Veileder for bruk av sosiale medier i kommunen

Foto: Adobe Stok

KOMMUNESEKTORENS ORGANISASJON
The Norwegian Association of Local and Regional Authorities

Innhold

1. Innledning 4
1.1 Avgrensninger 5
1.2 Behov for vurderinger 5

2. Systematisk beskrivelse av behandlingen 8
2.1 Formål 8
2.2 Art, omfang og sammenheng 8

3. Informasjonssikkerhet 12

4. Ansvarsforhold 14
4.1 Felles ansvar 14
4.2 Ordning ved felles behandlingsansvar 15
4.3 Etiske vurderinger 15

5. Behandlingsgrunnlag 18
5.1 Berettiget interesse 18
5.2 Utøvelse av offentlig myndighet 19
5.3 Forholdet til annet relevant regelverk 20

6. Overføring til utlandet 22

7. Risiko for de registreres rettigheter og friheter 24

8. Prosess og forankring i ledelsen 26

Vedlegg 29

Om veilederen

Offentlige myndigheters tilstedeværelse i sosiale medier er blitt aktualisert og problematisert av både Datatilsynet, Teknologirådet og Personvernkommisjonen det siste året. KS har i den forbindelse fått mange henvendelser fra kommuner som ønsker bistand til å ta forsvarlige valg knyttet til om de kan bruke sosiale medier, og eventuelt hvordan sosiale medier kan brukes på en måte som innebærer minst mulig risiko.

KS Fagråd for personvern og informasjonssikkerhet har derfor laget en veileder for bruk av sosiale medier som er tilpasset kommuner. Når KS velger å gjøre dette, er premisset at KS mener det er et visst handlingsrom når det gjelder bruk av sosiale medier innenfor rammene av regelverket. Samtidig vil KS understreke at det legges til grunn at risikoen for de registrertes rettigheter og friheter er høy ved bruken av mange sosiale medier. Dette betyr at kommuner må være aktsomme dersom de velger å være til stede på denne typen plattformer og sette av nødvendige ressurser til å følge opp bruken.

For visse tjenesteområder i kommunen fraråder KS bruk av sosiale medier. Dette gjelder bruk av sosiale medier på tjenesteområder hvor kommunens tilstedeværelse vil medføre en høy risiko for at det vil kommuniseres svært personlig informasjon om innbyggere. Eksempler på slike tjenesteområder er rusomsorg, barnevern osv. Sosiale medier bør bare vurderes for ren informasjonsvirksomhet, og ikke som et verktøy som kan minne om eller assosieres som «saksbehandling» eller meningsutveksling.

I store plattformer som Facebook, Tik Tok, Twitter med mer vil det kunne være vanskelig for kommunen til å inngå gjensidige avtale, eller kunne kommunisere med leverandøren av sosiale media plattformen. Som en tommelfingerregel kan man si at kommunen bør være svært påpasselig med å ta i bruk sosiale media hvis informasjon som skal kommuniseres ikke kan vurderes under kategorien ren informasjonsvirksomhet.

I denne veilederen finner kommuner hjelp til å komme i gang med de vurderingene som må gjøres før sosiale medier tas i bruk og hva disse vurderingene består av. Veilederen angir flere relevante momenter som bør inngå i vurderingene, men den er ikke uttømmende. Hvert tilfelle må vurderes konkret, og kommunen må ta i betraktning alle forhold som er relevant og påvirker risikoen i det konkrete tilfellet. Veilederen kan brukes uavhengig av risikonivå.

KS Fagråd for informasjonssikkerhet og personvern

1. Innledning

Kommunens bruk av sosiale medier (SoMe) innebærer behandling av personopplysninger. Dette betyr at kommunen er ansvarlig for at det skjer i samsvar med personvernregelverket.

KS fagråd for informasjonssikkerhet og personvern har laget denne veiledningen for bruk av sosiale medier i kommuner. Veiledningen retter seg mot alle virksomheter i kommunene, og gir en innføring i både regelverket som gjelder og hvilke vurderinger den enkelte virksomhet må gjennomføre før sosiale medier tas i bruk. Hensikten er å gi en forenklet gjennomgang, og på en kortfattet måte, forklare hvilke vurderinger som må gjøres før sosiale medier kan tas i bruk. Veiledningen lister også opp en rekke momenter innenfor aktuelle områder, som kan være relevante når dere vurderer om sosiale medier skal tas i bruk.

Når dere har lest denne veilederen bør dere enkelt kunne:

- Lage en prosess for vurdering i egen virksomhet før sosiale medier tas i bruk.
- Ta stilling til personvernrisiko ved bruk av sosiale medier.
- Identifisere risikoreduserende tiltak knyttet til bruk av sosiale medier.
- Ta i bruk av sosiale medier på en forsvarlig måte.

En del av teksten i denne veiledningen hentes fra juridisk vurdering om personvern ved virksomhetens bruk av sosiale medier fra Oslo kommune (vedlegg 1) og et eksempel på personvernkonsekvensvurdering fra Asker kommune (vedlegg 2). Det presenteres også et eksempel på hvordan en kan foreta etiske vurderinger av ulike handlingsalternativer ved bruk av sosiale medier (vedlegg 3). Eksempelet er basert på Øyvind Kvalnes bok med tittelen «Digital Dilemmas» (2020).

For oversikt over vurderingsmomenter ved gjennomføring av personvernvurderinger, se vedlegg 4.

Risikoscenariene som presenteres i vedlegg 5, tar utgangspunkt i utviklingen av en risikobank i regi av Foreningen kommunal informasjonssikkerhet (KINS) og som vi har tilpasset til bruk i forbindelse med sosiale medier. For et eksempel på oversikt over

risikoscenarier for bruk av Facebook fra Gjøvik-regionen, se vedlegg 6.

Veilederen har vært distribuert til et begrenset antall kommuner som har fått mulighet til å komme med innspill. I tillegg har KS Advokatene og kommunikasjonsavdelingen i KS gitt innspill. Området er under utvikling og KS Fagråd for informasjonssikkerhet og personvern mottar gjerne innspill som kan gjøre veideleder enda bedre.

1.1 Avgrensninger

Veiledningen handler om bruk av sosiale medier generelt, og retter seg ikke mot spesifikke tjenester eller plattformer. Veiledningen gjelder i all hovedsak vurderinger knyttet til personvernregelverket, selv om noen andre regelverk omtales der disse er relevante.

Denne veiledningen omfatter sosiale medier som 1) brukes som en kommunikasjonskanal rettet mot innbyggerne, **2)** som brukes for å nå virksomhetens definerte formål, **3)** og som er eid og driftet av en tredjepart.

Eksempler vil være Facebook, Twitter, Snapchat, Instagram, YouTube, Vimeo, Workplace, LinkedIn osv.

Veiledningen tar utgangspunkt i at kommunen har behov for ulike kommunikasjonsplattformer for å nå ut til innbyggere og andre interessenter generelt, og tar ikke for seg spesifikke målgrupper. Det er viktig å påpeke at det kan gjelde strengere regler for kommunikasjon med målgrupper definert som «sårbare», som for eksempel barn, pasienter eller brukere av sosiale tjenester. Dette er risikofaktorer som virksomhetene må være oppmerksomme på, og må vurdere om de er aktuelle for dem.

1.2 Behov for vurderinger

Alle virksomheter i kommunen som tar i bruk SoMe som kommunikasjonskanal må forsikre seg om at personvernregelverket etterleves. Dette er en del av kommunes ansvar som behandlingsansvarlig for behandling av personopplysninger i SoMe. Nærmere om kommunens rolle som behandlingsansvarlig, se kapittel 4.

Målet med bruk av SoMe kan være å innfri kommunens lovfestede plikt til aktivt å informere innbyggere.

I de tilfellene hvor kommunen initierer en behandling av personopplysninger som innebærer en *behandlingene»*[1]*.* er kommunen forpliktet til å gjennomføre en vurdering av personvernkonsekvenser i tråd med krav i personvernforordningen art. 35. Personvernkonsekvensvurderingene som gjøres vil bidra til at virksomhetene kan dokumentere at de har etterlevd personvernregelverket. Ett vanlig karaktertrekk ved SoMe er at algoritmene i programvaren er utviklet nettopp for å forutsi brukerens personlige preferanser og interesser, samt å plassere brukere innenfor gitte kategorier basert på deres interaksjon på plattformen. Dette er karaktertrekk som kan innebære høy risiko.

Kommuner vil bruke SoMe på ulik måte og behandle ulike typer personopplysninger der, så risiko vil nødvendigvis også bli ulik. I tillegg har SoMe ulike innstillinger eller muligheter for tilpasninger. Dette har betydning for risiko. Hvor omfattende og på hvilket nivå risikoen kan være, vil også avhenge av den konkrete behandlingen og omfanget av behandlingen. Ulike SoMe vil også utvikles over tid. Vi har ikke kartlagt alle SoMe og kan derfor ikke utelukke at det kan være tilfeller der bruken ikke vil medføre høy risiko. Derfor anbefales det å gjennomføre en innledende vurdering for å kartlegge behandlingen og risikonivå. Vi vil understreke at selv om bruken ikke vil medføre høy risiko, skal personvernregelverket etterleves og alle de registrertes rettigheter og friheter skal uansett innfris.

I tråd med Datatilsynets anbefaling om å gjøre en vurdering av personvernkonsekvenser i de tilfellene der det er usikkert om det er nødvendig, så anbefaler KS at kommunene gjennomfører dette fordi det er et nyttig verktøy for å sikre at personvernforordningen blir fulgt. I denne veiledningen beskrives hva en slik vurdering består av, og der det passer tas det inn momenter i vurderingen som er spesielle, sett fra et kommuneperspektiv.

[1] Personvernforordningen art. 26.

Foto: Austin Distel

2. Systematisk beskrivelse av behandlingen

I en systematisk beskrivelse skal kommunen redegjøre for hvilke(t) SoMe det er aktuelt å ta i bruk, hvordan personopplysninger behandles i SoMe, hva de(t) skal brukes til, hvem som er målgruppen, osv. Kommune skal kunne dokumentere at de har oversikt over hvordan personopplysninger behandles som konsekvens av at kommunen tar i bruk SoMe, og sørge for at beskrivelsene som er gjort er komplette og tydelige.

2.1 Formål

Mange kommuner bruker SoMe som supplement til andre kommunikasjonskanaler. Målet med bruk av SoMe kan være å innfri kommunens lovfestede plikt til aktivt å informere innbyggere, og sørge for at informasjonen de trenger for å orientere seg om kommunens tjenester er så lett tilgjengelig som mulig.

2.2 Art, omfang og sammenheng

Art

Med behandlingens art mener vi en beskrivelse av hva som karakteriserer behandlingen. Her beskriver vi blant annet hvordan personopplysninger skal samles inn, lagres og brukes, hvem som får tilgang, hvem det behandles opplysninger om osv.

Her bør man være nokså spesifikk når det gjelder hvilken funksjonalitet man bruker i det enkelte SoMe. Et eksempel kan være beskrivelsen av funksjonaliteten «like» i Facebook, kommentarfelt og funksjonaliteten «Sideinnsikt», se personvern-konsekvensvurdering av Asker kommune s. 4-5.

Omfang

Med omfang mener vi antall registrerte, volum av opplysninger, lagringstid og geografisk omfang. Vi beskriver her blant annet antall personer som berøres, hvilken type opplysninger som behandles, samt mengden av slike opplysninger.

Antall registrerte som omfattes av behandlingen avhenger av hvor mange man antar vil besøke og eventuelt samhandle med kommunens side på SoMe. For å gjøre et slikt anslag kan erfaring fra andre kommuner eller statistikk fra Ipsos eller Norsk mediebarometer fra SSB være nyttig.

Personopplysningene som behandles som følge av at kommunen har en side på SoMe er av ulik

karakter. Den mest åpenbare behandlingen er at det er synlig hvem som er interessert i å følge kommunen, hva disse personene eventuelt har gitt uttrykk for at de liker av innlegg og eventuelle kommentarer de skriver selv.

Når kommunen bruker SoMe har den normalt ingen intensjon om å samle inn særlige kategorier av personopplysninger (for eksempel helseopplysninger), men samtidig kan ikke kommunen garantere at ikke følgerne selv publiserer informasjon om seg selv som direkte eller indirekte sier noe om helse, politisk oppfatning osv. Her bør man si noe om risikoen for at dette skal skje. Sannsynligheten for at det kan komme frem helseopplysninger avhenger også av hvilke tjenester i kommunen som bruker SoMe.

Kommunen bør synliggjøre de avveiningene som er gjort med hensyn til både de positive sidene ved SoMe (for eksempel nå mange raskt og skape engasjement) og de negative sidene (engasjement i negativ retning og uhensiktsmessig utlevering av personlige meninger).

Sammenheng

Med sammenhengen opplysningene behandles mener vi hva slags relasjon man har til personene det behandles opplysninger om og hva slags forventninger disse vil ha.

I en vurdering av personvernkonsekvenser er det viktig å tydeliggjøre i hvilken sammenheng behandlingen finner sted, fordi dette har stor betydning for i hvilken grad behandlingen er forutsigbar for den registrerte.

Når det gjelder behandling av personopplysninger som en konsekvens av bruk av SoMe er det viktige spørsmålet om det er ny teknologi eller innovativ

teknologi som aktualiseres. Det er kjent at de fleste tilbydere av SoMe bruker og utvikler algoritmer for å analysere informasjon om brukerne. Denne informasjonen gir ny innsikt om disse brukerne som kan være nyttig i et kommersielt perspektiv.

Her er det relevant å trekke frem følgende:
I hvilken grad man mener et SoMe og dets egenskaper er kjent for innbyggerne (for eksempel hvor lenge SoMe har vært i bruk og om teknologien har vært gjenstand for debatt).

I hvilken grad SoMe selv gjør tilgjengelig informasjon om sin behandling av personopplysninger, hvordan de innhenter samtykke, hvordan brukeren kan endre innstillinger osv.

Kildene til personopplysningene som blir behandlet som konsekvens av at kommunen er på SoMe (den registrerte selv, analyser foretatt av SoMe, tema kommunen tar opp osv.)

Kommunens relasjon til innbyggerne – den typiske SoMe-bruker og dennes antatte kompetanse til å innhente relevant informasjon for å ha kjennskap til hvordan SoMe behandler personopplysninger. Her vil det for eksempel være av betydning om målgruppen man forsøker å nå er å regne som en sårbar gruppe. Her mener vi for eksempel blant annet barn og unge, asylsøkere, pasienter og bruker av sosialtjenester.

Kommunen bør synliggjøre de avveiningene som er gjort med hensyn til både de positive sidene ved SoMe (for eksempel nå mange raskt og skape engasjement) og de negative sidene (engasjement i negativ retning og uhensiktsmessig utlevering avpersonlige meninger).

3. Informasjonssikkerhet

Den tekniske IKT-sikkerheten ved behandlingen ivaretas som hovedregel av leverandøren av SoMe. Kommunen har likevel et ansvar for å forsikre seg om at leverandøren har evne og vilje til å sørge for den informasjonssikkerheten som er påkrevd etter personvernregelverket.

Kommunen bør spørre etter referanser til leverandørens forpliktelser angående organisering, fysisk og miljømessig sikring, opplæring, screening og disiplinærtiltak overfor ansatte, testing, tilgangskontroll, kommunikasjonssikkerhet, sårbarhetshåndtering og håndtering av sikkerhetshendelser. Leverandører som ikke kan ivareta og dokumentere tilstrekkelig informasjonssikkerhet bør kommunen avstå fra å inngå avtale med.

Kommunen skal ivareta informasjonssikkerheten for sin egen behandling, særlig gjennom opplæring av ansatte, samt tilgangsstyring når det gjelder muligheten for å administrere sidene.

I store plattformer som Facebook, Tik Tok, Twitter med mer vil det kunne være vanskelig for kommunen til å inngå gjensidige avtale, eller kunne kommunisere med leverandøren sosiale media plattformen. Som tidligere nevnt, kan man som en tommelfingerregel si at kommunen bør være svært påpasselig med å ta i bruk sosiale media hvis informasjon som skal kommuniseres ikke kan vurderes under kategorien ren informasjonsvirksomhet.

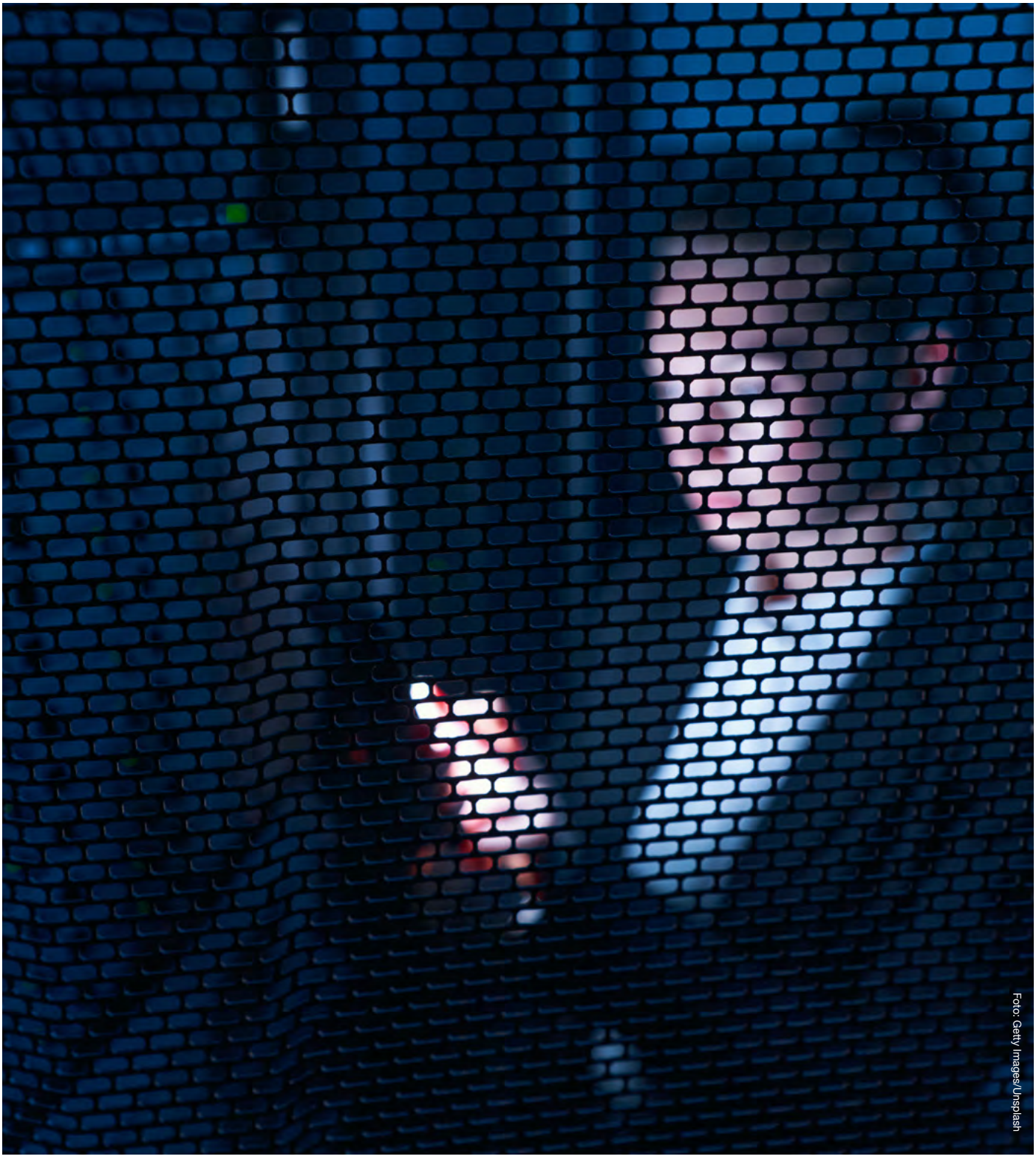

Foto: Getty Images/Unsplash

4. Ansvarsforhold

Med ansvarsforhold mener vi hvilke aktører som er involvert i behandlingen av personopplysninger og hvordan ansvarsforholdene er når det gjelder etterlevelse av personvernregelverket. Relevant informasjon her er hvilke kilder man har til informasjonen som behandles, hvem som er mottagere av informasjonen og hvem som er behandlingsansvarlig.

4.1 Felles ansvar

Vi legger til grunn i denne veiledningen at kommune og leverandøren av sosiale medier har felles behandlingsansvar. Dette er i tråd med praksis fra EU-domstolen.

Felles behandlingsansvar oppstår når to eller flere behandlingsansvarlige «i fellesskap fastsetter formålene med og midlene for behandlingene» . Personvernforordningen fastsetter videre at de felles behandlingsansvarlige skal fastsette sine respektive ansvar for å oppfylle forordningen i en «ordning» seg imellom. Det er ingen formkrav til ordningen, men det er vektlagt at det er rettighetene knyttet til informasjon og innsyn som skal ha primærfokus.

Personvernrådet (EDPB) har presisert at begge de behandlingsansvarlige har et overordnet ansvar for behandlingen i sin helhet, selv om de har fordelt ansvaret seg imellom i en ordning. EU-domstolen har uttalt at felles behandlingsansvar mellom to aktører ikke fører til at den ene aktøren også blir ansvarlig for forutgående eller etterfølgende behandling som den andre aktøren alene øver innflytelse på eller har ansvaret for.

På bakgrunn av det ovennevnte anbefaler vi at hver kommune gjør en konkret vurdering av ansvarsforholdene utfra en beskrivelse av behandlingsaktiviteten(e) som kommunen og SoMe får felles behandlingsansvar for.

Felles behandlingsansvar krever at den enkelte kommune må være aktiv og forsøke å finne ut av og kartlegge hvordan leverandørene skal bruke de innsamlede personopplysningene, selv om dette kan være svært utfordrende i praksis. Det er ofte snakk om store internasjonale aktører som står bak de ulike sosiale mediene, noe som gjør det vanskelig å oppnå kontakt og få den informasjonen man trenger. For å oppfylle kravene som stilles til kommunen som behandlingsansvarlig, bør kommunen kartlegge hvordan personopplysningene sikres, hva leverandøren gjør for å etterleve og ivareta personvernprinsippene, og hvordan den enkelte registrertes rettigheter og friheter ivaretas av leverandøren.

4.2 Ordning ved felles behandlingsansvar

Personvernforordningen art. 26 fastslår altså at det skal være på plass «en ordning» mellom partene ved felles behandlingsansvar. Spørsmålet er hva denne ordningen må bestå i.

For det første er det ingen formkrav til ordningen. Det er altså ikke et krav om at dette skal være en skriftlig, fremforhandlet ordning. Videre legges det spesielt vekt på pliktene som omhandler åpenhet – altså informasjon og innsyn.

Kommunen kan legge til grunn at det viktigste med ordningen som skal være på plass er at de registrerte får den informasjonen de trenger og i et format som er lett tilgjengelig og forståelig. Det viktigste er altså at de får informasjonen, ikke hvem de får den fra.

Når kommunen velger å ta i bruk SoMe som innebærer et felles ansvar, så anbefaler vi at kommunen tar et større ansvar enn dens andel i tjenesten skulle tilsi. Det kan for eksempel bety at kommunen tar et større ansvar for informasjonsplikten, og at man strekker seg langt for å opplyse innbyggere om de problematiske sidene ved SoMe sin forretningsmodell. Det kan også være aktuelt å gi tips til hvordan innbyggere kan tilpasse sin bruk for å redusere risikoen for å bli profilert på en uheldig måte.

4.3 Etiske vurderinger

Tilstedeværelse i sosiale medier kommer som regel med en viss kostnad og kostnaden betaler aktørene i form av brukerdata. De etiske spørsmålene knyttet til å være til stede i sosiale medier er i de senere årene løftet opp av flere forskere. Cambridge Analytica skandalen bidro til å få frem utfordringsbildet for folk flest. Cambridge Analytica kombinerte data mining og dataanalyse med strategisk kommunikasjon.[2] Brukerdataene selskapet samlet inn ble analysert og benyttet til å sende målrettede valgbudskap til ulike velgergrupper under Donald Trumps valgkampanje i 2016.

Når kommunen vurderer å bli en aktør i sosiale medier, må en være bevisst på utfordringene og foreta en etisk vurdering av de ulike dilemmaene som oppstår ved eventuell tilstedeværelse i sosiale medier og alternativt om man skal la være. Dersom kommunen beslutter at en ønsker å være til stede på sosiale media-plattformer, bør kommunen også gjøre en vurdering av hvilke aktiviteter en ønsker å fremme på plattformen/bruke plattformen til.

I veilederens vedlegg 3 gis det en innføring i et verktøy for etisk refleksjon som er utviklet av Einar Øverenget og Øyvind Kvalnes. Navigasjonshjulet (Kvalnes, 2020, s. 58) guider oss gjennom en etisk refleksjonsprosess innenfor seks ulike tema med tilhørende spørsmål. Står vi overfor et valg mellom mulige handlingsalternativer vil disse temaene og spørsmålene hjelpe oss til å foreta en beslutning basert på en saklig begrunnelse.

I boken «Digital Dilemmas Dilemmas – Exploring Social Media Ethics in Organizations» har Kvalnes (2020) identifisert fem typiske dilemmaer som oppstår ved tilstedeværelse i sosiale medier.[3] I vedlegget finnes også en tabell med en oversikt over de fem dilemmaene.

[2] Cambridge Analytica - Wikipedia

[3] Kvalnes, Ø. (2020). Digital Dilemmas, Exploring Social Media Ethics in Organizations. Palgrave MacMillan.

Foto: Dan Nelson

Tilstedeværelse i sosiale medier kommer som regel med en viss kostnad og kostnaden betaler aktørene i form av brukerdata.

5. Behandlingsgrunnlag

Personvernforordningen art. 6 nr. 1 fastslår at det kreves et behandlingsgrunnlag for at behandling av personopplysninger skal være lovlig. Riktig behandlingsgrunnlag må være på plass før behandlingen starter.

Når det gjelder kommunes bruk av SoMe, finnes det flere aktuelle behandlingsgrunnlag for bruk av SoMe. Bruken av disse behandlingsgrunnlagene vil være avhengig av hvilken rolle kommune har i kommunikasjon gjennom SoMe. Hvis kommunen bruker SoMe i utøvelse av offentlig myndighet kan personvernforordningen art. 6 nr. 1 bokstav e være aktuelle å bruke. Denne bestemmelsen slår fast at behandlingen av personopplysninger er lovlig dersom *behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt.* Dersom kommunen planlegger å bruke SoMe i en annen rolle enn som myndighetsorgan, kan personvernforordningen art. 6 nr. 1 bokstav f brukes som behandlingsgrunnlag. Et viktig poeng er at dette behandlingsgrunnlaget ikke kan benyttes på behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver.[4] Forskjellen mellom disse behandlingsgrunnlagene forklares i punktet under.

5.1 Berettiget interesse

Et av behandlingsgrunnlagene kommunen kan bruke for behandling av personopplysninger i SoMe er personvernforordningen art. 6 nummer. 1 bokstav f – nødvendig for å ivareta legitime interesser. For å kunne legge dette behandlingsgrunnlaget til grunn må tre vilkår være oppfylt. Kommunen må ha en saklig berettiget interesse, behandlingen må være nødvendig for å oppnå formålet knyttet til den berettigede interessen, og den berettigede interessen må veie tyngre enn de registrertes rett til personvern.

Når det gjelder hvilke momenter som kan legges til grunn i en vurdering av om de nevnte vilkårene er oppfylt, se veiledning fra Datatilsynet.

Å balansere interessen kommunen har i å behandle personopplysningene mot de registrertes personopplysningsvern er en konkret avveiing som hver kommune må gjøre. Noen fellestrekk kan likevel nevnes:

- Kommunens berettigede interesse består i å nå ut med relevant informasjon til innbyggerne, samt å skape engasjement i lokalmiljøene knyttet til leveranse av tjenester og demokratiske prosesser.

- Det unike med SoMe er evnen til å skape engasjement og sørge for stor rekkevidde.

- Kommunen har en informasjonsplikt som går utover det å passivt tilgjengeliggjøre informasjon.

- Kommunen skal legge til rette for lokaldemokrati og skape samfunnsengasjement med aktiv innbyggerdeltagelse.

- SoMe skal ikke være en eksklusiv kanal, men del av kommunenes helhetlige kommunikasjonsstrategi

- Personopplysningene behandles ikke for kommersielle hensyn

Det kan problematiseres hvorvidt kommunen kan anvende «berettiget interesse» som rettslig grunnlaget da det følger av forordningen at dette grunnlaget ikke får anvendelse på en behandling *som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver*.

Når kommunen velger kommunikasjonsplattformer for å nå innbyggere med informasjon, er dette på basis av kommunikasjonsstrategien sin, og ikke som ledd i utøvelse av myndighet. På denne bakgrunn mener KS at nevnte unntak ikke gjelder, og at kommunen følgelig kan basere seg på en interesseavveiing.

5.2 Utøvelse av offentlig myndighet

Et annet aktuelt behandlingsgrunnlag for virksomheter som vil ta i bruk SoMe kan være personvernforordningen art. 6 nr. 1 bokstav e. Denne bestemmelsen slår fast at behandlingen av personopplysninger er lovlig dersom *behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt*. Det må med andre ord først gjøres en vurdering av om behandlingen av personopplysninger i sosiale medier er nødvendig for å utføre en oppgave i allmenhetens interesse, eller om behandlingen kan anses som utøvelse av offentlig myndighet.

Hoveddelen av kommunes aktiviteter må kunne anses som offentlig myndighetsutøvelse, men det er likevel ikke slik at alle kommunale aktiviteter er

[4] GDPR art. 6 nr. 1 andre ledd fastslår at GDPR art. 6 nr. 1 bokstav f *ikke* kan benyttes av virksomhetene dersom behandlingen er å anse som offentlig myndighetsutøvelse.

Det kan tenkes at det å kommunisere med innbyggere gjennom sosiale medier er i allmenhetens interesse.

å anses som offentlig myndighet. Et eksempel på dette er rollen som arbeidsgiver. I arbeidsgiverrollen utøver ikke kommunen offentlig myndighet, og denne bestemmelsen kan følgelig ikke benyttes som behandlingsgrunnlag.

Hva som er i allmenhetens interesse, er ikke nødvendigvis det samme som det den offentlige virksomheten er pålagt å gjøre. Det kan tenkes at det å kommunisere med innbyggere gjennom sosiale medier vil kunne være i allmenhetens interesse.

Det er viktig å være oppmerksom på at å vise til personvernforordningen art. 6 nr. 1 bokstav e som behandlingsgrunnlag ikke er tilstrekkelig. Det følger av personvernforordningen art. 6 nr. 3 at det kreves et supplerende rettsgrunnlag for å kunne bruke art. 6 nr. 1 bokstav e. Det innebærer at dersom virksomhetene mener at behandlingen er i allmennhetens interesse eller innebærer utøvelse av offentlig myndighet, så må virksomheten ha hjemmel i en annen lovbestemmelse for å kunne bruke dette behandlingsgrunnlaget.

Kommunen må selv finne frem til et supplerende rettsgrunnlag dersom de mener at personvernforordningen art. 6 nr.1 bokstav e er passende, men den juridiske vurderingen fra Oslo kommune gir noen pekepinner. Det er likevel viktig å understreke at kommunene bør være varsomme med å legge til grunn utøvelse av offentlig myndighet som behandlingsgrunnlag ved bruk av sosiale medier. Og dersom dette alternativet legges til grunn er det viktig at det supplerende rettsgrunnlaget er tydelig nok til å begrunne behandlingen.

5.3 Forholdet til annet relevant regelverk

I tillegg til personvernregelverket er det også andre regelverk som er relevante for virksomhetene ved bruk av sosiale medier som kommunikasjonskanal.

Alle kommunale virksomheter er underlagt en arkivplikt etter arkivlova. Dette innebærer i praksis at dokumenter som er arkivverdige skal journalføres i henhold til virksomhetens rutiner. Den enkelte virksomhet må vurdere om og hvordan kommunikasjonen i sosiale medier skal arkiveres.

Dersom noe av innholdet som skapes i sosiale medier er arkivverdig og skal journalføres, er dette innholdet også som utgangspunkt å anse som et offentlig saksdokument som det kan gis innsyn i etter bestemmelsene i offentleglova.

Dersom kommunikasjonen som skjer i sosiale medier er å anse som saksbehandling, vil også forvaltningslovens regler gjelde for denne kommunikasjonen.

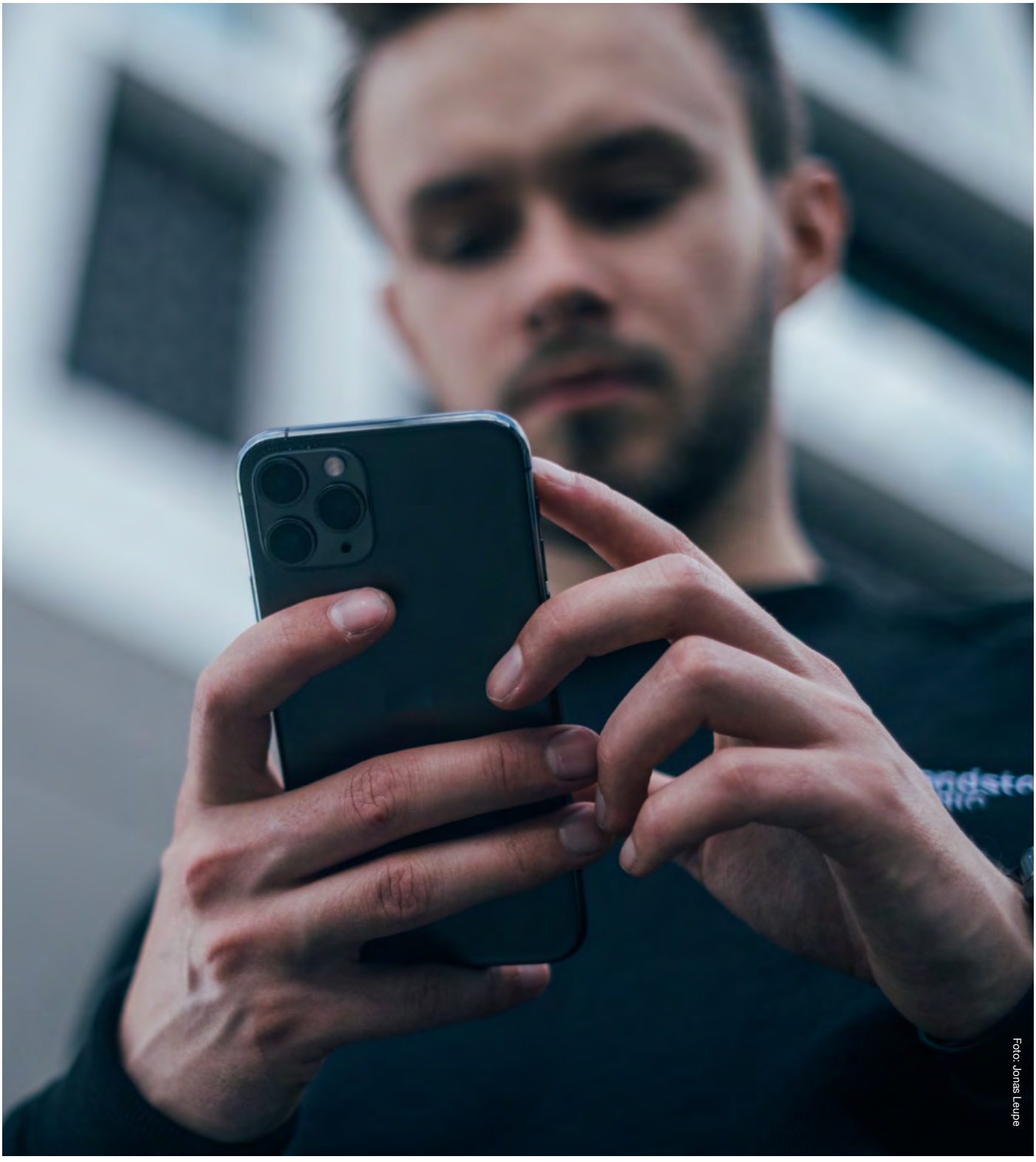

Foto: Jonas Leupe

6. Overføring til utlandet

De fleste aktørene som står bak ulike sosiale medier er utenlandske, og ofte amerikanske eller kinesiske. Dette utløser flere personvernrettslige problemstillinger.

Dersom aktøren bak det aktuelle sosiale mediet virksomheten vurderer å ta i bruk, tilhører et land utenfor EU/EØS som ikke er på EUs liste over godkjente land, må kommunen ha et gyldig overføringsgrunnlag. Kravet om gyldig overføringsgrunnlag kommer i tillegg til kravet om at kommunen må ha et behandlingsgrunnlag som nevnt under kap. 4. Kommunen bør også forsikre seg om at det ikke finnes lover og praksis i tredjelandet som til tross for et gyldig overføringsgrunnlag vil føre til et lavere beskyttelsesnivå i praksis. Det er også et krav om at det iverksettes ytterligere tiltak og at det gis nødvendige garantier for å sikre samme beskyttelsesnivået for personopplysningene som i EU/EØS.

Det kreves en ekstra vurdering av om overføringen er forholdsmessig dersom landet opplysningene blir overført til i tillegg har regelverk som muliggjør behandling av personopplysninger til formål som er vanskelig for den registrerte å forutsi.

Enkelte forhold knyttet til overføring til tredjeland avventer ytterligere avklaring både nasjonalt og i EU/EØS sammenheng. Datatilsynet har delt sine vurderinger knyttet til overføring av personopplysninger til tredjeland utenfor EU/EØS området. KS anbefaler at kommunal sektor følger med på utviklingen innenfor dette området.

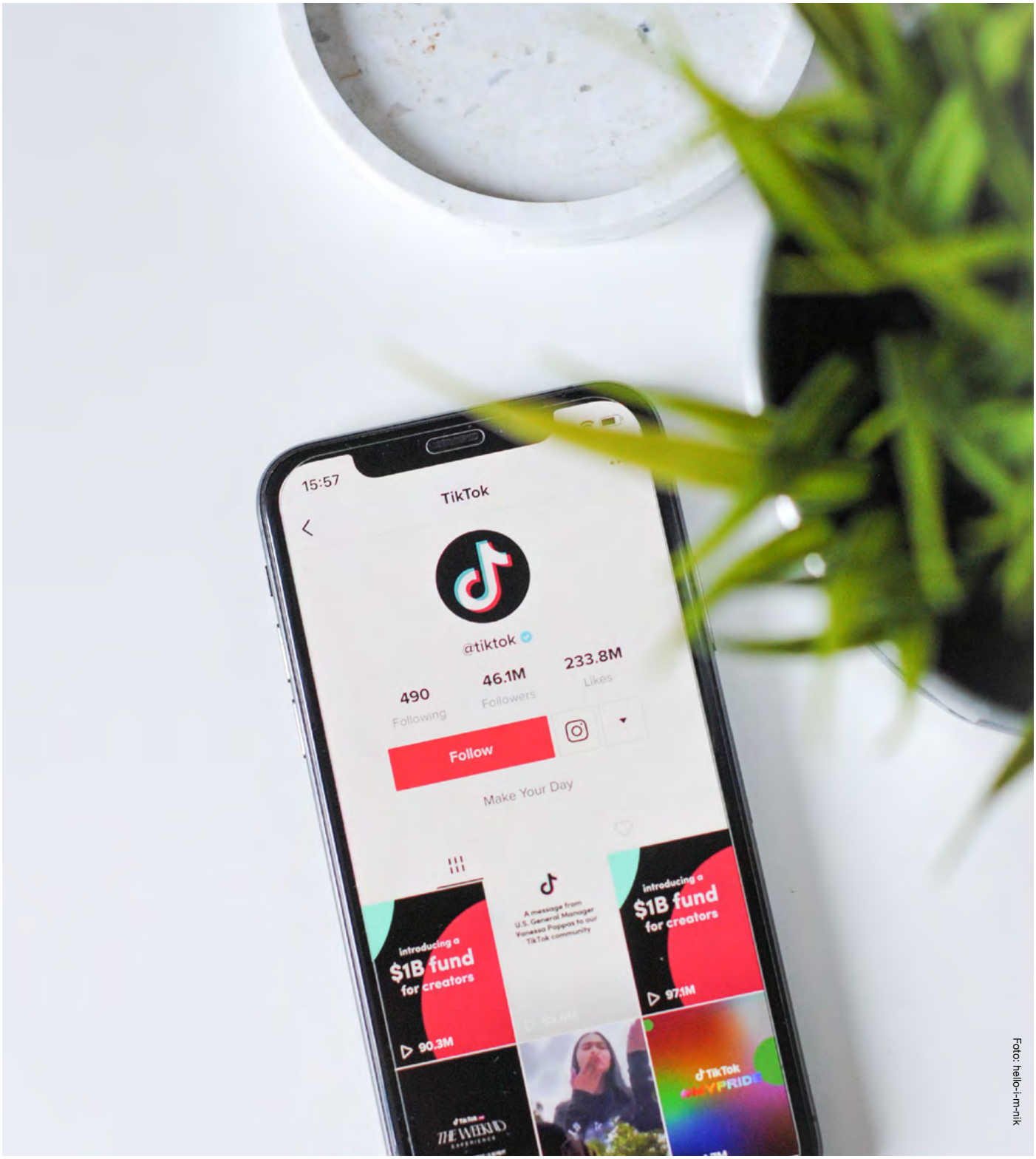

Foto: hello-i-m-nik


Foto: Tianyi Ma

7. Risiko for de registreres rettigheter og friheter

I en vurdering av personvernkonsekvenser er målet å redusere risikoen for at de registrerte ikke skal få ivaretatt sine rettigheter og friheter etter personvernregelverket.

Vi bør ha som mål at de som velger å interagere med kommunen på SoMe i så stor grad som mulig skal ha innflytelse på hvordan egne personopplysninger behandles (medbestemmelse), og at de får tilgang til nok informasjon om behandlingen til å kunne innrette seg slik de ønsker (åpenhet). Slik bør den måten kommunen tar i bruk et SoMe være forutsigbar og underbygge tillit.

I tabellen under finner dere noen iboende risikoer ved bruk av SoMe og forslag til tiltak for å redusere risiko. Tabellen nedenfor er ikke en uttømmende oversikt over risiko knyttet til bruk av sosiale medier, men er ment kun som eksempler.

Personvern mål	Risiko	Momenter	Tiltak
Med-bestemmelse	Utfordrende å få tilgang til informasjonen om hvordan SoMes algoritmer fungerer. Utfordrende å kommunisere tydelig og forståelig om hvordan algoritmene fungerer.	Utfordrende å kommunisere tydelig og forståelig om hvordan algoritmene fungerer.	
Åpenhet	Lite kjennskap til SoMe og forretningsmodellene deres. Enkelte typer tema som omtales kan føre til at enkeltpersoner utleverer sensitive personopplysninger i kommentarfelt.	Noen SoMe er mer innrettet mot målrettet annonsering enn andre. Rett beredskap for ulike type innhold.	Kommunen kan ta mer av ansvaret for å informere innbyggere sine om de underliggende risikoene ved å bruke SoMe. Bevissthet omkring hvilke tema det publiseres informasjon om. Ressurser for å moderere kommentarfelt eller slå av kommentar-funksjonalitet. Kategorisere innhold etter A, B, C poster, hvor kategori A krever full beredskap og rask respons. Kategori B er normal tematikk og har normal beredskap/oppfølging. Kategori C krever ingen oppfølging.
Ansvarlighet /Tillit	Liten kontroll med innholdet på kommunens sider. Liten kontroll med omfanget av personopplysninger som blir utlevert til leverandør av SoMe.	Muligheter for å minimere innsamlingen av personopplysninger. Særlig funksjonalitet utviklet for å identifisere kommunikasjonsløp og lage målrettet annonsering	Sentral redaksjon som kan jobbe med alt fra strategi, konseptplaner, rutiner og kursing. Følge opp og få et samarbeid med alle redaktører for SoMe i regi av kommunen. Kommunen må gjøre en konkret vurdering av hvilken funksjonalitet i SoMe som tas i bruk. Aktivt redusere innsamling av informasjon om enkeltpersoners bruk og interagering med SoMe.

8. Prosess og forankring i ledelsen

Utarbeidelsen av en vurdering av personvernkonsekvenser bør gjøres av en gruppe som er satt sammen av personer med ulik fagbakgrunn. Når det gjelder SoMe vil en sentral fagbakgrunn være den/de som kan kommunikasjonsfaget. Gode støttespillere er personer med kunnskap om informasjonssikkerhet og personvern.

En vurdering av personvernkonsekvenser og konklusjonen skal forankres i ledelsen. Ledelsen skal avgjøre hvorvidt de valgte tiltakene, restrisikoen og eventuell handlingsplan er akseptabel. Det er en del av ansvarlighetsprinsippet og dokumentasjonsplikten at vurderingene som er gjort og ledelsens gjennomgang blir dokumentert.

Ledelsen beslutter og begrunner et av de følgende alternativene:

1. Godkjenning
Vurdering av personvernkonsekvenser og dens avveiinger er godkjent.
Kommunen kan ta i bruk SoMe.

2. Betinget godkjenning
Vurdering av personvernkonsekvenser og dens avveiinger godkjennes under forutsetning av følgende forbedringer ... (beskriv forutsetningene).
Revidert vurdering av personvernkonsekvenser skal legges frem for ledelsen på nytt.

3. Ikke godkjent
Vurdering av personvernkonsekvenser og dens avveiinger godkjennes ikke.
Kommunen kan ikke ta i bruk SoMe.

Dersom en vurdering av personvernkonsekvenser behandles i ledergruppen mer enn én gang, risikoen fremdeles er høy og viljen til å ta i bruk SoMe fremdeles er stor, må kommunen anmode Datatilsynet om forhåndsdrøftelse. Kommunen må i så fall dokumentere at den ikke greier å gjøre risikoen lavere. Det er ledelsen som tar beslutningen om å anmode Datatilsynet om forhåndsdrøftelse.

Vi legger til grunn at forankring av vurderingen av personvernkonsekvenser i ledelsen er en forutsetning for at bruken av SoMe kan skje lovlig.

En vurdering av personvernkonsekvenser og konklusjonen skal forankres i ledelsen. Ledelsen skal avgjøre hvorvidt de valgte tiltakene, restrisikoen og eventuell handlingsplan er akseptabel.

Vedlegg

Design: Bly.as

KS
Postadresse: Postboks 1378 Vika, 0114 Oslo
Besøksadresse: Haakon VIIs gt. 9, 0161 Oslo

Telefon: 24 13 26 00

ks@ks.no
www.ks.no

ISBN 978-82-93866-30-5

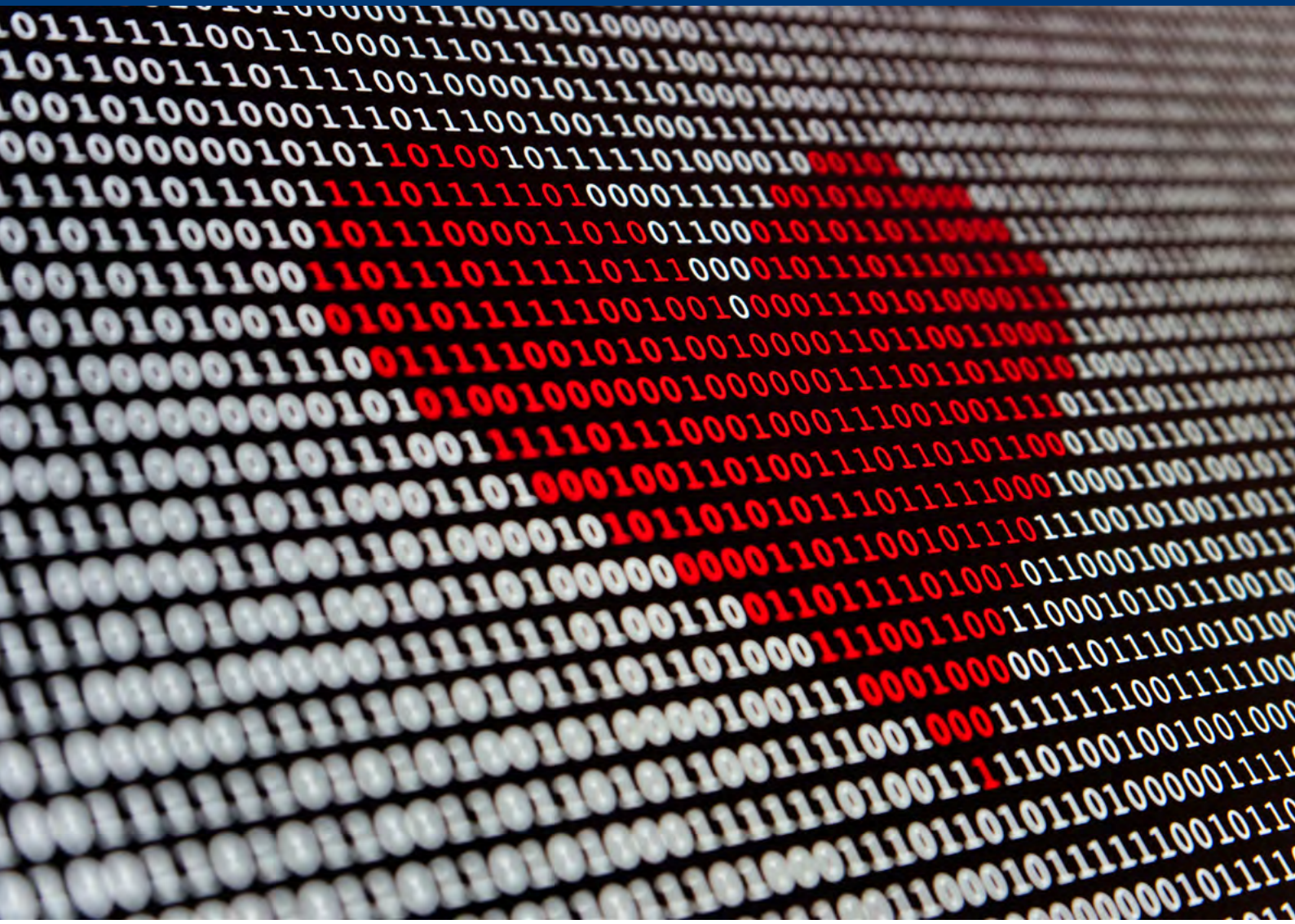

Foto: Xxxxxxxxxxxxx