Workshop 2: Personvern

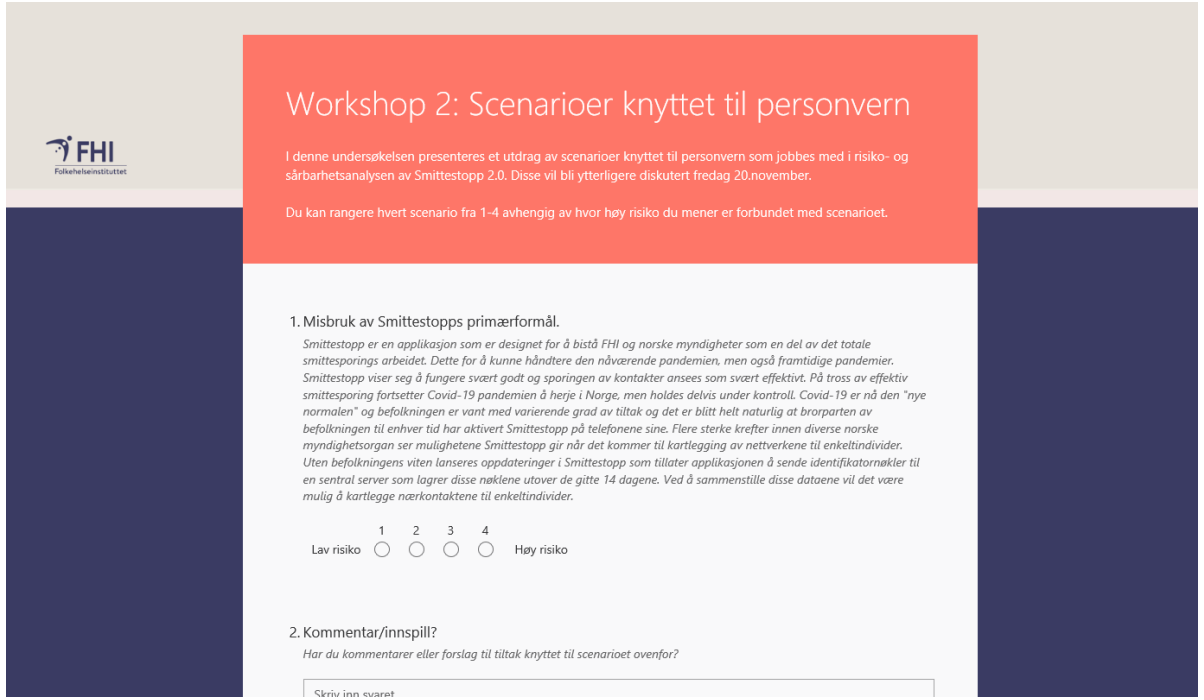
Gjennomgang av scenarioer

FHI 20.11.2020

Agenda

- Introduksjon v/ Stian
- Status v/ Pål
- Trusselbilde v/Stian
- Formål med dagens workshop v/ Tor Gaute Indstøy
- Scenarier og tiltak
- Åpen diskusjon om personvern

Introduksjon



FHI
Folkehelseinstituttet

Workshop 2: Scenarioer knyttet til personvern

I denne undersøkelsen presenteres et utdrag av scenarioer knyttet til personvern som jobbes med i risiko- og sårbarhetsanalysen av Smittestopp 2.0. Disse vil bli ytterligere diskutert fredag 20.november.

Du kan rangere hvert scenario fra 1-4 avhengig av hvor høy risiko du mener er forbundet med scenarioet.

1. Misbruk av Smittestopps primærformål.

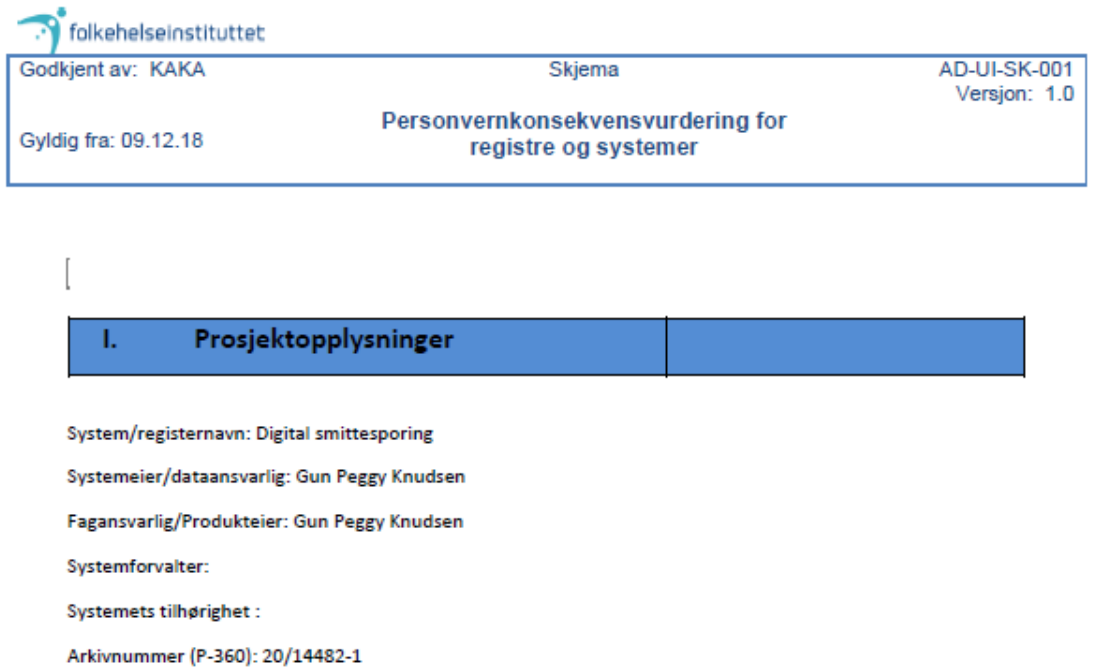
Smittestopp er en applikasjon som er designet for å bistå FHI og norske myndigheter som en del av det totale smittesporings arbeidet. Dette for å kunne håndtere den nåværende pandemien, men også framtidige pandemier. Smittestopp viser seg å fungere svært godt og sporingen av kontakter ansees som svært effektivt. På tross av effektiv smittesporing fortsetter Covid-19 pandemien å herje i Norge, men holdes delvis under kontroll. Covid-19 er nå den "nye normalen" og befolkningen er vant med varierende grad av tiltak og det er blitt helt naturlig at brorparten av befolkningen til enhver tid har aktivert Smittestopp på telefonene sine. Flere sterke krefter innen diverse norske myndighetsorgan ser mulighetene Smittestopp gir når det kommer til kartlegging av nettverkene til enkeltindivider. Uten befolkningens viten lanseres oppdateringer i Smittestopp som tillater applikasjonen å sende identifikatornøkler til en sentral server som lagrer disse nøklene utover de gitte 14 dagene. Ved å sammenstille disse dataene vil det være mulig å kartlegge nærkontaktene til enkeltindivider.

	1	2	3	4	
Lav risiko	◯	◯	◯	◯	Høy risiko

2. Kommentar/innspill?

Har du kommentarer eller forslag til tiltak knyttet til scenarioet ovenfor?

Skriv inn svaret



folkehelseinstituttet

Godkjent av: KAKA	Skjema	AD-UI-SK-001 Versjon: 1.0
Gyldig fra: 09.12.18	**Personvernkonsekvensvurdering for registre og systemer**	

I.	**Prosjektopplysninger**

System/registernavn: Digital smittesporing

Systemeier/dataansvarlig: Gun Peggy Knudsen

Fagansvarlig/Produkteier: Gun Peggy Knudsen

Systemforvalter:

Systemets tilhørighet :

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

Status på RoS-arbeidet

Sikringsbehov i forhold til trusselbildet

Smittestopp 1.0

- Lokasjonsdata for store deler av den norske befolkningen
- Statiske nøkler

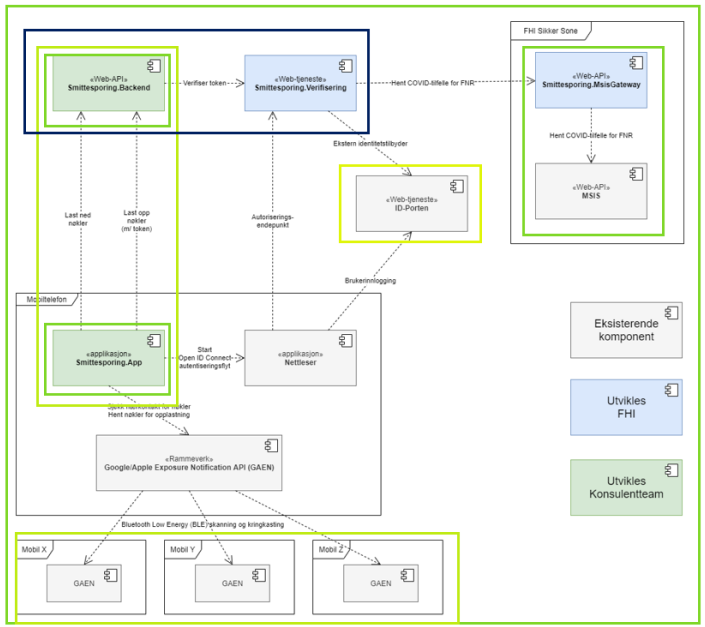
Smittestopp 2.0

- Ikke lokasjonsdata
- Temporære nøkler

Formål med dagens workshop

v/ Tor Gaute Indstøy

ROS



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

	Tittel	**Trussel**	**Tiltak**	**Etterlevelse basert på eksisterende tiltak.** **I henhold til beste praksis** **Tiltak eksisterer, men er ikke effektivt** **Tiltak mangler**	**Vurdering før ytterligere tiltak**			**Ytterligere tiltak (Føres inn i tiltaksliste)**	**Vurdering etter tiltak**			**Risikoeier** H: Hovedansvarlig U:Utførende K:Konsulteres I:Informeres
ID#	**Scenario**	**Scenario**		**Sårbarhetsbeskrivelse**	**S**	**K**	**U**		**Sr**	**Kr**	**Ur**	**H,U,K,I**

Scenarier og tiltak

Scenario 1

Misbruk av Smittestopps primærformål.

Smittestopp er en applikasjon som er designet for å bistå FHI og norske myndigheter som en del av det totale smittesporings arbeidet. Dette for å kunne håndtere den nåværende pandemien, men også framtidige pandemier. Smittestopp viser seg å fungere svært godt og sporingen av kontakter ansees som svært effektivt. På tross av effektiv smittesporing fortsetter Covid-19 pandemien å herje i Norge, men holdes delvis under kontroll. Covid-19 er nå den "nye normalen" og befolkningen er vant med varierende grad av tiltak og det er blitt helt naturlig at brorparten av befolkningen til enhver tid har aktivert Smittestopp på telefonene sine. Flere sterke krefter innen diverse norske myndighetsorgan ser mulighetene Smittestopp gir når det kommer til kartlegging av nettverkene til enkeltindivider. Uten befolkningens viten lanseres oppdateringer i Smittestopp som tillater applikasjonen å sende identifikatornøkler til en sentral server som lagrer disse nøklene utover de gitte 14 dagene. Ved å sammenstille disse dataene vil det være mulig å kartlegge nærkontaktene til enkeltindivider.

Tiltak scenario 1

Misbruk av Smittestopps primærformål.

A) Implementering av dataminimeringsprosesser for å redusere lagring av sensitiv persondata.

B) Sikre innebygget personvern i applikasjonen og gode prosesser for oppdatering og endringer i appen.

C) Sikker forvaltning av nøkkel benyttet for å lansere nye versjoner av applikasjonen.

D) Etablere ansvar og prosesser for at løsningen settes i dvale umiddelbart etter at myndighetene erklærer Covid-19-krisen som over.

E) Monitorere og vurdere oppdateringer av Smittestopp for å detektere mulig misbruk av primærformålet.

Scenario 2

Formålets omfang øker til å inkludere eksempelvis andre offentlige organers bruk, som ikke er i tråd med det originale formålet.

Smittestopps formål er å bidra til kontakt- og smittesporing i Norge og styrke FHIs responsinnsats. Det er en risiko for at formålet til applikasjonen endres eller at omfanget øker, slik at det ikke lenger er i tråd med det originale formålet. Det kan være gjennom at flere offentlige organer ønsker å benytte applikasjonen til ulike formål, eksempelvis håndhevingsformål. Det medfører en risiko for at færre vil benytte Smittestopp, i frykt for at dataen samlet inn via applikasjonen kan brukes mot deres favør i senere anledning. Det vil føre til mistillit mot norske myndigheter og skape uro i befolkningen.

Tiltak scenario 2

Formålets omfang øker til å inkludere eksempelvis andre offentlige organers bruk, som ikke er i tråd med det originale formålet.

A) Etablere vilkår for Produktstyret som inkluderer formålet med applikasjonen og pålegger komiteen ansvar for å sikre at data prosesseres i tråd med formålet. I tillegg må vilkårene sikre at alle endringer blir nøye vurdert, er lovlige og reflektert i DPIA-en.

B) Løpende vurdering av applikasjonen og dataen som prosesseres, spesielt fra et etisk, data- og personvernsperspektiv.

Scenario 3

Apple og Google samler inn og behandler personopplysninger via Smittestopp på en måte som strider med brukerens rettigheter, bla. Lokasjonsdata.

Google/Apple sender lokasjonsdata gjennom AppStore/Google Play med korte tidsintervall.

På Android-telefoner krever GAEN-rammeverket at Google Play services benyttes, og det betyr at telefonen sender en del informasjon til Google ca. hvert 20. minutt, inkludert lokasjonsdata, Dette er det ikke mulig for bruker å slå av så lenge Smittestopp skal virke etter hensikten som er å ha applikasjonen aktiv så mye som mulig. Dette vil medføre at norske borgere vil sende ut lokasjonsdata til Google hvert 20 minutt. Dette er ikke noe nytt da flere applikasjoner de fleste nordmenn allerede har installert på telefonen gjør nettopp dette (eksempelvis gjennom applikasjoner som Google Maps, Strava etc.). Å utvikle, tilgjengeliggjøre og anbefale en applikasjon som "tvinger" den norske befolkning til å sende posisjonsdata til Google hvert 20 minutt kan sees på som en annerkjennelse av praksisen, en anbefaling som ikke tidligere er gitt av norske myndigheter. Det foreligger ikke dokumentasjon som tilsier at Apple har samme funksjon på applikasjoner i AppStore, men vi kan anta at mekanismene er relativt like

Tiltak scenario 3

Apple og Google samler inn og behandler personopplysninger via Smittestopp på en måte som strider med brukerens rettigheter, bla. Lokasjonsdata.

A) Tydelig informasjon og kommunikasjon på området slik at innbyggere føler seg informert og opplyst. Det må bygges på tilgjengelig informasjon fra Google/Android/Apple.

B) Informere om at Google/Android opplyser om hvordan personopplysninger fra brukerne samles inn og brukes. https://developers.google.com/android/exposure-notifications/telemetry-design

C) Informere om at Apple ikke opplyser om hvordan de samler inn og behandler personopplysninger fra brukerne gjennom sine apper.

Scenario 4

Det er uklart for brukeren hvordan man skal utøve sine personvernrettigheter i Smittestopp

Etter at personvernforordningen (GDPR) trådde i kraft for et par år siden har personvern og brukers rettigheter har blitt stadig viktigere for både tilbydere og brukere. Brukeren oppfatter at Smittestopp ikke tar hensyn til personvern, og det er uklart for brukeren hvordan hen kan utøve sine rettigheter. Dette fører til at brukeren ikke ønsker å ta i bruk Smittestopp, og dens formål og virkning svekkes.

Tiltak scenario 4

Det er uklart for brukeren hvordan man skal utøve sine personvernrettigheter i Smittestopp

A) Tydeliggjøre samtykkefunksjonen Gjennom brukergrensesnittet i applikasjonen, både for å synliggjøre at samtykke kreves for bruk av Smittestopp, og at samtykke når som helst kan trekkes tilbake.

B) Det må være tydelig for brukeren hva man gir samtykke til, samt hvordan samtykke kan trekkes tilbake, gjennom samtykkefunksjonen og generell markedsføring og kommunikasjon av Smittestopp.

C) Tydelig kommunikasjon og markedsføring rundt hvordan data prosesseres og at ingen personlig data lagres i applikasjonen.

D) Lansere ny markedsføringskampanje for å øke bruken av Smittestopp og tilliten til applikasjonen noen uker/måneder etter lansering.

Scenario 5

Statistikk om bruk av Smittestopp samles inn og er ikke anonymisert.

For å kartlegge bruken av Smittestopp samler applikasjonen inn data for analyse. Denne dataen omfatter blant annet hvordan brukerne interagerer med applikasjonen, deres daglige bruk, raten av slettinger, kontaktsporing, eksponeringshendelser og lignende. Denne dataen er ikke anonymisert og det er en risiko for at brukerne ikke er klar over dette og forventer at dataen er anonymisert. Dersom Smittestopp og helsenorge.no kobles sammen kan man identifisere enkeltpersoners kontaktnett og bruke dette til andre formål enn Smittestopps primærformål.

Tiltak scenario 5

Statistikk om bruk av Smittestopp samles inn og er ikke anonymisert.

A) Implementere dataminimeringsprosesser og sørge for at denne type data ikke samles inn.

B) Hashing og salting av data for å sikre at det ikke er mulig å koble innlogging hos helsenorge.no med en opplasting til Smittestopp ved hjelp av opplastet token. Dette kan gjøres ved bruk av Privacy Pass.

Scenario 6

Smittestopp brukes til å vise en persons Covid-19 status.

Bruker blir smittet av Covid-19 og laster opp denne informasjonen i Smittestopp via en diagnosenøkkel. Det registreres at vedkommende er smittet. På denne måten vil man kunne se om en person er registrert smittet eller ikke. Aktør får tilgang til denne informasjonen og bruker dette til å ta avgjørelser, eller gjøre seg opp meninger om den registrerte. om brukerens Covid-19 status tas i bruk av andre, for eksempel til å ta avgjørelser om den registrerte.

Tiltak scenario 6

Smittestopp brukes til å vise en persons Covid-19 status.

A) Applikasjonen designes en måte slik at man ikke kan se Covid-19 statusen til personer.

B) Applikasjonen skal kun prosessere data i tråd med formålet og DPIA-en.

C) Randomisering av tokens for å hindre mulighet til å koble identitet til smittenøkler og dermed avgjøre Covid-19 statusen til personer.

Scenario 7

Angrep på MSIS gjør at persondata til personer med kode 6/7 blir tilgjengeliggjort.

Kode 6/7 personer har behov for særlig skjerming av persondata og geolokaliserende informasjon. Ved et angrep mot MSIS eller andre deler av informasjonskjeden kan informasjon komme på avveie som senere kan benyttes til ondsinnede handlinger.

Tiltak scenario 7

Angrep på MSIS gjør at persondata til personer med kode 6/7 blir tilgjengeliggjort.

A) Vurdere om Smittestopp skal anbefales for personer med kode 6/7.

Scenario 8

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

Leverandøren av SMS-tjenesten som benyttes til å sende flash meldinger i Smittestopp greier å identifisere enkeltpersoner. Ved å sammenstille dette med informasjon om hvilke meldinger personen har mottatt greier leverandøren å tolke seg fram til at brukeren har testet positivt for Covid-19.

Tiltak scenario 8

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

A) Tokens blir autorisert for å hindre at API-et blir spammet ned av informasjon og settes ut av spill. BankID skal benyttes med flash SMS fra SIM-kort for å sikre dette.

B) Sikre at korrekt databehandlingsavtale er lagt inn for SMS-utsendelsesservice for å beskytte konfidensialitet og på den måten beskytte innbyggerne.

C) Bruke kjente SMS-leverandører som man har tillit til.

D) Randomisering av tokens for å hindre mulighet til å koble identitet til smittenøkler.

E) Unngå at utsendingsmeldingen inneholder informasjon om FHI eller Smittestopp.

Scenario 9

Trusselaktør kan identifisere person som varsler om smitte gjennom bruk av pseudonym i varslingsløsningen.

Trusselaktøren har tilgang til pseudonym generert av ID-porten og kan ved hjelp av dette identifisere personen som har varslet om positivt prøvesvar gjennom Smittestopp-appen.

Tiltak scenario 9

Trusselaktør kan identifisere person som varsler om smitte gjennom bruk av pseudonym i varslingsløsningen.

A) Pseudonymet lagres kun i kort tid i varslingsløsningen (24 timer).

B) Utledning av personnummer fra pseudonymet krever tilgang til ID-porten.

Scenario 10

Overføring av personopplysninger ut av EU/EØS uten ytterligere tiltak fører til datalekkasje til utenlandske myndigheter.

Behandlingsansvarlig må sørge for tilstrekkelig sikkerhet også når opplysninger overføres ut av EU/EØS. Behandlingsansvarlig må derfor først undersøke om beskyttelsesnivået som vil oppnås i praksis, faktisk er tilsvarende som i EØS. Ref. Schrems II-dommen. Dette gjelder data som overføres til skytjenestene via backend eller verifiseringsløsningen.

Tiltak scenario 10

Overføring av personopplysninger ut av EU/EØS uten ytterligere tiltak fører til datalekkasje til utenlandske myndigheter.

A) Tekniske begrensninger

B) Due diligence undersøkelse av GDPR etterlevelse for land som det eventuelt skal deles informasjon med.

C) Ikke benytte leverandør i det som defineres som «tredje land» iht. GDPR. Hvis man skal bruke en tredjeland leverandør, og det blir lagret informasjon i dette landet, så kan informasjonen som lagres krypteres uten at leverandør får tilgang til kryptonøkkel. NB: Vurderinger må gjennomføres hvis tjenesten det er snakk om krever tilgang for support fra eks. USA (da med tilgang til sensitive data). Hvordan kan denne skrives ut

Øvrige kommentarer

Takk for din deltakelse.