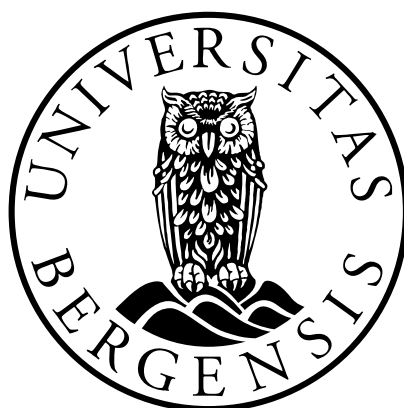


# Når er smittesporingsapplikasjoner uforenelige med personvernforordningen?

*En vurdering av ulike smittesporingsapplikasjoner i EØS-land sett i lys av prinsippene om formålsbegrensning og dataminimering etter personvernforordningens artikkel 5 (1) bokstav b og c.*

Kandidatnummer: 63

Antall ord: 13286



JUS399 Masteroppgave  
Det juridiske fakultet

UNIVERSITETET I BERGEN

10. desember 2021

# Innholdsfortegnelse

1. Innledning.....	2
1.1. Presentasjon av tema, problemstilling og aktualitet .....	2
1.2. Rettskilder og metodiske utfordringer.....	3
1.3. Avgrensninger .....	7
1.4. Den videre fremstillingen.....	8
2. Personvernprinsippene .....	8
2.1. Overordnet om personvernprinsippene .....	8
2.2. Om formålsbegrensningsprinsippet.....	9
2.2.1. Behandlingsformålene må være «spesifikke».....	10
2.2.2. Behandlingsformålene må være «uttrykkelige angitte» .....	10
2.2.3. Behandlingsformålene må være «berettigede».....	11
2.3. Om dataminimeringsprinsippet .....	11
2.3.1. Behandlingen må være «adekvat» .....	11
2.3.2. Behandlede opplysninger må være «relevante» .....	12
2.3.3. Behandlingen må være «nødvendig».....	12
3. Applikasjonene og deres komponenter .....	13
3.1. Hvilke applikasjoner skal vurderes? .....	13
3.1.1. Norske «Smittestopp 1» .....	13
3.1.2. Teknologien bak «Smittestopp 2» og «CWA» .....	14
3.1.3. Norske «Smittestopp 2» .....	14
3.1.4. Tyske «CWA» .....	15
3.1.5. Franske «TAC» .....	16
3.2. Hvilke komponenter skal vurderes? .....	17
4. Flere formål enn smittesporing.....	18
5. Hva om applikasjonens formål utgår?.....	21
6. Lokasjonsdata eller kontaktsporing?.....	24
7. Sentralisert eller desentralisert lagring? .....	26
7.1. Desentralisert løsning .....	27
7.2. Sentralisert løsning .....	28
8. Hvor lenge bør personopplysningene oppbevares? .....	30
9. Avsluttende ord.....	32
10. Litteraturliste.....	35
11. Vedlegg - Figurer og bilder .....	39

# 1. Innledning

## 1.1. Presentasjon av tema, problemstilling og aktualitet

I skrivende stund er covid-19-pandemien ikke over,<sup>1</sup> og stadig flere virusmuteringer vil trolig medføre at pandemien kommer til å vare i lang tid. Sannsynligheten for at menneskeheten kommer til å oppleve flere pandemier i fremtiden er også stor. Effektiv smittesporing er kritisk for å begrense smittenivået i samfunnet, for igjen å forhindre at helsesystemet kollapser. I Norge og store deler av verden har strategien gått ut på å teste, isolere, smittespore og sette i karantene (forkortet «TISK» på norsk).<sup>2</sup>

Mobilapplikasjonen Smittestopp 1 ble utviklet for å støtte opp om denne strategien i Norge.<sup>3</sup> Det samme har blitt gjort i mange europeiske land, der ulike smittesporingsapplikasjoner er blitt lansert.<sup>4</sup> Med smittesporingsapplikasjoner menes applikasjoner der hovedformålet er å bryte smittekjeder ved å varsle nærkontakter («kontaktsporing»). Applikasjoner som tilskudd til smittesporingsarbeidet har likevel ikke vært uten utfordringer, og disse kan ha negative konsekvenser for brukernes personvern. I juni 2020 uttalte Amnesty International at norske Smittestopp 1 var like invaderende som applikasjonene utviklet i Bahrain og Kuwait.<sup>5</sup> Etter varsel fra det norske Datatilsynet valgte Folkehelseinstituttet (heretter «FHI»), som var behandlingsansvarlig for Smittestopp 1,<sup>6</sup> å stoppe innsamling av personopplysninger, slette innsamlede opplysninger og deaktivere applikasjonen.<sup>7</sup>

Bruk av smittesporingsapplikasjoner krever at en balanserer personvern på den ene siden og virkemidler som kan bidra til å bekjempe pandemien på den andre siden. Om ikke kan konsekvensen bli at enkeltindividers personvern blir svekket i den grad at det gjør enkelte

---

<sup>1</sup> I løpet av oppgaven viser jeg til SARS-CoV-2, covid-19 og koronaviruset. I dagligtale brukes disse ofte om hverandre, men korrekt ordbruk er at viruset SARS-CoV-2 forårsaker sykdommen covid-19. Se Språkrådet, 27. mars 2020, <https://www.sprakradet.no/Vi-og-vart/hva-skjer/Aktuelt-ord/koronavirus/> (sist lest 25. nov. 2021).

<sup>2</sup> FHI, «Nedjustert TISK», 17. november 2021, <https://www.fhi.no/nettpub/coronavirus/testing-og-oppfolging-av-smittede/forsterket-tisk2> (sist lest 23. nov. 2021).

<sup>3</sup> FHI, «Smittestopp – prosjektbeskrivelse», 13. oktober 2021, <https://www.fhi.no/cristin-prosjekter/aktiv/smittestopp/>, første avsnitt under «Om Smittestopp» (sist lest 23. nov. 2021).

<sup>4</sup> EU-kommisjonen, «Mobile contact tracing apps in EU Member States», [ingen dato], [https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states\\_en](https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en) (sist lest 23. nov. 2021).

<sup>5</sup> Amnesty International, «Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy», 16. juni 2020, <https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/> (sist lest 23. nov. 2021).

<sup>6</sup> Behandlingsansvarlig er den som «som [...] bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes [...]» jf. PVF artikkel 4 (7).

<sup>7</sup> FHI, «FHI har svart Datatilsynet om Smittestopp», 24. juni 2020, <https://www.fhi.no/historisk-arkiv/covid-19/nyheter-2020/jun/fhi-har-svart-datatilsynet-om-smittestopp/> (sist lest 23. nov. 2021).

applikasjoner uforenelige med personvernforordningen. Av den grunn fortjener oppgavens tema oppmerksomhet.

Hensikten med oppgaven er å analysere tre ulike smittesporingsapplikasjoner sett i lys av personvernforordningens prinsipper om formålsbegrensning og dataminimering. For å kunne operasjonalisere disse prinsippene ser jeg henholdsvis til hva slags personopplysninger som samles inn, hvordan disse lagres i applikasjonene og hvilke formål applikasjonene har. Jeg skal vurdere norske Smittestopp 2, franske TousAntiCovid (heretter «TAC») og tyske Corona-Warn-App (heretter «CWA»). I tillegg kommer jeg også til å henvise til Smittestopp 1.

Hovedårsaken til at jeg har valgt disse applikasjonene er at de samlet sett representerer en rekke ulike løsninger, blant annet i form av rammeverk og formål. Der Smittestopp 2 kun har som formål å bedrive smittesporing, har både TAC og CWA ytterligere formål utover dette. Der Smittestopp 2 og CWA bruker Google og Apple sitt rammeverk, bruker TAC en sentralisert løsning. Disse ulikhetene gjør det lettere å synliggjøre hvilke personvernrettslige problemer som reises og hvordan enkelte løsninger kan være mer personvernvennlige enn andre.

## 1.2. Rettskilder og metodiske utfordringer

Europaparlaments- og rådsforordning (EU) av 2016/679 (heretter «PVF») ble gjeldende rett i EU-landene 25. mai 2018 jf. PVF artikkel 99.<sup>8</sup> For Norges del trådte den i kraft 20. juli 2018 med lov om behandling av personopplysninger (personopplysningsloven).<sup>9</sup> Fordi PVF er tatt inn i norsk lov, er den norske versjonen også gjeldende rett. Alle henvisninger til den er derfor også på norsk.

Da PVF trådte i kraft, ble også Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 («personverndirektivet», heretter «PVD») opphevet.<sup>10 11</sup> PVF er juridisk bindende «som den er» for EUs medlemsstater jf. TEUV artikkel 288 (2). Det samme gjelder ikke direktiver jf. TEUV artikkel 288 (3). For sistnevnte er medlemsstatene selv ansvarlige for at direktivets formål oppfylles gjennom nasjonal lovgivning, såkalt «implementering». At PVD ble erstattet med en forordning er et klart signal på at en ønsker lik praktisering av reglene i hele EU/EØS. Det sier også noe om hvor høyt personopplysninger og korrekt behandling av dem settes på dagsorden i EU-systemet.

---

<sup>8</sup> Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF («PVF»).

<sup>9</sup> Lov 15. juni 2018 nr. 38 om behandling av personopplysninger («personopplysningsloven»).

<sup>10</sup> PVF artikkel 94.

<sup>11</sup> Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

PVF er teknologinøytral, og ingen av bestemmelsene er ment å direkte regulere bruken av applikasjoner. Det gjelder både for smittesporingsapplikasjoner og applikasjoner med andre formål. Av den grunn må jeg se til de grunnleggende prinsippene i PVF artikkel 5 for å besvare oppgavens problemstilling. Disse er nærmere behandlet i oppgavens punkt 2.

Formålet med PVF er å fastsette «[...] regler om vern av fysiske personer i forbindelse med behandling av personopplysninger samt regler om fri utveksling av personopplysninger». Dette følger av PVF artikkel 1 (1). Alt som kan bidra til å identifisere fysiske personer, både direkte og indirekte, er «personopplysninger» jf. artikkel 4 (1). Av den grunn er det klart at opplysninger innsamlet gjennom en smittesporingsapplikasjon er «personopplysninger». Innsamlingen av personopplysninger gjennom smittesporingsapplikasjonene er også en «helt eller delvis automatisert behandling» jf. PVF artikkel 2 (1). PVF gjelder derfor ved behandling av oppgavens spørsmål.

Ved tolkningen av EU/EØS-rett er ensartethet kanskje det viktigste elementet.<sup>12</sup> Om en hadde hatt ulike regelverk på tvers av EØS-statene, ville en møtt større utfordringer med eksempelvis import av varer og overføring av personopplysninger. Ensartethet på tvers av landene bidrar til å forhindre disse utfordringene. Dette må ses i lys av hensikten om å verne om de fire frihetene, grunnpilarene i EU. Disse er fri flyt av kapital, varer, tjenester og personer. Et felles regelverk som tolkes på lik linje i medlemslandene bidrar til å oppfylle EU-traktatens formål - et mer sømløst indre marked.<sup>13</sup> Formål og kontekst er også sentrale elementer i EU/EØS-retten. Dette er fastsatt i både rettspraksis fra EU-domstolen og juridisk teori.<sup>14 15</sup>

Den mest sentrale bestemmelsen for denne oppgaven er PVF artikkel 5 (1). Bestemmelsen inneholder viktige prinsipper for hvordan resten av lovverket skal forstås. Det betyr likevel ikke at ordlyden i bestemmelsen er absolutt, og alt avhenger uansett av en konkret vurdering av det aktuelle tilfelle.<sup>16</sup> I litteraturen legger Schartum til grunn at prinsippene må forstås vidt, fordi de er ganske upresise i ordlyden. Videre påpeker han at i fravær av autoritative kilder, må en kunne tillegge prinsippene en viss vekt.<sup>17</sup>

Ettersom prinsippene gjelder et såpass stort område, er det også naturlig at de er relativt vage i sin ordlyd. Av den grunn er det særlig relevant å se til fortalen, som sier noe om hvordan Rådet og Europaparlamentet mener at forordningen skal forstås. Denne gir imidlertid lite hjelp i å forstå PVF, særlig fortalepunktene som gjelder prinsippene i artikkel 5. Fortalen er heller

---

<sup>12</sup> Halvard Haukeland Fredriksen og Gjermund Mathisen, *EØS-rett*, 3. utg., Fagbokforlaget, 2018, s. 296.

<sup>13</sup> Se f.eks. fortalen i TEUV og de innledende artiklene i traktaten.

<sup>14</sup> *Satakunnan Markkinapörssi* [GC], C-73/07, avsnitt 54.

<sup>15</sup> Fredriksen og Mathisen (2018) s. 298.

<sup>16</sup> Ibid.

<sup>17</sup> Dag Wiese Schartum, *Personvernforordningen - en lærebok*, 1. utg., Fagbokforlaget, 2020, s. 87.

ikke juridisk bindende jf. blant annet C-345/13 *Karen Millen Fashions*. I saken uttalte EU-domstolen at:

*«It should be borne in mind that the preamble to a Community act has no binding legal force and cannot be relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner clearly contrary to their wording».*<sup>18</sup>

Fortalen kan med andre ord kun brukes som et tolkningsbidrag, ikke som en selvstendig rettskilde hvis det avviker fra forordningens ordlyd. På bakgrunn av manglende veiledning i fortalen gjeldende artikkel 5 og at den heller ikke er rettslig bindende, får den begrenset vekt i denne oppgaven.

Rettspraksis vil også være relevant. Da PVF er ganske ny, har ikke EU-domstolen rukket å avsi mange avgjørelser som har direkte relevans for denne oppgaven. Når en da ikke har mange avgjørelser fra en autoritativ institusjon i EU-systemet, kan det være utfordrende å skulle vurdere uavklarte spørsmål som oppstår i fortolkning av forordningen. Øvrige rettskilder kan derfor få økt rettskildemessig vekt.

I PVD artikkel 6 (1) (c) er det en nokså likelydende bestemmelse til PVF artikkel 5 (1) (c). Sistnevnte sier at «personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for [...]». PVD sier at «personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected [...]».<sup>19</sup> I PVF artikkel 5 (1) (c) er vilkåret «not excessive» erstattet med «nødvendig». EU-domstolens avgjørelser som gjaldt PVD artikkel 6 kan likevel være relevante ved tolkningen av PVF artikkel 5, men da må overføringsverdien vurderes konkret.

I fravær av avgjørelser som er direkte relevant for problemstillingen, må en også se til andre rettskilder. Oppgavens problemstilling gjelder et svært dagsaktuelt og komplisert tema. I forbindelse med covid-19-pandemien har Det europeiske personvernrådet (heretter «EDPB») utgitt konkrete retningslinjer for utforming av smittesporingsapplikasjoner.<sup>20</sup> EDPB har ikke en lovgivende rolle slik som Europaparlamentet og Rådet. Det kan bidra til å svekke retningslinjenes rettskildemessige vekt.

---

<sup>18</sup> *Karen Millen Fashions [C5]*, C-345/13, avsnitt 31.

<sup>19</sup> Henvisningen er på engelsk ettersom PVD ikke ble inntatt i norsk lov, men heller implementert gjennom nasjonal lovgivning i personopplysningsloven av 2000.

<sup>20</sup> Det europeiske Personvernrådet (EDPB), «Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak», 21. april 2020, [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en) (sist lest 23. november 2021).

Samtidig er retningslinjene utformet av et ekspertorgan, og dets hovedrolle er å sørge for at reglene i forordningen blir overholdt jf. PVF artikkel 70 (1) flg. I tillegg utgjør EDPB en samling av tilsynssjefer fra hvert EU/EØS-land.<sup>21</sup> Det er kun datatilsyn fra EUs medlemsstater som har stemmerett. Ettersom Norge ikke er EU-medlem, kan det norske Datatilsynet kun delta i utformingen av retningslinjene og ellers lobbyvirksomhet for å fremme sine poeng.<sup>22</sup>

Som et ekspertorgan er det klart at EDPB har god kompetanse innenfor personvernspørsmål. Schartum argumenterer på sin side for at organet kan være mer «personvernvennlige» på grunn av deres sammensetning og ansvarsområde.<sup>23</sup> EDPBs retningslinjer er heller ikke rettslig bindende jf. PVF fortalepunkt 143.

I denne oppgaven er det uansett særlig relevant at EDPB har utformet egne retningslinjer om bruken av smittesporingsapplikasjoner i tråd med PVF. EDPBs retningslinjer er dermed direkte relevante for problemstillingen i denne oppgaven. Fordi EDPB er EUs ekspertorgan når det gjelder personvern, kan det argumenteres for at det å avvike fra retningslinjene deres krever særlig sterke holdepunkter. Det gjelder særlig når det ikke finnes noen autoritative kilder som antyder det motsatte. Retningslinjer fra EDPB må også godkjennes av organets medlemmer med simpelt flertall jf. PVF artikkel 72 (1). På bakgrunn av det overnevnte og mangel på autoritative kilder som direkte angår oppgavens spørsmål, må EDPBs retningslinjer tillegges betydelig vekt.

Der det er relevant kan en også se til Artikkel 29-arbeidsgruppen (heretter «WP29»). Gruppen hadde ansvaret for retningslinjer og uttalelser vedrørende PVD.<sup>24</sup> Selv om WP29 ble erstattet til fordel for EDPB da PVF trådte i kraft, har EDPB formelt påtegnet flere av uttalelsene.<sup>25</sup> Dette kan bidra til å øke uttalelsenes rettskildemessige vekt, fordi organet har tatt konkret stilling til deres uttalelser.

Nasjonal praksis vil også være relevant for oppgaven. Datatilsyn i de ulike medlemslandene, deriblant Norge, har flere oppgaver og myndigheter nedfelt i PVF artikkel 57 og 58. Det norske Datatilsynet har eksempelvis gjennomført en grundig redegjørelse av utfordringene tilknyttet Smittestopp 1.<sup>26</sup> Fordi organene er de ledende nasjonale organene på personvern, har deres

---

<sup>21</sup> PVF artikkel 68 (3).

<sup>22</sup> Datatilsynet, «Det europeiske Personvernrådet (EDPB)», 19. juli 2020, <https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/personvernradet/> (sist lest 23. nov. 2021).

<sup>23</sup> Schartum (2020) s. 87.

<sup>24</sup> Se PVD artikkel 29.

<sup>25</sup> EDPB, «Endorsement of GDPR WP29 guidelines by the EDPB», 25. mai 2018, [https://edpb.europa.eu/sites/default/files/files/news/endorsement\\_of\\_wp29\\_documents\\_en\\_0.pdf](https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf) (sist lest 23. nov. 2021).

<sup>26</sup> Datatilsynet, «Varsel om vedtak om midlertidig forbud mot å behandle personopplysninger – appen Smittestopp», 12. juni 2020, <https://www.datatilsynet.no/contentassets/1c72ac62cac145efa242942ca34c2cd0/20-02058-9-varsel-om-vedtak-om-midlertidig-forbud-mot-a-behandle-personopplysninger---smittestopp.pdf> (sist lest 23. nov. 2021).

uttalelser en viss rettskildemessig vekt. Samtidig vil ikke uttalelsene fra det norske Datatilsynet ha noen rettslig betydning for andre datatilsyn i EU, av årsaker forklart ovenfor. Organene har også mulighet til å komme med ulike sanksjonsmidler dersom de finner at behandlingen av personopplysninger har vært i strid med PVF jf. artikkel 58.

Andre retningslinjer og kilder kan være aktuelle å benytte i oppgaven. Eksempelvis har eHelse-nettverket, i samarbeid med EU-kommisjonen, utviklet egne retningslinjer for covid-19 og smittesporingsapplikasjoner.<sup>27</sup> Det samme har Verdens helseorganisasjon (WHO)<sup>28</sup> og EU-kommisjonen.<sup>29</sup> Førstnevnte er regulert i Europaparlaments- og rådsdirektiv 2011/24/EU og tatt inn i EØS-avtalen.<sup>30 31</sup> Deltakelse i eHelse-nettverket er likevel frivillig, og det kan bidra til å svekke den rettskildemessige vekten.

WHOs retningslinjer er heller ikke juridisk bindende. Likevel kan WHO sine betraktninger rundt problemstillingen være interessante, særlig sett i lys av organisasjonens sentrale rolle under pandemien. Videre er heller ikke EU-kommisjonens veiledning juridisk bindende. Begge kan derfor tjene som tolkningsbidrag, men ikke mer enn det.

Smittesituasjonen i verden utvikler seg til enhver tid, både juridisk og medisinsk. Siden starten av pandemien har det blitt produsert flere vitenskapelige artikler. Når situasjonen hele tiden er i endring, kan det være utfordrende å få et mer helhetlig overblikk. Det er naturlig at jeg i denne oppgaven støter på samme utfordring. Litteraturen kan likevel gi nyttig innsikt i den juridiske utviklingen, særlig i fravær av mer autoritative kilder. Videre finnes det en hel del litteratur som dekker forståelsen av PVF artikkel 5 og PVD artikkel 6.

### 1.3. Avgrensninger

Oppgaven er avgrenset til smittesporingsapplikasjonene nevnt i punkt 1.1 og vurderingen av dem i tråd med dataminimeringsprinsippet og formålsbegrensningsprinsippet. Ettersom jeg avgrenser til behandlingen av disse, vurderer jeg heller ikke de ulike behandlingsgrunnlagene jf. PVF artikkel 6. Personopplysninger samlet inn gjennom smittesporingsapplikasjoner kan i tillegg være «helseopplysninger» jf. PVF artikkel 9 (1). Slike personopplysninger er betegnet

---

<sup>27</sup> eHealth Network, «Mobile applications to support contact tracing in the EU's fight against COVID-19 - Common EU Toolbox for Member States», 15. april 2020, [https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19\\_apps\\_en.pdf](https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19_apps_en.pdf) (sist lest 23. nov. 2021).

<sup>28</sup> WHO, «Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing», 28. mai 2020, <https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19> (sist lest 23. nov. 2021).

<sup>29</sup> COM(2020) 2523 final.

<sup>30</sup> Europaparlaments- og rådsdirektiv 2011/24/EU av 9. mars 2011 om pasientrettigheter i forbindelse med grensekryssende helsetjenester.

<sup>31</sup> EØS-notatbasen, «Grensekryssende pasientrettigheter», 3. september 2014, <https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2008/juli/grensekryssende-pasientrettigheter/id2433855/> (sist lest 23. nov. 2021).



som «særlige kategorier av personopplysninger», og bestemmelsen stiller strengere krav til behandlingsgrunnlag enn artikkel 6.<sup>32</sup> Heller ikke disse er behandlet nærmere i oppgaven av samme grunn som nevnt ovenfor.

Videre har applikasjonene blitt endret av utviklerne på ulike tidspunkt. CWA har eksempelvis kommet til versjon 2.11. Av praktiske årsaker er oppdateringer av applikasjonene gjort etter 10. september 2021 ikke tatt med i oppgaven. Jeg forholder meg også til rettskildetilstanden slik den var 12. november 2021. Rettskilder som blir tilgjengelig etter dette tidspunktet er ikke tatt med i oppgaven.

## 1.4. Den videre fremstillingen

I den neste delen av oppgaven tar jeg stilling til PVF sine prinsipper om formålsbegrensning og dataminimering på generelt grunnlag (punkt 2.2 og 2.3) ved å gjennomgå vilkårene i artikkel 5 (1) (b) og (c). Jeg behandler formålsbegrensningsprinsippet før dataminimeringsprinsippet fordi førstnevnte alltid har vært sentral ved behandlingen av personopplysninger.<sup>33</sup>

Deretter følger en redegjørelse av de applikasjonene jeg har valgt til vurdering og hva som gjør dem relevante å vurdere (punkt 3.1). I punktet etter gjennomgår jeg de ulike komponentene som skal vurderes (punkt 3.2). Enkelte av disse er relativt tekniske og krever derfor ytterligere redegjørelse. I den videre drøftelsen (punkt 4 til 8) trekker jeg inn det juridiske aspektet sett i lys av de tekniske komponentene i applikasjonene. Til slutt kommer jeg med noen avsluttende betraktninger under punkt 9.

# 2. Personvernprinsippene

## 2.1. Overordnet om personvernprinsippene

Innledningsvis er det relevant med en kort gjennomgang av samtlige personvernprinsipper i PVF. Flere av disse overlapper og må dermed ses i lys av hverandre. Det er særlig aktuelt for prinsippene om formålsbegrensning og dataminimering, da disse er kjernen i oppgaven. En mer utførlig gjennomgang av disse to prinsippene er gjort under punkt 2.2 og 2.3, og de er dermed ikke inkludert i denne delen av oppgaven.

Personvernprinsippene er hjemlet i PVF artikkel 5. For det første må behandlingen av personopplysninger ha et behandlingsgrunnlag jf. artikkel 5 (1) (a). Om ikke vil behandlingen være lovstridig. En uttømmende liste over de mulige hjemmelsgrunnlagene står i PVF artikkel

---

<sup>32</sup> PVF artikkel 9 (2).

<sup>33</sup> de Terwangne, *Article 5. Principles relating to processing of personal data*, 1. utg., Oxford University Press, 2020, s. 315-316.

6, i tillegg til artikkel 9 dersom en skal behandle særlige kategorier av personopplysninger. Lovlighetsprinsippet innebærer også at behandlingen må være i samsvar med loven.

Riktighetsprinsippet er hjemlet i PVF artikkel 5 (1) (d). Personopplysninger må være riktige og slettes dersom de ikke er korrekte sett i lys av behandlingsformålet. Om ikke risikerer en at behandlingsansvarlig beholder opplysninger som er unødvendige for å oppfylle formålet. Prinsippet åpner i tillegg for at den registrerte har rett til å få rettet feil eller mangler i sine personopplysninger. Videre gjelder prinsippet om lagringsbegrensning jf. bokstav e. Her er hensikten er å sikre at opplysninger ikke lagres lengre enn det som er nødvendig. Begge av disse har med andre ord tydelige paralleller til dataminimeringsprinsippet.

Videre gjelder prinsippene om integritet og konfidensialitet, og dette er hjemlet i PVF artikkel (5) (1) (f). Prinsippet indikerer at det må etableres tiltak for å sikre at personopplysningene lagres på en sikker måte. Endelig har en ansvarsprinsippet jf. PVF artikkel (5) (2) som viser til at det er behandlingsansvarlig sitt ansvar at prinsippene i første ledd overholdes.

Selv om det ikke fremgår direkte i PVF artikkel 5 (1), må behandlingen av personopplysninger gjøres i lys av forholdsmessighetsprinsippet. Det står klart i fortalens punkt 4. I vårt tilfelle må det konkret avveies om behandlingen av personopplysninger for å begrense smittespredning i samfunnet veier opp for de de negative konsekvensene innsamlingen har på dem som bruker applikasjonen. Jeg går nå videre til gjennomgangen av prinsippene om formålsbegrensning og dataminimering.

## 2.2. Om formålsbegrensningsprinsippet

I tråd med PVF artikkel 5 (1) (b) skal personopplysninger «samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenelig med disse formålene». Den følgende vurderingen av vilkårene i bestemmelsen er delt opp i ulike avsnitt. Vilket om at «opplysningene ikke kan viderebehandles på en måte som er uforenelig med disse formålene» er ikke tatt med i oppgaven. Årsaken er at det ikke er like relevant for spørsmålet jeg ønsker å besvare.

Prinsippet om formålsbegrensning i PVF er likelydende til det som var i PVD. Av den grunn er WP29 sine retningslinjer for hvordan prinsippet skal forstås særlig relevant her.<sup>34</sup> Videre er ordlyden i artikkel 5 (1) (b) relativt vag. Ifølge WP29 ble bestemmelsen tolket ulikt fordi PVD

---

<sup>34</sup> Article 29 Data Protection Working Party (WP29), «Opinion 03/2013 on purpose limitation», WP203, 2. april 2013, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf) (sist lest 23. nov. 2021).

ble gjennomført ulikt i medlemsstatene.<sup>35</sup> Det er også blant årsakene til at WP29 valgte å publisere utførlige retningslinjer, og på den måten sikre en mer ensartet tolkning.<sup>36</sup>

Bruken av retningslinjene må likevel problematiseres noe først. Da PVD ble opphevet og EDPB tok over etter WP29, ga førstnevnte sin eksplisitte tilslutning til flere av de retningslinjene som WP29 hadde forfattet.<sup>37</sup> «Opinion 03/2013 on purpose limitation» var likevel ikke blant dem, og årsaken til dette er vanskelig å fastslå. Det kan fremdeles slås fast at manglende tiltredelse fra EDPB kan svekke dets rettskildemessige vekt.

Selv om EDPB ikke formelt gav sin tilslutning til retningslinjene, har de fremdeles relevans for oppgaven. PVD artikkel 6 (1) (b) er helt lik ordlyden i PVF artikkel 5 (1) (b). Fordi retningslinjene gjelder en helt likelydende bestemmelse, med nøyaktig samme formål, styrker dette den rettskildemessige vekten. Selv om det ikke er avgjørende, er «opinion 03/2013 on purpose limitation» også brukt i litteraturen, uten at dette problematiseres i stor grad.<sup>38</sup>

### **2.2.1. Behandlingsformålene må være «spesifikke»**

At formålet med behandlingen av personopplysninger må være «spesifikke» kan referere til flere ting. På den ene siden kan «spesifikke» bety at formålet må være klart nok utpenslet til at den registrerte forstår hva formålet bak innsamlingen egentlig er. Utdfordringen med en tolkning som denne, er at vilkåret om at formålet må være «uttrykkelig angitt» blir mer utvannet og står igjen uten særlig betydning.

På den andre siden kan «spesifikke» bety at formålene må være tydelig avgrenset og tydeliggjort. Det er denne tolkningen som er lagt til grunn av WP29.<sup>39</sup> På den måten vil det være tydelig for både behandlingsansvarlig og eventuelle tilsynsorganer hva som er det faktiske formålet med behandlingen av personopplysninger. Ved å tydelig avgrense hva som er formålet med innsamlingen, begrenser en også risikoen for at formålet kan strekkes utover det som opprinnelig var tenkt.

### **2.2.2. Behandlingsformålene må være «uttrykkelige angitte»**

Formålene må også være «uttrykkelig angitte». At de er «angitte», behøver ikke å være noe mer enn at de er nedfelt i dokumentasjon tilgjengelig for den registrerte og andre som har behov for å vurdere formålene for innsamlingen, eksempelvis tilsynsmyndigheter.

---

<sup>35</sup> WP29 (2013) s. 5.

<sup>36</sup> Ibid.

<sup>37</sup> EDPB (2018).

<sup>38</sup> de Terwangne (2020) s. 315.

<sup>39</sup> WP29 (2013) s. 12.

Terskelen for hvordan dette skal utformes heves når en har valgt å inkludere «uttrykkelige». Det kan med andre ord ikke være tvil om hva formålet med behandlingen er.<sup>40</sup> Det er særlig viktig om en ser det i lys av den registrerte, som i møte med større aktører oftest har et ønske om å vite hvorfor ens personopplysninger blir behandlet. På den måten styrkes den svake parts forutberegnelighet. Videre legger WP29 til i sine retningslinjer at alle involverte parter, ikke bare behandlingsansvarlig og den registrerte, skal være i stand til å sette seg inn i behandlingsformålet.<sup>41</sup> Hensikten er flerdelt. På den ene siden skal kontrollorgan og andre aktører kunne sette seg inn i behandlingsformålet. På den andre siden er det en fordel for den behandlingsansvarlige å tydeliggjøre overfor seg selv hva hensikten med behandlingen av personopplysningene er.

### **2.2.3. Behandlingsformålene må være «berettigede»**

Videre må formålene med behandlingen være «berettigede». Begrepet er vidt, og det er vanskelig å fastslå helt konkret hva som kan utledes av det. I sine retningslinjer legger WP29 til grunn at det må mer til enn å bare kontrollere behandlingens lovlighet i PVF artikkel 6.<sup>42</sup> I tillegg må en også foreta en vurdering i lys av den konteksten behandlingen foregår - en forholdsmessighetsvurdering. Det må med andre ord gjøres en balansevurdering av den registrertes rettigheter sett opp mot samfunnets interesser.<sup>43</sup> Det samme er eksplisitt lagt til grunn i PVF fortalepunkt 4.

## **2.3. Om dataminimeringsprinsippet**

Etter artikkel 5 (1) (c) må behandlingen av personopplysninger «være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for». Bestemmelsen er delt opp i tre vilkår, og samtlige av disse må være i tråd med innsamlingsformålet. Som vi skal se i de følgende underpunktene, er det nødvendig å se de tre vilkårene samlet.

### **2.3.1. Behandlingen må være «adekvat»**

For det første må behandlingen være «adekvat». En alminnelig språklig forståelse av at noe er «adekvat», er at det er nok eller tilstrekkelig til å oppfylle et ønsket formål. Om en legger til grunn en formålsorientert tolkning, betyr det at en må samle inn nok personopplysninger til at en faktisk får nytte av det. Dersom en ikke samler inn nok informasjon og en ikke oppfyller formålet, har innsamlingen i grunn vært unødvendig. Dette ville i så fall vært i strid med øvrige deler av dataminimeringsprinsippet.

---

<sup>40</sup> WP29 (2013) s. 17.

<sup>41</sup> Ibid.

<sup>42</sup> Ibid. s. 39.

<sup>43</sup> de Terwangne (2020) s. 315.

Forordningens fortale sier lite om hvordan en skal forstå vilkåret «adekvat» og nevnes kun i fortalepunkt 39 uten å gi særlig tolkningsbidrag. Heller ikke rettspraksis gir videre veiledning på hvordan begrepet isolert sett skal forstås. Tolkningen ovenfor er imidlertid i tråd med litteraturen, deriblant Schartum.<sup>44</sup>

### **2.3.2. Behandlede opplysninger må være «relevante»**

Videre må innsamlede personopplysninger være «relevante». Om en ser på vilkåret isolert, kan det late til at det er i orden å samle inn all informasjon som kan bidra til å oppfylle ønsket formål. Denne tolkningen er klart problematisk, fordi det på den måten ikke ville vært klare grenser for hva som er relevant. Også her må en legge en kontekstuell tolkning til grunn i lys av nødvendighetsvilkåret for å unngå unødvendig innsamling av personopplysninger.

I avsnitt 40 av EDPBs retningslinjer for kontaktsporing uttales det eksempelvis at «unrelated» informasjon ikke skal tas med i behandlingen av personopplysninger.<sup>45</sup> Å vite sivilstatus til en bruker av en smittesporingsapplikasjon kan være relevant i seg selv, fordi det kan si noe om en person sitt handlings- og bevegelsesmønster. Slik informasjon kan bidra til å effektivisere smittesporingsarbeidet.<sup>46</sup> Likevel er nok personopplysninger som dette ikke *rettslig* relevant, slik det er beskrevet av Schartum.<sup>47</sup> Fordi formålet er å vurdere hvem som er nærkontakter og på den måten bryte smittekjeder, vil ikke sivilstatus være en relevant personopplysning.

### **2.3.3. Behandlingen må være «nødvendig»**

I kjernen av dataminimeringsprinsippet er vilkåret om at behandlingen av personopplysninger må være «nødvendig». At det er «nødvendig» viser til at formålet ikke kan oppfylles uten disse opplysningene. Her kan fortalepunkt 39 i PVF brukes som tolkningsbidrag. Der står det at «[p]ersonopplysninger bør behandles bare dersom formålet med behandlingen ikke med rimelighet kan oppfylles på annen måte». Dersom formålet kan oppnås på annen måte, kan ikke behandlingen av personopplysningene være «nødvendig». De Terwangne beskriver dette som at opplysningene må være kvalitativt nødvendige, altså at en ikke bare har samlet inn nok informasjon, men også at de er gode nok til å oppfylle formålet.<sup>48</sup>

---

<sup>44</sup> Se f.eks. Schartum (2020) s. 92.

<sup>45</sup> EDPB (2020) avsnitt 40.

<sup>46</sup> Ibid.

<sup>47</sup> Schartum (2020) s. 92.

<sup>48</sup> de Terwangne (2020) s. 317.

## 3. Applikasjonene og deres komponenter

### 3.1. Hvilke applikasjoner skal vurderes?

Jeg har valgt ut tre smittesporingsapplikasjoner som skal vurderes. Disse er franske TAC, tyske CWA og norske Smittestopp 2. Det er også inkludert flere henvisninger til norske Smittestopp 1. Flere av applikasjonene har blitt endret etter at de ble tilgjengelig for allmennheten. Enkelte er også helt nye versjoner, slik som TAC og Smittestopp 2. Jeg viser her til figur 1 i oppgavens vedlegg, en tidslinje over når de ulike applikasjonene ble tilgjengeliggjort eller gjennomgikk endringer som er viktige for oppgavens tema.

Det er ikke rom for en kvantitativ analyse av for mange ulike smittesporingsapplikasjoner i denne oppgaven. Av den grunn har jeg gjort et utvalg på tre applikasjoner. Målet er at dette skal kunne vært bredt nok til å kunne gi et bilde på hvordan ulike applikasjoner virker, uten at det blir for overfladisk. På grunn av gjentatte henvisninger til Smittestopp 1, foretar jeg først en kort redegjørelse av denne. Deretter gjennomgår jeg de øvrige applikasjonene. Ettersom TAC bruker en annen teknologi enn Smittestopp 2 og CWA, beskriver jeg de to sistnevnte og deres teknologi før jeg avslutningsvis tar for meg TAC.

#### 3.1.1. Norske «Smittestopp 1»

Smittestopp 1 ble utviklet av Simula og lansert 16. april 2020.<sup>49</sup> FHI var behandlingsansvarlig for personopplysningene som ble innsamlet gjennom applikasjonen.<sup>50</sup> 15. juni 2020, om lag to måneder etter at den ble tilgjengeliggjort, sendte Datatilsynet varsel om vedtak til FHI.<sup>51</sup> Det var flere utfordringer med applikasjonen som førte til at Datatilsynet grep inn. Kanskje mest inngripende var det at Smittestopp 1 brukte GPS-teknologi til å spore brukere.<sup>52</sup> Brukere måtte også godkjenne alle formål samlet, og en kunne ikke bidra til smittesporingsarbeidet uten å også akseptere innsamling av personopplysninger til statistiske formål.<sup>53</sup> Allerede 16. juni valgte FHI å deaktivere applikasjonen, i påvente av Datatilsynets endelige vedtak.<sup>54</sup>

I forbindelse med Datatilsynets varsel ble FHI gitt kommenteringsfrist frem til 23. april 2020.<sup>55</sup> Datatilsynets konklusjon var at de foreslåtte utbedringene ikke var tilstrekkelige, og vedtaket

---

<sup>49</sup> Simula, «Kort om Smittestopp», [ingen dato], <https://www.simula.no/kort-om-smittestopp> (sist lest 23. nov. 2021).

<sup>50</sup> Datatilsynets varsel (2020) s. 15.

<sup>51</sup> Ibid.

<sup>52</sup> Ibid. s. 15, pkt. 7.1.

<sup>53</sup> Ibid. s. 6, pkt. 4.1.

<sup>54</sup> FHI, «Svar på varsel om vedtak», 23. juni 2020, [https://www.fhi.no/contentassets/8335598fc7b84637a35752760c125b3f/~-20\\_11308-13-svar-pa-varsel-om-vedtak-467321\\_3\\_1.pdf](https://www.fhi.no/contentassets/8335598fc7b84637a35752760c125b3f/~-20_11308-13-svar-pa-varsel-om-vedtak-467321_3_1.pdf) (sist lest 23. nov. 2021).

<sup>55</sup> Ibid. første avsnitt.

om midlertidig forbud mot innsamling av personopplysninger ble fattet av Datatilsynet 6. juli 2020.<sup>56</sup> Applikasjonen ble aldri gjenopprettet, men ble senere erstattet av Smittestopp 2.<sup>57</sup>

### 3.1.2. Teknologien bak «Smittestopp 2» og «CWA»

Norske Smittestopp 2 og tyske CWA er basert på Google og Apple sitt Exposure Notification System (ENS).<sup>58</sup> <sup>59</sup> For å kunne forstå hvordan applikasjonene opererer, er det nødvendig med en kort redegjørelse av hvordan ENS fungerer.

Etter at en har installert en smittesporingsapplikasjon eller aktivert ENS på sin enhet, kan mobilenheten din kommunisere med andre som har gjort det samme.<sup>60</sup> Når applikasjon er installert eller ENS aktivert, produserer mobilenheten din en «dagnøkkel» hvert døgn. Ut av denne genererer enheten din en «kontaktnøkkel» som byttes hvert 10. - 20. minutt.<sup>61</sup> Når en bruker er i nærheten av andre brukere, utveksles kontaktnøkklene på tvers av enhetene.<sup>62</sup> Utvekslingen skjer via Bluetooth, og det er ikke mulig å se hvilke av kontaktnøkklene som tilhører hvem. Om du senere blir bekreftet smittet, har du mulighet til å la applikasjonen din laste opp dagnøkkel og tilhørende kontaktnøkler til en server. Før dette steget forblir alle genererte nøkler lagret lokalt på din mobil. Listen over mulig smittede blir lastet ned av andre brukere daglig, og mobilenheten deres kontrollerer om noen av kontaktnøkklene har vært i kontakt med kontaktnøkler fra «smittelisten».<sup>63</sup> Hvis dette er tilfellet, vil applikasjonen varsle disse om at de har vært i mulig nærkontakt med en person smittet med SARS-CoV-2.

### 3.1.3. Norske «Smittestopp 2»

Smittestopp 2 ble lansert 21. desember 2020,<sup>64</sup> og FHI er behandlingsansvarlig. Applikasjonen erstattet Smittestopp 1 etter at Datatilsynet besluttet å nedlegge midlertidig forbud mot å behandle personopplysninger innsamlet gjennom applikasjonen. FHI adresserte mange av utfordringene med Smittestopp 1 da Smittestopp 2 ble lansert, og applikasjonen er i begynnelsen av september lastet ned av 1 080 000 personer.<sup>65</sup> Det tilsvarer omkring 20

---

<sup>56</sup> Datatilsynets vedtak (2020).

<sup>57</sup> Smittestopp 2 er nærmere forklart under pkt. 3.1.3.

<sup>58</sup> FHI, «Teknologien bak Smittestopp», 22. desember 2020, <https://www.fhi.no/om/smittestoppteknologien-bak-smittestopp/> (sist lest 23. nov. 2021).

<sup>59</sup> RKI (2021) pkt. 5 b.

<sup>60</sup> Google, «Exposure Notifications: Help slow the spread of COVID-19, with one step on your phone», [ingen dato], <https://www.google.com/covid19/exposurenotifications/> (sist lest 9. nov. 2021).

<sup>61</sup> Apple, «Exposure Notifications - Frequently Asked Questions», september 2020, <https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf>, pkt. 4 (sist lest 23. nov. 2021).

<sup>62</sup> Ibid.

<sup>63</sup> Ibid.

<sup>64</sup> FHI, «Ny Smittestopp-app klar for nedlasting», 23. desember 2020, <https://www.fhi.no/historisk-arkiv/covid-19/nyheter-2020/des2/ny-smittestopp-app-klar-for-nedlasting/> (sist lest 23. nov. 2021).

<sup>65</sup> FHI, «Nøkkeltall fra Smittestopp», 3. november 2021, <https://www.fhi.no/om/smittestoppteknologien-bak-smittestopp/> (sist lest 23. nov. 2021).

prosent av befolkningen. Applikasjonen har et begrenset bruksområde for dem under 16 år, fordi de ikke kan varsle om smitte gjennom applikasjonen.<sup>66</sup> Om den lastes ned av personer under 16 år kontrolleres likevel ikke.<sup>67</sup>

Applikasjonen bruker også Google og Apple sitt rammeverk. Datalagringen er desentralisert, og applikasjonens formål er å bidra til smittesporing. Applikasjonen samler også inn statistikk for å vurdere effekten av applikasjonen.<sup>68</sup> Dette er en klar forskjell fra statistisk bruk av data til å vurdere myndigheters *smitteverntiltak*.

### 3.1.4. Tyske «CWA»

CWA ble lansert 16. juni 2020.<sup>69</sup> Per 19. august 2021 er den nedlastet over 32 millioner ganger, noe som tilsvarer omtrent 27 prosent av befolkningen.<sup>70 71</sup> Det er mulig å slette applikasjonen fra en mobilenhet og deretter laste den ned igjen på samme enhet. Samtidig kan jeg ikke bekrefte at dette er tatt hensyn til i statistikken, og jeg tar derfor forbehold om at det er én nedlasting per bruker.

I personvernerklæringen er det eksplisitt lagt til grunn at applikasjonen er ment for tyske borgere som er eldre enn 16 år.<sup>72 73</sup> Som med franske TAC er det sannsynlig at prosentandelen nedlastinger er høyere om en tar utgangspunkt i at applikasjonen kun er lastet ned av voksne over 16 år.

Applikasjonens hovedformål er kontaktsporing, men den har også andre funksjoner. Disse inkluderer muligheten for å laste opp koronasertifikat og motta svar på hurtigprøver eller PCR-tester.<sup>74 75</sup> Sistnevnte er basert på samtykke, mens opplasting av koronasertifikat er regulert i

---

<sup>66</sup> FHI (2021).

<sup>67</sup> Ibid.

<sup>68</sup> Ibid.

<sup>69</sup> Telekom, «German Corona-Warn-App launched», 16. juni 2020, <https://www.telekom.com/en/company/details/german-corona-warn-app-launched-606824> (sist lest 23. nov. 2021).

<sup>70</sup> Statistisches Bundesamt, «Current population of Germany», [ingen dato], [https://www.destatis.de/EN/Themes/Society-Environment/Population/Current-Population/\\_node.html](https://www.destatis.de/EN/Themes/Society-Environment/Population/Current-Population/_node.html) (sist lest 10. nov. 2021).

<sup>71</sup> Robert Koch Institute (RKI), «Key figures for Corona-Warn-App», [ingen dato], <https://www.coronawarn.app/en/analysis/> (sist lest 19. august 2021).

<sup>72</sup> RKI (2021) pkt. 4.

<sup>73</sup> Det stilles imidlertid ikke krav om tysk statsborgerskap når en laster ned applikasjonen.

<sup>74</sup> RKI (2021) pkt. 6.

<sup>75</sup> PCR (polymerasekjedereaksjon) kan brukes til å avdekke om en person er smittet med SARS-CoV-2 ved å analysere prøvematerialet fra f.eks. en neseprøve. Se FHI, «Prøvetaking - praktisk gjennomføring», 3. september 2021, <https://www.fhi.no/nettpub/coronavirus/testing/provetaking/> (sist lest 23. nov. 2021).



PVF artikkel 9 (2) (g) og tyske Infektionsschutzgesetz (smittevernloven) § 22 (5).<sup>76 77 78</sup> Dersom en er nærmere enn 1,5 meter unna en annen mobilenhet med CWA installert, vil en etter 10 minutter bli definert som nærkontakter.<sup>79</sup>

### 3.1.5. Franske «TAC»

TAC er Frankrikes nåværende smittesporingsapplikasjon. Den ble lansert 22. oktober 2020 og erstattet «StopCovid».<sup>80</sup> Mange har omtalt det hele som en omprofilering av den eksisterende applikasjonen, som slet med få nedlastinger og lite bruk blant befolkningen.<sup>81</sup> Per dags dato er TAC lastet ned av omkring 35 millioner brukere.<sup>82</sup> Om en tar utgangspunkt i at alle disse er franske borgere, tilsvarer dette cirka 52 prosent av befolkningen. TAC har ingen aldersgrense, men det anbefales at barn under 15 år diskuterer installasjon av applikasjonen med enten foreldre eller verge.<sup>83</sup> Om installasjoner omtrent utelukkende er gjort av borgere over 15 år, er konsekvensen at de reelle tallene for antall nedlastinger blant den voksne befolkningen er enda høyere.

Per 3. september 2021 har applikasjonen ti ulike formål,<sup>84</sup> og flere av dem er knyttet til innsamling av personopplysninger. Blant disse er kontaktsporing, lagring av helseopplysninger i form av koronasertifikat og negative tester, innsamling av statistikk for å kunne vurdere myndighetenes tiltak samt registrering av gjester på utesteder og restauranter.<sup>85</sup> Det franske helsedirektoratet, underlagt det franske helsedepartementet, er behandlingsansvarlig for personopplysninger innsamlet gjennom applikasjonen.<sup>86</sup> Applikasjonen er også en av få som

---

<sup>76</sup> RKI (2021) pkt. 3, avsnitt 2.

<sup>77</sup> Min oversettelse av «Infektionsschutzgesetz» til «smittevernloven».

<sup>78</sup> Bundesministeriums der Justiz und für Verbraucherschutz (BMJV), «Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen», trådte i kraft 1. januar 2001, [https://www.gesetze-im-internet.de/ifsg/\\_22.html](https://www.gesetze-im-internet.de/ifsg/_22.html) (sist lest 23. nov. 2021).

<sup>79</sup> RKI, «Frequently Asked Questions about the Corona-Warn-App», [ingen dato] [https://www.coronawarn.app/en/faq/#check\\_in\\_how\\_does\\_it\\_work](https://www.coronawarn.app/en/faq/#check_in_how_does_it_work), under «How does event registration work in the Corona-Warn-App?» (sist lest 15. nov. 2021).

<sup>80</sup> BBC, «French Covid app relaunches to bumpy start», 23. oktober 2020, <https://www.bbc.com/news/technology-54660499> (sist lest 23. nov. 2021).

<sup>81</sup> TechCrunch, «France rebrands contact-tracing app in an effort to boost downloads», 23. oktober 2020, <https://techcrunch.com/2020/10/22/france-rebrands-contact-tracing-app-in-an-effort-to-boost-downloads/> (sist lest 23. nov. 2021).

<sup>82</sup> APP Covid, «Statistiques TousAntiCovid», [ingen dato], <http://www.appcovid.net/pages/tous-anticovid-et-applications-en-france/statistiques-application-TAC.html> (sist lest 15. nov. 2021).

<sup>83</sup> Se oversettelse 1 i oppgavens vedlegg. La Direction Générale de la Santé (DGS), «Vous êtes un mineur de moins de 15 ans ?», [ingen dato], <https://faq.tousanticovid.gouv.fr/kb/guide/fr/vous-etes-un-mineur-de-moins-de-15-ans-f6hXeZzPOg/Steps/129792> (sist lest 10. nov. 2021).

<sup>84</sup> DGS (2021) under «Data Controller and Purpose».

<sup>85</sup> Ibid.

<sup>86</sup> DGS (2021) under «Data Controller and Purpose».

ikke benytter seg av Google og Apple sitt rammeverk for smittesporing.<sup>87</sup> Franske myndigheter begrunner dette med at smittesporing er et nasjonalt anliggende.<sup>88</sup>

Fordi TAC ikke er basert på Google og Apple sitt rammeverk, kan franske myndigheter også benytte seg av en sentralisert løsning for lagring av data. Det har de gjort.<sup>89</sup> At applikasjonen bruker en sentralisert løsning i tillegg til å ha så mange ulike formål, er de viktigste årsakene til at den er tatt med i oppgaven. Sett i lys av de andre applikasjonene som er tilgjengelig i Europa, er dette ganske unikt. Applikasjonen bruker Bluetooth-teknologi for å knytte kontakt mellom brukere som er i nærkontakt med hverandre over et visst tidsrom. Der Google og Apple sitt ENS kun henter informasjon fra en sentralisert server når en person er bekreftet smittet, lagres «nøkler» generert i TAC på en sentralisert server umiddelbart.<sup>90</sup>

## 3.2. Hvilke komponenter skal vurderes?

Under skal jeg forklare hvorfor de ulike komponentene i smittesporingsapplikasjonene er valgt til analysen. Med «komponenter» mener jeg de ulike delene av applikasjonen som samlet sett utgjør helheten av den. Eksempelvis er hvorvidt personopplysningene lagres på en sentral server eller desentralt på brukernes mobilenhet en av disse komponentene.

Som tidligere henvist til henger prinsippene om formålsbegrensning og dataminimering tett sammen, og vurderingene av disse kan gli over i hverandre. Av den grunn har jeg strukturert drøftelsen på en måte som gjør at dette fremgår tydeligere. Det gjøres ved at jeg gjennomgår applikasjonenes komponenter enkeltvis og vurderer dem i lys av de prinsippene som er aktuelle. Dette kan være bare ett av prinsippene eller begge. For enkelthetens skyld kan disse komponentene lettere beskrives ved hjelp av spørreord.

For det første er det aktuelt å se på *hvilke* personopplysninger som innsamles, enten i form av kontaktsporing via Bluetooth eller lokasjonsdata via GPS. Som jeg skal vise til nedenfor, er dette aktuelt i lys av formålet en ønsker å oppnå med applikasjonene og hvor nødvendig det er samle inn slike opplysninger. Det er i tillegg relevant å se på *hvorfor* personopplysninger samles inn via applikasjonene. Som jeg har beskrevet i diskusjonsdelen av oppgaven, er dette

---

<sup>87</sup> Apple, «Exposure Notifications - Frequently Asked Questions», september 2020, <https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf> (sist lest 23. nov. 2021).

<sup>88</sup> Ministère des solidarités et de la sante, 21. oktober 2020, <https://web.archive.org/web/20201031233234/https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/TousAntiCovid> (sist lest 23. nov 2021). Se oversettelse 1 i oppgavens vedlegg.

<sup>89</sup> EU-kommisjonen, «How tracing and warning apps can help during the pandemic», [ingen dato], [https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/how-tracing-and-warning-apps-can-help-during-pandemic\\_en](https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/how-tracing-and-warning-apps-can-help-during-pandemic_en) (sist lest 15. nov. 2021).

<sup>90</sup> DGS (2021) pkt. 2.

særlig viktig der applikasjonen har flere formål utover hovedformålet om smittesporing. Som vist under er det eksempelvis av betydning hvor tydelig disse formålene er separert.

Avslutningsvis skal jeg se på *hvordan* personopplysningene lagres. Her er det særlig relevant hvorvidt personopplysningene lagres sentralisert eller desentralisert. Det er også en fordel å vurdere lagringsvarighet og hvordan dette eventuelt kan være uforenelig med hovedformålet om smittesporing i samfunnet.

Jeg begynner drøftelsen av problemstillingen ved å se på de tilfellene der applikasjonene har flere formål enn smittesporing. Deretter går jeg videre på hva som kan være konsekvensen av at hovedformålet om smittesporing utgår. En problemstilling som dette kan være relevant der smittenivået i samfunnet går nedover. Til slutt vurderer jeg hvordan personopplysninger i de ulike applikasjonene lagres og i hvor lang tid de lagres.

## 4. Flere formål enn smittesporing

En av hensiktene med formålsbegrensningsprinsippet i PVF artikkel 5 (1) (b) er å forhindre formålsutglidning.<sup>91</sup> I korte trekk betyr det at innsamlede opplysninger benyttes til andre formål enn det som var opprinnelig bestemt. Det er spesielt viktig når applikasjonene kan brukes til å samle inn store mengder personopplysninger på tvers av befolkningen. Hvis en applikasjon har flere formål enn smittesporing, må disse være separert fra hverandre.<sup>92 93</sup>

Først skal jeg se på formålene i de ulike applikasjonene, om enkelte av dem har flere formål enn smittesporing og hva slags konsekvenser dette kan ha. Deretter diskuterer jeg hvor klart de ulike formålene må være separert fra hverandre for å kunne være i tråd med prinsippet om formålsbegrensning. Jeg skal også vurdere dette i lys av dataminimeringsprinsippet, da det kan være vanskeligere å vite hva som er «nødvendig» behandling av personopplysninger dersom formålene glir over i hverandre.

Hovedformålet med de tre utvalgte applikasjonene er, som nevnt, smittesporing. Dette er Smittestopp 2 sitt eneste formål.<sup>94</sup> CWA og TAC har flere formål enn dette, og en av de øvrige funksjonene i begge applikasjonene er at brukeren kan laste opp koronasertifikatet sitt.<sup>95 96</sup> Sertifikatet viser blant annet hva slags vaksine brukeren har fått, hvor mange doser og når siste dose ble satt. I TAC kan applikasjonen også brukes til å skanne en QR-kode når en har vært på restauranter eller utesteder. Franske myndigheter har satt et krav om at dette må

---

<sup>91</sup> WP29 (2013) s. 4.

<sup>92</sup> Ibid. s. 16.

<sup>93</sup> EDPB (2020) avsnitt 26.

<sup>94</sup> FHI (2021).

<sup>95</sup> RKI (2021).

<sup>96</sup> DGS (2021).

gjøres for å kunne benytte seg av slike tilbud.<sup>97</sup> Selv om EDPB legger til grunn at applikasjoner kun bør ha som formål å drive smittesporing,<sup>98</sup> må det igjen vektlegges at EDPBs uttalelser kun er retningslinjer. Det viktigste er at prinsippene overholdes, og dette er sannsynligvis enklere når applikasjonen har kun ett formål.

For at prinsippene om formålsbegrensning og dataminimering er fulgt, stilles det blant annet krav til at applikasjonen må kunne brukes til sitt hovedformål uten å måtte godta alle formål samlet.<sup>99</sup> <sup>100</sup> Om denne grunnsteinen ikke er på plass, vil det også være langt vanskeligere å vurdere de enkelte formålene separat. Smittestopp 1 er høyst aktuell her. FHI samlet inn personopplysninger til to ulike formål, selv om disse ikke var separate. Det første av disse var smittesporing. Det andre var evaluering av effekten av myndighetenes iverksatte tiltak i forbindelse med covid-19.<sup>101</sup>

Ekspertgruppen for kodegjennomgang av løsning for digital smittesporing (heretter «ekspertgruppen»), konkluderte i likhet med Datatilsynet med at det var særlig problematisk at de to formålene i applikasjonen ikke var separate. Videre uttalte gruppen at en fremtidig versjon av applikasjonen bør ha oppdelte formål, da det ikke var mulig å akseptere kun ett av de to formålene.<sup>102</sup> Konsekvensen var at brukere som eksempelvis kun ønsket å bruke applikasjonen til smittesporing ikke kunne gjøre det. Da måtte de også la FHI bruke personopplysningene for statistiske formål, som igjen skulle brukes til å vurdere effektiviteten av smitteverntiltakene. Ekspertgruppen ble satt ned av Helse- og omsorgsdepartementet, og den har ingen autoritativ rettskildemessig vekt. Samtidig består gruppen av en rekke eksperter i sine respektive områder, og gruppens konklusjon inkluderer mye av det samme som er lagt til grunn av eksempelvis EDPB. Ekspertgruppens vurderinger er dermed også relevante her.

Spørsmålet er så hvor tydelig de ulike formålene må være separert for at en ikke skal havne i samme situasjon som med Smittestopp 1. Fordi installasjon av smittesporingsapplikasjonene er frivillig, kan det at formålene er samlet under ett skape et tillitsproblem der færre laster ned applikasjonen. Når utstrakt bruk av applikasjonene er en forutsetning for deres effekt, er dette spesielt viktig.<sup>103</sup> TAC og CWA har flere funksjoner i samme applikasjon, og det blir da et

---

<sup>97</sup> Reuters, «Coffee and croissant in a French cafe? You'll need a COVID pass for that», 9. august 2021, <https://www.reuters.com/world/europe/coffee-croissant-french-cafe-youll-need-covid-pass-that-2021-08-09/> (sist lest 23. nov. 2021).

<sup>98</sup> EDPB (2020) avsnitt 5.

<sup>99</sup> WP29 (2013) s. 16.

<sup>100</sup> EDPB (2020) avsnitt 26.

<sup>101</sup> Datatilsynets varsel (2020) s. 6.

<sup>102</sup> Ekspertgruppen for kodegjennomgang av løsning for digital smittesporing, «Endelig rapport for kildekodegjennomgang av løsning for digital smittesporing av koronaviruset», 18. mai 2020, [https://www.regjeringen.no/contentassets/88ec3360adae44a1a9635fd6c1a58fca/200520\\_rapport\\_ekspertgru\\_ppa\\_smittestopp.pdf](https://www.regjeringen.no/contentassets/88ec3360adae44a1a9635fd6c1a58fca/200520_rapport_ekspertgru_ppa_smittestopp.pdf), s. 29 (sist lest 23. nov. 2021).

<sup>103</sup> University of Oxford, «Digital contact tracing can slow or even stop coronavirus

spørsmål om hvordan applikasjonen er strukturert. Dersom en skulle påkrevd at samtlige av disse funksjonene hadde en egen applikasjon, er det mulig at færre ville lastet dem ned. På den måten ville det i så fall gått mot sin hensikt og potensielt gå utover det en kan forvente av befolkningen.

Måten dette er gjort på i TAC er at applikasjonens formål er mer tydelig delt opp ulike steder i applikasjonen. Brukeren må fysisk navigere seg videre inn i den funksjonen som ønskes brukt. For å legge til koronasertifikat eller registrere at en har vært på restaurant eller lignende, må brukeren eksplisitt velge dette i applikasjonsvinduet. Der blir brukeren møtt med ny tekst som forklarer formålet bak den aktuelle funksjonen.<sup>104</sup> Alle disse funksjonene kan brukes selv om kontaktsporing er avslått i hovedmenyen.<sup>105</sup> På den måten skiller applikasjonen seg radikalt fra Smittestopp 1, som gav befolkningen mindre grad av valgfrihet. Dersom smittesporing var aktivert i Smittestopp 1, hadde en ikke annet valg enn å også la applikasjonen samle inn personopplysninger til sekundærformålet sitt.

På dette punktet er TAC og CWA mer forenelige med prinsippet om formålsbegrensning enn det norske Smittestopp 1 noen gang var. Her må det likevel presiseres at der Smittestopp 1 samlet inn GPS-lokasjon og Bluetooth-data til smittesporing og vurdering av tiltak, bruker TAC helseopplysninger til koronasertifikat og Bluetooth-data til smittesporing. Opplysningene som samles inn i TAC har med andre ord to ganske ulike formål, noe som lar dem separeres lettere.

Dataminimeringsprinsippet er også relevant her. Hvis behandlingsformålene ikke er tydelig nok separert, er det vanskeligere å vite hvilke personopplysninger som er nødvendig å samle inn. På den måten er det tydelig at formålsbegrensningsprinsippet er mye av bærebjelken i personvernspørsmål. Om grunnlaget ikke er tilstrekkelig lagt til grunn, blir det vanskeligere å utføre det påfølgende arbeidet i tråd med personvernreglene. Igjen er Smittestopp 1 aktuell. FHI samlet inn både GPS-lokasjon og Bluetooth-data gjennom applikasjonen.<sup>106</sup> Lokasjonsdata skulle ikke bare brukes til å spore smitte, men også for å analysere om myndighetenes tiltak var effektive.<sup>107</sup> En bruker kunne ikke velge at lokasjonsdata kun skulle brukes til analysebruk eller smittesporing alene vice versa. Når alle disse personopplysningene uansett ble samlet inn, vanskeliggjorde FHI sitt eget arbeid. Fordi en da ikke kunne «slå av» lokasjonsdata for smittesporing, ble det betraktelig vanskeligere å vurdere om lokasjonsdata var nødvendig eller om Bluetooth-data i seg selv var tilstrekkelig.

---

transmission and ease us out of lockdown», 16. april 2020, <https://www.research.ox.ac.uk/article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown> (sist lest 23. nov. 2021).

<sup>104</sup> Se bilde 2 og 3 i oppgavens vedlegg.

<sup>105</sup> Se bilde 4 i oppgavens vedlegg.

<sup>106</sup> En utfyllende beskrivelse av dette finnes under overskriften «lokasjonsdata vs. kontaktsporing» nedenfor.

<sup>107</sup> Forskrift 27. mars 2020 nr. 475 om digital smittesporing og epidemikontroll i anledning utbrudd av Covid-19 § 1 (2).

Som jeg har vist til over har Smittestopp 2 kun ett formål, og det er ikke overraskende sett i lys av hvordan det endte for Smittestopp 1. Å skulle samle inn personopplysninger til kun ett formål kan ha sine klare fordeler. Når applikasjonen kun har ett formål, vil det være enklere å begrunne hvorfor applikasjonen samler inn visse typer personopplysninger. Av den grunn kan det også være lettere å sikre forenelighet med formålsbegrensningsprinsippet. Samtidig øker smitten i store deler av Europa per medio november 2021. I Tyskland kan restauranter, barer og lignende nå nekte personer uten gyldig koronasertifikat adgang til fasilitetene.<sup>108</sup> I Norge annonserte regjeringen den 12. november 2021 at Helse- og omsorgsdepartementet skal gi kommunene forskriftsfestet rett til å kreve gyldig koronasertifikat på lokalnivå.<sup>109</sup> Fremdeles er det viktigste at formålene kan skilles tydeligere fra hverandre, slik som både CWA og TAC lar en gjøre gjennom applikasjonens brukergrensesnitt. På den måten kan en unngå å havne i samme situasjon som en hadde med Smittestopp 1.

## 5. Hva om applikasjonens formål utgår?

I den følgende drøftelsen skal jeg vurdere hva som kan være konsekvensene av at formålet for innsamling av personopplysninger gjennom en smittesporingsapplikasjon utgår. Igjen kan en se til forholdsmessighetsprinsippet nedfelt i PVF fortalepunkt 4. Fordi retten til personvern ikke er absolutt, må situasjonen vurderes etter de samfunnsmessige forholdene.<sup>110</sup> Derfor er den til enhver tid gjeldende smittesituasjonen viktig når en skal vurdere om innsamling av personopplysninger gjennom smittesporingsapplikasjoner er forholdsmessig.

Norske medier har gitt meg et langt bedre overblikk over smittesituasjonen i Norge enn i Tyskland og Frankrike. Derfor bruker jeg Smittestopp 2 som hovedeksempel i drøftelsen. Det betyr ikke at drøftelsen ikke kan være relevant for de to andre tilfellene. Smittesituasjonen er også i stadig endring, og jeg forholder meg derfor til situasjonen da Norge ble gjenåpnet og smittetallene var lavere enn dagens nivå (primo desember 2021).<sup>111</sup>

Hovedformålet med de tre applikasjonene er å forhindre smittespredning, og disse formålene ble satt før innsamlingen av personopplysninger begynte. Det er likevel ikke tilstrekkelig at formålet var oppfylt ved starten av innsamlingen. For å være i tråd med prinsippet om formålsbegrensning, må formålet være møtt til enhver tid. EU-domstolen har fastslått dette i

---

<sup>108</sup> CNN, «Berlin bans unvaccinated from entertainment venues, as Germany battles record-breaking Covid cases», 11. november 2021. <https://edition.cnn.com/2021/11/11/europe/berlin-unvaccinated-rules-germany-covid-intl-grm/index.html> (sist lest 23. nov. 2021).

<sup>109</sup> SMK og Helse- og omsorgsdepartementet, «Lokale tiltak er mest treffsikkert», 12. november 2021, <https://www.regjeringen.no/no/aktuelt/lokale-tiltak-er-mest-treffsikkert/id2886657/> (sist lest 23. nov. 2021).

<sup>110</sup> PVF fortalepunkt 4.

<sup>111</sup> Regjeringen.no, «En normal hverdag med økt beredskap», 24. september 2021, <https://www.regjeringen.no/no/tema/Koronasituasjonen/en-normal-hverdag-med-okt-beredskap2/id2872184/> (sist lest 23. nov. 2021).

*Tele2 Sverige og Watson*.<sup>112</sup> I saken hadde britiske og svenske domstoler bedt EU-domstolen om en redegjørelse av hvorvidt nasjonal lovgivning som tillot lagring av personopplysninger for bekjempelse av kriminalitet var lovlig. EU-domstolens konklusjon var at dette var i strid med direktiv 2002/58/EF («kommunikasjonsverndirektivet»<sup>113</sup>). Saken gjaldt verken PVF eller PVD, men annen sekundærlovgivning. Samtidig er dommen fremdeles relevant for oppgaven, ettersom domstolen også diskuterte forholdet mellom innsamlede opplysninger og formålet med behandlingen.

Spørsmålet er uansett når formålet med en smittesporingsapplikasjon er utgått. Det er ikke mulig å gi et konkret svar til et slikt spørsmål. Smittesituasjonen er veldig flyktig, og det ville være vanskelig å sette et konkret tidspunkt for når formålet om smittesporing har utspilt sin rolle. Samtidig forventet Datatilsynet at FHI kunne dokumentere den faktiske nytteverdien av Smittestopp 1, også sett i lys av den daværende smittesituasjonen.<sup>114</sup>

Om formålet med innsamlingen ikke lenger er gjeldende, kan behandlingen heller ikke være berettiget. Dette er nok likevel ikke særlig aktuelt. Pandemien var ikke over da gjenåpningen fant sted i slutten av september. Det var fremdeles smitte i samfunnet, og Smittestopp 2 sitt formål om smittesporing var fremdeles høyst relevant. Smittesporingsapplikasjoner har heller aldri vært ment som eneste tiltak mot økende smitte, men heller som et bidrag til manuell smittesporing.<sup>115</sup> Om ikke annet kan det argumenteres for at Smittestopp 2 sitt formål ble styrket da Norge ble gjenåpnet. Sammen med gjenåpningen av landet endret regjeringen strategien fra «TISK» til «nedjustert TISK». En av endringene var at smittede selv ble ansvarlige for å varsle potensielle nærkontakter.<sup>116</sup> Ved å bruke Smittestopp 2, kan brukere også varsle øvrige nærkontakter, selv om de ikke vet hvem det skulle være. På den måten kan en også effektivisere smittesporingsarbeidet enn å gjøre dette på egenhånd manuelt.

Smittenivået i Norge har økt betraktelig siden Norge ble gjenåpnet. Den 2. november 2021 ble det registrert 1406 smittede i landet.<sup>117</sup> 8,9 prosent av alle PCR-tester var positive, og dette er en av de høyeste prosentandelene positive tester som er avlagt i løpet av pandemien.<sup>118</sup> Om en skulle deaktivert Smittestopp 2 når smittekurven pekte nedover, men aktivert og fortsatt innsamlingen av personopplysninger når den peker oppover ville sannsynligvis vært vanskelig

---

<sup>112</sup> *Tele2 Sverige AB og Watson* [GC], C-203/15 og C-698/15, avsnitt 110.

<sup>113</sup> Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon.

<sup>114</sup> Datatilsynets varsel (2020) pkt. 4.2.

<sup>115</sup> EDPB (2020) avsnitt 4.

<sup>116</sup> FHI, «Nedjustert TISK», 17. november 2021, <https://www.fhi.no/nettpub/coronavirus/testing/nedjustert-tisk> (sist lest 23. nov. 2021).

<sup>117</sup> FHI, «Statistikk om koronavirus og covid-19», 15. november 2021, <https://www.fhi.no/sv/smittsomme-sykdommer/corona/dags--og-ukerapporter/dags--og-ukerapporter-om-koronavirus>, under «antall meldte» (sist lest 23. nov. 2021).

<sup>118</sup> *Ibid.* under «antall testet».

og lite formålstjenlig. FHI brukte samme argumentasjon da de svarte på Datatilsynets varsel om midlertidig forbud av Smittestopp 1.<sup>119</sup>

Det neste spørsmålet er om behandlingen av personopplysninger i Smittestopp 2 fremdeles er nødvendig og om samme effekt kan oppnås på mindre inngripende måter. Mot slutten av september hadde Smittestopp 2 blitt lastet ned 1.083.200 ganger.<sup>120 121</sup> Dette utgjør omkring 20 prosent av hele den norske befolkningen og omkring 25 prosent av befolkningen over 16 år.<sup>122 123 124</sup>

Den 24. september ble syv personer meldt smittet gjennom Smittestopp 2.<sup>125</sup> Samme dag ble 649 personer meldt smittet via Meldingssystem for smittsomme sykdommer (MSIS). Med andre ord ble én prosent av alle meldte smittetilfeller i Norge gjort via Smittestopp 2. Det er likevel under forutsetningen om at alle som har lastet ned applikasjonen ikke har slettet den eller deaktivert kontaktsporing. Den 2. november 2021 ble 1406 registrert smittet i Norge, og kun 14 av disse ble meldt gjennom Smittestopp 2. Dette utgjør fremdeles én prosent av alle meldte smittetilfeller, slik som i september.<sup>126 127</sup>

Det er vanskelig å gi et godt svar på når en smittesporingsapplikasjon sitt formål utgår. Om en kun tar utgangspunkt i perioder med lavt smittetrykk er svaret sannsynligvis at innsamling av personopplysninger via Smittestopp 2 er unødvendig. Årsaken er at manuell smittesporing, både i regi av kommunen og privat, vil kunne være tilstrekkelig. Om smittetrykket blir så høyt at kommunene overbelastes og privatpersoner ikke kan drive smittesporing på egenhånd, kan svaret være det motsatte.

Alt dette forutsetter uansett at nok mennesker har lastet ned applikasjonen og har aktivert den. Enkelte modelleringer viser at omkring 60 prosent av et lands befolkningen må bruke en smittesporingsapplikasjon dersom en skal kunne begrense smittespredningen, selv om færre

---

<sup>119</sup> FHI, «Svar på varsel om vedtak», 23. juni 2020, [https://www.fhi.no/contentassets/8335598fc7b84637a35752760c125b3f/~-20\\_11308-13-svar-pa-varsel-om-vedtak-467321\\_3\\_1.pdf](https://www.fhi.no/contentassets/8335598fc7b84637a35752760c125b3f/~-20_11308-13-svar-pa-varsel-om-vedtak-467321_3_1.pdf), s. 3, siste avsnitt (sist lest 23. nov. 2021).

<sup>120</sup> FHI, «Nøkkeltall fra Smittestopp», 10. november 2021, <https://www.fhi.no/om/smittestopp/nokkeltall-fra-smittestopp/> (sist lest 23. nov. 2021).

<sup>121</sup> Merk at statistikken viser antall nedlastinger, ikke antall aktive brukere.

<sup>122</sup> Statistisk sentralbyrå, «Befolkning», 19. august 2021, <https://www.ssb.no/befolkning/folketall/statistikk/befolkning> (sist lest 23. nov. 2021).

<sup>123</sup> Ibid. tabell 3 («Befolkningen fordelt på aldersgrupper, 1. januar»).

<sup>124</sup> Som nevnt under forklaringen av Smittestopp 2 er det et krav om at brukeren er over 16 år for å kunne bruke applikasjonen.

<sup>125</sup> FHI, «Nøkkeltall fra Smittestopp», 10. november 2021, <https://www.fhi.no/om/smittestopp/nokkeltall-fra-smittestopp/> under «Antall meldt smittet i Smittestopp» (sist lest 23. nov. 2021).

<sup>126</sup> Ibid.

<sup>127</sup> Prosentandelen av smittede varslet via Smittestopp 2 er utregnet ved å dele antall varslede smittetilfeller via applikasjonen på antall meldte smittetilfeller. Hele tallet er deretter delt på 100.



brukere også bidrar.<sup>128</sup> Siden starten av april 2021 har Smittestopp 2 kun hatt ca. 100.000 nedlastinger, og det kan late til at antall nedlastinger har stagnert på omkring 1.000.000. Det kan også argumenteres for at innsamlingen av personopplysninger blant dem som har lastet applikasjonen er unødvendig, fordi de lave tallene per nå ikke bidrar til formålet i nevneverdig grad.

Samlet sett er det vanskelig å fastslå et konkret tidspunkt for når en applikasjon sitt formål er utgått. At et land gjenåpner slik som Norge gjorde i september 2021 betyr ikke at pandemien er over. Ettersom smittesituasjonen stadig utvikler seg, er det nærmest urimelig å kreve at teknologien skal holde tritt med smittenivået. Det vil i så fall kunne legge et uforholdsmessig press på behandlingsansvarlig.

## 6. Lokasjonsdata eller kontaktsporing?

Hvorvidt smittesporingsapplikasjoner skal benytte seg av lokasjonsdata eller kontaktsporing har vært gjenstand for debatt. Fordi de fleste applikasjoner i medlemsstatene nå benytter seg av Google og Apple sitt rammeverk er ikke dette like relevant lenger.<sup>129</sup> Smittestopp 1 i Norge var likevel blant få applikasjoner som i 2020 benyttet seg av lokasjonsdata.<sup>130</sup> Det tok heller ikke lang tid før Datatilsynet til slutt la ned forbud om innsamling av opplysninger gjennom applikasjonen, mye på bakgrunn av bruk av lokasjonsdata.<sup>131</sup> Verken TAC, CWA eller Smittestopp 2 benytter seg av lokasjonsdata.

Videre kan det være nyttig å se på nettopp hvorfor kontaktsporing er blitt det foretrukne middelet fremfor innsamling av lokasjonsdata. Da er det i første omgang nødvendig med en kort redegjørelse av disse to.

Lokasjonsdata gir en nøyaktig geografisk plassering av hvor mobilenheten befinner seg ved å måle breddegrad, lengdegrad, høyde over havet og tid brukt på lokasjoner.<sup>132</sup> Mobilenheter kommer oftest med egen GPS-teknologi innebygd, og det er denne teknologien som brukes. Ettersom store deler av verdens befolkning oftest har med seg mobilen sin, betyr dette også at en kan overvåke den enkelte person. Applikasjoner med kontaktsporing benytter seg av Bluetooth-teknologi og mobilenhetens geosentriske plassering blir ikke samlet inn. I stedet

---

<sup>128</sup> University of Oxford, «Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown», 16. april 2020, <https://www.research.ox.ac.uk/article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown> (sist lest 23. nov. 2021).

<sup>129</sup> XDA, «Here are the countries using Google and Apple's COVID-19 Contact Tracing API», 25. februar 2021, <https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/> (sist lest 23. nov. 2021).

<sup>130</sup> Simula (2020) under «Hva slags data samles inn og hvordan blir dataene brukt?».

<sup>131</sup> Datatilsynets vedtak (2020).

<sup>132</sup> EDPB (2020) s. 13 under «Location data».

utveksler mobilenhetene digitale nøkler med andre mobilenheter i nærheten. Dersom en i henhold til epidemiologiske definisjoner blir regnet som en nærkontakt, blir brukeren varslet om dette.<sup>133</sup>

Om en benytter seg av lokasjonsdata eller kontaktsporing er høyst relevant i lys av prinsippet om formålsbegrensning. Eksempelvis kan lokasjonsdata bli brukt for å se om brukeren befant seg innenfor eget bosted eller annet egnet sted å være i karantene. Selv om dette ikke er et formål i noen av applikasjonene i mitt utvalg, finnes det i andre tilfeller. Eksempelvis må polske borgere som er blitt underlagt karanteneplikt ta et bilde av seg selv og laste det opp i en egen applikasjon. Ansiktsgjenkjenning og geosentrisk plassering brukes deretter for å bekrefte at brukeren gjennomfører den lovpålagte karantenen.<sup>134</sup> Slik innsamling ville ikke vært i tråd med hovedformålet om smittesporing i Smittestopp 2, CWA og TAC og dermed heller ikke vært i tråd med formålsbegrensningsprinsippet.

Det er også bred enighet om at innsamling av lokasjonsdata bør unngås, fordi det strider med nødvendighetskravet i dataminimeringsprinsippet. EDPB uttaler i sine retningslinjer at en løsning som bygger på kontaktsporing er å foretrekke.<sup>135</sup> EU-kommisjonen legger det samme til grunn i sin anbefaling. Der uttaler de at lokasjonsdata ikke er nødvendig, da hensikten ikke er å følge brukerens bevegelser.<sup>136</sup> Også WHO legger seg på samme linje.<sup>137</sup>

Disse tre organene er så tydelig samstemte på grunn av nødvendighetskravet i prinsippet om dataminimering. Når formålet er å bryte smittekjeder i befolkningen, må nødvendighetskravet ses i lys av dette. Å skulle spore hvor enkeltpersoner befinner seg til enhver tid ville gått langt utover det som er nødvendig. Det gjelder spesielt når mindre inngripende tiltak, eksempelvis kontaktsporing, kan bidra til å oppnå formålet. Da vil helsemyndighetene heller ikke kunne fastslå hvor brukeren til enhver tid befinner seg. Samtidig vil de kunne bruke teknologien til å bryte smittekjeder i samfunnet gjennom Bluetooth-teknologi.

Basert på de rettskildene jeg har gjennomgått til nå, skal en ha svært gode holdepunkter for å kunne påstå at det å bruke lokasjonsdata Smittestopp 2, CWA og TAC ville vært i tråd med både prinsippet om dataminimering og formålsbegrensning.

---

<sup>133</sup> Se f.eks. personvernerlæring for Smittestopp 2. Der er den epidemiologiske definisjonen satt til to meters avstand i mer enn 15 minutter i det tidsrommet en bruker antas å være smittsom.

<sup>134</sup> European Union Agency for Fundamental Rights, «Coronavirus pandemic in the EU – Fundamental rights implications: With a focus on contact tracing apps», 30. april 2020, [https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may\\_en.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf), s. 55, første avsnitt. Originalkilden er på polsk og er ikke oversatt (sist lest 23. nov. 2021).

<sup>135</sup> EDPB (2020) avsnitt 27.

<sup>136</sup> COM(2020) 2523 final pkt. 3.4 under «Contact tracing and warning functionality».

<sup>137</sup> WHO (2020) s. 4 under «Data minimization».

## 7. Sentralisert eller desentralisert lagring?

Under skal jeg redegjøre for hvordan enkelte lagringsformer kan være mer i strid med både prinsippene om formålsbegrensning og dataminimering enn andre. PVF artikkel 5 (1) (e) stadfester prinsipper for hvordan personopplysninger skal lagres. I bestemmelsen står det at «personopplysninger skal lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er *nødvendig for formålene* som personopplysningene behandles for [...]» (min utheving). Grunnet likhetstrekkene til dataminimeringsprinsippet i artikkel (5) (1) (c) gir jeg derfor ingen ytterligere introduksjon av prinsippet om lagringsbegrensning.

Først tar jeg for meg de ulike metodene for lagring av personopplysninger, og deretter ser jeg på varigheten av hvor lenge disse opplysningene lagres. Fordi det hele har et relativt teknisk aspekt ved seg, er det nødvendig med en redegjørelse av forskjellene på en sentralisert og en desentralisert løsning for lagring av personopplysninger. Deretter foretar jeg en gjennomgang av svakheter og styrker av de to løsningene, sett opp mot de smittesporingsapplikasjonene som er tatt med i oppgaven.

Med en sentralisert løsning blir innsamlede personopplysninger pseudonymisert og lagret på en sentral server.<sup>138</sup> Opplysninger som er blitt pseudonymisert kan kun identifiseres ved bruk av tilleggsopplysninger.<sup>139</sup> Dette kan eksempelvis være en permanent unik ID-kode, som igjen er koblet til en bestemt bruker.<sup>140</sup> Når brukeren rapporteres å ha testet positivt for SARS-CoV-2, rapporteres det direkte til den sentrale serveren, og personer som har vært i kontakt med brukeren blir varslet om en mulig nærkontakt.<sup>141</sup> Denne løsningen er brukt i TAC.<sup>142</sup>

Opplysninger kan også anonymiseres, i hvert fall i teorien. I motsetning til pseudonymiserte personopplysninger, kan ikke anonymiserte opplysninger identifiseres. Det gjelder også hvis en har tilgang på nødvendige tilleggsopplysninger.<sup>143</sup> Likevel viser ulik forskning at fullstendig anonymisering av personopplysninger er vanskeligere enn antatt, om ikke umulig, og at det er mulig å dekonstruere innsamlede opplysninger for å indentifisere brukere.<sup>144</sup> <sup>145</sup> Fullstendig

---

<sup>138</sup> Lucie White og Phillipe van Basshuysen, «Privacy versus Public Health? A Reassessment of Centralised and Decentralised Digital Contact Tracing» *Science and Engineering Ethics*, 27 (2021) s. 2. DOI: <https://doi.org/10.1007/s11948-021-00301-0> (sist lest 23. nov. 2021).

<sup>139</sup> PVF artikkel 4 (5).

<sup>140</sup> White og van Basshuysen (2021) s. 4.

<sup>141</sup> Ibid.

<sup>142</sup> DGS (2021) under «personal data processed on the central server».

<sup>143</sup> EDPB (2020) avsnitt 15.

<sup>144</sup> Luc Rocher, Julien M. Hendrickx og de Montjoye, «Estimating the success of re-identifications in incomplete datasets using generative models» *Nature Communications*, 10 (2019). DOI: <https://doi.org/10.1038/s41467-019-10933-3> (sist lest 23. nov. 2021).

<sup>145</sup> Apostolos Pyrgelis, Carmela Troncoso og Emiliano De Cristofaro, *Knock Knock, Who's There? Membership Inference on Aggregate Location Data*, innsendt i forbindelse med det 25. Network and Distributed System Security symposium 21. august 2017. DOI: <https://arxiv.org/abs/1708.06145> (sist lest 23. nov. 2021).

anonymiserte personopplysninger faller ikke innenfor forordningens virkeområde.<sup>146</sup> De kan dermed brukes fritt, under forutsetning av at de faktisk er fullstendig anonymiserte.

Med en desentralisert løsning blir det meste av personopplysninger lagret lokalt og kryptert på brukerens enhet, uten at tredjeparter har tilgang.<sup>147</sup> Det er først når brukeren rapporteres som smittet at informasjonen sendes til en sentral server for å rapportere til andre brukere.<sup>148</sup> Teknologien bak den desentraliserte løsningen er allerede presentert under punkt 3.1.2.

Det er en pågående debatt rundt hvilken løsning som er den mest effektive for å bidra til å bekjempe pandemien. Løsningen som kan være mest velfungerende sett i lys av å bevare personopplysninger, er ikke nødvendigvis den som er mest velfungerende sett i lys av effektiv bekjemping av smitte. Igjen må en finne en balansegang mellom personvernet og det formålet som behandlingen av opplysninger er ment å oppnå. Under skal jeg forklare hvilke fordeler og ulemper som er forbundet med sentraliserte og desentraliserte løsninger, sett i lys av effektiv smittesporing og hensynet til den registrertes personvern. I løpet av vurderingen trekker jeg også inn eksempler fra de applikasjonene jeg har valgt ut til oppgaven.

## 7.1. Desentralisert løsning

Som tidligere nevnt benytter store deler av EØS-statenes applikasjoner en desentralisert løsning. Dette inkluderer CWA og Smittestopp 2. EDPB påpeker at både sentraliserte og desentraliserte løsninger kan være bærekraftige.<sup>149</sup> Likevel har EDPB valgt å skrive i en fotnote at en desentralisert løsning sannsynligvis er mer i tråd med prinsippet om dataminimering.<sup>150</sup> EU-kommisjonen sier videre rett ut at den desentraliserte løsningen er mer i tråd med prinsippet, og WHO stiller seg også bak en slik fremgangsmåte.<sup>151 152</sup> Fra et personvernvennlig standpunkt kan det med andre ord late til at en desentralisert løsning er å foretrekke. Fordi personopplysningene lagres lokalt på brukerens egen mobilenhet og ikke på en sentralisert server er det begrenset hvor store mengder av personopplysningene som deles. Det deles med andre ord ikke mer enn det som er nødvendig, i tråd med dataminimeringsprinsippet.

Videre må brukere av både CWA og Smittestopp 2 selv varsle om at de har testet positivt for SARS-CoV-2 eller har vært i fare for å bli smittet.<sup>153 154</sup> Først da blir personopplysningene sendt til en sentral server, som igjen varsler potensielle nærkontakter om at de kan være smittet. På den måten er det et ekstra lag med sikkerhet for brukeren. Det er også her store deler av

---

<sup>146</sup> PVF fortalepunkt 26.

<sup>147</sup> White og van Basshuysen (2021) s. 4.

<sup>148</sup> Ibid.

<sup>149</sup> EDPB 04/2020 avsnitt 42.

<sup>150</sup> EDPB 04/2020 fotnote 18.

<sup>151</sup> COM(2020) 2523 final under « — Data of the infected person ».

<sup>152</sup> WHO (2020) s. 4 («Privacy-preserving data storage»).

<sup>153</sup> CWA (2021) pkt. 6 a.

<sup>154</sup> FHI (2021) pkt. 2.2.

forskjellene mellom applikasjoner med en sentralisert og desentralisert løsning ligger. Dersom en applikasjon har en sentralisert løsning, er denne informasjonen allerede innsamlet på en sentral server. Alternativet gir dermed brukeren mer kontroll over egne personopplysninger, fordi de kan velge å ikke melde ifra om at de er smittet og på den måten ikke laste opp ytterligere personopplysninger til den sentrale serveren.

## 7.2. Sentralisert løsning

Selv om EDPB og øvrige organer påpeker at desentraliserte løsninger kan være mer i tråd med prinsippet om dataminimering, sier ingen av dem at en sentralisert løsning er uaktuelt. EDPB skriver imidlertid i sine retningslinjer at det forutsetter et sterkt fokus på sikkerhet og at begge alternativene må avveies i lys av personvernet.<sup>155</sup> Selv om den brede konsensusen blant EØS-statene er å bruke den desentraliserte løsningen via Google og Apple sitt felles rammeverk, er det ikke utenkelig at en sentralisert løsning kan ha nyttige sider ved seg.

TAC er blant de få smittesporingsapplikasjonene som benytter seg av en sentralisert løsning. Franske helsemyndigheter har lagt til grunn at denne løsningen er den mest sikre og sikrer størst grad av statlig autonomi.<sup>156</sup> Tilhengere av en sentralisert løsning argumenterer oftest for at det er mer effektivt enn en desentralisert løsning.<sup>157</sup>

Simula, utvikleren av Smittestopp 1, påpeker eksempelvis på sine nettsider at en sentralisert løsning gir raskere og mer nøyaktig smittesporing.<sup>158</sup> Videre skriver White og van Basshuysen at dersom en kan rapportere symptomer før testresultatene bekrefter at en er smittet med SARS-CoV-2, kan dette øke applikasjonens effektivitet.<sup>159</sup> Problemet med et slikt premiss er at applikasjonen faktisk lar brukeren gjøre dette. I TAC må brukeren selv loggføre at de har testet positivt for viruset. Dette gjøres ved å skanne en QR-kode som brukeren blir tilsendt.<sup>160</sup> Dersom effektivitet er en av de største betingelsene for å velge den sentraliserte løsningen, er det klart at et slikt trinn i varslingsprosessen kan medføre større forsinkelser i å varsle andre om at de kan være smittet. Det gjelder særlig dersom testkapasiteten er lav og det er mange som tester seg, noe som igjen kan lede til forsinkede resultater.

Dette kan videre være en enda større utfordring i forbindelse med Delta-varianten av SARS-CoV-2. En studie viser at mutasjonen er langt mer smittsom, og at reproduksjonstallet for

---

<sup>155</sup> EDPB (2020) avsnitt 42 flg.

<sup>156</sup> Se oversettelse 2 i oppgavens vedlegg.

<sup>157</sup> F.eks. White og van Basshuysen (2021).

<sup>158</sup> Simula (2020) under «Hvorfor ikke lokal lagring av data».

<sup>159</sup> White og van Basshuysen (2021) s. 2, nederst i første avsnitt.

<sup>160</sup> Bilde 1 i oppgavens vedlegg illustrerer dette.

varianten var på hele 5.08 sammenlignet med 2.79 for den originale varianten.<sup>161</sup> Ifølge denne studien smittet én person i gjennomsnittet fem andre. Derfor er effektivitet i smittesporingen ekstra viktig, men kan bli bremsset av at TAC kun lar deg varsle om smitte etter at du først har blitt bekreftet smittet selv.<sup>162</sup> Om en uansett står overfor dette hinderet når en skal rapportere smitte, som igjen begrenser effektiv smittesporing, kan det tale for at en desentralisert løsning uansett er mer bærekraftig.

Fordi kommunikasjonen med den sentrale serveren går automatisk, har brukeren heller ikke noe annet valg enn å la personopplysningene bli overført til serveren. Alternativet er å slette eller deaktivere applikasjonen på mobilenheten sin. Det gjelder uansett om du bekrefter deg selv som smittet eller ei, noe som er en av de større innsigelsene mot løsningen.

Ved bruk av sentraliserte løsninger må dataminimeringsprinsippet også ses i lys av et sikkerhetsaspekt. Fordi store mengder informasjon er samlet på samme sted, betyr det at fiendtlige aktører kan benytte seg av eksempelvis tjenestenektangrep («Distributed Denial of Service» eller DDOS-angrep) for å sette en server ut av spill.<sup>163</sup> Et tjenestenektangrep betyr i korte trekk at en tar kontroll over intetanende eiere sine enheter. Deretter styrer en disse enhetene til å hente innhold fra en server på normalt vis, slik som med en nettvavis. I større skala klarer ikke serveren å møte denne etterspørselen og serveren ender opp med å krasje. Det kan på mange måter sammenlignes med trafikkork.<sup>164</sup> Skulle dette skje, vil en ikke lenger ha tilgang til den sentraliserte serveren, og det kan ha store konsekvenser for smittesporingen dersom en er avhengige av smittesporingsapplikasjonen.

Samtidig har enkelte forskere tatt til orde for at det er mulig å reversere anonymiseringen av personopplysninger.<sup>165</sup> Det vil i praksis bety at det, med forbehold, kan være mulig å få tilgang til personopplysninger tilknyttet brukere av smittesporingsapplikasjoner dersom angripere får tilgang til serverne. WP29 har også uttalt i sine retningslinjer at fullstendig anonymisering kan være vanskelig å gjennomføre i praksis.<sup>166</sup> EDPB har likevel ikke gitt sin formelle tilslutning til disse retningslinjene, noe en må ha i mente.<sup>167</sup> Dersom det i praksis er mulig å identifisere

---

<sup>161</sup> Ying Liu og Joacim Rocklöv, «The reproductive number of the Delta variant of SARS-CoV-2 is far higher compared to the ancestral SARS-CoV-2 virus» *Journal of Travel Medicine*, 28 (2021), 7. DOI: <https://doi.org/10.1093/jtm/taab124>, s. 1 (sist lest 23. nov. 2021).

<sup>162</sup> Se bilde 1 i oppgavens vedlegg.

<sup>163</sup> Zhou m.fl. «A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic» *Neural Computing and Applications* (2021). DOI: <https://doi.org/10.1007/s00521-021-06389-6> (sist lest 23. nov. 2021).

<sup>164</sup> Nettvett.no, «DDoS-angrep», 13. januar 2020, <https://nettvett.no/ddos-angrep/> (sist lest 23. nov. 2021).

<sup>165</sup> Luc Rocher, Julien M. Hendrickx og de Montjoye (2019).

<sup>166</sup> Article 29 Data Protection Working Party (WP29), «Opinion 05/2014 on Anonymisation Techniques», WP216, 10. april 2014, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf), s. 3 (sist lest 23. nov. 2021).

<sup>167</sup> EDPB (2018).

brukere på grunn av mangelfull anonymisering, er dette klart problematisk i lys av prinsippet om dataminimering.

Som jeg har vist til over, er det klare fordeler og ulemper ved bruk av både sentraliserte og desentraliserte løsninger. Likevel kan ting tyde på at TAC er mer problematisk enn CWA og Smittestopp 2. Dersom effektiv smittesporing er et av de bærende argumentene for å bruke en sentralisert løsning, kan det være et stort hinder at brukere av TAC uansett må bekrefte via applikasjonen at de er smittet. Hvis en da legger til grunn at begge løsninger er like effektive, er det rimelig å anta at en desentralisert løsning er å foretrekke fordi den i utgangspunktet er mer forenelig med dataminimeringsprinsippet.

## 8. Hvor lenge bør personopplysningene oppbevares?

Hvor lenge personopplysningene lagres vil også være relevant, og dette er nedfelt i et eget prinsipp i PVF.<sup>168</sup> Samtidig kan dette også utledes av vilkårene om nødvendighet og relevans i PVF artikkel 5 (1) (c). Jeg viser til den generelle fremstillingen av vilkårene i punkt 2.3. Dersom en lagrer opplysninger lengre enn nødvendig sett i lys av formålet eller beholder opplysninger som ikke lenger er relevante, kan dette være i strid med prinsippet om dataminimering. Det er særlig aktuelt for denne oppgaven, fordi det er begrenset hvor lenge en person er smittsom med SARS-CoV-2. Dette er nærmere redegjort for under.

I sine retningslinjer uttaler EDPB at lagringstid må baseres på hva som er medisinsk relevant, deriblant inkubasjonstid.<sup>169</sup> Hvor lenge dette er har EDPB ikke konkret fastslått. Videre legger både WHO<sup>170</sup> og EU-kommisjonen<sup>171</sup> til grunn at personopplysningene ikke skal lagres lenger enn det som er nødvendig for å oppfylle formålet om smittesporing. E-helsenettverket er det eneste som konkret legger til grunn at personopplysningene bør slettes etter 14-16 dager, i tråd med Det europeiske smittevernbyråets anbefalinger.<sup>172</sup> Fordi situasjonen er i stadig endring, kan det være en fordel at lagringsperiode ikke fastsettes konkret.

Inkubasjonstiden for covid-19, tiden det tar fra en blir smittet til symptomer blir synlige, er estimert til å være opp til 14 dager.<sup>173</sup> Mediantiden antas, basert på nåværende forskning, å

---

<sup>168</sup> PVF artikkel 5 (1) (e).

<sup>169</sup> EDPB (2020) avsnitt 35.

<sup>170</sup> WHO (2020) s. 4 under «Data minimization».

<sup>171</sup> COM(2020) 2523 final pkt. 3.7. under «Contact tracing and warning functionalities».

<sup>172</sup> eHealth Network (2021) s. 26 - appendix I, id EF-02.

<sup>173</sup> Centers for Disease Control and Prevention (CDC), «Interim Clinical Guidance for Management of Patients with Confirmed Coronavirus Disease (COVID-19)», 21. februar 2021, <https://www.cdc.gov/coronavirus/2019-ncov/hcp/clinical-guidance-management-patients.html> (sist lest 23. nov. 2021).

være rundt 4-5 dager.<sup>174</sup> Centers for Disease Control and Prevention (CDC) i USA kom frem til at 97.5 prosent av alle personer smittet med SARS-CoV-2 vil utvikle symptomer innen 11 ½ dager. Samtidig er det variasjon i inkubasjonstid basert på aldersgrupper, demografi, mutasjon og lignende.<sup>175</sup> Å fastslå et konkret tidsrom kan dermed være vanskelig. Fordi lagringstiden av personopplysninger skal gjelde på tvers av en rekke ulike tilfeller, kan det være utfordrende å fastslå hva som er optimal lagringstid av personopplysninger.

Inkubasjonstid alene gir heller ikke hele svaret når det gjelder hvor lenge personopplysninger bør lagres. Formålet med smittesporingsapplikasjoner er å bryte smittetekjeder.<sup>176</sup> Da er det høyst relevant å vite når en person har potensiale for å videreføre smittsom sykdom. Studier viser at personer smittet med SARS-CoV-2 ofte er mest smittsomme fem dager før symptomer blir synlige og sjeldent mer enn ni dager etter sykdom – et spenn på 14 dager.<sup>177</sup>

I TAC sin personvernerklæring er det opplyst at opplysninger i forbindelse med kontaktsporing («proximity history data»), ikke lagres lengre enn to uker.<sup>178</sup> For tyske CWA er dette spesifikt satt til 14 dager.<sup>179</sup> Kontaktsporingsopplysninger samlet inn i Smittestopp 2 lagres også i 14 dager.<sup>180</sup> Til sammenligning ble personopplysninger i Smittestopp 1 lagret i hele 30 dager, men dette ble senere justert til 10 dager.<sup>181</sup> Med dette i mente, skal jeg nå vurdere om lagringstid kan være i strid med prinsippene om formålsbegrensning og dataminimering.

Behandlingsansvarlig må vurdere hva som er tilstrekkelig lagringstid for å oppfylle formålet om å bryte smittetekjeder. Innledningsvis i pandemien var en av de største utfordringene at en ikke hadde nok informasjon om viruset og sykdommen til å fastslå hva som var en nødvendig lagringstid. I sin vurdering av personvernkonsekvenser (DPIA) av 13. april 2020 la FHI til grunn at lagringstid ville bli nedjustert dersom det skulle bli unødvendig å lagre personopplysninger i 30 dager.<sup>182</sup> På det tidspunktet hadde Norge kun vært nedstengt i én måned, og situasjonen var veldig uoversiktlig.

---

<sup>174</sup> Guan m.fl., «Clinical Characteristics of Coronavirus Disease 2019 in China» *The New England Journal of Medicine*, 382 (2020) s. 1708-1720 på s. 1710. DOI: <https://www.nejm.org/doi/10.1056/NEJMoa2002032> (sist lest 23. nov. 2021).

<sup>175</sup> Cheng m.fl., «The incubation period of COVID-19: a global meta-analysis of 53 studies and a Chinese observation study of 11 545 patients» *Infections Diseases of Poverty*, 10 (2021) nr. 119 s. 9. DOI: <https://doi.org/10.1186/s40249-021-00901-9> (sist lest 23. nov. 2021).

<sup>176</sup> Se personvernerklæringene til Smittestopp 2, CWA og TAC.

<sup>177</sup> Cevik m.fl., «Virology, transmission, and pathogenesis of SARS-CoV-2» *The BMJ*, 371 (2020) s. 2-3. DOI: <https://doi.org/10.1136/bmj.m3862> (sist lest 23. nov. 2021).

<sup>178</sup> DGS (2021) under «retention period».

<sup>179</sup> RKI (2021) pkt. 5 b.

<sup>180</sup> FHI (2021) pkt. 4.1.

<sup>181</sup> Datatilsynets varsel om vedtak (2020) pkt. 7.1.

<sup>182</sup> FHI, «DPIA smittesporing», 13. april 2020, <https://www.fhi.no/contentassets/67d72db7c1ba4e2f9a70e9606b1c7ab0/dpia-smittestopp.pdf>, s. 8-9 (sist lest 23. nov. 2021).



Nå er situasjonen en annen, og vi vet langt mer om covid-19 og dens konsekvenser nå enn da. Det reflekteres også i antall dager kontaktsporingsopplysninger lagres – 14 dager. Om en på bakgrunn av eksisterende forskning legger til grunn at en person er smittebærende med SARS-CoV-2 i 14 dager, vil dette være i tråd med nødvendighetsvilkåret. Da vil opplysningene lagres i akkurat den tiden som er nødvendig for å oppnå formålet – verken mer eller mindre.

Her kan en også vurdere vilkåret om adekvans eller at innsamlingen er tilstrekkelig. På samme måte som at 14 dagers oppbevaring av kontaktsporingsopplysninger er nødvendig, må det også vurderes i motsatt retning. Dersom en hadde slettet innsamlede opplysninger etter for eksempel syv dager, kunne en risikert at personer som har vært i nærkontakt med en smittet person ikke blir varslet fordi opplysningene er blitt slettet. Det ville vært i strid med formålet om å bryte smittekjeder, fordi personopplysningene som ble lagret i syv dager kan ha vært utilstrekkelige for å oppfylle formålet.

Av lignende årsaker er varigheten også relevant i lys av formålsbegrensningsprinsippet. I alle tre applikasjonene blir innsamlede opplysninger slettet etter 14 dager. Formålet er å bryte smittekjeder og på den måten forhindre at ytterligere personer smittes. Som vist til overfor, antas det at en person smittet med SARS-CoV-2 er på sitt mest smittsomme i en tidsperiode på 14 dager. Hvis en beholder personopplysningene utover disse 14 dagene, vil de ikke være relevante for smittesporingen. Av den grunn kan de heller ikke oppbevares lengre uten å være i strid med formålet.

SARS-CoV-2 har mutert flere ganger, og det finnes nå mange ulike varianter.<sup>183</sup> Dersom viruset skulle mutere til en variant med betraktelig lengre smitteperiode, kan det være aktuelt å utvide varigheten på hvor lenge kontaktsporingsopplysningene lagres. Å utvide lagringstiden kan imidlertid by på utfordringer. Som jeg har vist til over er det ofte store variasjoner i hvor lang inkubasjonstiden er i hvert enkelt smittetilfelle. Dersom en ny, hypotetisk variant har et inkubasjonsintervall på 4 til 30 dager, må behandlingsansvarlig ta hensyn til dette. Å skulle endre lagringsvarigheten mens applikasjonen er i bruk kan være problematisk ikke bare fra et personvernperspektiv, men også rent teknisk. Løsningen blir da sannsynligvis, lik den som er i dag, å legge til grunn et lengre intervall for å fange opp de fleste typetilfellene.

## 9. Avsluttende ord

Smittesporingsapplikasjoner og hva slags konsekvenser de kan ha for personvernet har vært en viktig del av det offentlige ordskiftet under pandemien. Applikasjonene har i varierende grad bidratt til konvensjonell smittesporing, for å igjen kunne hindre økt spredning av SARS-CoV-2. Målet med denne oppgaven har vært å belyse om enkelte smittesporingsapplikasjoner

---

<sup>183</sup> WHO, «Tracking SARS-CoV-2 variants», 10. november 2021, <https://www.who.int/en/activities/tracking-SARS-CoV-2-variants/> (sist lest 23. nov. 2021).

kan være mer forenelige med prinsippene om dataminimering og formålsbegrensning jf. PVF artikkel 5 (1) (b) og (c) enn andre. For å lettere kunne synliggjøre dette har jeg benyttet et utvalg bestående av Smittestopp 2, CWA og TAC og komponentene i disse applikasjonene. Samlet sett er det ikke mulig å gi et entydig svar på hvorvidt smittesporingsapplikasjoner er forenelig med PVF. Fordi applikasjonene er ment som virkemiddel mot en viruspandemi som er i stadig endring, vanskeliggjøres spørsmålet ytterligere. Det er likevel mulig å komme med noen generelle betraktninger.

Hovedformålet med applikasjonene er å stanse spredning av smitte. Det gjøres ved at brukere kan bli varslet dersom de har vært nærkontakt med en smittet person. Ved å så teste seg kan brukeren senere varsle helsemyndighetene dersom vedkommende også viser seg å ha blitt smittet. Deretter isoleres de smittede, og det ønskede resultatet er at en da får begrenset smittetrykket i samfunnet.

Enkelte smittesporingsapplikasjoner har formål utover smittesporing, deriblant muligheten til å opplaste eget koronasertifikat. Smittestopp 1 har vist oss at det å ha flere formål kan være problematisk hvis disse ikke er tilstrekkelig adskilt. Brukere av CWA og TAC kan eksempelvis bruke applikasjonen til å kun oppbevare et koronasertifikat. Applikasjonenes grensesnitt gjør det mulig for brukeren å ha kontaktsporing avslått og likevel bruke den til sine øvrige formål. Fordi formålene er separert gjennom applikasjonens brukergrensesnitt, er det enklere for behandlingsansvarlig å fastsette applikasjonens innsamlingsformål og på den måten være mer i tråd med prinsippet om formålsbegrensning. Når formålene også er tydelig separert, er det enklere for både behandlingsansvarlig og kontrollorganer å vurdere hvorvidt applikasjonen er forenelig med dataminimeringsprinsippet.

Da Smittestopp 1 ble lansert i april 2020, var den blant få applikasjoner som benyttet seg av lokasjonsdata. Sett i lys av de formålene som ligger til grunn i Smittestopp 2, CWA og TAC, er det klart at bruk av lokasjonsdata ville vært uforenelig med både dataminimeringsprinsippet og formålsbegrensningsprinsippet.

Videre har deler av det offentlige ordskiftet angått hvorvidt innsamlede personopplysninger bør lagres lokalt eller sentralt. Forkjempere av sentraliserte løsninger peker på hensynet til effektivitet og at det veier tyngst i en forholdsmessighetsvurdering. Løsningen i den franske applikasjonen krever imidlertid at brukeren bekrefter at en er smittet, og nærkontakter får ingen varsel før bekreftelse er gjennomført. At brukere av TAC har denne muligheten, kan bidra til å styrke deres personvern. Samtidig kan det bidra til at den sentraliserte løsningen mister forspranget sitt når det gjelder effektivitet. Det kan bidra til at Smittestopp 2 og CWA er mer forenelige med dataminimeringsprinsippet enn sin franske motpart.

Hvor lenge personopplysningene lagres er også relevant i tråd med begge prinsippene. Alle tre applikasjonene lagrer kontaktsporingsopplysninger i 14 dager. Som jeg har vist, er dette

ment å være dekkende for brorparten av typetilfeller av SARS-CoV-2. Opplysningene lagres da lenge nok til å kunne spore smitten i nærmest alle tilfeller, men også i kort nok tid til at en ikke beholder opplysninger om personer som ikke lenger er smittebærende.

Da Datatilsynet skulle vurdere hvorvidt Smittestopp 1 var i tråd med personvernprinsippene, ba de også FHI om å dokumentere applikasjonens nytteverdi i lys av samfunnsforholdene. Av den grunn kan det argumenteres for at Smittestopp 2 hadde utspilt sitt formål da Norge ble gjenåpnet i slutten av september 2021. Applikasjonen fungerer likevel ikke i et vakuum, og en må stadig ta hensyn til den gjeldende smittesituasjonen. At smittetrykket i Norge var lavt på daværende tidspunkt, betyr ikke at det forblir slik. Å skulle be behandlingsansvarlig om å avvike applikasjonen fordi smitten går nedover kan være problematisk og ikke minst lite effektivt om man kort tid senere skulle oppleve en økning i smittetilfeller. Applikasjonene har tross alt aldri vært den eneste veien ut av pandemien, men kun et tilleggsverktøy.

# 10. Litteraturliste

## Trakter, direktiver og forordninger

TEUV	Traktaten om Den Europeiske Unions Virkeområde.
Direktiv 95/46/EF	Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger («personverndirektivet»).
Direktiv 2000/58/EF	Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon («Kommunikasjonsverndirektivet»).
Direktiv 2011/24/EU	Europaparlaments- og rådsdirektiv 2011/24/EU av 9. mars 2011 om pasientrettigheter i forbindelse med grensekryssende helsetjenester.
Forordning 2016/679	Europaparlaments- og rådsforordning (EU) av 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF («personvernforordningen»).

## Rettspraksis fra EU-domstolen

<i>Satakunnan Markkinapörssi</i> [GC] C-73/07	Dom av 16. desember 2008 [GC] <i>Satakunnan Markkinapörssi</i> , C-73/07, EU:C:2008:727.
<i>Karen Millen Fashions</i> [C5], C-345/13	Dom av 19. juni 2014 [C5], <i>Karen Millen Fashions</i> , C-345/13, EU:C:2014:2013.
<i>Tele2 Sverige AB og Watson</i> C-203/15 og C-698/15 [GC]	Forente saker av 21. desember 2016 [GC], <i>Tele2 Sverige AB og Watson</i> . C-203/15 og C-698/15, EU:C:2016:970.

## Retningslinjer og veiledere

WP29 (2013)	Article 29 Data Protection Working Party (WP29), «Opinion 03/2013 on purpose limitation», WP203, 2. april 2013.
WP29 (2014)	Article 29 Data Protection Working Party (WP29), «Opinion 05/2014 on Anonymisation Techniques», WP216, 10. april 2014.

EDPB (2018)	Det europeiske Personvernrådet (EDPB), «Endorsement of GDPR WP29 guidelines by the EDPB», 25. mai 2018.
EDPB (2020)	Det europeiske Personvernrådet (EDPB), «Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak», 21. april 2020.
WHO (2020)	World Health Organization (WHO), «Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing», 28. mai 2020.
COM(2020) 2523	Communication from the Commission, «Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124», 16. april 2020.
eHealth Network (2021)	eHealth Network, «Mobile applications to support contact tracing in the EU's fight against COVID-19 - Common EU Toolbox for Member States», 15. april 2021.

## Personvernerklæringer og FAQ

Simula (2020)	Simula (2020), «Digital smittesporing - spørsmål og svar», 9. april 2020, <a href="https://www.simula.no/news/digital-smittesporing-sporsmal-og-svar">https://www.simula.no/news/digital-smittesporing-sporsmal-og-svar</a> .
DGS (2021)	Direction générale de la Santé (DGS). «TousAntiCovid – Personal Data». <a href="https://bonjour.tousanticovid.gouv.fr/privacy-en.html">https://bonjour.tousanticovid.gouv.fr/privacy-en.html</a> [Ingen dato for sist endring].
FHI (2021)	Folkehelseinstituttet (FHI). «Personvernerklæring - Behandling av personopplysninger i Smittestopp». <a href="https://www.fhi.no/om/smittestopp/personvern/">https://www.fhi.no/om/smittestopp/personvern/</a> . Sist redigert 15. februar 2021.
RKI (2021)	Robert Koch Institute (RKI), «Privacy Notice», 8. september 2020, versjon 2.9, <a href="https://www.coronawarn.app/assets/documents/cwa-privacy-notice-2.9-en.pdf">https://www.coronawarn.app/assets/documents/cwa-privacy-notice-2.9-en.pdf</a> .

## Nasjonal praksis

Datatilsynets varsel (2020)	Datatilsynet, «Varsel om vedtak om midlertidig forbud mot å behandle personopplysninger - appen Smittestopp», 12. juni 2020. <a href="https://www.datatilsynet.no/contentassets/1c72ac62cac145efa242942ca34c2cd0/20-02058-9-varsel-om-vedtak-om-">https://www.datatilsynet.no/contentassets/1c72ac62cac145efa242942ca34c2cd0/20-02058-9-varsel-om-vedtak-om-</a>
-----------------------------	--

[midlertidig-forbud-mot-a-behandle-personopplysninger---smittestopp.pdf.](#)

Datatilsynets vedtak (2020)

Datatilsynet, «Vedtak om midlertidig forbud mot å behandle personopplysninger – appen Smittestopp», 6. juli 2020. <https://www.datatilsynet.no/contentassets/ae1905a8b88d4d869f1e059b60be35fd/Vedtak-om-midlertidig-forbud-mot-a-behandle-personopplysninger.pdf>.

## Fagbøker

de Terwangne (2020)

de Terwangne, «Article 5. Principles relating to processing of personal data» I *The EU General Data Protection Regulation (GDPR): A Commentary*, Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Laura Drechsler (red.), Oxford: Oxford University Press 2020, s. 309-320.

Frederiksen og Mathisen (2018)

Fredriksen, Halvard Haukeland og Gjermund Mathisen, *EØS-rett*, 3. utgave, Bergen: Fagbokforlaget, 2018.

Schartum (2020)

Schartum, Dag Wiese, *Personvernforordningen - en lærebok*, 1. utgave., Bergen: Fagbokforlaget, 2020.

## Vitenskapelige artikler

Cevik m.fl. (2020)

Cevik, Muge, Kuppalli, Krutka, Kindrachuck, Jason og Peiris, Malik. «Virology, transmission, and pathogenesis of SARS-CoV-2» *The BMJ*, 371 (2020). DOI: <https://doi.org/10.1136/bmj.m3862>.

Cheng m.fl. (2021)

Cheng Cheng, DongDong Zhang, Dejian Dang, Juan Geng, Peiyu Zhu, Mingzhu Yuan, Ruonan Liang, Haiyan Yang, Yuefei Jin, Jing Xie, Shuaiyin Chen og Guangcai Duan. «The incubation period of COVID-19: a global meta-analysis of 53 studies and a Chinese observation study of 11 545 patients» *Infections Diseases of Poverty*, 10 (2021) nr. 119. DOI: <https://doi.org/10.1186/s40249-021-00901-9>.

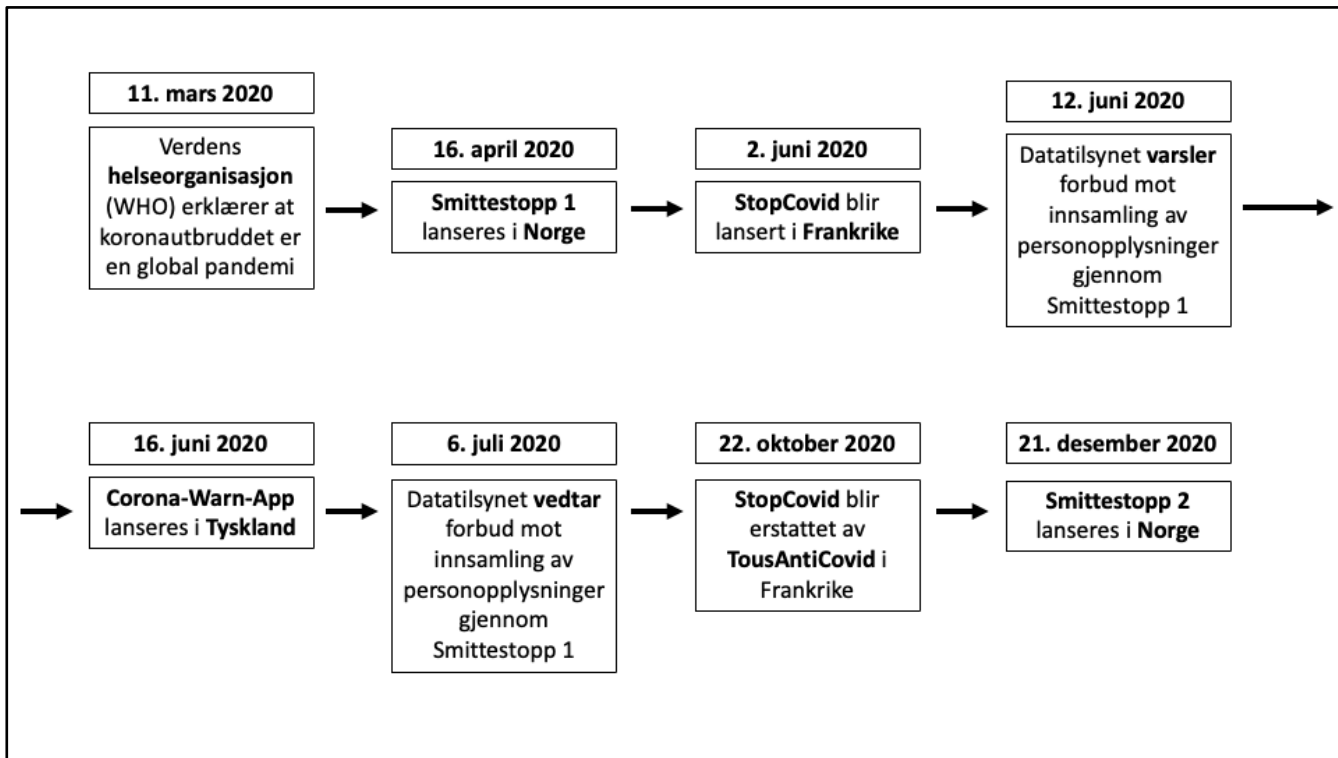
Guang m.fl. (2020)

W. Guan, Z. Ni, Yu Hu, W. Liang, C. Ou, J. He, L. Liu, H. Shan, C. Lei, D.S.C. Hui, B. Du, L. Li, G. Zeng, K.-Y. Yuen, R. Chen, C. Tang, T. Wang, P. Chen, J. Xiang, S. Li, Jin-lin Wang, Z. Liang, Y. Peng, L. Wei, Y. Liu, Ya-hua Hu, P. Peng, Jian-ming Wang, J. Liu, Z. Chen, G. Li, Z. Zheng, S. Qiu, J. Luo, C. Ye, S. Zhu, og N. Zhong, for the China Medical Treatment Expert Group for Covid-19. «Clinical Characteristics of Coronavirus Disease 2019 in China» *The New England Journal of Medicine*, 382 (2020) s. 1708-1720. DOI: <https://www.nejm.org/doi/10.1056/NEJMoa2002032>.

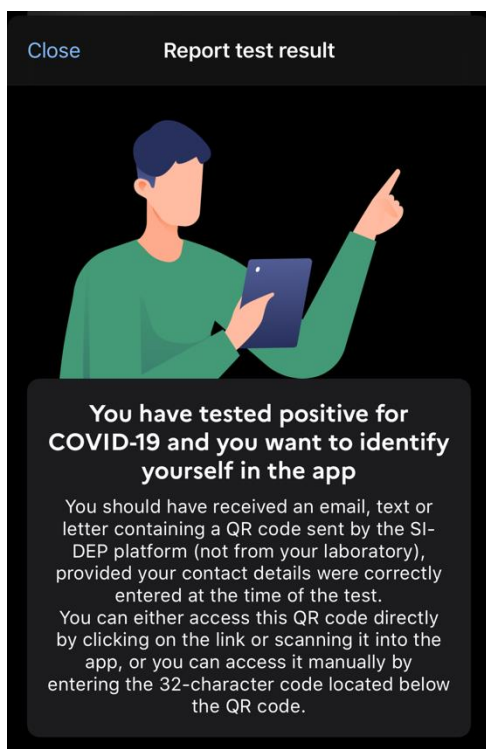
- Liu og Rocklöv (2021) Liu, Ying og Rocklöv, Joacim, «The reproductive number of the Delta variant of SARS-CoV-2 is far higher compared to the ancestral SARS-CoV-2 virus» *Journal of Travel Medicine*, 28 (2021), 7. DOI: <https://doi.org/10.1093/jtm/taab124>.
- Pyrgelis, Troncoso og de Cristofaro (2017) Pyrgelis, Apostolos, Troncoso, Carmela og De Cristofaro, Emiliano, *Knock Knock, Who's There? Membership Inference on Location Data*, innsendt i forbindelse med det 25. Network System Security symposium 21. august 2017. DOI: <https://arxiv.org/abs/1708.06145>.
- Rocher, Hendrickx og de Montjoye (2021) Rocher, Luc, Hendrickx, Julien M. og de Montjoye, Yves. A, «Estimating the success of re-identifications in incomplete datasets using generative models» *Nature Communications*, 10 (2019). DOI: <https://doi.org/10.1038/s41467-019-10933-3>.
- White og van Basshuysen (2021) White, Lucie og van Basshuysen, Phillipe, «Privacy versus Public Health? A Reassessment of Centralised and Decentralised Digital Contact Tracing» *Science and Engineering Ethics*, 27 (2021) s. 2. DOI: <https://doi.org/10.1007/s11948-021-00301-0>.
- Zhou m.fl. (2021) Zhou Zhili, Gaurav Akshat, Gupta BB, Hamdi Hedi, Nedjah Nadia. «A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic». *Neural computing & applications*, 1-14. (2021), DOI: <https://doi.org/10.1007/s00521-021-06389-6>.

# 11. Vedlegg - Figurer og bilder

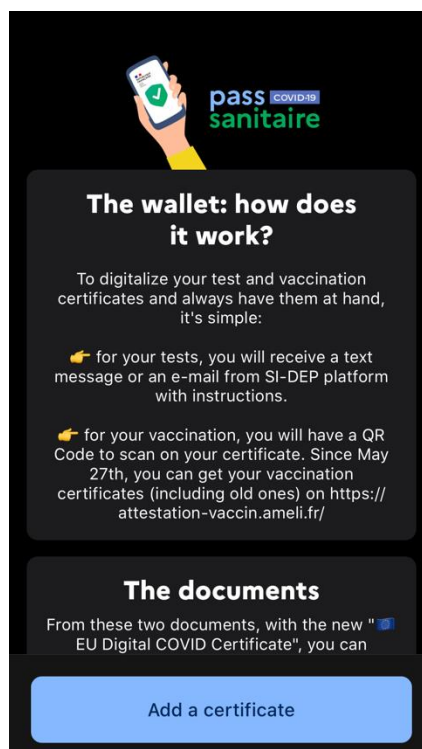
Figur 1 – Tidslinje for de ulike smittesporingsapplikasjonene



Bilde 1 - TAC «report test result» (Skjerm bilde fra TAC)

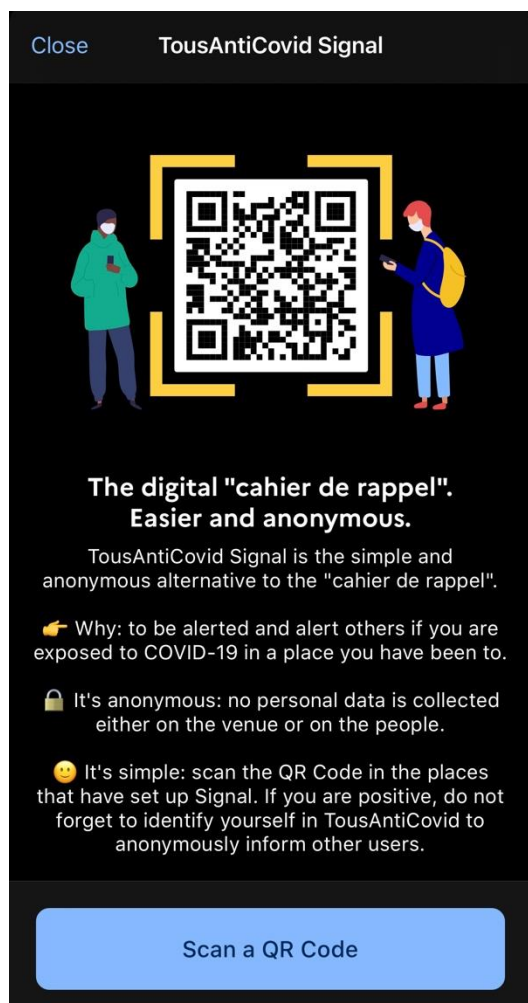


Bilde 2 - TAC «pass sanitaire» (Skjerm bilde fra TAC)

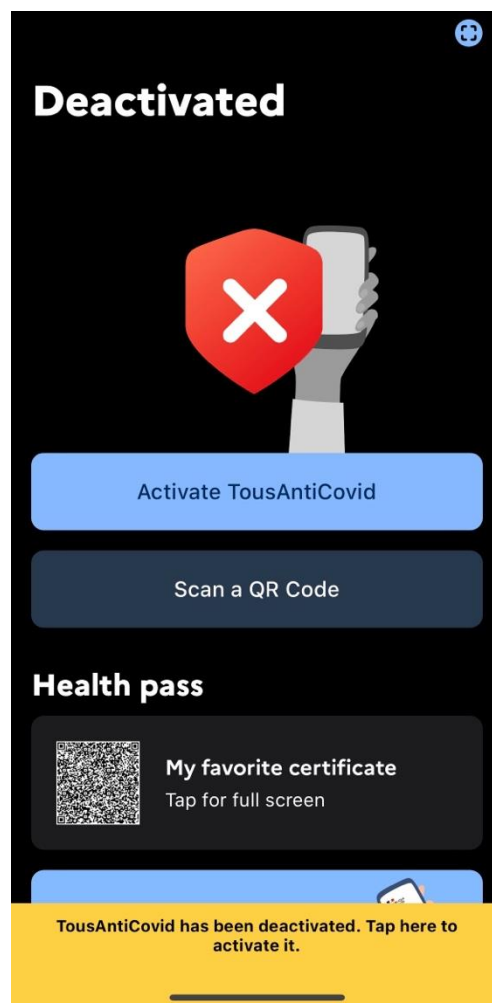




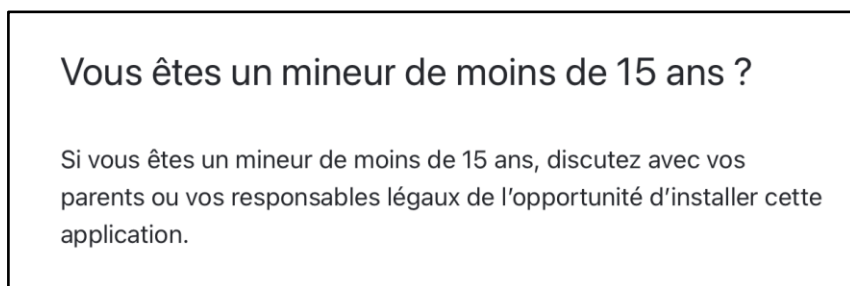
Bilde 3 - TAC «Signal»  
(Skjerm bilde fra TAC)



Bilde 4 - TAC kontaktsporing  
(Skjerm bilde fra TAC)



### Oversettelse 1



Skjermbildet er hentet fra <https://faq.tousanticovid.gouv.fr/kb/guide/fr/vous-etes-un-mineur-de-moins-de-15-ans-f6hXeZzPOg/Steps/129792>.

### «Er du under 15 år gammel?»

«Hvis du er under 15 år gammel, snakk med foreldrene dine eller andre foresatte om muligheten for å installere denne applikasjonen».

## Øversettelse 2

### ☐ Qu'en est-il de l'initiative lancée par Apple et Google ?

Concernant l'initiative lancée par Apple et Google, la France n'envisage pas d'y recourir. Leur solution ne correspond pas aux choix qui ont été faits en termes d'architecture (architecture dite décentralisée). Les solutions proposées par Apple et Google reposent sur la transmission dans tous les smartphones de pseudonymes pour les personnes diagnostiquées positives. Cela revient à dire qu'un diagnostic médical, même sous une forme encryptée, circule dans toutes les applications. Les risques de failles sont importants et des modèles d'attaques informatiques sont déjà disponibles sur le Web.

De plus, recourir à l'initiative d'Apple et Google poserait de graves questions de souveraineté. Le Gouvernement considère que la protection de la santé des Français est une mission qui relève exclusivement de l'État et non d'acteurs privés internationaux. La définition de l'algorithme de contact-tracing et la capacité de l'autorité de santé à disposer de toutes les données statistiques pour améliorer l'efficacité de son action, ne peuvent donc être laissées entre les mains d'une autre entité : c'est une question de souveraineté sanitaire et technologique.

Skjermbildet er hentet fra <https://web.archive.org/web/20201031233234/https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/TousAntiCovid>, under «Qu'en est-il de l'initiative lancée par Apple et Google?»

### «Hva med løsningen lansert av Google og Apple?»

«I tillegg vil det å ty til Apple og Google sin løsning reise alvorlige spørsmål om suverenitet. Regjeringen mener at beskyttelsen av helsen til franskmenn er et oppdrag som kun tilfaller staten og ikke internasjonale private aktører».