Foto: NTB scanpix



**INNHOLD**

1. Sju råd om Smittestopp og kildevern
2. Hvorfor en veileder
3. Slik virker appen Smittestopp
4. Kildevernet
5. Slik utfordrer Smittestopp kildevernet og personvernet
6. Eksempler på interne råd fra ulike redaksjoner

**1. SJU RÅD OM SMITTESTOPP OG KILDEVERN**

1. Godt kildevern krever at du er i forkant. Kildevernet er et helt sentralt prinsipp i journalistikken. Vær på vakt mot alle trusler mot kildevernet og sørg for at alle redaksjonelle medarbeidere er klar over farer knyttet til å gi fra seg digitale spor eller andre opplysninger som kan avsløre kilder du ønsker å beskytte.

2. Vær oppmerksom på nedkjølingseffekten. Vi må kunne overbevise publikum om at vi ivaretar kildevernet, også når det settes under press. Hvis ikke, risikerer vi at flere vil vegre seg for å ta kontakt med, eller la seg kontakte av, journalister og redaktører.

3. Skaff deg oversikt. Sett deg inn i problemstillingene knyttet til appen Smittestopp. Det er opp til deg som redaktør å velge om du vil åpne for bruk av appen på redaksjonens arbeidsverktøy. Det viktigste er at du og redaksjonen forøvrig har et bevisst forhold til denne appen og andre tjenester som lagrer geo- og persondata.

4. Gi klare og tydelige råd. Lytt til synspunkter fra medarbeiderne og ha god dialog med de tillitsvalgte. Lag gjerne egne råd om bruk av appen. Husk at rådene trenger ikke å være de samme til alle redaksjonelle medarbeidere. Særlig er det viktig at du er oppmerksom på journalister som ofte har - og kan tenkes å ha – fortrolige kildesamtaler.

5. Benytt anledningen til en generell bevisstgjøring rundt betydningen av godt kildevern. Minn om at fortrolig kildekontakt i størst mulig bør grad bør skje enten ved fysiske møter uten medbrakt mobiltelefon eller annet utstyr som kan spores, eller via krypterte kanaler som f eks Signal. Bevisstgjør også kildene om de er godt nok beskyttet, blant annet overfor egen arbeidsgiver.

6. Søk råd og oppdater deg jevnlig. Det hjelper ikke å ha kildevernet som en generell verdi, dersom vi ikke sørger for at de digitale systemene – f eks tipshåndtering – er sikre. Kildevern bør være jevnlig tema i redaksjonen. Utarbeid gjerne en enkel «kildevernmanual».

7. Del gjerne. Åpenhet er en grunnleggende verdi i et demokrati. Mediene bør selv tilstrebe åpenhet om interne rutiner og etiske vurderinger, selvsagt innenfor rammene av kildekritikken og presseetikken forøvrig. Fortell gjerne andre om hvilke rutiner dere har for bruk av Smittevern-appen både i egen organisasjon (også utenfor redaksjonen) og til publikum. NR deler gjerne videre med medlemmene.

**2. HVORFOR EN VEILEDER**

16. april 2020 lanserte Folkehelseinstituttet applikasjonen Smittestopp. Hensikten med appen er samle data om hvordan grupper beveger seg i samfunnet for å måle effekten av tiltakene mot smittespredning og gi brukerne et varsel dersom de har vært i nærkontakt med personer som er smittet av korona-viruset, for på den måten å kunne drive effektiv smittesporing og dermed hindre ukontrollert spredning av viruset.

Norsk Redaktørforening har forståelse for at myndighetene tar i bruk verktøy for å hindre smittespredning i Norge, og viktigheten av at flest mulig deltar i den dugnaden det er å få epidemien under kontroll og i størst mulig grad å beskytte folks liv og helse.

Samtidig er det grupper i samfunnet som vil ha gode grunner for å vegre seg for å installere appen Smittestopp på sin mobiltelefon. Vi har fulgt utviklingen av appen, og har også fulgt debatten om appen helt fra det ble kjent at den var under utvikling, en knapp måned før den ble lansert.

Kildevernet er et helt sentralt prinsipp i journalistikken. Men for å sikre kildevernet er vi nødt til å være i forkant og tenke sikkerhet og vern av kilden i hele prosessen. Smittestopp-appen byr på åpenbare utfordringer knyttet til person- og kildevernet. Den gir langt større muligheter for innsyn i mobil-, geo- og persondata enn det som hittil har vært regulert i lovgivningen og av rettsapparatet.

Problemstillingene knyttet til kildevernet har vært vektlagt av mange i mediebransjen, men også utenfor mediehusene. Både statsminister Erna Solberg og prosjektleder for Smittestopp-appen, Gun Peggy Knudsen i Folkehelseinstituttet, har uttrykt forståelse for at journalister er blant gruppene som må være særlig forsiktig med deling av data i forbindelse med kildekontakt. Til [Dagens Næringsliv 17. april](https://www.dn.no/teknologi/smk/pst/koronaviruset/gjor-sikkerhetsunntak-for-at-erna-solberg-kan-bruke-smitteappen/2-1-793687) sa for eksempel statsministeren følgende

*«Noen kan ha helt spesielle grunner, for eksempel en journalist som treffer en kilde som de absolutt vil være garantert sikker på. Da kan du slå av lokasjonen når du er sammen med den kilden. Jeg har respekt for folks følelser, men jo færre som deltar, desto lengre tid vil det være strengere tiltak på andre områder.»*

En av de viktigste oppgavene til Norsk Redaktørforening er å gi råd til norske redaktører i alle typer publisistiske og andre redaktørfaglige spørsmål. Siden mange redaktører tidlig fikk spørsmål i egen redaksjon om hvordan journalistene og øvrige redaksjonelt ansatte skulle forholde seg til appen, var det naturlig for NR å være raskt på banen og varsle om at vi ville utforme råd til redaktørene. 3. april varslet NR at vi jobbet med en veileder, og samme dag som appen ble lansert kom NR også med foreløpige råd til redaktørene.

Redaktøren har det fulle ansvaret for redaksjonens virksomhet og leder de redaksjonelle medarbeiderne. Det er dermed også opp til den enkelte (ansvarlige) redaktør å avgjøre hvordan man skal forholde seg til appen Smittestopp i den enkelte redaksjon. Noen redaktører har allerede laget egne råd til journalistene om hvordan de skal forholde seg til appen. Andre har bevisst avventet å komme med råd til de vet mer om appen. I noen redaksjoner er det naturlig å skille mellom de journalistene som har – og kan tenkes å ha – fortrolige kildesamtaler og de øvrige medarbeiderne i redaksjonen.

Diskusjonen omkring appen gir også en god anledning for en generell debatt om kildevern og sikkerhet i redaksjonene – særlig knyttet til digitale hjelpemidler. For hva hjelper det at journalister og redaktører har kildevernet sentralt i vår etiske ryggmarg dersom vi ikke samtidig har kunnskaper nok til å forutse situasjoner der teknologien utfordrer vår evne til å beskytte kildene våre? Og hva hjelper det om rutinene våre er gode og systemene sikre, hvis potensielle kilder likevel oppfatter det som utrygt å kontakte oss?

Vi er nøye på å understreke at dette er en veileder, ikke et forsøk på en felles «bransjestandard» eller en fasit. Det er ikke NRs oppgave å fortelle deg hva du skal gjøre, men å gi deg tilstrekkelig informasjon slik at du er best mulig i stand til å finne ut hva som er riktig for deg og din redaksjon.

Tusen takk til alle som har bidratt til denne veilederen. Vi har særlig hatt nytt av bistand fra Frank Gander i NRK, Espen Andersen i Kommunal Rapport/NRs teknologiskvadron, Gard Steiro i VG, Karianne Solbrække i TV 2, Alexandra Beverfjord i Dagbladet, Svein Erik Hole i Teknisk Ukeblad og Ingeborg Volan i Dagens Næringsliv/NRs teknologiskvadron og fra medlemmer i NR-styret. Takk også til nyttig hjelp fra Folkehelseinstituttet, fra Jon Wessel-Aas og andre personverneksperter og fra ulike redaksjoner og kommentatorer som har satt temaet på dagsorden. Samtidig vil vi understreke at innholdet i denne veilederen står for NR-sekretariatets regning.

Informasjonen om appen er ferskvare, og vi vil få bedre kjennskap til den etter hvert. Derfor oppdaterer vi informasjonen fortløpende, og vi er også interessert i dine synspunkter og kommentarer. Har din redaksjon laget interne råd som dere vil dele, så setter vi stor pris på det. Husk at du alltid kan kontakte NRs hotline for individuell rådgivning - både om kildevern og andre spørsmål.

Oslo/Bodø, 28.april 2020

Arne Jensen, generalsekretær

Reidun Kjelling Nybø, ass. generalsekretær

**3. SLIK VIRKER APPEN SMITTESTOPP**

27. mars trådte Forskrift om digital smittesporing og epidemikontroll i anledning utbrudd av Covid-19 i kraft. Forskriften som gjelder fram til 1. desember 2020, er en forutsetning for at myndighetene kan etablere et system for digital og automatisert sporing av nærkontakter til personer som er smittet av koronaviruset.

# Ifølge [forskriften](https://lovdata.no/dokument/SF/forskrift/2020-03-27-475) er formålet med appen todelt. Den skal:

1. bidra til rask oppsporing av og formidling av råd til personer som kan være smittet av koronaviruset SARS CoV-2
2. gjennom overvåkning og analyse på befolkningsnivå bidra til å følge smitteutbredelse og vurdere effekt av smitteverntiltak

Appen Smittestopp er utviklet av det statlige forsknings- og utviklingsselskapet Simula Research Laboratory. Appen bruker telefonnummeret ditt til å identifisere deg. Via GPS blir posisjonen din lagret på mobiltelefonen din. Samtidig bruker appen Bluetooth til å lete opp andre enheter i nærheten som også har appen installert. Appen estimerer avstanden din til disse.

Smittestopp innebærer at det lagres data om brukernes bevegelsesmønster og kontakt med andre mobiltelefoner som har lastet ned den samme appen. Ifølge forskriften skal lokasjons-data slettes etter 30 dager. Ved lansering av appen er det kontakt nærmere enn 2 meter i mer enn 15 minutter i løpet av 24 timer som defineres som nærkontakt ved smittefare.

Når en person får påvist Covid 19 via en test, blir dette registrert i den såkalte MSIS-basen hos Folkehelseinstituttet. MSIS står for Meldingssystem for smittsomme sykdommer. I MSIS-basen blir du registrert med ditt 11-sifrede fødselsnummeret. Dersom du har lastet ned appen, kan fødselsnummeret ditt kobles mot mobilnummeret ditt. Mobiltelefonnummeret hentes fra det sentrale kontakt- og reservasjonsregisteret. Er mobilnummeret ditt ikke registrert her, vil du ikke kunne motta varsel fra appen via sms.

Folkehelseinstituttet bruker følgende eksempel på å beskrive et eksempel på en smittesituasjon: Kari, Georg, Sheila og Per har alle lastet ned Smittestopp. Alle fire er friske. De omgås med ujevne mellomrom. Kari tester etter en stund positivt på covid-19. Idet dette registreres hos FHI, får Georg, Sheila og Per varsel om at de har vært i nærheten av en person som er smittet. De kan da passe på egen helse og gå i karantene.  De får ikke vite når eller hvor dette skjedde. De får ikke vite at det er Kari som er den personen som er "kilden" til at de blir varslet, men det kan heller ikke utelukkes at de vil forstå at det er henne. De vil få vite hvilken dag de var i nærheten av en smittet, så de vet startdatoen for hvor lenge de skal være i karantene.

I beskrivelsen til Folkehelseinstituttet heter det at personopplysningene som samles inn bare vil bli brukt til dette formålet og ikke til å følge med på om enkeltpersonene overholder råd eller pålegg. De understreker at helseopplysningene eller lokasjonsdataene ikke kan gjøres tilgjengelig for politi eller påtalemyndigheter eller brukes i forsikringsøyemed eller av arbeidsgivere og at personopplysningene ikke kan utnyttes kommersielt.

[Her finner du personvernerklæringen](https://www.fhi.no/sv/smittsomme-sykdommer/corona/bruk-av-smittestopp/) for Smittestopp-appen som du må godkjenne dersom du tar den i bruk.

Smittestopp samler inn følgende opplysninger om brukerne:

* Mobilnummer
* Alder
* En ID som genereres for din telefon
* GPS-posisjonen din - det vil si lengdegrad, breddegrad, hastighet, høyde over havet, tid på ulike lokasjoner - når appen er aktivert og mobiltelefonen er påslått
* Informasjon om operativsystem, mobiloperatør, versjonsnummer og telefonmodell
* Bluetooth-data om Smittestopp-apper på andre telefoner som er innen rekkevidde av telefonen, (dvs. starttidspunkt og sluttidspunkt for kontakt, ID-en for telefoner i nærheten, vektor med signalstyrke for telefoner i nærheten) logges kontinuerlig

Disse personopplysningene kan kobles mot personopplysninger i Meldingssystem for smittsomme sykdommer.

En gang i timen sendes alle disse opplysningene fra telefonen din, og de lagres så i en sentral skyløsning tilhørende Microsoft i Irland. Dataene her skal i utgangspunktet bare være tilgjengelige for Folkehelseinstituttet (FHI), og kun et fåtall personer vil ha tilgang til denne informasjonen. All tilgang til denne informasjonen logges, og logger gjennomgås hyppig.

FHI vil oppbevare informasjon om hvilke mobiltelefonnumre som har vært varslet om at de har vært i nærkontakt med en smittet, i 30 dager. FHI vil vurdere behov for denne lagringen og vil gi beskjed om denne tidsperioden endres eller om slik lagring utelates. Du vil i så fall få beskjed om dette.

Rammeverket for appen skal tillate lagring av geolokasjonsdata også ut over de 30 dagene, men da skal de ifølge FHI lagres i anonymisert form, fortrinnsvis til bruk i forskningsformål.

Det er ikke beskrevet konkret hvordan de identifiserbare dataene skal anonymiseres etter 30 dager. (Les mer om dette i kapittel 5)

Faste opplysninger som mobiltelefonnummer, din unike ID og versjonsnummer på mobiltelefonens operativsystem lagres så lenge du bruker Smittestopp. Ved å trykke på «slett data»-knappen i appen kan du slette dine personopplysninger. Ifølge personvernerklæringen vil personopplysningene dine da bli slettet både i mobiltelefonen og sentralt. Deretter kan du slette selve appen fra mobiltelefonen. Hvis du bare sletter Smittestopp fra mobiltelefonen (uten å trykke på slett data-knappen), slettes dine personopplysninger sentralt etter en uke, heter det i informasjonen fra FHI. Alle innsamlede personopplysninger skal ifølge FHI slettes når forskriften opphører å gjelde den 1. desember 2020. Du har rett til å kreve innsyn, retting eller sletting av personopplysninger Folkehelseinstituttet behandler om deg.

Du kan få innsyn i hvilke GPS-opplysninger FHI har registret for din telefon ved å [logge inn her.](https://minhelse.helsenorge.no/innsynsmittestopp)

Folkehelseinstituttet bruker følgende databehandlere til å samle inn, lagre eller på annen måte behandle personopplysninger på våre vegne

* Simula Research Laboratory AS, Simula Metropolitan Center for Digital Engingeering AS (Simula Met) og Simula Consulting AS for utvikling av tjenesten
* Microsoft Ireland Operations Ltd for lagring av personopplysningene i MS Azure
* Norsk Helsenett for innsynsløsningen
* All behandling av personopplysninger som vi foretar skjer innenfor EU/EØS-området, slik at personvernforordningen gjelder fullt ut.

[Her er tek.no sin guide til Smittestopp](https://www.tek.no/nyheter/guide/i/e8LLWQ/smittestopp)

[Digi.no anmeldte appen like etter lansering](https://www.digi.no/artikler/forsteinntrykk-smittestopp-appen-er-enkel-a-bruke-men-trolig-har-den-har-et-alvorlig-problem/490150)

Ekspertgruppe kontrollerer appen

Fredag 3. april oppnevnte Helse- og omsorgsdepartementet en ekspertgruppe som fikk i oppdrag å gjennomgå appen. I sin [foreløpige rapport](https://www.regjeringen.no/no/dokumenter/forelopig-rapport-for-kodegjennomgang-av-losning-for-digital-smittesporing-av-koronaviruset/id2697286/) levert 9. april, påpeker ekspertgruppen flere mangler:

«Appen bærer preg av at konfidensialitet er bedre ivaretatt enn integritet og tilgjengelighet. Vi har gjort funn innen skalering, robusthet, sårbarheter i tredjepartsbiblioteker, utviklingsmetodikk, bruk av protokoller, dataintegritet, datalekkasje, datavalidering, og svakheter i konfigurasjon.»

Ekspertgruppen understreker imidlertid at det ikke er overraskende at de har gjort funn innen så mange områder i en løsning som er laget på så kort tid.

FHI opplyser om at det fortløpende [er gjort endringer](https://www.fhi.no/nyheter/2020/flere-tiltak-innfort-i-app-losning/) i koden basert på ekspertgruppens innspill.

Et hovedfunn hos ekspertutvalget var at manglende kryptering av data lokalt på telefonen gjør det mulig å manipulere data, og dermed bryte dataintegritet. Simula har uttalt at de vil kunne endre dette i kommende versjoner.

- Imidlertid mener vi at siden det kun er mulig for kompetente brukere med motivasjon å manipulere posisjonsdata på egen telefon, har dette svært liten påvirkning på den totale datakvaliteten. Videre vil data som tas inn kvalitetssikres ved at åpenbart ugyldige verdier filtreres bort. FHI mener derfor at risikoen er akseptabel, sier prosjektleder Gun Peggy Knudsen. [Les mer her.](https://www.fhi.no/nyheter/2020/flere-tiltak-innfort-i-app-losning/)

Datatilsynet kontrollerer appen

27. april ble det klart at Datatilsynet har opprettet sak for å kontrollere appen Smittestopp.

Ved å opprette denne saken, ivaretar Datatilsynet sin rolle som tilsynsorgan og kan kontrollere om innsamlingen og bruken av data som samles inn i appen er i overensstemmelse med personvernreglementet og forskrift om digital smittesporing og epidemikontroll. [Les mer her.](https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/starter-kontroll-av-smittestopp/)

**4. KILDEVERNET**

Kildevern er både en rett og en plikt for redaktører og journalister. I tillegg er kildevernet et vern som er til av hensyn til kilden. Kildevernet har først og fremst en viktig samfunnsmessig begrunnelse. Kildevernet skal sikre at allmennheten får informasjon som vi eller ikke ville fått kjennskap til.

Kildevernet som rettighet er i Norge regulert i straffeprosessloven og tvisteloven. I [straffeprosesslovens §125](https://lovdata.no/lov/1981-05-22-25/%C2%A7125) er dette formulert slik:

*«Redaktøren av et trykt skrift kan nekte å svare på spørsmål om hvem som er forfatter til en artikkel eller melding i skriftet eller kilde for opplysninger i det. Det samme gjelder spørsmål om hvem som er kilde for andre opplysninger som er betrodd redaktøren til bruk i hans virksomhet.*

*Samme rett som redaktøren har andre som har fått kjennskap til forfatteren eller kilden gjennom sitt arbeid for vedkommende forlag, redaksjon, pressebyrå eller trykkeri.»*

Tilsvarende bestemmelse er tatt inn i tvisteloven. Rettslig sett er altså kildevernet formulert som et fritak fra forklaringsplikt i forbindelse med rettssaker.

Denne retten er imidlertid ikke hundre prosent «vanntett». Det heter videre i samme paragraf:

*«Når vektige samfunnsinteresser tilsier at opplysningen gis og den er av vesentlig betydning for sakens oppklaring, kan retten etter en samlet vurdering likevel pålegge vitnet å oppgi navnet. Dersom forfatteren eller kilden har avdekket forhold som det var av samfunnsmessig betydning å få gjort kjent, kan vitnet bare når det finnes særlig påkrevd pålegges å oppgi navnet.»*

Etter rettspraksis i Norge de siste årene skal det imidlertid svært mye til for at en

journalist eller redaktør skal bli pålagt å oppgi navnet på en kilde. Høyesterett har i flere kjennelser etter år 2000 styrket selve den rettslige kjernen i kildevernet. Det er i tråd med utviklingen ved Den europeiske menneskerettsdomstolen i Strasbourg (EMD), som i en rekke avgjørelser har understreket kildevernets betydning i demokratiske samfunn, og at enhver svekkelse av kildevernet kan bidra til en såkalt «chilling effect» på ytringsfriheten og på medienes muligheter for å oppfylle sin rolle som «public watchdog».

Parallelt med at kildevernet er styrket juridisk har de faktiske truslene mot kildevernet økt. Det skyldes flere forhold:

* Tvangsmessig innsamling og lagring av data fra offentlige myndigheter – ofte til bruk for å forhindre terror eller såkalte hybride trusler – jfr [regjeringens forslag til ny lov om etterretningstjenesten](https://www.medier24.no/artikler/frykter-at-ny-lov-for-e-tjenesten-vil-svekke-kildevernet/490535) som ble lansert nylig.
* Frivillig avgivelse av lokasjonsdata og andre opplysninger til ulike operativsystemer og leverandører av apper og tjenester.
* Som en konsekvens av begge disse punktene: økte muligheter for kriminelle, fremmed etterretning/land med fiendtlige hensikter eller andre som ønsker tilgang til denne informasjonen, å hacke seg inn på systemene for å kunne hente ut data.

Det er også viktig å være oppmerksom på at kildenes arbeidsgivere som eier og kontrollerer kildens utstyr – f eks mobiltelefon - kan være en trussel mot vernet av kilden, ved at det startes kildejakt i etterkant av en avsløring i mediene.

Det *formelle* kildevernet er altså styrket, mens det *reelle* kildevernet trolig er svekket. Det siste krever at redaktører og journalister hever bevissthets- og beredskapsnivået med tanke på hvordan vi rent praktisk håndterer kildevernet.

[Les mer om det juridiske kildevernet her.](https://www.nored.no/Juss/Kildevern)

Kildevernet står i tillegg helt sentralt i presseetikken og er beskrevet Vær Varsom-plakatens punkt 3.4: *«Vern om pressens kilder. Kildevernet er et grunnleggende prinsipp i et fritt samfunn og er en forutsetning for at pressen skal kunne fylle sin samfunnsoppgave og sikre tilgangen på vesentlig informasjon.»*

**5. SLIK UTFORDRER SMITTESTOPP KILDEVERNET OG PERSONVERNET**

Kan avdekke kildekontakt

Dersom en person som har installert appen, får bekreftet koronasmitte, vil alle andre som har appen få et varsel dersom de har vært i nær kontakt, for eksempel tettere enn to meter på denne personen i mer enn 15 minutter i løpet av den siste tiden. Dersom en journalist som blir smittet har hatt et fortrolig møte med en kilde vil vedkommende bli identifisert og kontaktet av myndighetene. Hvis en journalist har kildemøte med en fortrolig kilde, og en tredjeperson i umiddelbar nærhet av disse viser seg å være smittet, kan myndigheter også gjennom påfølgende smittekartlegging sannsynliggjøre en kontakt mellom kilde og journalist gjennom «overskuddsinformasjon».

Fra myndighetene har det vært påpekt at man da – hvis man kommer i en situasjon med fortrolig kildekontakt – enkelt kan slå av lokasjonen på appen. Men det vil kunne oppstå situasjoner der man først i etterkant vil forstå hvor sensitiv informasjon man fikk fra kilden.

Fare for nedkjølende effekt

Det er også naturlig å være oppmerksom på at nettopp det at det skapes usikkerhet rundt at myndighetene vil kunne ha tilgang til kildesensitiv informasjon, vil kunne ha en nedkjølende effekt på medienes tilgang på kilder.

Medienes omdømme er helt avhengig av at publikum skal være overbevist om at de kan kontakte og kommunisere med en journalist uten å risikere bli overvåket av myndighetene eller å bli avslørt som kilde.

Utviklet på rekordtid

Smittesporingsappen er utviklet på svært kort tid, med en type teknologi som forbindes med regimer og samfunn vi ikke liker å bli assosiert med. Dette er påpekt av flere instanser, også den nedsatte ekspertgruppen i deres foreløpige rapport. «Denne lukkede hurtigtogsbehandlingen er en svært dårlig start for myndighetenes nye virkemiddel i kampen mot coronaviruset», skrev [Dagbladet på lederplass 31. mars](https://www.dagbladet.no/kultur/dette-hastverket-er-livsfarlig/72313681)

Innsamling og lagring av data i bulk

Enhver form for innsamling av person- og lokasjonsdata i bulk, uten forhåndsvurdering og uten et klart formål knyttet til den enkelte innsamling utgjør et potensielt personvern- og kildevernproblem. Når denne typen informasjon blir lagret i så stort omfang øker det attraksjonsverdien for dem som har andre hensikter enn det som er poenget med innsamlingen.

Personvernrådet i EU mener smittesporingsapper som samler inn posisjonsdata opererer i strid med prinsippet om dataminimering. Dataminimering innebærer å velge den fremgangsmåten som er minst mulig inngripende, og som bare samler inn akkurat de persondataene som behøves for å oppfylle et formål. [Les mer her.](https://nrkbeta.no/2020/04/16/personvernrad-i-eu-mener-norsk-app-bryter-med-viktig-personvernprinsipp/) Programutvikler Patricia Aas fra it-selskap, Turtlesec, med spesielt fokus på personvern og sikkerhet, uttaler til [Dagens Næringsliv 14. april](https://www.dn.no/teknologi/koronaviruset/regjeringen/apper/it-sikkerhetsekspert-mener-den-norske-smitteappen-samler-unodvendig-og-utrolig-privat-informasjon/2-1-790895): *Det er attraktivt for en statlig aktør å ha fullstendig oversikt over alle bevegelsene til den norske befolkning.*

Sentral lagring av data.

At FHIs løsning forutsetter at alle sporingsdataene som appen samler løpende på den enkeltes telefon skal overføres til og lagres sentralt, på en server som myndighetene kontrollerer, er ett grunnleggende problem som er reist både av jurister og teknologer – blant annet av advokat Jon Wessel-Aas i en [kronikk i VG 2. april](https://www.vg.no/nyheter/meninger/i/dO14rO/app-app-app). Det finnes andre alternativer enn sentral lagring av data. Sør-Korea har benyttet en app i sitt smittesporings-arbeid der alle personlige geo, og identifiserende data blir liggende i telefonen. De sensitive opplysningene deles verken med operatør, app-eier eller myndighetene.

Det samme gjelder initiativet fra Apple og Google som [ble kjent i begynnelsen av april.](https://www.nrk.no/norge/it-giganter-samarbeider-om-smittevarsling-1.14979648)

Den nye løsningen til IT-gigantene baserer seg utelukkende på Bluetooth, og den innsamlede informasjonen lagres stort sett kun på brukerens egen telefon, noe som blir vurdert som en mindre personvernsinngripende løsning. [Les mer her.](https://www.nrk.no/norge/google-og-apple-vil-ha-myndigheter-med-pa-smittesporing-uten-overvaking-1.14982492)

Den norske løsningen er langt mer invaderende, fordi den en gang pr time flytter dataene fra telefonen til et sentralt lager med den risikoen dette kan innebære. Slik forklarte FHI-direktør Camilla Stoltenberg valget av en sentral løsning under lanseringen av Smittestopp-appen 16. april:

*- Grunnen til at vi har valgt en sentral løsning, er at det åpner for muligheten til å følge utviklingen av pandemien gjennom bevegelsesmønstre i befolkningen. Uten denne sentrale lagringen ville ikke dette vært mulig. Med sentrallagringen blir kontaktsporingen i tillegg mer nøyaktig og vi kan raskere varsle personer som har vært i nærkontakt med en som har vært smittet.*

Innsamling til flere formål

FHI har bestemt at appen skal ha et tilleggsformål: Foruten å drive smittesporing, skal den også brukes til å måle effekten av samfunnstiltak, gjennom at man studerer og forsker på de aggregerte dataene på befolkningsnivå.

Anonymiserte data fra appen om hvordan folk beveger seg, og hvor mange de møter vil bli brukt i arbeidet med å utforme effektive smitteverntiltak. Informasjonen vil bli analysert for å få vite mer om hvorvidt folk og grupper holder avstand til hverandre, omfanget av nærkontakter og om de smittede får flere nærkontakter når restriksjonene lettes. Data fra appen vil også bli brukt til forbedring av modellene som beregner den videre utviklingen av utbruddet.

I møte med FHI 23. april, fikk NR opplyst at løsningen for anonymisering av dataene ikke er klar ennå. Selv om man fjerner informasjon om telefonnumre og ID-en den enkelte bruker har i systemet, vil nøyaktige lokasjonsdata i mange tilfeller langt på vei kunne fortelle hvem dette er. FHI er oppmerksom på denne utfordringen og har erfaring fra anonymisering av pasienter med smittsomme sykdommer i datasett. På spørsmål om dette opplyser de at det jobbes med løsninger som flytter lokasjoner eller aggregerer data på en måte som gjør at det ikke er mulig å identifisere enkeltpersoner i etterkant. Dette er svært viktig for å sikre kildevernet.

Programutvikler Patricia Aas har også problematisert dette. Til [Dagens Næringsliv 14. april](https://www.dn.no/teknologi/koronaviruset/regjeringen/apper/it-sikkerhetsekspert-mener-den-norske-smitteappen-samler-unodvendig-og-utrolig-privat-informasjon/2-1-790895) påpeker hun at det man vanligvis designer for sikkerhetsmessig, er å lagre akkurat så mye informasjon du trenger for den oppgaven du skal utføre. I smitteappen er det annerledes, mener hun:

– *Her blander man sammen to forskjellige ting: På én side vil man spore opp folk du har vært sammen med, i tilfelle du har vært smittsom. Det er én ting. Problemet er at man blander det sammen med forskning om hvordan folk beveger seg. Det er to helt forskjellige ting.*

Også ekspertgruppen som har vurdert appen har kommentert dette:

*«Ved å gi brukere en mulighet til å bruke appen til kun smittesporing, vil gjerne brukere oppleve større kontroll på egen data»,* heter det i [ekspertgruppens foreløpige rapport.](https://www.regjeringen.no/globalassets/departementene/hod/fellesdok/rapporter/200409_forelppig_rapport_ekspertgruppe_sporingsapp.pdf)

Folkehelseinstituttet har signalisert at de i senere versjoner vil vurdere om tillatelse for de ulike formålene (kartlegging av bevegelsesmønster og smittevarsling) kan deles opp, og om lokaliseringsdata eventuelt kan erstattes av blåtannteknologi.

Fare for formålsutglidning og lekkasjer

I forskriftens § 4 heter det at

*«Personopplysninger i sporingssystemet kan bare behandles for formålene som nevnt i § 1, med mindre annet følger av lov eller etter samtykke fra den registrerte. Personopplysningene kan ikke benyttes for å kontrollere om enkeltpersoner overholder råd eller pålegg. Helseopplysninger eller lokasjonsdata kan ikke gjøres tilgjengelig for politi eller påtalemyndighet eller brukes i forsikringsøyemed eller av arbeidsgivere selv om den registrerte samtykker. Personopplysningene kan ikke utnyttes kommersielt.»*

Flere uavhengige eksperter mener likevel at muligheten er stor for en formålsutglidning i en gitt situasjon er stor, eksempelvis i forbindelse med en alvorlig kriminell handling, og at dette kan åpne for at alle opplysningene i appen blir brukt til noe helt annen enn det opprinnelige formålet. Advokat Jon Wessel-Aas trakk fram den såkalte [DNA-kjennelsen](https://www.vg.no/nyheter/meninger/i/dO14rO/app-app-app) som et eksempel på formålsutglidning. I medieorganisasjonene vet vi også at det fort kan bli press på de som sitter på dataene og forsøk på å etablere formelle unntakshjemler som likevel vil innebære en formålsutglidning.

Også Norges institusjon for menneskerettigheter (NIM) påpeker i et [brev til FHI og Helse- og omsorgsdepartementet 17. april](https://www.nhri.no/wp-content/uploads/2020/04/Brev-fra-NIM-til-HOD-og-FHI-%E2%80%93-2020-04-17-.pdf?fbclid=IwAR16OfUF005m9ZQjGHcQSFbh0ShgVpK-eGxreDd1H8yuhj2qAqvX2UO6cps) at det synes «noe uklart» hva som er behovet for formuleringen «*med mindre annet følger* *av lov eller etter samtykke fra den registrerte» i forskriftens § 4.* NIM anbefaler *«at et eventuelt tiltenkt bruksområde, det vil si andre lovhjemler som skal kunne danne grunnlag for tilgang til opplysningene, i så fall tydeliggjøres i forskriften.»*

Manglende åpenhet om kildekoden

Folkehelseinstituttet og Simula er blitt kritisert av mange for ikke å offentliggjøre kildekoden for appen**.** Dagbladet skriver på [lederplass 31. mars](pa%CC%8A%20lederplass%2031.%20mars):

*«Åpen kildekode regnes som standard for å sikre åpenhet, og gir mulighet for kompetente miljøer til å påpeke hull og mangler».* Og legger til at *«lydighet i et land som Norge oppnår du bare ved å vise åpenhet og gi gode forklaringer.»*

Teknologiskribent Sigve Indregard problematiserte dette i [Agenda Magasin 30. mars:](https://agendamagasin.no/kommentarer/bekjempe-pandemi-finnes-app/)

*«Det eneste som kan sikre tilliten til en app som dette, er at all informasjon om infrastruktur og all kildekode kan bli gjennomgått av borgerne. Alt annet vil gi inntrykk av at det er noe å skjule»*,

Simula forklarer manglende åpenhet om kildekoden slik: Hensynet til sikkerhet og personvern tilsier at det for øyeblikket ikke er klokt å dele kildekoden til appen åpent. [Les mer her](https://www.simula.no/news/digital-smittesporing-apen-kildekode)

Fare for hacking og svindel

Den type personopplysninger som appen Smittestopp samler inn er meget attraktive å få tilgang på. Det at hver telefon får sin unike ID i systemet gjør det enklere for hackere å følge enkeltbrukere.

Kort tid etter lansering av appen hadde datautvikler Hallvard Nygård laget et eget sporingsprogram til sin mobiltelefon som lytter etter signalene som Smittestopp-appen sender til andre telefoner i nærheten. Det utgjør en potensiell sikkerhetsrisiko for regjeringsmedlemmene, som nesten alle lastet ned appen umiddelbart. [VG omtalte saken 19. april](https://www.vg.no/nyheter/innenriks/i/y3dwae/har-funnet-sikkerhetsrisiko-i-smittestopp-appen-kan-brukes-til-aa-spore-andre). Ifølge FHI jobbes det med en løsning slik at appen sender med ulike id-er slik at dette ikke lenger vil være en aktuell problemstilling. Det tok 10 minutter for NRK å sette opp et system som sender ut falske sms-varsel fra Smittestopp, ifølge en [artikkel publisert 20. april.](https://nrkbeta.no/2020/04/20/sa-enkelt-er-det-a-forfalske-sms-er-fra-smittestopp/)

**Les mer om Smittestopp og personvern her:**

Datatilsynet følger utviklingen av Smittestopp-appen nøye. De har gitt veiledning til både Folkehelseinstituttet og Helse- og omsorgsdepartementet i utviklingsarbeidet, slik at appen i størst mulig grad skal harmonere med prinsippene i personvernforordningen.

27. april ble det klart at Datatilsynet [starter kontroll](https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/starter-kontroll-av-smittestopp/) av Smittestopp-appen.

– Vi har fått inn flere henvendelser som viser at det er mange spørsmål om appen. Det ser vi også i det offentlige ordskiftet. Spørsmål om formål, hva dataene faktisk skal brukes til, nytteverdi og tekniske innretninger er gjengangere. Det er store forventninger til hva Datatilsynet nå skal gjøre, uttalte direktør Bjørn Erik Thon.

[Her er Datatilsynets spørsmål og svar-sider](https://www.datatilsynet.no/regelverk-og-verktoy/sporsmal-svar/korona/) om korona, der flere spørsmål om Smittevern-appen besvares.

Datatilsynet er positive til at det brukes apper og annen type teknologi for å bekjempe pandemien – og i siste instans bidra til å redde liv, men har samtidig understreket at alle personverninngripende tiltak må være nødvendige, egnede og forholdsmessige.

Også Norges institusjon for menneskerettigheter (NIM) har fulgt utviklingen av Smittestopp-appen med stor interesse. [I et brev](https://www.nhri.no/wp-content/uploads/2020/04/Brev-fra-NIM-til-HOD-og-FHI-%E2%80%93-2020-04-17-.pdf?fbclid=IwAR0IYSQyejSnQb5SkrHtRKXJjTSsBCUBlOA29-hZxvnPY5e_A8tszgtag68) til Helse- og omsorgsdepartementet og Folkehelseinstituttet fra 17. april understreker de at et hovedperspektiv fra deres side er at appen formodentlig vil kunne bidra til at andre inngrep i beskyttede menneskerettigheter, begrenses. Men samtidig minner de om at *«det til enhver tid må foretas vurderinger av om tiltaket ivaretar minste inngreps prinsipp, og ikke minst omringes av gode rettsikkerhetsmekanismer.»*

EU-kommisjonen har utarbeidet [en verktøykasse](https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/en-eu-tilnarming-for-effektive-kontaktsporingsapper-til-stotte-for-gradvis-opphevingletting-av-tiltak/) med felles veiledning om smittesporingsapper. Sterke personverngarantier er imidlertid en forutsetning, sa kommisæren for det indre marked, Thierry Breton, da han lanserte verktøykassen 17. april.

**Eksperter innen personvern-teknologi og kryptografi fra hele verden gått sammen om**

[et opprop](https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view) **mot inngripende smittesporingssystemer som rulles ut i flere land.**

Over 280 eksperter fra sentrale forskningsmiljøer innen feltet i 26 land har signert.

– Vi er bekymret for at noen av «løsningene» for krisen kan muliggjøre et omfang av overvåking av samfunnet som man aldri før har sett, skriver de i oppropet, omtalt av

 [NRK 20. april.](https://www.nrk.no/norge/hundrevis-av-it-eksperter-fra-hele-verden-ut-mot-sporingsapper-som-norske-smittestopp-1.14988352)

**6. EKSEMPLER PÅ INTERNE RÅD FRA ULIKE REDAKSJONER**

VERDENS GANG

Her er VGs foreløpige anbefalinger til redaksjonelle medarbeidere:

*Appen kan utgjøre en trussel mot kildevernet. Potensielt kan den avsløre kildemøter om journalist og/eller kilde har appen installert. Appen har åpenbare samfunnstjenlige formål, og i en tid der det tas i bruk kraftfulle virkemidler for å begrense smitte, er det krevende å fraråde alle ansatte i VG å installere appen. Enkeltmedarbeidere kan også ha særlige og personlige behov for smittesporing.*

**Foreløpige retningslinjer**

*1. Redaksjonelle medarbeidere i Verdens Gang****bør****av kildevernhensyn ikke installere FHIs applikasjon for smittesporing.*

*2. Uavhengig av om appen er installert,****skal****VG-journalister utvise varsomhet i møter med fortrolige kilder. En bør vurdere å ikke ta med telefon til møter av sensitiv art.  Om telefonen er skrudd av, bør den først aktiveres når man har tilstrekkelig avstand til stedet der kildemøtet fant sted.*

*3. Det fremstår uklart hvor mye overskuddsinformasjon appen kan samle inn. På generelt grunnlag anbefaler vi at fortrolige kildesamtaler krypteres.*

*Vi viser til de generelle varsomhetsreglene for håndtering av kilder og sensitivt materiale. Vær oppmerksom på at datalekkasjer og hacking kan eksponere kildene dine. Ansatte som installerer FHIs app, rådes til å slette den når epidemien er over.*

NRK

**NRK har meldt ut følgende foreløpige retningslinjer:**

* *Appen «Smittestopp» er en del av myndighetenes arbeid med smittesporing i det norske samfunnet. Appen samler inn detaljert informasjon om brukernes bevegelser og kontaktpunkter, og det er frivillig å laste den ned. Opplysningene kan bidra med viktig informasjon om smittespredning, samtidig som det må være opp til den enkelte også i NRK om man vil samtykke til å dele den personlige informasjonen som brukerne av appen gir fra seg.*
* *Appen har et åpenbart samfunnstjenlig formål, hvor også enkeltmedarbeidere i NRK kan ha særlige og personlige behov for en best mulig smitteovervåkning rundt seg selv og egen familie. Samtidig utgjør appen åpenbart - gjennom måten den samler og registrerer informasjon på - en risiko, når det gjelder hensynet til kildevern. Dette fordi myndighetene med journalistens samtykke har muligheten til å kartlegge hvem og når journalisten møter andre – også fortrolige kilder.*
* *Enhver redaksjonell medarbeider i NRK (journalist, fotograf, researcher o.l.) som jobber med fortrolige kilder har et selvstendig ansvar for å sikre at kilden forblir skjult. Det innebærer også en kritisk holdning til dokumentsikkerhet, datasikkerhet og hvordan man bruker mobilen og hvilke apper man installerer. Har du en rolle eller er i en situasjon hvor du jevnlig har fortrolige kildemøter, bør du ikke installere smittesporing-appen.*
* *Dersom appen er installert på telefonen bør redaksjonelle medarbeidere være ekstra varsomme mht fysiske møter med fortrolige kilder. Dette betyr i praksis å vurdere å la være å ta med telefonen, eller å slå den av og slå den på igjen i god tid og avstand før og etter kildemøtet. Dette varsomhetsprinsippet bør naturligvis også vurderes dersom du ikke har denne spesifikke appen installert.*
* *Alle NRK-medarbeidere som velger å installere appen, oppfordres til å slette dataene i appen, og så slette appen, umiddelbart etter at «korona-situasjonen» er over.*
* *Uavhengig av smittesporing-appen som sådan, oppfordres det generelt til at fortrolig kildekontakt på mobil i størst mulig grad gjøres via krypterte apper som Signal.*

AFTENPOSTEN

Disse retningslinjene gjelder Smittestopp og alle andre apper og mobile tjenester.
Det betyr at hver enkelt av oss må vurdere bruk av FHI-appen i lys av egen journalistisk aktivitet. Bruk av appen er uforenlig med å omgås kilder du har lovet anonymitet. Dersom du laster ned appen, må du være ekstra nøye med å følge retningslinjene.

Et aktuelt eksempel: Dersom du sitter hjemme og ringer til åpne kilder, vil bruk av appen ikke være i strid med retningslinjene. Ved behov kan du slå av tilgangen til stedstjenester for appen.

**Her er våre retningslinjer for mobilbruk og kildevern:**

* Aftenpostens journalister skal utvise varsomhet i møter med fortrolige kilder
* Vær bevisst på hvilke spor du legger igjen og hvilke data du deler, med tanke på kildevern.
* Vær særlig oppmerksom på mobiltelefonens bruk av stedstjenester.
* Slå av bluetooth og mobildata før sensitive kildemøter.
* Ved kildemøter av svært sensitiv karakter bør man vurdere ikke å ta med telefon eller annet elektronisk utstyr med radiosender/-mottager til møtet.
* Husk at også kilden kan ha slikt utstyr med til møtet. Gjør kilden oppmerksom på risikoen dette medfører. Samme forsiktighetsregler bør gjelde for kilden.
* Vær oppmerksom på at datalekkasjer og - innbrudd kan eksponere kontakten mellom journalister og kilder.
* Sensitiv tele-/datakommunikasjon bør være kryptert.

Har din redaksjon laget råd om bruk av Smittestopp-appen? Del gjerne med oss, så deler vi videre her.