Datatilsynet

FOLKEHELSEINSTITUTTET
Postboks 222 Skøyen
0213 OSLO

Deres referanse	Vår referanse	Dato
20/11308-6	20/02058-9	12.06.2020

Varsel om vedtak om midlertidig forbud mot å behandle personopplysninger - appen Smittestopp

1. Datatilsynets saksbehandling

Datatilsynet viser til tidligere kontakt i forbindelse med appen Smittestopp, som ble lansert 16.04.2020.

I brev av 08.05.2020 varslet vi Folkehelseinstituttet (FHI) om pålegg knyttet til behandlingsprotokollen og risiko- og sårbarhetsanalysen (ROS-analysen). Vi mente at det forelå grunnleggende mangler ved disse dokumentene som måtte rettes umiddelbart. FHI har senere sendt inn oppdaterte versjoner av protokoll og ROS-analysen, og vi har ikke sett det nødvendig å fatte vedtak om pålegg i saken.

Den 19.05.2020 ba vi om en redegjørelse for flere forhold, blant annet FHIs evaluering av Smittestopp, særskilt knyttet til appens nytteverdi og forholdsmessigheten av personverninngrepet. Etter vårt syn tilsa opplysningene vi hadde om oppslutningen om og nytteverdien av Smittestopp at det er nødvendig å kontrollere om personverninngrepet som Smittestopp utgjør er nødvendig og forholdsmessig ut fra dagens situasjon.

FHI har redegjort for saken i brev av 01.06.2020. Etter henvendelse fra Datatilsynet, har FHI også oversendt manglende dokumentasjon den 08.06.2020.

Som vi tidligere har informert om, vil vårt kontrollarbeid foregå trinnvis. Enkelte forhold har vi ennå ikke vurdert, herunder sikkerheten i de tekniske løsningene som er valgt for Smittestopp. Vi mangler blant annet informasjon om den oppnevnte ekspertgruppens vurderinger på dette punktet.

Vi har imidlertid hentet inn og gjennomgått mye dokumentasjon knyttet til Smittestopp, både fra FHI og andre. Gjennom den trinnvise tilnærmingen mener vi at FHI har hatt god nok mulighet til å redegjøre for sine synspunkter og løsningene som er valgt.

Datatilsynet vil presisere at vi ikke ønsker å stå i veien for bruk av en digital løsning som er et reelt bidrag i arbeidet med å begrense spredning av covid-19-smitte i befolkningen.

Pandemien er svært alvorlig, og konsekvensene har allerede vist seg å være store – både på et menneskelig og økonomisk plan. Som vi også tidligere har fremhevet, kan en digital løsning for smittesporing være et relevant, effektivt og forholdsmessig tiltak i en krisesituasjon.

Ut fra dagens situasjon – med lav smitteutbredelse, lav oppslutning om Smittestopp og mangelfull oppnåelse av formålene om smittesporing og evaluering av smitteverntiltak – anser vi imidlertid ikke lenger Smittestopp som et forholdsmessig inngrep i den enkelte brukers personvern.

Vi mener at det er nødvendig å varsle FHI om vedtak om et midlertidig forbud mot å behandle personopplysninger knyttet til Smittestopp. Begrunnelsen for dette vil fremgå i det følgende.

2. Smittestopp – et inngrep i personvernet

Enhver har rett til vern av sitt privatliv. Dette er en grunnlovfestet rettighet[1] og en rett som også er beskyttet av Den europeiske menneskerettskonvensjonen (EMK)[2].

Gjennom Smittestopp samler FHI inn et svært store mengder personopplysninger, til dels av sensitiv art. FHI kan blant annet overvåke bevegelsesmønsteret til den enkelte som har tatt appen i bruk. I tillegg samler Smittestopp inn opplysninger om brukernes kontakter med andre brukere av appen. Avhengig av hvor mange som laster ned og bruker appen, kan overvåkingen skje i stor skala. Det at staten kan følge med på enkeltpersoners bevegelsesmønster og kontakt med andre mennesker, innebærer i alle tilfeller et svært stort inngrep i den enkeltes personvern.

Smittestopp er hjemlet i en forskrift[3] som er innført i en unntakssituasjon der samfunnet har forsøkt å begrense skadevirkningene av en pandemi. Et så inngripende tiltak som Smittestopp utgjør, vil vanligvis måtte vedtas ved lov. En lovreguleringsprosess innebærer demokratisk kontroll og er i seg selv en rettssikkerhetsgaranti.

Ettersom covid-19-pandemien har ført til en unntakssituasjon i samfunnet, og formålet med Smittestopp er å bekjempe covid-19-smitte, er det likevel aksept for at løsningen er gjennomført uten de kontrollmekanismene som vanligvis kreves ved et så inngripende tiltak.

Selv i en unntakssituasjon må imidlertid den enkeltes grunnleggende rettigheter ivaretas. Datatilsynet er ansvarlig for å kontrollere at behandlingen av personopplysninger i Smittestopp fortsatt utgjør et forholdsmessig inngrep i personvernet og at reguleringen som tillater behandlingen kan anses som rettslig grunnlag uten å ha vært gjenstand for normal demokratisk kontroll.

Appen Smittestopp er som nevnt et svært inngripende tiltak å ta i bruk potensielt overfor hele befolkningen. Jo større inngrepet i personvernet er, jo strengere krav må det stilles til nødvendigheten av behandlingen av personopplysninger. For at personverninngrepet ved

[1] Se grunnloven § 102.
[2] Se EMK artikkel 8.
[3] https://www.regjeringen.no/contentassets/116076d9a39b473a97d97474048e1fb0/kgl.-res.-27.-mars-digital-smittesporing.pdf

Smittestopp skal kunne anses forholdsmessig, må derfor innsamlingen og lagringen av opplysninger om befolkningens bevegelser og kontakt med andre mennesker være strengt nødvendig for å nå formålet. Dette vil igjen blant annet avhenge av samfunnsnytten av løsningen.

3. Rettslig grunnlag

Datatilsynet fører kontroll med etterlevelsen av personvernregelverket, jf. personvern-forordningen artikkel 57 og personopplysningsloven § 20.

3.1 Nærmere om grunnprinsippene i personvernforordningen

De grunnleggende prinsippene for behandling av personopplysninger er angitt i personvernforordningen artikkel 5. Særlig sentrale i denne saken er prinsippene om formålsbegrensning og dataminimering.

Prinsippet om formålsbegrensning fremgår av personvernforordningen artikkel 5 nr. 1 bokstav b. I dette prinsippet ligger blant annet at personopplysninger skal samles inn for spesifikke og uttrykkelig angitte formål.

Dersom en behandlingsansvarlig ønsker å oppnå flere formål, må hvert av disse formålene formuleres presist og fremgå klart. Spesifikke formålsangivelser er blant annet en forutsetning for å kunne ta stilling til hvilke personopplysninger det er nødvendig å behandle for å oppnå det enkelte formål og for å kunne vurdere om det foreligger rettslig grunnlag for behandlingsformålet, jf. personvernforordningen artikkel 6.

Et annet grunnleggende prinsipp ved behandling av personopplysninger er prinsippet om dataminimering. Prinsippet fremgår av personvernforordningen artikkel 5 nr. 1 bokstav c, hvoretter personopplysninger skal være «adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for».

Der en behandlingsansvarlig har definert flere formål, gjelder kravet om relevans og nødvendighet for hvert av de angitte formålene. Behandlingsansvarlig må altså gjøre konkrete vurderinger av hvilke personopplysninger det er nødvendig å behandle knyttet til hvert enkelt formål. Dersom den behandlingsansvarlige velger felles behandlingsløsning for mange ulike formål, må dette være basert på en konkret vurdering av at kravene i personvernregelverket kan oppfylles selv om behandlingen foregår på samme måte for alle formål.

Etter prinsippet om dataminimering er det ikke tilstrekkelig at det er praktisk eller ønskelig å behandle personopplysninger; behandlingen må være *nødvendig* for at formålet kan nås. Kravet til nødvendighet vil naturlig nok skjerpes jo større personverninngrepet er.

I prinsippet om dataminimering ligger også en overordnet forutsetning om at behandlingen av personopplysninger bidrar til å oppnå et konkret formål. Formålsbeskrivelsene vil være det naturlige utgangspunktet for vurderinger av nytteverdien av en behandling. Dersom det er flere formål, må nytteverdien vurderes opp mot de enkelte formålene. Det samme gjelder for evalueringer av om de personopplysningene man samler inn faktisk er nødvendige for å oppnå formålet.

Hvis et tiltak som innebærer behandling av personopplysninger ikke er nyttig for å oppnå de(t) angitte formål(ene), kan personverninngrepet vanskelig forsvares. Jo mer inngripende tiltaket er, jo større krav stilles til en dokumentert nytteverdi av tiltaket.

Også prinsippet om åpenhet vil være relevant når det gjelder Smittestopp. Enhver behandling av personopplysninger skal være åpen og gjennomsiktig overfor de registrerte, jf. personvern-forordningen artikkel 5 nr. 1 bokstav a. Dette innebærer blant annet at de registrerte skal få informasjon om hvilke personopplysninger om seg som behandles, hvem som har tilgang til disse osv.

Prinsippet om åpenhet kommer til uttrykk ved at de registrerte er gitt en rett til informasjon om og innsyn i personopplysningene om seg, personvernforordningen artikkel 13 t.o.m. 15. I artikkel 12 fremgår det at den behandlingsansvarlige plikter å legge til rette for at de registrerte kan utøve sine rettigheter.

3.2 EDPBs retningslinjer og veiledning fra WHO

EUs personvernråd (EDPB) har kommet med retningslinjer (*guidelines*) knyttet til bruk av lokasjonsdata og kontaktsporing i forbindelse med covid-19-pandemien.[4] Retningslinjene regulerer bruk av slike data både til vurdering av effekt av smitteverntiltak og til kontaktsoppsporing ved smitte, jf. avsnitt 5 i retningslinjene.

EDPBs retningslinjer er ikke juridisk bindende. Retningslinjene gir likevel uttrykk for god praksis for bruk av personopplysninger i arbeidet med å begrense covid-19-smitte. Avvik fra retningslinjene kan representere et samtidig brudd på personvernregelverket. Generelt bør det ligge gode, konkrete og dokumenterte vurderinger til grunn dersom man velger ikke å følge offisielle retningslinjer fra EDPB.

I EDPBs retningslinjer avsnitt 24 fremgår følgende om frivillighet for de registrerte:

> «The systematic and large scale monitoring of location and/or contacts between natural persons is a grave intrusion into their privacy. It can only be legitimised by relying on a voluntary adoption by the users *for each of the respective purposes* (vår utheving)».

Prinsippet om dataminimering er omtalt i avsnitt 27, som lyder:

> «In the context of a contact tracing application, careful consideration should be given to the principle of data minimisation and data protection by design and by default.
> - contact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used;

[4] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

- as contact tracing applications can function without direct identification of individuals, appropriate measures should be put in place to prevent re-identification;
- the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary».

I retningslinjenes avsnitt 42 fremgår følgende om valg av lagringsløsning ved kontaktsporing:

> «Implementations for contact tracing can follow a centralized or a decentralized approach. Both should be considered viable options, provided that adequate security measures are in place, each being accompanied by a set of advantages and disadvantages. Thus, the conceptual phase of app development should always include thorough consideration of both concepts carefully weighing up the respective effects on data protection /privacy and the possible impacts on individuals rights».

EDPBs vilkår for å ta en sentralisert lagringsløsning i bruk er utdypet i avsnitt 43:

> «Any server involved in the contact tracing system must only collect the contact history or the pseudonymous identifiers of a user diagnosed as infected as the result of a proper assessment made by health authorities and of a voluntary action of the user. Alternately, the server must keep a list of pseudonymous identifiers of infected users or their contact history only for the time to inform potentially infected users of their exposure, and should not try to identify potentially infected users».

Også Verdens helseorganisasjon (WHO) har kommet med flere publikasjoner knyttet til digital kontaktsporing (*digital proximity tracking*) ved covid-19[5]. Vi presiserer at heller ikke WHOs anbefalinger er juridisk bindende, men de gir uttrykk for hva WHO mener er god praksis for behandling av personopplysninger i forbindelse med digital kontaktsporing.

I en midlertidig veiledning (*interim guidance*) fra 28.05.2020[6] har WHO kommet med konkrete anbefalinger knyttet til digital kontaktsporing.

Under punktet «Proportionality» (side 3) fremgår det:

> «The least intrusive (privacy-preserving) measures should always be preferred for an application's design, including avoiding the use of physical location (geographic position) tracking for digital proximity tracking».

[5] https://www.who.int/publications/i
[6] https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

Videre fremgår det under «Data minimization»:

> «[D]ata collection should not require the identity or location data of a user, or a time stamp of a proximity event (though the date of a proximity event may be useful). Data collected, retained and aggregated must be limited in scope».

3.3 Midlertidig forbud mot å behandle personopplysninger

Datatilsynets myndighet til å ilegge sanksjoner er nærmere regulert i personvernforordningen artikkel 58. I artikkel 58 nr. 2 fremgår det hvilke korrigerende tiltak vi kan vedta.

Artikkel 58 nr. 2 bokstav f lyder:

> «2. Hver tilsynsmyndighet skal ha myndighet til å beslutte følgende korrigerende tiltak: (…)
> f) innføre en midlertidig eller varig begrensning av, herunder et forbud mot, behandling».

4. Nærmere om appen Smittestopp

Datatilsynet har gjennomgått FHIs personvernkonsekvensvurdering, ROS-analyse, personvernerklæringen for Smittestopp og den øvrige informasjonen om Smittestopp på FHIs nettside.

Vi har også gjennomgått FHIs redegjørelse i saken og rapporten fra den oppnevnte ekspertgruppen. Vi kommer nærmere tilbake til disse under punkt 5 og 6.

I det følgende vil vi gjennomgå forhold som vi anser sentrale for å kunne vurdere forholdsmessigheten av personverninngrepet som Smittestopp utgjør, herunder formålene og nytteverdien ved appen.

4.1 Formålene ved Smittestopp og behandlingen av personopplysninger

I foreliggende personvernkonsekvensvurdering (DPIA), ROS-analyse, personvernerklæring og informasjonen på FHIs nettside, fremstår rask og effektiv oppsporing av og SMS-varsling om covid-19-smitte som appen Smittestopps «hovedformål».

Varsling om covid-19-smitte per SMS er per i dag kun innført i testkommunene (Drammen, Trondheim og Tromsø).

I tillegg vil FHI gjennom overvåking og analyse av befolkningens bevegelsesmønster kunne få oversikt over smitteutbredelse og effekt av smitteverntiltak. Analyse av anonyme og aggregerte data samt forskning på disse dataene er også uttalte formål.

FHI har per i dag ikke en analyseløsning eller løsning for anonymisering og aggregering av data på plass.

Den enkelte som laster ned og bruker Smittestopp kan per i dag ikke velge å dele sine personopplysninger for kun ett (eller enkelte) av de nevnte formålene.

Appen Smittestopp henter inn data via GPS og Bluetooth (blåtann) samt fra personen som laster ned appen og tar den i bruk.

Av personvernkonsekvensvurderingen, ROS-analysen og personvernerklæringen fremgår det at følgende personopplysninger samles inn:

- mobiltelefonnummer
- alder
- GPS-posisjon (kontinuerlig registrering av bevegelsesmønster (lengdegrad, breddegrad, høyde over havet, hastighet og tid på ulike lokasjoner) når Smittestopp er aktivert og mobiltelefonen er påslått)
- generert UUID fra Smittestopp (unik ID som følger telefonnummeret)
- operativsystem, mobiloperatør, versjonsnummer og telefonmodell
- Bluetooth-data om Smittestopp-apper på andre mobiltelefoner innenfor telefonens Bluetooth-rekkevidde (kontinuerlig logging av start- og sluttidspunkt for kontakt, UUID for telefoner i nærheten og vektor med signalstyrke)

I FHIs varslingsløsning vil i tillegg følgende personopplysninger lagres:

- fødselsnummer
- bostedskommune
- prøvesvardato fra MSIS-registeret[7]
- den smittedes mobiltelefonnummer (hentet fra Kontakt- og reservasjonsregisteret)
- subdatasett hentet fra data innsamlet fra Smittestopp (dag for nærkontakt og mobiltelefonnummer til alle som har vært i nærkontakt med smittede)

Personopplysningene lagres først lokalt på den enkeltes mobiltelefon. Da Smittestopp ble lansert, skjedde lagringen i ukryptert form. I en oppdatert versjon av appen, er lagringen gjort kryptert.

Omtrent én gang i timen (forutsatt at Smittestopp er aktivert og telefonen er påslått) sender appen dataene til den sentrale skylagringsløsningen. Appen vil forsøke å sende data frem til kontakt er oppnådd og i inntil syv dager. Dataene lagres så sentralt i maksimalt 30 dager.

I personvernkonsekvensvurderingen (under trinn 4) og i ROS-analysen (punkt 7.3 flg.) påpeker FHI at det å lagre data sentralt innebærer et større inngrep i personvernet enn lokal lagring på den enkeltes mobiltelefon. Sentral lagring må derfor være *nødvendig* for at formålene skal kunne oppnås.

FHI begrunner sentral lagring med at det vil gi mer presis sporing av nærkontakter og at det muliggjør analyser av befolkningens bevegelsesmønster og effekten av smitteverntiltak. I enkelte punkter i ROS-analysen har FHI redegjort nærmere for bakgrunnen for beslutningen om sentral lagring, og vi vil gjennomgå disse under.

[7] MSIS er et akronym for Meldingssystem for smittsomme sykdommer.

Smittestopp baserer seg på at den enkelte skal kunne varsles om covid-19-smitte hos en såkalt «nærkontakt». I personvernkonsekvensvurderingen og personvernerklæringen redegjør FHI for definisjonen av nærkontakt: det vil si en person (mobiltelefon) der kontakten har vært innenfor to meters avstand i et tidsrom på minst 15 minutter.

I personvernkonsekvensvurderingen og ROS-analysen fremgår det at Bluetooth-dataene som samles inn og lagres sentralt ikke er begrenset til definisjonen av «nærkontakt» (to meter). Bluetooth-data samles inn for hele telefonens Bluetooth-rekkevidde. FHI begrunner dette med at definisjonen av nærkontakt vil kunne forandre seg og at man derfor ønsker å hente inn data for en større mengde kontakter (innenfor ca. 10 meter og av varighet under 15 minutter). FHI mener også at kontaktdataene vil kunne bli mer presise dersom lokasjonsdataene fra GPS og Bluetooth-dataene sammenstilles sentralt.

I ROS-analysens punkt 7.3.13 har FHI vurdert risikoen for at det samles inn og lagres personopplysninger som ikke er nødvendige for å oppnå formålet. Når det gjelder smittesporing og varsling, viser FHI til at informasjon om nærkontakter må lagres i en periode fordi påvisning av og varsling om smitte kan ta tid. FHI mener også at annen kontaktinformasjon (fra GPS/Bluetooth) må lagres i en periode fordi definisjonen av en nærkontakt kan bli endret i fremtiden.

Det fremgår videre at personidentifiserbare data vil bli lagret i maksimalt 30 dager. FHI har opplyst at lagringstiden vil bli redusert til maksimalt 10 dager; se nærmere om dette under punkt 5 under.

Hva gjelder overvåking av befolkningens bevegelser og evaluering av effekten av smitteverntiltak, angir FHI at analysene trolig vil basere seg på alle innsamlede opplysninger, men i anonym og aggregert form. Ifølge FHI er det foreløpig vanskelig å si hvilke data som vil ha størst nytteverdi; dette vil bli avdekket gjennom analysene. FHI mener likevel at evaluering av nytteverdien av konkrete innsamlede data bør gjøres «når økt kunnskap og erfaring tilsier det».

I punkt 7.3.14 i ROS-analysen har FHI vurdert risikoen for at formålene med Smittestopp-løsningen kunne vært oppnådd med lokal lagring på den enkeltes mobiltelefon, som er en mindre personverninngripende løsning. Det fremgår at FHI konkluderer med at nytteverdien av sentral lagring oppveier ulempene. FHI viser igjen til at sentral lagring av GPS- og Bluetooth-data gjør at man kan overvåke og analysere anonyme data om befolkningens bevegelsesmønster samt effekt av smitteverntiltak. Slike analyser forutsetter at dataene lagres sentralt.

Videre viser FHI til at sentral lagring av lokasjons- og kontaktinformasjon kan føre til mer nøyaktig sporing og mer presise vurderinger av nærkontakt. Ved å ha dataene lagret sentralt kan man også varsle raskere ved smitte, ettersom man unngår forsinkelsen det kan innebære å kontakte den smittede, som så må laste opp sine data.

4.2 Evaluering av nytteverdi

I det innledende sammendraget i ROS-analysen (punkt 1.2 Anbefalte tiltak) har FHI presisert at appen Smittestopp er en inngripende løsning og at inngrepet i personvernet kun kan forsvares dersom løsningen er tilstrekkelig samfunnsnyttig.

FHI anbefaler at det gjøres nye vurderinger av nødvendigheten av og forholdsmessigheten ved appen Smittestopp etter hvert som FHI får mer kunnskap om oppslutning i befolkningen og effekt av tiltaket. Også av personvernkonsekvensvurderingen fremgår det at denne må oppdateres/revideres når man har mer kunnskap.

I punkt 7.3.4 i ROS-analysen er risikoen knyttet til nødvendighetskravet vurdert. FHI har konkludert med at «samfunnsnytten av sporingssystemet i vesentlig grad overgår de mulige ulempene for personene som velger å benytte Smittestopp». Det fremgår videre at samfunnsnytten av tiltaket vil øke med antall personer som tar appen i bruk. FHI har likevel vurdert at Smittestopp vil være nyttig selv om en mindre andel av befolkningen bruker appen.[8] Det er anført at overvåkingen på befolkningsnivå vil kunne gjøre det mulig å følge smitteutbredelse og dermed lempe på inngripende samfunnsmessige restriksjoner på et tidligere tidspunkt fordi tiltakene blir mer målrettede.

I ROS-analysens punkt 7.3.12 har FHI vurdert risikoen for at nytteverdien ikke står i forhold til inngrepet Smittestopp utgjør. Det fremgår at nytteverdien av digital smittesporing avhenger av flere faktorer, som antall personer som bruker appen og presisjonen av den tekniske datainnsamlingen. FHI har også her konkludert med at appen vil ha nytteverdi selv om en mindre andel av befolkningen enn det uttalte målet på 60 % tar appen i bruk. Ifølge ROS-analysen kan også mindre mengder data gi kunnskap om befolkningens bevegelsesmønster, og man kan følge med på antall kontakter og varighet av kontakter i ulike områder. Det er vist til at slik kunnskap er viktig for utarbeidelsen av matematiske modeller, som kan brukes til simulering av beredskapstiltak.

I ROS-analysen er det ikke angitt noen grenseverdi for når appen ikke lenger vil ha samfunnsnytte når det gjelder overvåking av befolkningens bevegelser og analyse av smitteutbredelse.

I punkt 7.3.12 fremheves det også at presisjonsnivået på de innsamlede dataene er noe usikkert. Ifølge FHI viser tester at kombinasjonen av GPS- og Bluetooth-data gir god informasjon. Det er presisert at kvaliteten på innsamlede data bør vurderes fortløpende og nytteverdien evalueres.

Ifølge de siste tilgjengelige tallene fra FHI per 03.06.2020[9], var det 592 924 aktive brukere av Smittestopp. Etter våre beregninger tilsvarer dette snaut 14 % av befolkningen over 16 år.

[8] FHIs uttalte mål om oppslutning og bruk av appen Smittestopp er på 60 % av befolkningen.
[9] https://www.fhi.no/sv/smittsomme-sykdommer/corona/nokkeltall-fra-smittestopp/

4.3 Innsynsløsningen

Gjennom klager fra enkeltpersoner og en avviksmelding fra FHI har det kommet frem at innsynsløsningen for Smittestopp, en digital løsning via Helsenorge.no, ikke fungerer.

Avviksmeldingen er registrert mottatt hos oss den 05.06.2020. I meldingen fremgår det at kall mot databasen (fra Helsenorge.no) bruker for lang tid, og løsningen går derfor i time-out. Ifølge FHI har avviket sammenheng med hvordan Simulas database er strukturert. FHI har ingen manuell løsning for håndtering av innsynsbegjæringene.

Avviket har vedvart fra løsningen ble lansert den 16.04.2020, og FHI har vært kjent med avviket siden 25.05.2020. Det er angitt at Simula arbeider med å løse problemet.

5. Redegjørelse fra FHI

I en redegjørelse datert 01.06.2020 har FHI uttalt seg til spørsmålene Datatilsynet stilte i brev av 19.05.2020.

Når det gjelder smittesporing, har FHI gjennom appen kunnet sammenligne smittesporing for 28 personer i testkommunene. Flere av disse var i karantene, mens andre allerede var kjent for kommunens smittesporingsteam, slik at SMS-varsling ikke ble ansett hensiktsmessig. FHI angir at andre smittede igjen har hatt kontakter som Smittestopp har identifisert.

Ifølge FHI er imidlertid datagrunnlaget ikke tilstrekkelig for å justere algoritmene slik man må for å optimalisere treffsikkerheten når det gjelder identifikasjon av nærkontakter. Erfaringsgrunnlaget har også pekt på andre forhold som FHI trenger mer data om, særlig knyttet til bruk av GPS-data i kombinasjon med Bluetooth.

FHI har ikke analyseløsningen og en løsning for anonymisering på plass. Det er dermed ikke analyseresultater å redegjøre for. FHI jobber med å få etablert den tekniske løsningen; det er tunge spørringer som skal gjøres i databasen for å sikre anonymitet.

FHI anfører at vurderingen av nytteverdien av Smittestopp er sammensatt og avhengig av epidemiens utvikling så vel som utviklingen av andre tiltak som testing, isolering og karantene. FHI mener at dagens smittesituasjon, som har medført forlengelse av perioden med validering og justering av algoritmene, tilsier at det er for tidlig å vurdere nytteverdien for Smittestopps enkeltformål så vel som appen som helhet. Ifølge FHI er det også et spørsmål om *i hvilken grad* formålene kan nås snarere enn om de kan nås eller ikke.

Videre viser FHI til at krisen og beredskapssituasjonen ikke er over selv om Norge har fått kontroll på smitteutbredelsen i befolkningen gjennom svært omfattende samfunnstiltak. Covid-19-pandemien må fortsatt håndteres, og risikoen for smitte vil øke etter hvert som samfunnet åpnes opp, all den tid det ikke er flokkimmunitet i befolkningen og en vaksine ikke foreligger. Ifølge FHI er Smittestopp et av flere tiltak som må sees i sammenheng. Digital smittesporing gjennom Smittestopp vil være et supplement til manuell smittesporing, og appen vil potensielt kunne fange opp nærkontakter smittede ikke kjenner eller husker. FHI mener også at Smittestopp vil kunne gi indikatorer som er nyttige for vurderinger av lokale, regionale eller nasjonale målrettede tiltak.

Når det gjelder spørsmålet om sentral lagring, viser FHI at det er begrensninger ved kapasiteten til Bluetooth. Bluetooth alene vil for eksempel ikke vise varigheten av en kontakt. FHI anfører også at EDPB åpner for en sentralisert tilnærming, jf. EDPBs retningslinjer avsnitt 42. Videre angir FHI at det ved oppstarten (medio mars) var få gode alternativer til bruk av Bluetooth og GPS samlet, noe også den oppnevnte ekspertgruppen har uttalt seg om. Det fremgår at FHI nå vil vurdere Google og Apples løsning med forbedret Bluetooth-funksjonalitet og den totale nytteverdien ved denne løsningen.

Videre opplyser FHI at det i Produktstyremøte[10] 27.05.2020 ble besluttet at FHI skal redusere lagringstiden for personopplysninger. Etter denne beslutningen skal data kun lagres i det antall dager som FHI på bakgrunn av erfaring finner det nødvendig for å kunne spore kontakter i smittesporingsarbeidet. Antatt antall dager vil være under 10 dager. Nøyaktig antall dager var ikke endelig fastsatt på tidspunktet for redegjørelsen, men var forventet innen kort tid. Brukerne av Smittestopp vil få beskjed om endringen så snart den er implementert.

I en revidert fremdriftsplan for Smittestopp, datert 08.06.2020, viser FHI til at det er gjort en forholdsmessighetsvurdering av løsningen på overordnet nivå. Videre fremgår det: «Dette er gjort gjennom DPIA og samfunnsnytten av en slik løsning er også vurdert av Helse- og omsorgsdepartementet gjennom kongelig resolusjon i forbindelse med vedtagelse av forskriften».

6. Ekspertgruppens rapport

Helse- og omsorgsdepartementet oppnevnte den 04.04.2020 en ekspertgruppe som skulle gjennomgå sikkerheten i kildekoden til appen Smittestopp. Ekspertgruppen leverte sin endelige rapport den 18.05.2020.

Ekspertgruppen har ikke omtalt nærmere komponentene for automatisk smittevarsling per SMS og modulen for avidentifiserte og aggregerte data, ettersom disse komponentene ikke var tatt i bruk på tidspunktet for rapporten.

Under overskriften «Data og personvern» (side 19), fremhever ekspertgruppen at Smittestopp avviker fra andre digitale løsninger for å håndtere covid-19-pandemien ved at den har to formål: smittesporing og evaluering av effekt av smitteverntiltak. Smittestopp kan dermed ikke uten videre sammenlignes med andre digitale smittesporingsløsninger som kun dekker ett av formålene.

Ekspertgruppen skriver: «De to forskjellige formålene har ikke nødvendigvis behov for samme type data. For å kunne diskutere dette i en personvernkontekst må vi se på disse hver for seg».

I rapportens avsnitt om kontaktsporing (side 19) drøfter ekspertgruppen muligheten for å begrense innsamlingen og lagringen av data (dataminimering). Det fremgår at man teoretisk

[10] Produktstyremøtet ledes av FHI som prosjekteier/dataansvarlig og består av representanter fra Direktoratet for e-helse, Helsedirektoratet, Simula, Norsk helsenett og flere sentrale prosjektressurser internt ved FHI.

sett vil kunne oppnå kontaktsporing ved å lagre Bluetooth-ID-en til alle mobiltelefoner i nærheten lokalt på den enkelte mobiltelefon. Deling av enhets-ID-ene vil så kunne skje ved registrert smitte. Ekspertgruppen angir at verken Bluetooth eller GPS i praksis vil gi perfekte data for kontaktsporing. Bluetooth kan ha problemer med manglende kontakt på grunn av sovende mobiltelefoner og varierende signalstyrke. GPS har som regel en nøyaktighet på tre til 10 meter og fungerer best utendørs. Med sentral lagring av begge typer data, kan man kompensere noe for disse svakhetene, ved å korrelere forskjellige datakilder. Ifølge ekspertgruppen var det få gode alternativer til slik sentral lagring ved prosjektstart.

I ettertid har Google og Apple kunngjort at de vil lansere utvidelser av Bluetooth-API-er for kontaktsporing, noe som kan redusere behovet for sentral lagring. Ekspertgruppen mener at lagring av data lokalt på mobiltelefonen nå kan være et realistisk alternativ, men det er per i dag ukjent hvor gode resultater man kan få uten å gjøre kompensering med sentralt lagrede data.

Under avsnittet om analyse av hvordan smitteverntiltak påvirker befolkningens bevegelsesmønster (side 20), fremgår det at det er behov for GPS-data for å kunne vite hvordan befolkningen beveger seg. Når det gjelder Bluetooth-data, blir de i denne sammenheng brukt for å telle antall nærkontakter mellom personer på ulike stedskategorier.

Ekspertgruppen angir at det vil være mulig i stedet å «aggregere GPS- og Bluetooth-data på mobiltelefonen og legge til støy med visse statistiske egenskaper, som ledd i en «differential-privacy»-tilnærming, før de blir lastet opp til en sentral server uten at dette vil forringe kvaliteten til datasettet».

Ekspertgruppen har gjort en evaluering av Smittestopp (side 22 flg.).

Under overskriften «Innsynsløsning» fremgår det at sletting av opplastede data fra mobiltelefonen også medfører sletting av lagrede data om hvem som har hatt innsyn i opplysningene.

Under «Flere formål» (side 23) påpeker ekspertgruppen:

> «Ved å kombinere de to formålene smittesporing og vurdering av effekt av smitteverntiltak i samme app forventes det at flere vil laste ned appen, enn det som ville lastet ned en app som bare deler data for forskning/analyse. Man risikerer likevel at potensielle brukere som ville ha lastet ned en ren smittesporingsapp, ikke er komfortable med å laste ned den kombinerte appen.
>
> Andelen av befolkningen som må laste ned appen er veldig forskjellig for de to formålene. For å oppnå god effekt ved smittesporing må godt over halvparten av befolkningen ha appen. For å få gode datasett for forskning/analyse kan så lite som 10% utbredelse være nok.
>
> Å oppnå 60% utbredelse av kontaktsporing er et ambisiøst mål. Hvis man lot brukerene selv bestemme om de vil dele data til forskning/analyse, ville nok flere

> valgt å laste ned appen. I og med at utbredelseskravene for å oppnå formålet er så mye mindre for forskning/analyse, tror vi heller ikke at dette formålet ville blitt negativt påvirket med et slikt valg».

Under «Sentral vs. lokal lagring» (side 24) angir ekspertgruppen at sentral lagring av dataene bidrar til kontaktsporing av høyere kvalitet. Det fremgår at sentral lagring kan kompensere for svakheter i måten Bluetooth er implementert på i løsningen.

Det er likevel påpekt at man etter hvert vil kunne gå over til en mer distribuert løsning (lokal lagring på den enkeltes mobiltelefon). Ekspertgruppen angir også at man ved å skille formålet om smittesporing fra andre formål vil kunne redusere mengden innsamlede data for de som kun ønsker å gi fra seg data til smittesporing.

Ekspertgruppen peker også på at dette kan redusere risikoen ved sentral lagring, ettersom de negative konsekvensene vil være store dersom sentralt lagrede data blir utsatt for datainnbrudd eller andre former for misbruk eller sikkerhetsbrudd.

Under «Utviklingsløpet» (side 27) har ekspertgruppen fremhevet at det å bruke mobiltelefoner i smittesporing er helt nytt, og det har ikke tidligere vært implementert og testet i stor skala. Teknologien som brukes, Bluetooth og GPS, er verken laget for formålet eller helt nøyaktig. Ifølge ekspertgruppen er det derfor «uklart om man vil kunne oppnå praktisk fungerende kontaktsporing».

Videre skriver ekspertgruppen:

> «For å ivareta personvernet er det viktig at det strammes inn på innsamling og bruk av personlig data så tidlig som mulig i utviklingsprosessen. Man kan argumentere for at man fremdeles er så tidlig i utviklingsløpet at man ikke har kommet til et punkt der det er naturlig å starte innstrammingen. I så fall ville man forventet at man bare samler inn data som hjelper med å forbedre appen. Man burde ikke åpne for å laste ned appen utenfor testkommuner før man er ferdig med valideringsfasen».

Ekspertgruppens oppsummering (side 28) lyder slik:

> «I en test- og utviklingsfase hvor man hurtigst mulig ønsker å validere hvordan mobiltelefonbasert kontaktsporing kan implementeres, kan man bruke testdata som er frivillig donert av beta brukere. Når man har funnet en funksjonell løsning, må man sørge for å ta hensyn til ikke-funksjonelle krav som sikkert og personvern, før man starter på neste fase av utviklingsløpet.
>
> At ikke-funksjonelle krav ikke enda var ivaretatt var grunnen til at vi anbefalte å ikke ta appen ut av testfasen i vår midlertidige rapport. Vi mente at den ikke var klar i forhold til sikkerhet. De tekniske og arkitektoniske valgene i løsningen slik den foreligger i dag har betydelige personvernskonsekvenser. Vi kan ikke se at disse er tilstrekkelig hensyntatt i utformingen av løsningen. Det er fremdeles viktige betraktninger rundt personvern som bør hensyntas før lansering».

Og videre under «Konklusjon» (på side 29):

> «**Personvern**
> (…) Vi mener det finnes mange muligheter for å redusere mengden data som lagres i eksisterende løsning eller ved å bytte ut deler eller hele systemet med andre funksjonelt ekvivalente løsninger. Derfor mener vi at personvernet ikke er forsvarlig ivaretatt per i dag».

Ekspertgruppen kommer også med flere konkrete anbefalinger (side 29 og 30). Vi vil gjengi enkelte av disse.

Det anbefales å dele opp formålene om smittesporing/-varsling og evaluering av smitteverntiltak gjennom analyser/forskning, slik at brukerne kan velge å bidra til kun ett av formålene. Ifølge ekspertgruppen kan dette være et godt virkemiddel både for å ivareta brukernes interesser og for å øke oppslutningen om Smittestopp.

Ekspertgruppen mener også at FHI bør vurdere en mer distribuert løsning når valideringsfasen er over, det vil si når det finnes en stabil algoritme for kontaktsporing. Gruppen peker på at en helt eller delvis distribuert implementasjon[11] vil kunne være mindre inngripende i personvernet og samtidig øke oppslutningen.

Videre peker ekspertgruppen på at man på dette tidspunktet også vil kunne gå over til en distribuert modell for innsamling av data; det vil si at man gjør kontaktsporing uten å laste opp lokasjonsdata og Bluetooth-data sentralt, men produserer datasett uten å laste opp rådata. I stedet kan man lage datasett med bruk av «*differential privacy*»-filtre før data lastes opp sentralt. Ekspertgruppen angir at dette vil bidra til ytterligere å redusere inngrepet i personvernet.

7. Datatilsynets vurderinger

Appen Smittestopp er et svært personverninngripende tiltak, også i en unntakssituasjon. Datatilsynet er ansvarlig for å kontrollere at behandlingen av personopplysninger i tilknytning til Smittestopp er nødvendig for å nå formålene og at personverninngrepet er forholdsmessig. Dette vil blant annet avhenge av samfunnsnytten av løsningen.

I de siste offisielle anslagene har FHI anslått at mellom 50 og 550 personer i Norge i dag er smittet av koronaviruset.[12] Dette tilsvarer 0,01 % av Norges befolkning.[13] Mange av landets kommuner vil dermed være helt fri for smitte, og smitterisikoen har sunket betraktelig siden Smittestopp ble lansert 16.04.2020.

[11] Vi forstår dette som lagring lokalt på den enkeltes mobiltelefon og at data deles først når smitte er påvist.
[12] Se for eksempel https://forskning.no/ntb-sykdommer-virus/opp-mot-550-koronasmittede-i-norge-na-anslar-fhi/1694566.
[13] Norges befolkning 1. kvartal 2020 er ifølge Statistisk sentralbyrå på 5 372 355 personer. Lenke: https://www.ssb.no/befolkning/faktaside/befolkningen

De eksisterende smitteverntiltakene (testing, isolering, manuell smittesporing og karantene) samt manuell smittesporing synes å fungere godt, og covid-19-smitten må i dag kunne sies å være under tilstrekkelig kontroll.

Vi vil også påpeke at det per 28.05.2020[14] er opprettet et beredskapsregister for covid-19 som gir FHI daglig oversikt over antall smittetilfeller, sykehusinnleggelser, intensivinnleggelser og dødsfall. Smitte registreres også i MSIS-registeret. Helsemyndighetene har dermed mye kunnskap om smitteutbredelsen i samfunnet uavhengig av Smittestopp, et faktum som har innvirkning på vurderingen av tiltakets nødvendighet.

7.1 Formålsbegrensning og dataminimering

Appen Smittestopp har flere ulike formål: Oppsporing av og varsling om covid-19-smitte, evaluering av effekt av smitteverntiltak og smitteutbredelse på bakgrunn av analyser av befolkningens bevegelsesmønster samt forskning. FHI samler inn svært store mengder personopplysninger gjennom appen Smittestopp, herunder inngripende opplysninger som lokasjonsdata.

Datatilsynet har tidligere stilt spørsmål ved nødvendigheten av å lagre samtlige personopplysninger som samles inn i en periode på 30 dager. FHI har opplyst at det er besluttet å endre lagringstiden fra 30 dager til maksimalt 10 dager. Dette ser vi positivt på.

Som behandlingsansvarlig er FHI ansvarlig for å klargjøre hvilke personopplysninger som behandles til hvilke formål, og FHI må godtgjøre at det er *nødvendig* å behandle hver konkrete (kategori av) personopplysning for det enkelte formål.

FHI har redegjort for hvilke personopplysninger som behandles for formålet om oppsporing av og varsling om smitte. Det er imidlertid fortsatt ikke angitt hvilke personopplysninger som skal anonymiseres og aggregeres for analyse (og eventuelt forskning). Slik vi har forstått det, har dette sammenheng med at analyseløsningen ikke er på plass. Vi er likevel svært kritiske til at det etter nærmere to måneder ikke er mulig å presisere hvilke av de innsamlede personopplysningene som vil bli benyttet til formålet analysearbeid.

Videre vil vi presisere at personverninngrepet skjer ved selve innsamlingen av personopplysningene, og ikke først når dataene behandles videre. Slik Smittestopp er utformet, skjer innsamlingen av personopplysninger fra samtlige brukere løpende. Personverninngrepet er dermed like stort uavhengig av at funksjonaliteten til varslingsordningen og analysesystemet ennå ikke er på plass. Omfattende mengder personopplysninger om alle Smittestopps brukere samles inn til enhver tid, selv om det per i dag verken er mulig å benytte disse dataene til smittesporing/-varsling (annet enn i testkommunene) eller i analysearbeid.

Vi viser også til at Ekspertgruppen har konkludert med at man ikke burde åpne for å laste ned appen utenfor testkommuner mens man fortsatt er i valideringsfasen, slik som i dag.

[14] https://www.fhi.no/sv/smittsomme-sykdommer/corona/norsk-beredskapsregister-for-covid-19/

På denne bakgrunn mener Datatilsynet at personopplysningene som per i dag samles inn gjennom Smittestopp *ikke* er begrenset til det som er nødvendig for å nå formålene, slik prinsippet om dataminimering krever, jf. personvernforordningen artikkel 5 nr. 1 bokstav c.

Når det gjelder GPS-data, har FHI argumentert for hvorfor det er nødvendig med bruk av lokasjonsdata i tillegg til Bluetooth-data for å oppnå en kontaktsporing og varsling om covid-19-smitte som er så presis som mulig. Ekspertgruppen understøtter at det på tidspunktet da løsningen ble utarbeidet ikke fantes noen gode alternativer til sammenstilling av data fra Bluetooth og GPS.

Ekspertgruppen mener imidlertid at FHI kan gå over til en mer distribuert (desentralisert) løsning når det finnes en stabil algoritme for kontaktsporing. I en slik modell vil man også kunne desentralisere selve innsamlingen av data; det vil si at kontaktsporingen kan skje uten at lokasjonsdata og Bluetooth-data lastes opp sentralt. Det er også vist til at Google og Apple utarbeider en løsning som kan gi tilstrekkelig god Bluetooth-funksjonalitet. FHI har selv vist til at man skal vurdere om denne løsningen kan tas i bruk.

Både EDPB og WHO fraråder også å bruke lokasjonsdata i smittesporingsarbeidet. Bruk av lokasjonsdata er svært inngripende ettersom det vil gi myndighetene full oversikt over et individs bevegelser til enhver tid.

Ifølge en rapport fra FRA – European Agency for Fundamental Rights[15] har minst 13 land i EU utarbeidet smittesporingsapper som kun baserer seg på Bluetooth-teknologi. Minst ni av landene har også en fullt ut desentralisert tilnærming, der brukerne kan velge å dele data med myndighetene ved behov.

Etter vårt syn, taler dette klart i retning av at Bluetooth-teknologi er tilstrekkelig til å oppnå formålet om oppsporing av og varsling om covid-19-smitte. Vi mener at FHI ikke har godtgjort at bruk av GPS-lokasjonsdata er *strengt nødvendig* for dette formålet, jf. prinsippet om dataminimering og kravet om nødvendighet i personvernforordningen artikkel 5 nr. 1 bokstav c.

Vi mener dessuten at FHI har misforstått EDPBs anbefaling om sentraliserte løsninger. Valget mellom en sentralisert og desentralisert modell knytter seg til hvordan smittesporingen skal foregå når en person har blitt bekreftet smittet. Forutsetningen i EDPBs retningslinjer er at de berørte personenes enhets-ID-er skal lagres på den enkeltes enhet (mobiltelefon) inntil smitte er påvist. En eventuell sentral server skal kun motta data når smitte er bekreftet og etter at brukeren frivillig har godkjent at dataene lastes opp til serveren. FHIs sentrale løsning er klart i strid med denne anbefalingen fra EDPB.

Slik vi ser det, er en viktig grunn til at FHI lagrer dataene sentralt at man også vil bruke lokasjonsdata til analyser og modellering. I EDPBs retningslinjer er det presisert at

[15] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf. Se punkt 4.2 i rapporten.

smittesporing og analysearbeid er to ulike formål og at det må være valgfrihet for brukerne når det gjelder hvilke(t) formål man vil bidra til.

Vi viser ellers til at ekspertgruppen har angitt at forskjellige typer data er nødvendige for de ulike formålene om smittesporing/-varsling og analysearbeid.

FHI har angitt at man vil vurdere en løsning der det skilles mellom formålene, slik at brukerne kan velge å avgi data til kun ett (eller enkelte) av formålene. Dette vil i tilfelle være en vesentlig mer personvernvennlig løsning, særlig dersom det ikke lenger vil være nødvendig å samle inn GPS-data for formålet om smitteoppsporing/-varsling.

7.2 Evaluering av nytteverdi

At personopplysningene som samles inn er nødvendige for formålet, er grunnleggende for å ivareta prinsippet om dataminimering. For at personopplysninger skal kunne anses nødvendige, forutsettes det at dataene bidrar til at formålet nås. Dersom behandlingen av personopplysninger ikke viser seg nyttig, kan dataene heller ikke anses nødvendige.

Det er også et grunnleggende krav at ethvert inngrep i privatlivet og personvernet er forholdsmessig; inngrepet må stå i forhold til nytteverdien.

I FHIs ROS-analyse fremheves det flere steder at inngrepet i personvernet som Smittestopp utgjør kun kan forsvares dersom appen viser seg å være nyttig i arbeidet med spore opp og varsle om covid-19-smitte samt evaluere smitteverntiltak.

I sin redegjørelse til Datatilsynet viser FHI til at det er gjort en overordnet vurdering av forholdsmessigheten av Smittestopp gjennom personvernkonsekvensvurderingen. Videre viser FHI til at Helse- og omsorgsdepartementet vurderte forholdsmessigheten av tiltaket da det ble besluttet en forskrift for formålet.

Til dette vil vi påpeke at vurderinger som gjøres i forbindelse med vedtakelse av forskrifter og før oppstart av en behandling ikke er tilstrekkelige til å konkludere med at inngrep i grunnleggende personvernrettigheter er forholdsmessige til enhver tid. Vurderingene av nytteverdi og forholdsmessighet må være dynamiske og ta høyde for endringer i de faktiske forutsetningene.

I Norge har vi i dag en helt annen smitteutbredelse enn det som var tilfellet da arbeidet med Smittestopp ble påbegynt. Den teknologiske utviklingen er også stadig pågående. Dette vil spille inn i den løpende vurderingen av hva som til er et forholdsmessig tiltak.

Nytteverdien ved appen Smittestopp har hele tiden vært angitt som usikker og betinget av befolkningens deltakelse. Smittestopp har nå vært virksom i nærmere to måneder. Andelen aktive brukere er på ca. 14 % av befolkningen. Siden lanseringen har appen imidlertid hatt mer enn 1,5 millioner nedlastninger[16], noe som innebærer at enorme mengder personopplysninger totalt sett er samlet inn i perioden.

[16] https://www.fhi.no/sv/smittsomme-sykdommer/corona/slik-har-fhi-utviklet-smittestopp/

Ut fra FHIs redegjørelse, har den praktiske nytten i testkommunene når det gjelder smittesporing/-varsling vært begrenset til et fåtall personer. Den lave datamengden gjør at nødvendig justering av algoritmene ikke er mulig, noe som gjør at det per nå ikke er mulig å konstatere noen nytteverdi av smittesporings-/varslingsløsningen for det store flertallet brukere.

Analyseløsningen og løsningen for anonymisering og aggregering av data er ikke på plass. De store mengdene innsamlede personopplysninger kan dermed ikke ha hatt noen nytte for formålet om evaluering av smitteverntiltak og smitteutbredelse.

Det fremgår av både FHIs redegjørelse og ekspertgruppens rapport at Smittestopp vil kunne være et nyttig tiltak selv om kun en mindre andel av befolkningen bruker appen. Datatilsynet bestrider ikke dette. Vi vil imidlertid peke på at funksjonaliteten per i dag ikke er på plass eller god nok for noen av formålene.

Vi kan ikke se at FHI gjennom personvernkonsekvensvurderingen eller redegjørelsen i saken har gjort en reell vurdering av den løpende situasjonen når det gjelder nytteverdi og omfanget av personverninngrepet som innsamlingen av de store mengdene data utgjør. FHI har hittil fastholdt at innsamlingen av personopplysninger til alle de uttalte formålene skal vedvare selv om den faktiske nytteverdien av Smittestopp hittil har vist seg svært begrenset.

Vi mener derfor at det vesentlige personverninngrepet som Smittestopp utgjør ikke er forholdsmessig ut fra dagens situasjon. Dette knytter vi både til løsningene som er valgt i Smittestopp, dagens oppslutning om appen og smitteutbredelsen i befolkningen. Vi viser til de grunnleggende kravene til inngrep i privatlivet i grunnloven § 102 og EMK artikkel 8.

7.3 Ivaretakelse av den registrertes rettigheter

God ivaretakelse av den registrertes rettigheter har vært løftet frem som et viktig kompenserende tiltak i vurderingen av Smittestopp som et inngrep i personvernet. Den automatiske innsynsløsningen har imidlertid ikke fungert i perioden Smittestopp har vært virksom, og FHI har ikke noen manuell backupløsning for håndtering av innsynsbegjæringer.

Ekspertgruppen har også påpekt at sletting av opplastede data fra mobiltelefonen medfører sletting av lagrede data om hvem som har hatt innsyn i opplysningene.

Begge disse forholdene er klare brudd på retten til innsyn etter personvernforordningen artikkel 15, og det medfører igjen at prinsippet om åpenhet ikke er overholdt, jf. artikkel 5 nr. 1 bokstav a.

At de registrerte ikke får ivaretatt sine grunnleggende rettigheter etter personvernregelverket, understøtter også vårt synspunkt om at personverninngrepet ikke kan anses forholdsmessig.

7.4 Oppsummering

Datatilsynet mener at datainnsamlingen som foregår i tilknytning til Smittestopp ikke er begrenset til det som er nødvendig for å nå formålene. Dette gjelder spesifikt også for bruk av

lokasjonsdata for smittesporing/-varsling. Prinsippet om dataminimering er dermed ikke overholdt, jf. personvernforordningen artikkel 5 nr. 1 bokstav c.

Videre kan vi ikke se at Smittestopp har en dokumentert nytteverdi for formålene om smittesporing/-varsling og evaluering av smitteverntiltak/smitteutbredelse gjennom analysearbeid. Vi mener at Smittestopp ikke er et forholdsmessig inngrep i personvernet ut fra dagens situasjon, ut fra løsningene som er valgt i appen, oppslutningen om Smittestopp og smittesituasjonen i Norge. Vi viser i den forbindelse til de grunnleggende kravene i grunnloven § 102 og EMK artikkel 8.

Både EDPB og ekspertgruppen anbefaler å skille formålet om smittesporing/-varsling fra andre formål, slik at den enkelte bruker kan velge å dele data til kun ett eller enkelte formål. Vi mener at dette vil være en vesentlig mer personvernvennlig innretning av appen. Vi har merket oss at FHI jobber med dette som en mulig løsning.

FHI har opplyst at man vurderer å ta i bruk Google og Apples løsning der kun Bluetooth brukes til smittesporing/-varsling.

Vi vil også gjenta at det er positivt at det er vedtatt å redusere lagringstiden til maksimalt 10 dager. Denne beslutningen kan likevel teoretisk sett omgjøres, ettersom forskriftshjemmelen tillater fortsatt lagring av dataene i inntil 30 dager.

Datatilsynet ser det derfor nødvendig å nedlegge et midlertidig forbud mot behandling av personopplysninger knyttet til Smittestopp nå. FHI har ennå ikke konkludert med tanke på om, og eventuelt hvordan, eventuelle tiltak skal iverksettes. Dersom beslutningene overlates til FHI alene, har vi heller ikke noen garanti for at personvernet er godt nok ivaretatt etter vår vurdering.

Som det fremgår, vil et forbud mot å behandle personopplysninger gjelde midlertidig. Slik vi ser det, må FHI enten kunne dokumentere en bedre nytteverdi og forholdsmessighet av løsningen, eller så må vesentlige deler av løsningen endres. Skulle smittesituasjonen i samfunnet endre seg drastisk, kan også vår vurdering av Smittestopp stille seg annerledes.

Vi vil også gjenta at sikkerheten i løsningene for Smittestopp per i dag ikke er ferdig vurdert av oss. Vi vil jobbe videre med dette, og tilfredsstillende sikkerhet i løsningen vil være avgjørende i en vurdering av om behandlingen av personopplysninger knyttet til Smittestopp kan gjenopptas.

8. Varsel om vedtak
Datatilsynet varsler herved følgende vedtak:

> *Folkehelseinstituttet ilegges et midlertidig forbud mot å behandle personopplysninger knyttet til Smittestopp, jf. personvernforordningen artikkel 58 nr. 2 bokstav f.*

9. Videre saksgang
Dette brevet er et forhåndsvarsel om vedtak om pålegg, jf. forvaltningsloven § 16.

FHI har uttrykt ønske om et møte i sakens anledning. Vi stiller oss til disposisjon til et slikt møte og vil ta egen kontakt om dette. Vi presiserer for ordens skyld at alle innspill fra FHI i saken også må gis skriftlig.

Eventuelle kommentarer til dette varselet må sendes til oss senest **innen 23.06.2020**. Ettersom Datatilsynet er av den oppfatning at behandlingen av personopplysninger som skjer i tilknytning til Smittestopp er ulovlig, og dermed burde opphøre umiddelbart, settes det en kort frist for tilbakemelding.

Dersom dere har spørsmål, kan dere ta kontakt med saksbehandler Susanne Lie (tlf.: 22 39 69 57, e-post: suli@datatilsynet.no).

Med vennlig hilsen

Bjørn Erik Thon
direktør

Susanne Lie
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer.