no/contentassets/32b6f777d7474486820d339724f3aa5f/vedlegg/dokumenter/aktivitetsplaner-for-kommunikasjon-koronasertifikat.pdf
Det samles inn mer personopplysninger enn det som er nødvendig for formålet (kap 2.1),	minimal	Her er det jobbet iherdig for at det ikke skal behandles mer opplysninger enn nødvendig utfra EUs krav. Det er laget et koronasertifikat som ikke fremviser alt som et EU-sertifikat krever, som en dataminimert versjon til bruk i Norge der detaljerte helseopplysninger og fødselsnummer ikke er nødvendig.	Det grundig gjennomgått hvilke variabler som er nødvendige på et koronasertifikat. Sertifikatet må tilfredsstille kravene i EU. Det er i tillegg laget en datamimimert utgave, som vil kunne benyttes i Norge. Dataene i koronasertifikatet hentes spesifikt til koronasertifikatet fra et API.
Saksbehandler på løsning for ikke-digitale innbyggere misbruker tilgang til sensitive personopplysninger for	Betydelig / Alvorlig	Utro tjenere hos Helfo har tilgang til å søke opp opplysningene til innbyggere, og videre til å generere	Saksbehandlere har taushets-plikt og gjennomgår opplæring. Saksbehandleres telefonlogg kan monitoreres og

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
snoking eller økonomisk vinning		koronasertifikater (pdf). Disse sertifikatene kan misbrukes.	stikkprøver hvor man sjekker dette opp mot oppslag på innbyggere kan gjennomføres. Saksbehandlere med tilgang til public 360 monitoreres gjennom registreringer eller endringer de gjør i saken
Andre enn registrerte ringer inn til Helfo og ber om et koronasertifikat	Betydelig/alvorlig	Hvis et individ kjenner navn, fødselsnummer og folkeregistret adresse, vil vedkommende i teorien kunne bestille et koronasertifikat for den registrerte. Dette er ulovlig. Individet vil kunne få en bekreftelse på om registrerte kan få et koronasertifikat, men ikke detaljerte helseopplysninger om sertifikatet. En slik oppringing vil også kunne medføre at personer som ikke har bestilt et koronasertifikat kan få dette i posten. Det vil kunne skape frustrasjon, mistillit m.m. Det vil også være en risiko for at innringer forsøker å fange opp brevet som kommer i den registrertes postkasse. Individet vil da kunne tilegne seg andre sine helseopplysninger og et annet sitt koronasertifikat. Dette er ulovlig.	Informasjon ved oppringing til Helfo om hva man har rett på. Koronasertifikater sendes kun til folkeregistret adresse. Det vil logges når og av hvem et koronasertifikat utstedes fra, i den ikke-digitale løsningen, slik at den registrerte kan få vite når koronasertifikatet ble bestilt.
Andre enn registrerte sender brev til Helfo og ber om utskrift av et koronasertifikat	Betydelig/alvorlig	Hvis et individ kjenner navn, fødselsnummer eller d-nummer, har tilgang på kopi av gyldig identifikasjon og signatur, vil vedkommende i teorien kunne bestille et	Det vurderes at tiltak med kopi av gyldig identifikasjon og signatur reduserer risikoen for misbruk. Registrering i public360 sørger for at alle

I: **Uønsket hendelse/situasjon**	II: **Alvorlig-hetsgrad**	III: **Vurdering**	**IV: Forslag til tiltak**
		koronasertifikat for den registrerte. Dette er ulovlig. Individet vil kunne få en bekreftelse på om registrerte kan få et koronasertifikat, men ikke detaljerte helseopplysninger om sertifikatet. En slik henvendelse vil også kunne medføre at personen kan få tilsendt koronasertifikat til valgfri adresse oppgitt per brev. Individet vil da kunne tilegne seg andre sine helseopplysninger og et annet sitt koronasertifikat. Dette er ulovlig.	henvendelser per brev dokumenteres.
Saksbehandler på løsning for kommunene misbruker tilgang til koronasertifikatløsningen for snoking eller økonomisk vinning	Betydelig/alvorlig	Utro tjenere hos kommunen har tilgang til å søke opp opplysningene til innbyggere, og videre til å skrive ut koronasertifikater. Disse sertifikatene kan misbrukes.	Saksbehandlere har godkjent bruksvilkår, taushetsplikt og gjennomgår opplæring.

Klikk her for å skrive inn tekst.

6.2 Tiltak personvern

[Spesifiser tiltak for å håndtere risikoene for de registrerte og andre berørte personers rettigheter og berettigede interesser. Stryk det som ikke er relevant]

Uønsket hendelse	Tiltak	Tidsfrist	Ansvar
Det oppstår uklarheter knyttet til formål og rettslig grunnlag for bruk av koronasertifikatet.	Lovfeste presise formål, bruksområder, behandlingsgrunnlag og varighet med koronasertifikatet;	løpende	FHI
Det er uklart når og hvordan koronasertifikatet	Gjennomføre en kommunikasjons-kampanje til innbyggere og reisende	løpende	FHI

Uønsket hendelse	Tiltak	Tidsfrist	Ansvar
skal benyttes	om bruk av koronasertifikatet;		
Mange innbyggere mister rettigheter og friheter fordi de ikke kan benytte Helsenorge.	Etablere en analog kanal for å kunne bestille et koronasertifikat utenom Helsenorge; Første trinn er nådd. Det gjenstår personer med kode 6 og 7.	løpende	FHI
Utro tjener hos Helfo misbruker tilgang til korona-sertifikater	Bevisstgjøring, opplæring og stikkprøver som kan avdekke misbruk.	løpende	FHI

7. Informasjonssikkerhet; risikoanalyse og tiltak

7.1 Risikovurdering av systemets informasjonssikkerhet

Risiko- og sårbarhetsanalyse er gjennomført av løsningen, og for innenlands bruk er det identifisert en rekke risikoscenarier og tilhørende tiltak.

Risikobildet for Trinn 4 av koronasertifikatløsningen viser at informasjonssikkerhetsrisiko er totalt sett vurdert som akseptabelt, innenfor de tiltenkte bruksområdene. De mest relevante risikoområdene er:

- Det er uklarheter rundt presist formål, bruksområder, behandlingsgrunnlag og varighet med koronasertifikatet, både innenlands og ved grensepassering. Dette kan føre til ulike samfunnsimplikasjoner som for eksempel mistillit til løsningen, tilsiktet eller utilsiktet misbruk av løsningen og politiske eller tilsynsdiskusjoner.
- Kontrollørappen blir trolig lett tilgjengelig både i Norge og i utlandet. Misbruk av appen og kontrollørfunksjonen vil kunne føre til uønsket innsamling av sensitiv informasjon, profilering og et svekket tillitssystem.
- Innbyggere som ikke er digitalt aktive eller benytter seg ikke av Helsenorge av andre grunner får ikke tilgang til et koronasertifikat. En analog kanal for å kunne få tak i et papirsertifikat blir ikke etablert før at Trinn 4 kommer på plass. Dette kan føre til (midlertidig) forskjellsbehandling.

Det bør nevnes at risikobildet har høy usikkerhet av blant annet følgende årsakene:

- Praktisk bruk og formål med bruk av innlands koronasertifikat kan endres. Det er forventet at det kommer endringer eller utvidelser i bruk av innlands koronasertifikat

basert på smittetrykket. Det gjør at risikovurderingen ikke kan ta utgangspunkt i alle mulige bruksscenarier og relaterte risikopunkter og dermed kan være upresis.

- Risikovurderingen har blitt gjennomført parallelt med utvikling av koronasertifikatløsningen. Det har derfor kun vært mulig å ta utgangspunkt i dokumentasjon, opplysninger og kunnskap som har vært tilgjengelig under vurderingsperioden. Det gjør at risikovurderingen muligens ikke har fanget opp detaljer som er av betydning for risikobildet.

Det er identifisert tiltak knyttet til scenarier med middels og høy risiko. Med at koronasertifikatløsningen videreutvikles etter Trinn 3, er det mulig at risikoen kan endre for en fremtidig versjon av løsningen. Utover tiltakene nevnt i kap 6.2 anbefales det å utvide monitorering over kritiske prosesser rundt (digitale) sertifikater og nøkler.

Risikoanalyser blir utført for de ulike leveransetrinnene, og disse blir fortløpende publisert når de blir godkjent.

7.2 Tiltak informasjonssikkerhet

ROS-analysen lister opp tiltak knyttet til informasjonssikkerhet, ROS_koronasertifikat_trinn_4.

8. Samlet vurdering av personvernet og informasjonssikkerheten

Prosjektleder skal gjøre en oppsummering av personvern og personopplysningssikkerheten Se retningslinjen for relevante drøftingspunkter:

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 og smittevernrestriksjoner som ikke har vært benyttet før. Hensynet til smittevern må avveies mot andre interesser. Denne personvernkonsekvensvurderingen gjelder etablering av et koronasertifikat.

Personvernkonsekvensene ved et koronasertifikat må veies opp mot samfunnsnytten, herunder og behovet for å kunne dokumentere en smittestatus status for å slippe smittevernrestriksjoner. Et koronasertifikat vil utfordre personvernet på mange områder. Samtidig vil et koronasertifikat gi borgeren mulighet til å dokumentere en status som kan frita borgeren for smittevernrestriksjoner og reguleres i lov og forskrift. De mest grunnleggende vurderingene rundt lovlighet, rettferdighet og åpenhet er vurdert av lovgiver. Det samme gleder hvilke formål et koronasertifikat kan benyttes til. Det vil ikke være lovlig å benytte koronasertifikatet til andre formål enn det som er fastsatt i lov og forskrift.

Etter en helhetsvurdering anser FHI den utviklede løsningen for et koronasertifikat som forholdsmessig og at muligheten for å starte gjenåpningen av samfunnet basert på et koronasertifikat vesentlig overgår personvernulempene.

Lovgivning

Koronasertifikatet er besluttet opprettet av både Storting og Regjering og reguleres i smittevernloven kapittel 4A, covid-19-forskriften og forskrift om innreiserestriksjoner for utlendinger av hensyn til folkehelsen. Reglene er antatt å vare i seks måneder.

Dataminimering

Hvilke data som skal inngå i sertifikatet er i all hovedsak besluttet av EU, etter nøye vurderinger om dataminimering. For å sikre en sikker identifisering av borgeren vil det være et behov for at borgeren i tillegg fremviser gyldig legitimasjon. Dette er inngripende for borgeren, men vurdert at lovgiver.

Til innenlands bruk er det utarbeidet en egen dataminimert løsning. Det er de samme opplysningene som ligger til grunn i dette sertifikatet, men det vil kun vise første bokstav i fornavn og tre første i etternavn, samt vise om sertifikatet er grønt og gyldig eller rødt og ugyldig. Dette vil være tilstrekkelig til å indentifisere innbygger ved annen gyldig legitimasjon, men vil forhindre at borgerens personopplysning eksponeres dersom koronasertifikatet kommer på avveie. Den forenklede utgaven kan kun benyttes i Norge, og vil ha en QR-kode som viser færre helseopplysninger og andre personopplysninger enn det europeiske koronasertifikatet.

Medbestemmelse

Borgeren vil ha medbestemmelse i om et koronasertifikat skal opprettes og om borgeren ønsker å fremvise et koronasertifikat. Opprettelsen av et koronasertifikat skjer kun på bakgrunn av borgers ønske om å kunne dokumentere sin av vaksinasjonsstatus, gjennomgått koronasykdom (covid-19) og testresultat. Borger vil kunne ha et behov for å fremvise et koronasertifikat for å unngå smitterestriksjoner. Det er borger selv som beslutter om koronasertifikatet skal lagres, hvor det skal lagres og når det skal slettes. Folkehelseinstituttet lagrer ikke koronasertifikater.

Koronasertifikatet kan anskaffes ved å logge inn på Helsenorge.no. Her kan det vises i sanntid, lastes ned digitalt eller printes ut. Det er også mulig å få et Koronasertifikat via Helfo, dersom man ikke ønsker å benytte Helsenorge.no løsningen.

Bruksområder

Koronasertifikat vil kunne gi borgeren tilgang til lettelser i gjeldende koronarestriksjoner i henhold til de til enhver tid gjeldende regler i Norge og lettelser som andre EU/EØS-land tilbyr sine borgere på grunnlag av et koronasertifikat.

Hva koronasertifikatet kan brukes til er ikke endelig fastsatt. Det vil kunne skje flere og hyppige endringer i forskrift tråd med smittesituasjonen. Raske endringer kan være en utfordring for forutsigbarheten til når og hvor et koronasertifikat kan benyttes.

Bruksområdene til et koronasertifikat vil reguleres i covid-19-forskriften og forskrift om innreiserestriksjoner for utlendinger av hensyn til folkehelsen.

For å sikre god forutberegnelighet og åpenhet rundt bruken av et koronasertifikat vil være behov for en god kommunikasjonsplan. Kommunikasjonsplan er etablert i samarbeid med HOD, Hdir, FHI og NHN.

Riktigheten av dataene

Koronasertifikatet samler ikke inn nye opplysninger, men henter opplysninger i eksisterende registre (SYSVAK, MSIS og PREG) basert på et API. Derom dataene som kommer inn til MSIS er uriktige, vil det være en risiko for at et koronasertifikat ikke blir gyldig. Det er helt nødvendig at helsepersonell som har meldeplikt til MSIS og SYSVAK melder korrekte opplysninger i rett tid for at et koronasertifikat skal kunne opprettes. Dette er tatt inn i kommunikasjonsplanen. Det er også kommunisert ut at borgeren selv må sjekke koronasertifikatet sitt i god tid før planlagt bruk, for å påse at riktige opplysninger har kommet inn.

Kontroll av et koronasertifikat

Et koronasertifikat kontrollers ved at innbygger fremviser sin QR-kode til en kontrollør. Kontrolløren skal ha et eget rettslig grunnlag for å be om sertifikatet, og vil være dataansvarlig for kontrollen.

FHI har utviklet en egen applikasjon (skanner) basert på teknologi fra Google og Apple med funksjonalitet for å kontrollere at koronasertifikat er gyldig ved å skanne QR-koden i koronasertifikatet. Opplysningene som samles inn ved skanningen vises for kontrolløren, men de videresendes ikke og de lagres ikke i skanneren.

Vi vet ikke hvem som vil få et rettslig grunnlag for å kontrollere et koronasertifikat. Vi har derfor heller ikke satt begrensninger for hvem som kan laste den ned. Det betyr at alle i prinsippet kan laste ned verifiseringsappen og kontrollere andres koronasertifikater. Dette er ikke lovlig, men åpner en risiko for misbruk. Risikoen er forsøkt avhjulpet ved at de som laster ned verifikasjonsappen, må godkjenne brukervilkår. Her vil det fremgå hvem som kan benytte appen og hvem som er ansvarlig. Dersom det viser seg at det er få som vil få rett til å benytte appen, kunne man vurdert å regulere nedlasting av appen ytterligere.

I uke 27 ble appen utvidet med en regelmotor for å bistå kontrollør i å tolke om koronasertifikatet oppfyller norske krav.

Det ble implementert ny funksjonalitet hvor regelmotoren ble brukt for henholdsvis «Grensepassering» og «Innenlandskontroll». Dette ga appen mulighet til å tolke to forskjellige regelsett og angi om reglene var oppfylt eller ikke. Reglene for «Grensepassering» er relatert til hvilke krav, dokumentert i koronasertifikatet, som gir rett til lettelser i innreiserestriksjonene (typisk knyttet til antall vaksinedoser, tidsperiode siden gjennomgått sykdom, etc.) og kan endres dynamisk etter som reglene for innreise endrer seg uten å endre app'en. Tilsvarende vil «Innenlandskontroll» vurdere et sett regler som må være oppfylt for å oppnå lettelser i innenlandske smitteverntiltak.

Regelsettene vedlikeholdes i Verifikasjonsløsningens back-end og inneholder ikke persondata. I app'en vises hvilke regler som er oppfylt / ikke oppfylt på det enkelte koronasertifikat. Ved «Innenlands kontroll» må man aktivt søke opp resultatet av regeltolkningen etter å ha scannet koronasertifikatet. Ved «Grensepassering» vises disse automatisk ved scanning.

Ved lesing av norsk kontrollside valideres ingen regler (da kontrollsiden ikke inneholder medisinsk informasjon). Regelmotoren er kun i bruk ved lesing av koronasertifikat basert på EU DCC.

Det er kontrollør som er behandlingsansvarlig for denne prosessen og det opplyses om dette i bruksvilkårene til appen.

Informasjonssikkerhet
Det er 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. Detaljer om risiko-vurderinger finnes i ROS-analysen.

Ikke-digitale brukere

For å ivareta innbyggere med lav eller manglende digital kompetanse som ønsker å benytte seg av koronasertifikat er det utviklet et tilbud der de kan kontakte Helfo for bistand. Det er utviklet en frittstående web-applikasjon som gjennom API sender spørring basert på fødsels- eller D-nummer til PREG, SYSAVAK og Labdatabasen. Saksbehandler vil få et oversiktsbilde som viser folkeregistrert adresse og markerer om det finnes gyldig koronasertifikat basert på vaksine eller gjennomgått sykdom. Ved gyldig bevis sendes koronasertifikatene til print. Web-applikasjon er koblet til sentralprint fra Skatteetaten som ivaretar utskrift, pakking og utsendelse av sertifikatene gjennom en automatisert prosess. Det vedlegges automatisk et følgebrev som kort beskriver bruk av sertifikatene og innbyggeres innsynsrett i oppslag som er gjort på deres identifikasjonsnummer. Før dokumentet sendes til print har saksbehandler mulighet til å be om en pdf-versjon av gyldige koronasertifikat som gir mer detaljert informasjon. Dette krever en aktiv handling fra saksbehandlere og er vurdert som nødvendig for å kunne svare på eventuelle spørsmål innringer måtte ha samt ivareta brukere med folkeregistrert adresse i utlandet, da løsningen ikke støtter bruk av sentralprint for utenlandsk adressefelt.

Web-applikasjonen er tilgangsstyrt med en whitelist som vedlikeholdes gjennom eksisterende rutiner ved Helfo og pålogging med personlig bank-ID. Det er utarbeidet en personvernerklæring som informerer saksbehandlere med tilgang til applikasjonen om rutiner for logging og kontroll av oppslag som gjøres gjennom applikasjonen. Saksbehandlere signerer på taushetserklæring ved ansettelse i Helfo og instrueres om særlig taushetsplikt som følge av tilgang til applikasjonen.

Når innbyggere tar kontakt med informasjonstelefonen og ber om utskrift av koronasertifikat vil de bli opplyst om hvilken informasjon saksbehandler får tilgang til som følge av oppslaget før selve oppslaget gjennomføres.

Identifikasjonskontroll gjennomføres ved at innringer opplyser om fødsels- eller D-nummer.

- Basert på identifikasjonsnummer får saksbehandler opp pasientens folkeregistrerte navn og adresse
- Innringer vil bli bedt om å opplyse om navn og adresse, som saksbehandler kontrollerer mot registrert navn og adresse
- Saksbehandler skal ikke opplyse om eller bekrefte informasjon fra PREG
- Hvis opplyste opplysninger ikke stemmer med registrert navn og adresse henvises innringer til folkeregisteret og vil ikke få tilsendt koronasertifikat
- Koronasertifikat sendes til folkeregistrert adresse. Det vil ikke være anledning å avvike fra dette.

Når innbygger tar kontakt med Helfo per brev og ber om en utskrift av koronasertifikat vil de bli få tilsendt personvernerklæring sammen med koronasertifikatet.

Identifikasjonskontroll gjennomføres ved at innbygger opplyser om fødselsnummer eller d-nummer, legger ved fotokopi av gyldig identifikasjon, opplyser om oppholdsadresse og signerer brevet. Hvis noen av identifikatorene mangler vil henvendelse besvares per brev og koronasertifikatet utleveres ikke.

Det vil føres logging av oppslag fra web-applikasjonen gjennom eksiterende loggrutiner i SYSVAK og Labdatabasen. Følgende identifikatorer logges:

- Personidentifikator til innbygger det gjøres oppslag på
- Personidentifikator til den som gjør oppslaget
- Tidspunkt for oppslag
- Meldings id (hva var det som ble slått opp)
- Årsak

Det vil føres logging av oppslag og saksbehandling utført i public 360

- Personidentifikator til innbygger det gjøres oppslag på
- Personidentifikator til den som gjør oppslaget
- Tidspunkt for oppslag
- Meldings id (hva var det som ble slått opp)
- Det vil også logges opprettelse av saker og saksbehandling

Kommunens tilgang til web-applikasjon

Som følge av covid-19-forskriften § 5h skal kommunen kunne utstede et koronasertifikat etter anmodning fra innehaveren eller dennes representant. Det medfører at kommunen må kunne skrive ut koronasertifikat til de som møter opp på egnet sted hos kommunen. Det er utviklet en løsning for å gi kommunene tilgang web-applikasjon for ikke-digitale brukere. Det er utarbeidet et brev til kommunene for at de skal være kjent med ansvaret sitt.

Kommunen må delegere hvem som skal få tilgang til systemet. Den kommunalt ansatte som får tilgang må akseptere FHIs bruksvilkår for løsningen. I teorien kan den kommunalt ansatte som er gitt tilgang slå opp andre enn enkeltindividet som anmoder kommunen om å få utstedt et sertifikat. Det vil være brudd med taushetsplikten. FHI oppretter kommunen som egen organisasjon i løsningen og tildeler rollen som koordinator til den som er tildelt rollen av kommunen. Koordinator vil bare ha tilgang til løsningen gjennom norsk helsenett og må logge seg på løsningen med e-ID på sikkerhetsnivå 4. Koordinator kan deretter administrere egen organisasjon ved å gi og fjerne tilganger til medarbeidere med tjenstlig behov for å skrive ut koronasertifikat. Koordinator har bare tilgang til denne funksjonaliteten innenfor egen organisasjon. FHI kan til enhver tid overstyre koordinators rolle og tilganger.

Den enkelte saksbehandler som er tildelt tilgang fra koordinator kan har bare tilgang til løsningen gjennom norsk helsenett og etter pålogging med e-ID på sikkerhetsnivå 4. Gjennom bruksvilkår og opplæring skal den enkelte koordinator og saksbehandler bekrefte at de bare gjør oppslag på anmodning fra innbygger og bare når innbygger eller dennes representant, tilsvarende verge, er fysisk til stede. For hvert oppslag som gjennomføres må saksbehandler bekrefte i løsningen at oppslaget gjøres på anmodning fra innbygger og at legitimasjon er kontrollert. Kommunen har gjennom bruksvilkår et selvstendig ansvar for å påse at den enkelte etterlever dette.

Ved oppslag vil saksbehandler få tilgang til følgende informasjon om innbygger:

- Identitetsnummer som følge av kontroll av legitimasjon (fødselsnummer, d-nummer eller felles nasjonalt hjelpenummer)
- Innbyggers navn
- Type sertifikat innbygger har tilgjengelig for utskrift (nasjonalt koronasertifikat, Immunitetssertifikat/EU og/eller testsertifikat)

Kommunen har et selvstendig ansvar for å påse at innbyggers personvern ivaretas når tjenesten utføres og ved utskrift av koronasertifikat, herunder tilgangsstyring av printer og type printer.

Løsningen skriver automatisk ut et følgebrev med koronasertifikatene som beskriver fremgangsmåte for å be om innsyn i hvem som har hatt tilgang til innbyggers data gjennom løsningen.

Se også punkt 12. vedlegg

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:

Gjennom arbeid med utvikling av løsning for koronasertifikat, våren 2021, ble synspunkter fra de registrerte innhentet gjennom en rekke «fagråd». Det ble gjennomført flere møter i brukerråd og «teknisk fagråd» med informasjon om og fokus på personvern.

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:

Det har vært en Høring i forbindelse med lov prosessen, med over 10.000 høringsuttalelser. Det er også foretatt informasjonskampanjer rettet mot helsepersonell som melder inn opplysninger til SYSVAK og MSIS. Fagansvarlig for MSIS og SYSVAK har deltatt i prosjektet mot å etablere et koronasertifikat.

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:

RÅD FRA PERSONVERNOMBUDET I ANLEDNING PERSONVERNKONSEKVENSVURDERING FOR «KORONASERTIFIKAT»

Det er gjort en personvernkonsekvensvurdering for «Koronasertifikat».

Det følgende er et råd fra personvernombudet ved FHI etter FHIs mal for personvernkonsekvensvurderinger. Rådet gis med grunnlag i personvernforordningen artikkel 35 nr. 2.

Det presiseres at personvernforordningen ikke legger en godkjennelsesmyndighet til personvernombudet. Det er likevel antatt at rådet fra personvernombudet bør tillegges vekt ved en evt. godkjennelse av personvernkonsekvensvurderingen.

Personvernombudet har i dag fått forelagt et «utkast» til personvernkonsekvensvurdering, og det foreligger en ROS i ikke-endelig utgave.

Det er særlig sett på følgende forhold:

- Behandlingen av personopplysninger, herunder dataflyt
- Det rettslige grunnlag for behandlingen av personopplysninger
- De registrertes rettigheter
- Risikoanalyse og tiltak

Personvernombudets råd

Personverombudet tilrår at personvernkonsekvensvurderingen ikke godkjennes.

Tidspunkt for en personvernkonsekvensvurdering

Innledningsvis vil det presiseres at en personvernkonsekvensvurdering skal gjennomføres *før* en behandling av personopplysninger starter, jf. personvernforordningen art. 35. Her er det tilsynelatende behandlet person- og helseopplysninger allerede, ifølge regjeringen, NHN (HelseNorge) og siste dagers mediaoppslag. Dette kan i seg selv utgjøre et avvik etter art. 33. Dette bes vurdert av behandlingsansvarlig.

Behandlingsansvarlig

Plikten til å gjennomføre en vurdering påligger *behandlingsansvarlig*. Det er ønskelig å knytte kommentarer til dette. Selv om proposisjonen peker på FHI, bør en gjøre en selvstendig vurdering etter personvernforordningens art. 4 nr. 7. Det kan argumenteres for at både FHI, NHN eller HDIR er behandlingsansvarlig. Imidlertid er HDIR prosjekteier, styringsgruppen er ledet av HDIR, prosjektleder er HDIR og HDIRs samfunnsoppdrag ligger nærmere behandlingen av personopplysninger enn for eksempel FHIs. Dette er særlig relevant all den tid HDIR er HODs utøvende organ og det ikke foreligger noen konkret regulering p.t. utover en mindre, upresis og lite konkret forskriftsadgang i smittevernloven § 4-A 1. Etter personvernombudets oppfatning burde HDIR være behandlingsansvarlig idet det er de som «bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes». Dermed burde HDIR gjennomføre en personvernkonsekvensvurdering for behandlingen.

Behandling

Det vil da også være naturlig å knytte noen kommentarer til det nærliggende begrepet *behandling.*

Så vidt ombudet har forstått er NHN ansvarlig for den registrertes kopi på grunnlag av samtykke til vilkår, og tar vare på kopien på vegne av den registrerte. NHN er også ansvarlig for nedlasting av koronasertifikat til Helsenorgeappen slik at den kan brukes offline (valg fra registrert basert på bruksvilkår for appen, og første gangs bruk av appen samtykkes det til evt. nedlasting eller ikke).

FHI er ansvarlig for datakildene MSIS og SYSVAK, samt etableringen av sertifikatet.

Det følger av personvernforordningen at en eller flere operasjoner med likelydende formål skal anses som *en* behandling. Dette gir ryddige forhold, det ansvarliggjør, hindrer pulverisering av ansvar, det bidrar til bedre rolleforståelse – og ikke minst – det er enklere for publikum og de registrerte å forholde seg til. Etter ombudets oppfatning burde operasjonene ovennevnt være *en* behandling med *en* behandlingsansvarlig.

Behandlingsgrunnlag

Det er utfordrende at det supplerende nasjonale rettsgrunnlag bare foreligger i en vid og lite konkret forstand i form av en forskriftsadgang i smittevernloven § 4-A 1 med antatt ikrafttredelse 11. juni 2021. Forordningen stiller ikke krav til en eksplisitt nedfellelse av behandlingen i grunnlaget, men formålet må være rimelig presist og konkret angitt. Ordlyden i nevnte lovforslag er ikke slik angitt etter personvernombudets oppfatning. Videre er det snakk om å behandle helseopplysninger, og det for et meget stort antall av befolkningen. Behandlingen vil dessuten ha stor betydning for de som tar sertifikatet i bruk. Også personvernforordningens art. 5 setter noen rammer og skranker for det supplerende nasjonale rettsgrunnlaget. For at behandlingen bl.a. skal være lovlig, rettferdig og åpen, slik at den blir forutsigbar, må det stilles særskilte krav til grunnlaget. Etter ombudets oppfatning er det usikkert om det angitte supplerende nasjonale rettsgrunnlag er dekkende på det nåværende tidspunkt.

Antatt bruk eller tilgjengeliggjøring

Det er gjort noen beskrivelser og vurderinger i personvernkonsekvensvurderingen av tilgjengeliggjøringsmåter eller bruk som ombudet forstår er uavklarte. De uavklarte forhold gjør

beskrivelsene og vurderingene usikre eller ufullstendige. Det forutsettes at personvernkonsekvensvurderingen endres og oppdateres når forholdene er mer klarlagte.

Dette bidrar også til at grensen for FHIs behandling og behandlingsansvar fremstår noe utydelig i personvernkonsekvensvurderingen.

Dessuten er det noen punkter som fremstår som ufullstendige eller uferdige. Dette gjelder bl.a. pkt. 2.2 om lagring (dataflyt, manglende beskrivelse), pkt. 2.7 lagringssted/logg og pkt. 3 om databehandler (antatt bl.a. HELFO) og 6.2 om angivelse av tiltak. Det gjør det vanskelig å rådgi på et slikt grunnlag.

Informasjon

Av det ovenstående fremgår det så mange uavklarte forhold at det stiller særskilte krav til informasjon og kommunikasjon i tiden fremover. Det forutsettes at kommunikasjonsplanen for dette tar nødvendig høyde for de mange uavklarte forhold.

Arkivering/lagring

Det bes om at vurderingen gis et saksnummer i P360 og lagres/arkiveres der så snart som mulig.

Med vennlig hilsen
Erlend Bakken
personvernombud
(sign.)

Gun Peggy S. Knudsen
Postboks 222, Skøyen
0213 Oslo

Att:
Siri A. Aasness

Deres ref:	Vår ref:	Dato:
21/14200	[xxxxxx]	21.07.2021

RÅD FRA PERSONVERNOMBUDET I ANLEDNING ENDRING I PERSONVERNKONSEKVENSVURDERING FOR «KORONASERTIFIKAT»

Det er gjort endring i personvernkonsekvensvurdering for «Koronasertifikat» i anledning løsning for ikke-digitale brukere mv.

Det følgende er et råd fra personvernombudet ved FHI etter FHIs mal for personvernkonsekvensvurderinger. Rådet gis med grunnlag i personvernforordningen artikkel 35 nr. 2.

Det presiseres at personvernforordningen ikke legger en godkjennelsesmyndighet til personvernombudet. Det er likevel antatt at rådet fra personvernombudet bør tillegges vekt ved en evt. godkjennelse av personvernkonsekvensvurderingen.

Det er særlig sett på følgende forhold:

- Behandlingen av personopplysninger, herunder dataflyt
- Det rettslige grunnlag for behandlingen av personopplysninger
- De registrertes rettigheter
- Risikoanalyse og tiltak

Personvernombudets råd

Personvernombudet har kun mindre kommentarer til endring i forbindelse med løsningen for ikke-digitale brukere.

Til vurderingens pkt. 1.1 og 2.2 så legges det legges til grunn at alternativet med at noen gir fullmakt til annen person for å hente ut sertifikatet digitalt i stor grad vil ligge utenfor behandlingsansvarliges kontroll og er ikke ytterligere gjenstand for vurdering av risiko eller personvernkonsekvenser her.

For pkt. 2.3 (2) og løsning for validering av innringer kunne det beskrives og vurderes om skissert løsning er tilstrekkelig trygg og om evt. andre eller ytterligere tiltak trengs for å oppnå tilstrekkelig sikkerhet omkring valideringen.

Det forutsettes at saksbehandlere i HELFO opplyses at stikkprøver etc. vil kunne gjøres, jf. pkt. 6.1 og 6.2.

Det er antatt at det ved mottak av sertifikat i posten vil følge med et skriv, men det er også ønskelig at det gis innledende informasjon til brukere allerede ved innringing til HELFO. Denne informasjonen kan bl.a. inkludere hva saksbehandler trenger tilgang til og rettigheter.

Med vennlig hilsen
Erlend Bakken
personvernombud
(sign.)

Gun Peggy Knudsen
FHI
Postboks 222, Skøyen
0213 Oslo

Att:
Siri A. Aasness

Deres ref:	Vår ref:	Dato:
21/14200	[xxxxxx]	18.01.2022

RÅD FRA PERSONVERNOMBUDET I ANLEDNING ENDRINGER I PERSONVERNKONSEKVENSVURDERING FOR «KORONASERTIFIKAT»

Det er gjort endringer i personvernkonsekvensvurdering for Koronasertifikat.

Det følgende er et råd fra personvernombudet ved FHI etter FHIs mal for personvernkonsekvensvurderinger. Rådet gis med grunnlag i personvernforordningen artikkel 35 nr. 2.

Det presiseres at personvernforordningen ikke legger en godkjennelsesmyndighet til personvernombudet. Det er likevel antatt at rådet fra personvernombudet bør tillegges vekt ved en evt. godkjennelse av personvernkonsekvensvurderingen.

De ansvarlige har vedlagt ROS, brukervilkår og personvernerklæring.

Personvernombudet har særlig sett på følgende forhold:

- Behandlingen av personopplysninger, herunder dataflyt
- Det rettslige grunnlag for behandlingen av personopplysninger
- De registrertes rettigheter
- Risikoanalyse og tiltak

Personvernombudets råd

Personvernombudets tilrår at endringene i personvernkonsekvensvurderingen godkjennes på følgende forutsetninger:

Det kan synes å være noe uklarhet mht. rolle for kommunene og FHI. I vedlagt personvernerklæring pekes kommunene ut som *databehandler* for FHI. I brukervilkår/brev til kommunene omtales kommunene som selvstendige *behandlingsansvarlige* for samme behandling. Dette må avstemmes/avklares før godkjenning.

Gitt den løsning som er valgt, så finnes det ikke mange alternativer for å avhjelpe utfordringer og risikoer med logging, tilgangsstyring osv. utover de som er angitt. Skriv med brukervilkår og betingelser, krav om opplæring mv. i kommunene vil være positivt, men det er gjenstående hvordan kommunene selv, og evt. FHI, vil kunne kontrollere den behandling som skal skje. Det kan på denne bakgrunn vurderes å sette som en forutsetning for godkjenning av personvernkonsekvens-vurderingen at skriftlige rutiner for dette bør være på plass innen en nærmere angitt frist.

I vurderingens pkt. 3.1 er det konkret angitt at FHI skal «*gjennomføre månedlig kontroll med gitte tilganger ved å sende oversikt til (kommunenes) koordinator med aktive tilganger og etterspørre bekreftelse på at personer på listen har tjenstlig behov for tilgang».* Det vil være en ikke ubetydelig prosess og gitt at alle kommunner tar denne løsningen i bruk er det 4 272 kontroller (12 x 356 kommuner) pr år. Godkjenner kan vurdere å sette som forutsetning for godkjenning av personvernkonsekvensvurderingen at skriftlige rutiner for dette er på plass innen en nærmere angitt frist.

Avslutningsvis minnes det om at lagring og arkivering av vurderingen i P360 må følge FHIs rutiner.

Med vennlig hilsen

Erlend Bakken
personvernombud
(sign.)

9.4 Konklusjon:

Kommentarer til personvernombudets vurdering

Tidspunkt for en personvernkonsekvensvurdering
PVO ber om behandlingsansvarliges vurdering av hvorvidt behandling av data er startet før DPIA er gjennomført, i forbindelse med at NHN produksjonssatte fremvisning i Helsenorge av QR kode 8.juni. Hensikten med «å gå i produksjon» før «lansering» er å få en kort periode i reelt produksjonsmiljø for å avdekke driftsproblemer eller feil før selve lanseringen. Det har hele tiden vært planlagt lansering og ibruktakelse fredag kl 15 i tråd med regjeringens beslutninger og forventet lovgrunnlag. Selve koronasertifikatet har ikke blitt tatt i bruk med tanke på kontroll og avlesning av QR koden, slik at det kun var fremvisning av informasjon på Helsenorge som

ble produksjonssatt. Vurderingen har vært at personvernkonsekvensvurdering skulle være ferdig for trinn3 for koronasertifikatet til fredag 11.juni kl 15 – da først er det lov å verifisere og kontrollere og dermed ta i bruk koronasertifikatet.

Behandlingssansvarlig

Det er vurdert og besluttet av departementet at FHI er behandlingsansvarlig for utstedelse av et koronasertifikat, jf. Prop. 203 LS (2020-2021) pkt. 6.12.1.

> *Dette fordi Folkehelseinstituttet også er ansvarlig for dataene som skal inngå i sertifikatet, og at sertifikatet på mange måter kun er en avansert innsyns- og verifiseringsløsning. Det er også et argument at koronasertifikatet i stor grad vil bli benyttet til bruk internasjonalt ved reisevirksomhet. Den siste delen er tett knyttet opp til Folkehelseinstituttets rolle som smitteverninstitutt med særskilt ansvar innenfor vaksiner. Norsk Helsenett SF vil tilgjengeliggjøre koronasertifikatet på helsenorge.no. Helsenorge.no er en plattform som muliggjør digitale helsetjenester og innsynstjenester. Norsk Helsenett SF er imidlertid ikke ansvarlige for innholdet i tjenestene som leveres. Departementet viser til at Folkehelseinstituttet er dataansvarlige for MSIS og SYSVAK, som vil være datakilde for et koronasertifikat. Norsk Helsenett SF behandler opplysninger på Helsenorge-plattformen i henhold til bruksvilkår som innbyggerne samtykker til.*

Det er ikke opp til prosjektet eller FHI å beslutte hvem som er behandlingsansvarlig for etableringen av et koronasertifikat. FHI har lang erfaring med å håndtere et behandlingsansvar pålagt i forskrift, jf. MSIS og SYSVAK.

Det stemmer at Helsedirektoratet er gitt ansvar for å koordinere oppdraget med å planlegge og gjennomføre koronasertifikat, på lik linje med det koordineringsansvaret de har for alle oppdrag som gis fra departementet i forbindelse med håndteringen av koronasituasjonen. For dette oppdraget har Helsedirektoratet organisert arbeidet med en prosjektorganisasjon, hvor FHI har ansvar for flere delprosjekter.

Behandling

Det må skilles mellom behandlingen som FHI foretar i forbindelse med etablering av et koronasertifikat og hvor innbygger ønsker å lagre opplysningene. Den første delen må anses nødvendig og den andre delen er frivillig. Det er ikke samme behandling til samme formål. Kontrollen av koronasertifikatet kan heller ikke bli samme behandling. FHIS behandling av personopplysninger for å etablere sertifikatet er nødvendig og lovregulert i smvl kap 4A, og må være tilgjengelig for registrerte i Helsenorge. Den enkelte må likevel samtykke til bruksvilkår og selv bestemme selve bruken av sertifikatet for å oppnå eventuelle lettelser i smitteverntiltak. Det må skilles mellom FHIs behandling ved å etablere et sertifikat og den registrertes eventuelle frivillige bruk. I tillegg vil det ved bruk skje en kontroll av den registrertes sertifikat som også faller utenfor FHIs dataansvar ved at kontrollører må ha et selvstendig behandlingsgrunnlag for å lovlig verifisere sertifikatet.

DPIA gjelder etableringen av et koronasertifikat. Det er Stortinget og regjeringen som har besluttet at dette skal være nødvendig i pandemien. Så lenge et koronasertifikat skal kunne benyttes for å oppnå lettelser i smittevernrestriksjoner, kan dette vanskelig anses å bygge på reell frivillighet for innbygger og trenger regulering i lov og forskrift.

NHN er leverandør av tjenester og ansvarlig for Helsenorge og Helsenorgeappen. Denne tjenesten gjelder er en samling av nasjonale e-helseløsninger for innbygger. Nedlastning på Helsenorge er et valg innbygger har og følger av bruksvilkårene på Helsenorge Det er ikke alle som kan benytte Helsenorge. Det er her et poeng at vi er i en pandemi og at koronasertifikatet er en midlertidig løsning. Det er hensiktsmessig å benytte allerede etablerte løsninger, som store deler av befolkningen allerede kjenner til. De ulike elementene i verdikjeden kan med fordel illustreres tydeligere med tanke på å få frem hvem som er behandlingsansvarlig eller databehandler for hvilke elementer, dette skal vi forbedre.

Behandlingsgrunnlag
Det er gjennomført en lovendring for å sikre etablering og bruk av et koronasertifikat. Denne DPIAen gjelder etablering av et koronasertifikat, ikke bruken som sådan. Bruken må ha et eget behandlingsgrunnlag, og en egen behandlingsansvarlig.
I forhold til personvernet henger etablering og bruk nært sammen. Bruken er derfor omhandlet i DPIAen.
I Stortingsbehandlingen ble det fremmet forslag om justeringer i ordlyden, men de ble nedstemt. Stortingsflertallet med 71 mot 16 stemmer gikk inn for ordlyden som ble foreslått av departementet.
Det har kommet endringer i covid-19 forskriften og DPIA oppdateres med at det fra 11. juni vil bli lettelser i smittevernrestriksjonene ved et koronasertifikat, jf covid-19 forskriften § 4, § 4a, § 4c, § 4d og endringer i vedlegg D.

Antatt bruk eller tilgjengeliggjøring
Det er presisert under formålsangivelsen at vi vil oppdatere nettsider ved endring av bruksområder. Dette har vært en del av vår kommunikasjonsplan og kanskje ikke fremkommet tydelig nok i DPIA.
Punktene som påpekes er mangelfullt utfylt ferdigstilles 11.juni.

Informasjon
Informasjon og kommunikasjon er det stort fokus på, med en særlig stor innsats på koordinering og samarbeid mellom FHI, Helsedirektoratet og NHN.

Konklusjon

DPIA for koronasertifikat, versjon mottatt 11. juni, for trinn 3 av koronasertifikatet, godkjennes. Det legges til grunn at arbeidet med utvikling av koronasertifikat har gått svært raskt, utarbeidelse av lovgrunnlag og forskrifter har gått parallelt og personvernkonsekvensvurderingene har dermed også blitt utført med løpende vurderinger og med svært høyt tidspress opp mot planlagt lanseringstidspunkt. Det er videre en trinnvis tilnærming til leveranser i utviklingen av koronasertifikatet, noe ROS og DPIA reflekterer. Både DPIA og ROS vil bli oppdatert og utvidet til trinn 4.

Kommentar til personvernombudets vurdering 18.01.2022:

Prosjektet beklager at PVO fikk oversendt da gjeldene og ikke oppdatert personvernerklæring for ikke-digitale-brukere. I den personvernerklæringen var kommunen omtalt som databehandler, da det var inngått tre databehandleravtaler ved årsskiftet, for at kommunen skulle kunne skrive ut koronasertifikat til innbygger. Dette var før endringen i covid-19-forskriften § 5h. Personvernerklæringen er rettet opp i trådt med PVOs anbefaling og legges inn samtidig med at løsningen tas i bruk.

Skriftlige retningslinjer som PVO sikter til vil være på plass ila 10. februar.

9.5 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: Ja/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
Viser til ROS-analysen		

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
Siri Aasness	Jurist	FHI
Kjetill Vassmo Lund	Arkitekt	NHN
Terje Granum	prosjektleder	FHI
Line Andreassen Sæle	Arkitekt	FHI
Kjetil Berg Veire	kommunikasjon	FHI
Vivi Haaheim	Ikke-digitale brukere	Innleid

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
2.0	22.06.2021	- en løsning for ikke-digitale brukere - EU-forordningene, som er vedtatt i EU - nye bruksområder for koronasertifikat, vedtatt i forskrift - noen presiseringer
2.5.		- tillegg til løsning for ikke digitale. De kan sende brev til Helfo
	08.09.2021	- endring i gyldighet for nasjonalt/dataminimert koronasertifikat. Gyldighet for gjennomgått sykdom går fra 6 til 12 måneder, på bakgrunn av oppdrag 484C fra HOD.
	24.09.2021	-tatt inn løsning for utstedelse av testsertifikat for de uten f. og d.nr. -lagring hos HElfo i maximun 30 dager -gjennomgått endringer i DPIA med PVO
	12.11.2021	- De uten f. og d.nr kan få koronasertifikat basert på etter-registret vaksine -Ros er oppdatert

Versjon	Dato	Endring
3.0	30.11.2021	-Det er åpnet for nasjonal bruk og Nasjonal kontrollside er gjenopptatt, harmonisert med EU-regler, jf. oppdrag 559
4.0	19.01.2022	Kommunen skal kunne skrive ut koronasertifikater på vegne av innbygger

11.1 Godkjenning

Dato	Versjon av DPIA	Godkjent av (henhold til fullmakt)
11.06.2021	For trinn 3, 11.juni 2021	Gun Peggy Knudsen
22.06.2021	For trinn 4, 24. juni 2021	Gun Peggy Knudsen
02.07.2021	For trinn 4 b 2. juli 2021	Gun Peggy Knudsen
08.09.2021	For endring varighet immunitet	Gun Peggy Knudsen
29.09.2021	For testsertifikat uten f. og d.nr	Gun Peggy Knudsen
12.11.2021	For koronasertifikat basert på etterregistrering av vaksinasjon for de uten f. og d. nr	Gun Peggy Knudsen
01.12.2021	Åpnet for nasjonal bruk og nasjonal kontrollside harmonisert med EU er klar	Gun Peggy Knudsen
19.01.2021	Kommunen skal kunne skrive ut koronasertifikater på vegne av innbygger	Gun Peggy Knudsen

12. Vedlegg

Husk å legge ved dokumentasjon eller oppgi arkivreferanse

☐ Systemdokumentasjon

☒ Risikovurdering av informasjonssikkerhet

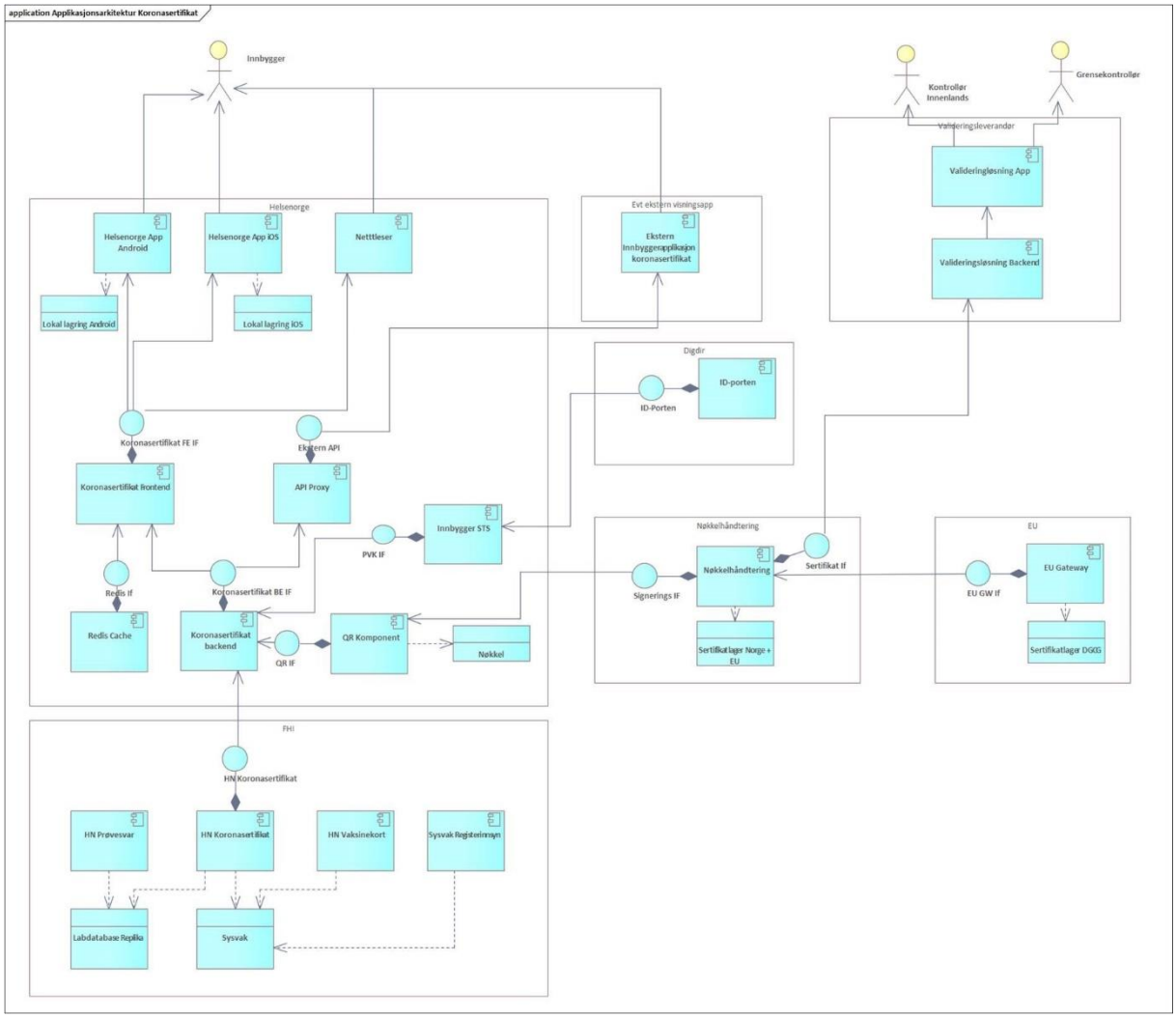
☐ Samtykkeerklæring og informasjonsskriv

☒ Informasjonsmateriell (evt link til nettside)

☒ Skjema over dataflyt

☐ ….

Dataflyt koronasertifikat

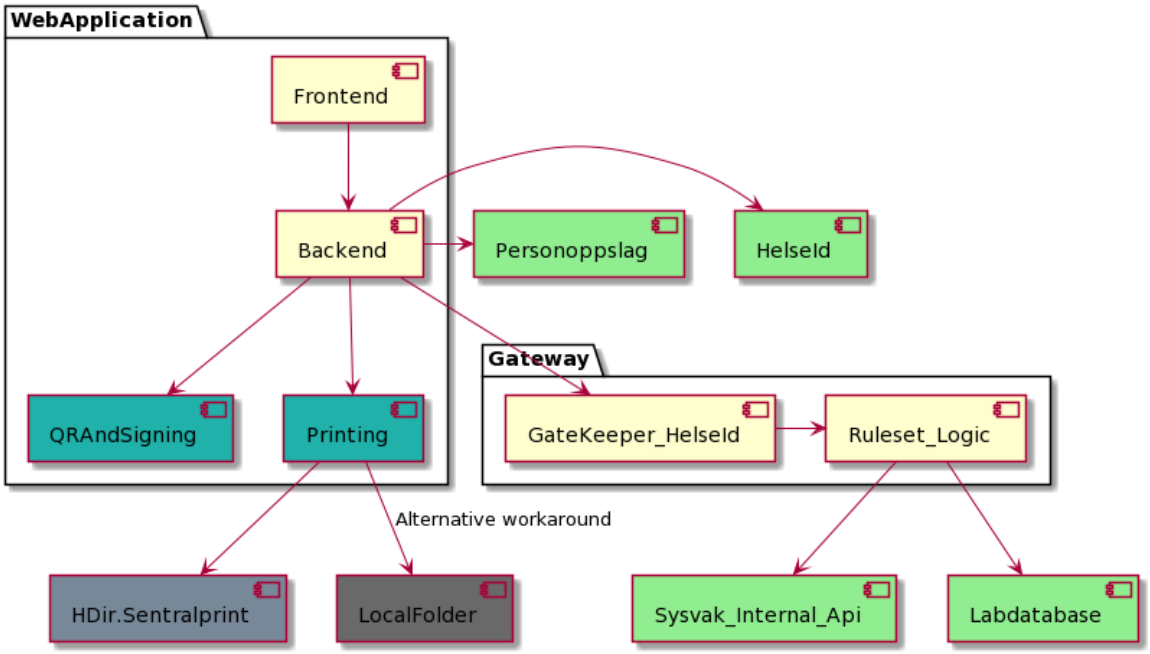


Dataflyt «Ikke digitale innbyggere – koronasertifikat»

Løsningen har følgende flyt:

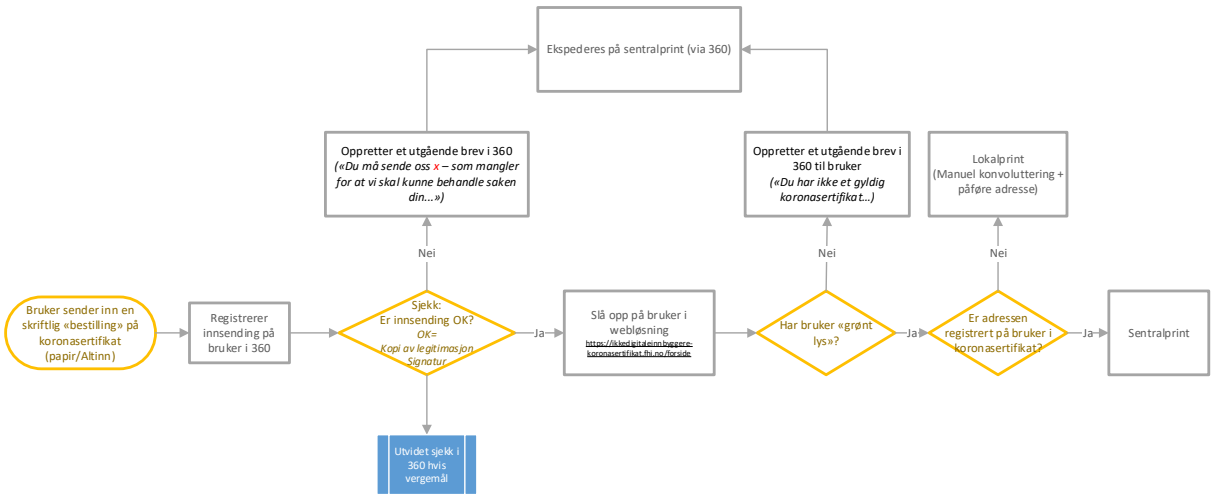
1. Helfo ansatt logger seg på løsningen ved bruk av HelseID/BankID
2. Innbyggers navn og folkeregistrerte adresse hentes via Preg og presenteres i løsningen
3. Koronasertifikatet hentes gjennom et API som ligger på helsenorge.no. Dette API'et henter data fra Sysvak og Labdatabase. Regler i API'et brukes til å avgjøre om Koronasertifikatene er gyldige eller ei
4. For å sende Koronasertifikatet til innbygger er det to muligheter
    a. Sende sertifikatene og følgebrev til Sentralprint. Dette gjøres via et API som Helsedirektoratet forvalter, Skatteetaten administrerer prosessen med å skrive ut og pakke brevene
    b. Sertifikat og følgebrev lastes ned lokalt og sendes manuelt i posten til innbygger

Av de to alternativene for utsending er det A. sentralprint som er forventet brukt i de aller fleste tilfeller. B er å regne som en manuell rutine der A ikke er mulig å benytte.



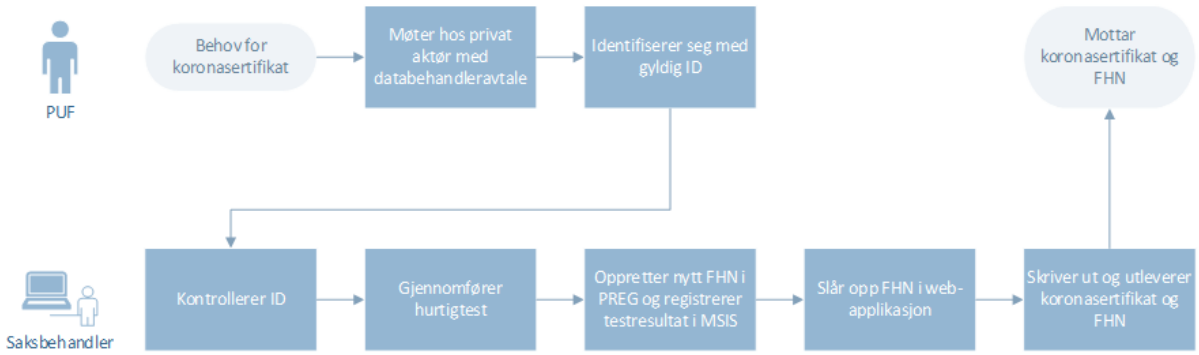
Prosessflyt «Ikke digitale innbyggere – koronasertifikat per brev»

1. Helfo ansatt ved dokumentasjonssenteret med tilgang til web-applikasjon og public 360 håndterer forespørsel per brev.
2. Innkommende brev registreres på innbygger i public 360
3. Henvendelsen kontrolleres og skal inneholde
    a. Innbyggers navn og oppholdsadresse
    b. Kopi av gyldig identifikasjon (pass, nasjonalt id-kort, førerkort eller bankkort med bilde)
    c. Brevet skal signeres
    d. Ved henvendelse fra verge verifiseres vergemål i public 360
4. Ved mangler i innsendt brev
    a. Brevet besvares med utgående dokument i public 360 om mangler og at koronasertifikat ikke kan sendes.
    b. Saken lukkes i public 360
5. Ved akseptert innsendt brev
    a. Saksbehandler følger *Dataflyt «Ikke digitale innbyggere – koronasertifikat»*
6. Ved ikke tilgengelig koronasertifikat
    a. Brevet besvares med utgående dokument i public 360 om at koronasertifikat ikke kan sendes.
    b. Saken lukkes i public 360
7. Ved tilgengelig koronasertifikat
    a. Sertifikat sendes til innbyggers oppholdsadresse via sentralprint hvis denne er registrert i public 360
    b. Sertifikatet skrives ut manuelt via secure print og sendes innbyggers oppholdsadresse hvis denne ikke er registrert i public 360
    c. Saken avskrives og lukkes i public 360 med kommentar om utsendt koronasertifikat



Prosessflyt «Koronasertifikat over disk til personer med felles hjelpenummer»

1. Person uten fødselsnummer eller d-nummer (PUF) møter fysisk ved privat aktør med databehandleravtale
2. PUF identifiserer seg med gyldig ID
3. Saksbehandler gjennomfører hurtigtest
4. Saksbehandler oppretter et nasjonalt felles hjelpenummer (FHN) og registrerer resultatet inn til MSIS
5. Saksbehandler gjør oppslag på det nylig opprettede FHN i web-applikasjonen for ikke-digitale brukere. Private aktører har en tilpasset versjon av applikasjonen som bare muliggjør oppslag på felles hjelpenummer.
6. Saksbehandler skriver ut koronasertifikat på lokal skriver og utleverer sertifikatet sammen med personvernerklæring til PUF.



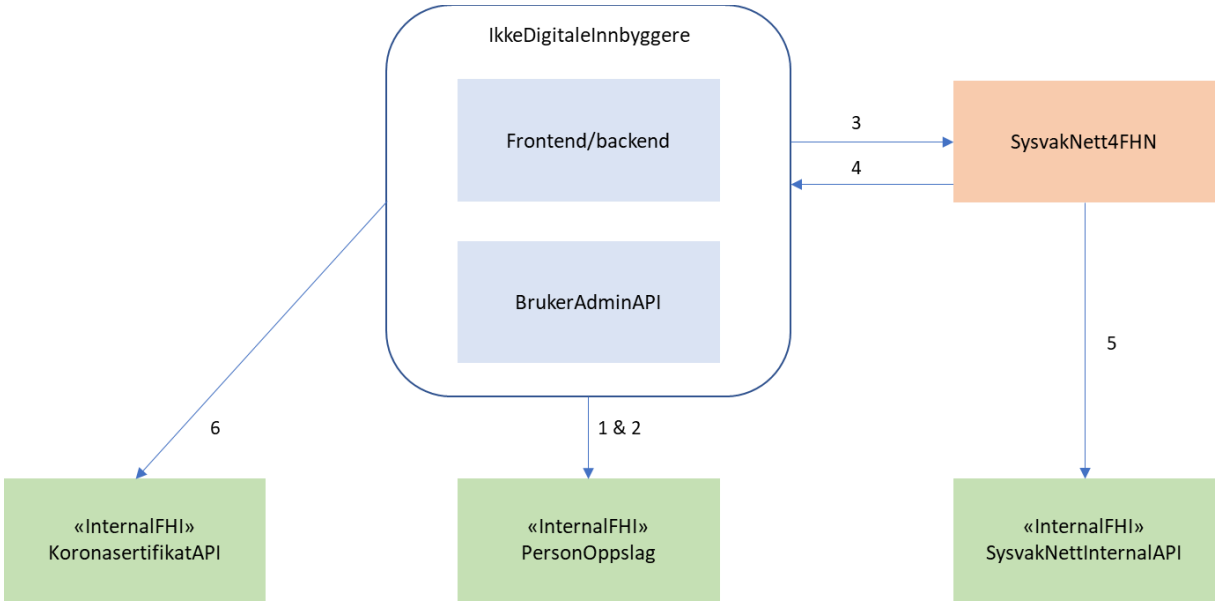
Prosessflyt «Etter-registrering av koronavaksiner satt i Norge til personer uten fødselsnummer eller d-nummer

1. Helfo ansatt ved dokumentasjonssenteret med tilgang til web-applikasjon og public 360 håndterer forespørsel per brev.
2. Innkommende brev registreres på innbygger i public 360
3. Henvendelsen kontrolleres og skal inneholde
    a. Innbyggers navn og oppholdsadresse
    b. Kopi av gyldig identifikasjon (pass, nasjonalt id-kort, førerkort eller bankkort med bilde)
    c. Kopi av vaksinasjonsbevis fra kommunen som har satt vaksinen med følgende nformasjon
        i. Navn, fødselsdato, vakinasjonsdato, vaksinetype og batchnummer
        ii. Vakinasjonsbeviset skal signeres og stemples av kommunen
    d. Brevet skal signeres
4. Ved mangler i innsendt brev

   a. Brevet besvares med utgående dokument i public 360 om mangler og at koronasertifikat ikke kan sendes.
   b. Saken lukkes i public 360

5. Ved akseptert innsendt brev følger saksbehandler *Dataflyt «Etter-registrering vaksiner»*
   a. Etterregistrering av vaksiner gjøres kun for personer med Felles hjelpenummer. Det finnes to alternative startpunkter:
      i. Personen har et Felles hjelpenummer
         1. Hvis personen har et Felles hjelpenummer må dette søkes opp for å være grunnlag for videre håndtering. Følgende steg utføres:
         2. Saksbehandler søker etter aktuelt FHN gjennom FHI's Personoppslagstjeneste som gjør oppslag i Preg. IDnr og Utstederland for ID benyttes som søkekriterier
         3. Søkeresultat presenteres i brukergrensesnittet
         4. Når aktuelt FHN er funnet åpnes Sysvak4FHN og brukeren tas sømløst med inn i denne løsningen
         5. Brukeren etterregistrerer vaksinen i Sysvak4FHN og knytter ID-nummer fra kopi av legitimasjon til registreringen.
         6. Brukeren genererer Koronasertifikat og sender dette til oppgitt adresse
      ii. Personen har ikke et Felles hjelpenummer
         1. I de tilfeller personen ikke har et kjent Felles Hjelpenummer må dette opprettes. Dette gjøres ved å registrere aktuelle data om personen i brukergrensesnittet. Så opprettes nytt Felles hjelpenummer gjennom FHI sin Personoppslagstjeneste, som igjen bruker PReg. Når dette er gjort følges stegene for alternativ 1.

6. Etter registrering av vaksinen følger vanlig rutine for *«Ikke digitale innbyggere – koronasertifikat per brev»*



1. Personoppslagtjenesten kalles for å hente data om den aktuelle personen. Oppslag gjøres på Felles Hjelpenummer
2. Hvis det ikke er treff på FHN vil man opprette et nytt FHN med Personoppslagstjenesten
3. Fra løsningen IkkeDigitaleInnbygere trigges SysvakNett4FHN
4. SysvakNett4FHN sjekker autoriserer bruker gjennom et kall til IkkeDigitaleInbyggere BrukerAdminAPI
5. Syvak4FHN kommuniserer med SysvakNettInternal for utveksling av vaksineinformasjon

Koronasertifikat API kalles for å hente data om koronapass slik at koronapass kan skrives ut og overleveres

Prosessflyt kommuner

1. Innbygger eller dennes representant møter fysisk opp ved kommunens sted for utskrift av koronasertifikat.
2. Innbygger eller dennes representant identifiserer seg med gyldig identifikasjon og ber om utskrift av koronasertifikat
3. Utskrift av koronasertifikat basert på vaksine:
    a. Saksbehandler logger seg inn i løsningen med e-ID på sikkerhetsnivå 4 på PC med tilgang til norsk helsenett og som er tilknyttet skriver.
    b. Saksbehandler søker opp innbyggers fødselsnummer, d-nummer eller felles nasjonale hjelpenummer i løsningen
    c. Saksbehandler vil få opp en oversikt over innbyggers navn, ID-nummer, og tilgjengelige koronasertifikat for utskrift. Se vedlagt bilde for detaljert informasjon.
    d. Saksbehandler trykker «print ut sertifikat»
    e. Alle tilgjengelige koronasertifikat for innbygger skrives ut sammen med følgebrev som beskriver innbyggers innsynsrett og hvor de kan ta kontakt for å bruke innsynsretten.
    f. Saksbehandler leverer koronasertifikat og følgebrev til innbygger eller dennes representant. Ved behov skal legitimasjon kontrolleres igjen før utlevering.
4. Utskrift av koronasertifikat basert på test
    a. Innbygger møter fysisk opp ved kommunens sted for test.
    b. Innbygger identifiserer seg med gyldig identifikasjon.
    c. Helsearbeider gjennomfører test av innbygger og registrerer resultatet elektronisk til MSIS Labdatabase på innbyggers fødselsnummer eller d-nummer.
    d. Hvis innbygger ikke har norsk ID-nummer, må det brukes felles nasjonalt hjelpenummer.
    e. Saksbehandler logger seg inn i løsningen med e-ID på sikkerhetsnivå 4 på PC med tilgang til norsk helsenett og som er tilknyttet skriver.
    f. Saksbehandler søker opp innbyggers fødselsnummer, d-nummer eller felles nasjonale hjelpenummer i løsningen
    g. Saksbehandler vil få opp en oversikt over innbyggers navn, ID-nummer, og tilgjengelige koronasertifikat for utskrift. Se vedlagt bilde for detaljert informasjon.
    h. Saksbehandler trykker «print ut sertifikat»
    i. Alle tilgjengelige koronasertifikat for innbygger skrives ut sammen med følgebrev som beskriver innbyggers innsynsrett og hvor de kan ta kontakt for å bruke innsynsretten.
    j. Saksbehandler leverer koronasertifikat og følgebrev til innbygger eller dennes representant. Ved behov skal legitimasjon kontrolleres igjen før utlevering.

Saksbehandler får følgende informasjon om innbygger ved oppslag gjennom løsningen:

FHI
Koronasertifikat – Ikke-digitale innbyggere
Forside
Profil
Personvernerklæring
Koronasertifikat
Koronasertifikat FHN
Koronasertifikat for ikke-digitale brukere
FHN
80014813148
Navn
RULLE OVER
Fødselsdag
10.3.1921
Personen har et gyldig sertifikat
Har nasjonalt koronasertifikat :
Har immunitetssertifikat (EU) :
Har test sertifikat :
Print ut sertifikat
Start på nytt