Datatilsynet

FOLKEHELSEINSTITUTTET
Postboks 222 Skøyen
0213 OSLO

Deres referanse	Vår referanse	Dato
	20/01170-5/SLI	08.05.2020

Varsel om vedtak om pålegg - appen Smittestopp

Datatilsynet viser til tidligere kontakt i forbindelse med appen Smittestopp.

Folkehelseinstituttet (FHI) ble i brev av 21.04.2020 informert om at vi har opprettet kontrollsak knyttet til Smittestopp.

I brevet ba vi også om å få oversendt protokollen for behandling av personopplysninger samt de endelige risiko- og sårbarhetsanalysene (ROS-analysene) som ligger til grunn for løsningen. FHI oversendte dokumentasjonen den 23.04.2020.

1. Varsel om vedtak om pålegg

Datatilsynet varsler med dette følgende pålegg, jf. personvernforordningen artikkel 58 nr. 2 bokstav d:

> *I medhold av personvernforordningen artikkel 58 nr. 2 bokstav d, pålegges Folkehelseinstituttet å utarbeide en behandlingsprotokoll som tilfredsstiller kravene i personvernforordningen artikkel 30.*
>
> *Folkehelseinstituttet pålegges også å utarbeide en risiko- og sårbarhetsanalyse som omfatter varslingsløsningen knyttet til appen Smittestopp og behandlingen av personopplysninger som vil skje i forbindelse med anonymisering og analyser.*
>
> *Dokumentasjonen skal sendes til Datatilsynet* ***innen 22.05.2020****.*

2. Nærmere om Datatilsynets saksbehandling

Løsningene som er valgt for appen Smittestopp reiser flere personvernmessige problemstillinger, blant annet spørsmål knyttet til formål, frivillighet, nytteverdi, innsamling og lagring av personopplysninger og sikkerhet i løsningen. Dette er forhold vi vil se på i vårt kontrollarbeid. På grunn av sakens omfang og kompleksitet, vil dette skje trinnvis.

I første omgang har vi sett mangler ved dokumentasjonen FHI har oversendt som vi finner det nødvendig å påpeke. Datatilsynet har forståelse for at dokumentasjonen er utarbeidet under

Postadresse: Postboks 458 Sentrum 0105 OSLO | Kontoradresse: Tollbugt 3 | Telefon: 22 39 69 00 | Telefaks: 22 42 23 50 | Org.nr: 974 761 467 | Hjemmeside: www.datatilsynet.no

tidspress. Vi mener likevel at enkelte mangler er så vidt grunnleggende at de må rettes umiddelbart.

Vi legger til grunn at dokumentasjonen som er oversendt er de siste versjonene og at denne dokumentasjonen lå til grunn for Smittestopp-appen da den ble lansert 16.04.2020. Dersom mer fullstendig dokumentasjon foreligger per i dag, ber vi om at den oversendes snarest.

2. Rettslig grunnlag
Datatilsynet fører kontroll med etterlevelsen av personopplysningsregelverket, jf. personvernforordningen artikkel 57.

2.1 Pålegg
Datatilsynets påleggsmyndighet i denne saken fremgår av personvernforordningen artikkel 58 nr. 2 bokstav d, som lyder:

> «2. Hver tilsynsmyndighet skal ha myndighet til å beslutte følgende korrigerende tiltak: (…)
> d) pålegge den behandlingsansvarlige eller databehandleren å sørge for at behandlingsaktivitetene skjer i samsvar med bestemmelsene i denne forordning og, dersom det er relevant, på en bestemt måte og innen en bestemt frist».

2.2 Behandlingsprotokoll
Enhver behandlingsansvarlig plikter å føre protokoll over behandlingsaktivitetene, det vil si de ulike behandlingene av personopplysninger, jf. personvernforordningen artikkel 30. Behandlingsprotokollen er ment å være et verktøy som kan gi de registrerte, tilsynsmyndigheten og andre informasjon om behandlingsaktivitetene på en enkel og oversiktlig måte. Protokollen er også et viktig verktøy og et naturlig utgangspunkt for de øvrige vurderingene som skal gjøres etter personvernregelverket.

De nærmere kravene til en behandlingsprotokoll fremgår av personvernforordningen artikkel 30 nr. 1. I bestemmelsen kreves det blant annet at formålene med behandlingen oppgis, jf. artikkel 30 nr. 1 bokstav b. Dette innebærer at det for hvert formål skal informeres om hvilke personopplysninger som behandles, hvem som har tilgang til disse osv.

Vi viser også til prinsippet om formålsbegrensning, som fremgår av personvernforordningen artikkel 5 nr. 1 bokstav b. I artikkel 5 nr. 2 fremgår det at den behandlingsansvarlige skal kunne påvise at personvernprinsippene som er nevnt i artikkel 5 nr. 1 overholdes. Protokollen kan fungere som dokumentasjon på at den behandlingsansvarlige etterlever prinsippet om formålsbegrensning.

I artikkel 30 nr. 4 fremgår det at behandlingsprotokollen skal kunne legges frem for tilsynsmyndigheten. På den måten kan protokollen være et utgangspunkt for tilsynsmyndighetens kontrollarbeid, jf. også fortalepunkt 82.

2.3 Risiko- og sårbarhetsvurderinger/ROS-analyser

Videre viser vi til personvernforordningen artikkel 24 og 32, hvor det stilles krav til personopplysningssikkerhet. I artikkel 32 nr. 1 om sikkerhet ved behandlingen fremgår det:

> «1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen (...)».

Risiko- og sårbarhetsvurderinger (ROS-analyser) er ikke nevnt eksplisitt, men at slike vurderinger er gjort, er en nødvendig forutsetning for å kunne vurdere hva som er egnet sikkerhetsnivå. Vi viser også til ansvarlighetsprinsippet som fremgår av personvernforordningen artikkel 5 nr. 2. Den behandlingsansvarlige skal kunne påvise at personvernprinsippene nevnt i artikkel 5 nr. 1 overholdes, herunder prinsippet om konfidensialitet og integritet (artikkel 5 nr. 1 bokstav f). Skriftlige risiko- og sårbarhetsvurderinger kan fungere som dokumentasjon på at personvernregelverket etterleves.

Formålet med risiko- og sårbarhetsvurderinger er å gi den behandlingsansvarlige oversikt over og informasjon om hvilke konsekvenser en aktuell behandling av personopplysninger kan få. Konsekvensene kan være mangeartede og kan for eksempel omfatte brudd på personopplysningsvernet, økonomisk tap, og omdømmetap. Den behandlingsansvarlige må kjenne til aktuelle risikoer og sårbarheter for å kunne beslutte om behandlingen og løsningen er gjennomførbar. Videre er kjennskap til risikoer og sårbarheter en forutsetning for å kunne iverksette risikoreduserende tiltak og vurdere om en eventuell restrisiko er akseptabel og dermed i tråd med forutsetningene i personvernregelverket.

Risiko- og sårbarhetsvurderinger er altså en viktig del av den behandlingsansvarliges beslutningsgrunnlag når nye løsninger skal innføres. Vurderingene som er gjort vil også være sentrale i tilsynsmyndighetens kontrollarbeid.

3. Datatilsynets vurderinger

3.1 Behandlingsprotokollen

I FHIs protokoll over behandlingsaktivitetene er formålet angitt slik: «Digitalt smittesporing knyttet til utbrudd av covid-19». Dette er en svært overordnet formulering som etter vår vurdering ikke tilfredsstiller kravene i personvernforordningen artikkel 30.

Det fremgår ikke i behandlingsprotokollen at appen Smittestopp har flere ulike formål: Rapportering og varsling om covid-19-smitte, overvåking av befolkningens bevegelsesmønster, analysearbeid og forskning. Disse formålene fremgår av ROS-analysen, personvernkonsekvensvurderingen, personvernerklæringen for Smittestopp og FHIs nettsider. Analyser og forskning skal ifølge FHI foregå på anonymiserte data. Anonymisering er i seg selv en behandling av personopplysninger.

Ulike personopplysninger vil samles inn og behandles for disse forskjellige formålene. Vi forutsetter at også forskjellige personer vil ha tilgang til ulike opplysninger avhengig av formålet. Dette må gjøres klart gjennom behandlingsprotokollen, noe vi ikke kan se er tilfelle i dag. Mangelfull formålsangivelse i protokollen gjør det også vanskelig å vurdere om prinsippet om formålsbegrensning overholdes.

3.2 ROS-analysen

Behandlingen av personopplysninger gjennom appen Smittestopp innebærer et svært stort inngrep i grunnleggende personvernrettigheter. Dette skjerper kravene til sikkerhet i løsningen og de underliggende risiko- og sårbarhetsvurderingene. Utstrakt behandling av sensitive personopplysninger er også ellers en del av FHIs kjernevirksomhet. Vi stiller derfor høye krav til FHI som profesjonell part og behandlingsansvarlig.

I den fremlagte ROS-analysen fremgår det i sammendraget (punkt 1) at analysen er modulær, det vil si at analysen vil bli bygget ut etter hvert som nye deler av løsningen skal fases inn. Videre fremgår det at følgende elementer ikke er del av den foreliggende ROS-analysen: Varslingsløsning, anonymisering og analyse.

Som nevnt over, er formålet med en ROS-analyse å avdekke risiko og sårbarheter før nye løsninger anskaffes og tas i bruk. De grunnleggende risikoene ved aktuelle løsninger må dermed være kjent før man velger løsning og inngå som et sentralt element i beslutningsgrunnlaget. Dersom analysene ikke er gjort i forkant, har man ikke mulighet til å ta ned risikoen som eventuelt er til stede og vurdere om en eventuell restrisiko er akseptabel. Ettersom FHI ikke har gjort en risiko- og sårbarhetsvurdering av varslings- og analyseløsningene, kan heller ikke risikoen (og eventuell restrisiko) ved appen Smittestopp ha vært kjent.

I en ROS-analyse kan det også være viktig å løfte frem at det er en risiko i seg selv at man ikke har all nødvendig informasjon tilgjengelig. Risikoen ved hvert enkeltelement i en teknisk løsning vil kunne være en annen enn risikoen som oppstår når de ulike komponentene skal interagere.

Selv om en ROS-analyse ofte vil måtte oppdateres etter hvert som man får mer informasjon, er det viktig å ha gjort vurderinger av den informasjonen man til enhver tid har. Vi mener at denne grunnleggende metodikken må følges også når man er under tidspress. Vi forutsetter at FHI har oversikt over hvilke grunnleggende tekniske komponenter som skal inngå i Smittestopp, herunder i løsningene for varsling og analyse.

Generelt er det mulig å gjøre en ROS-analyse kun av enkeltkomponenter eller deler av en større løsning. Man kan likevel ikke unnlate å gjøre risiko- og sårbarhetsvurderinger av grunnkomponentene.

Både i den fremlagte ROS-analysen, i vurderingen av personvernkonsekvenser (DPIA) og på FHIs nettsider er oppsporing av og varsling om covid-19-sykdom og -smitte angitt som hovedformålet med appen Smittestopp. Også analyse av befolkningens bevegelsesmønster og

virkningen av smitteverntiltak er angitt som formål. Risiko og sårbarheter ved varslings- og analyseløsningene, herunder løsningen for anonymisering, er imidlertid ikke vurdert.

Datatilsynet mener at grunnleggende risikoer og sårbarheter ved løsningene for varsling, analyse og anonymisering skulle vært vurdert før FHI besluttet å anskaffe løsningen, og senest før appen Smittestopp ble gjort tilgjengelig for bruk i befolkningen. Slik vi vurderer det, har ikke FHI overholdt forpliktelsene de er pålagt som behandlingsansvarlig etter personvernforordningen artikkel 32, jf. artikkel 24 og artikkel 5.

4. Videre saksgang

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

Dersom dere har kommentarer til dette varselet, ber vi om at de sendes oss så snart som mulig og senest **innen 14.05.2020**. Vi ber om at eventuell tilleggsdokumentasjon sendes oss så snart som mulig.

Vi gjentar også for ordens skyld at fristen for innsending av dokumentasjonen som nevnt i pålegget er **21.05.2020**.

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

Med vennlig hilsen

Bjørn Erik Thon
direktør

Susanne Lie
juridisk seniorrådgiver

Dette brevet er godkjent elektronisk i Datatilsynet og har derfor ingen signatur.