Veileder for bruk av sosiale medier i kommunen

Foto: Adobe Stok

KOMMUNESEKTORENS ORGANISASJON
The Norwegian Association of Local and Regional Authorities

Innhold

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.

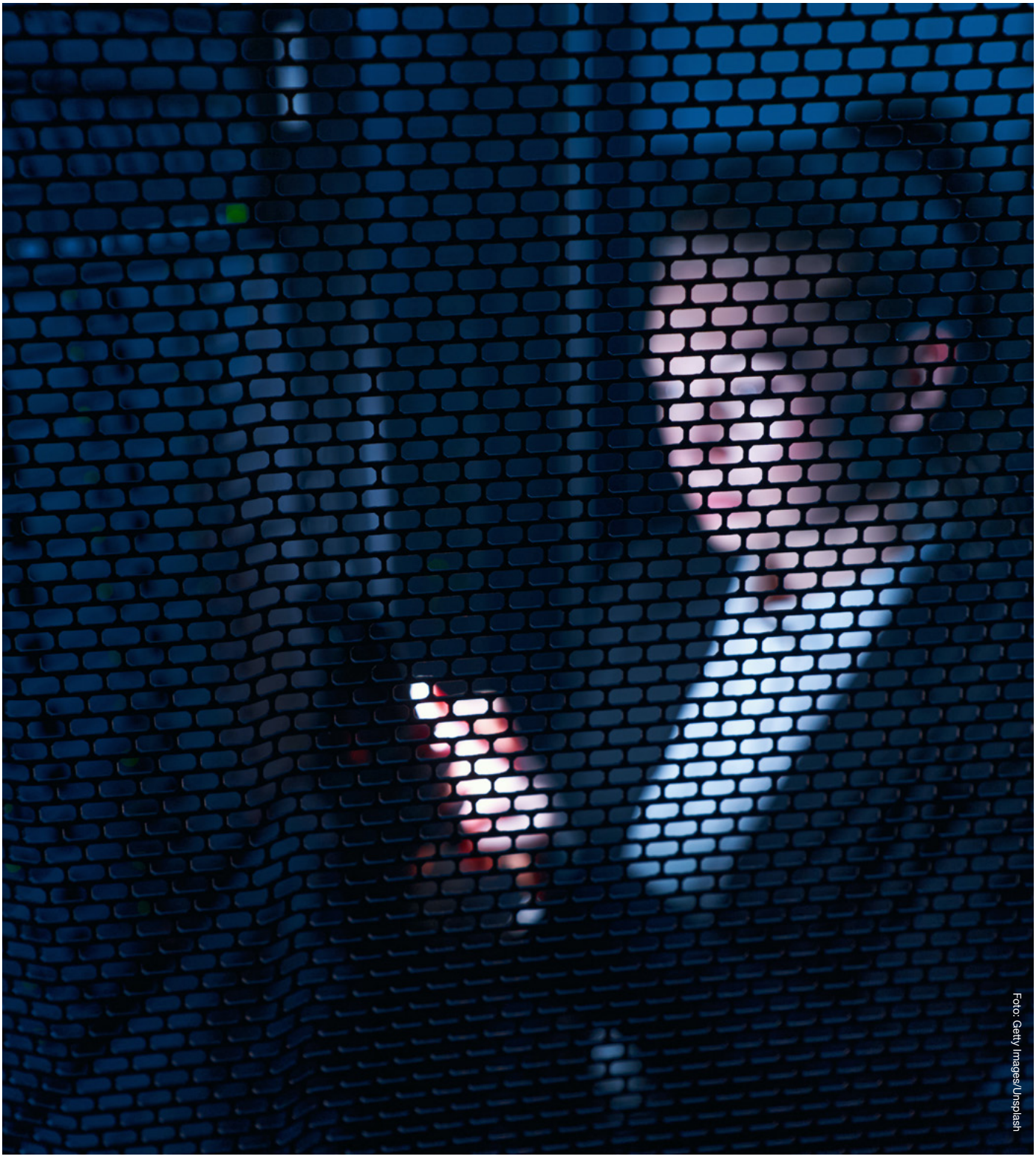

Foto: Getty Images/Unsplash

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.

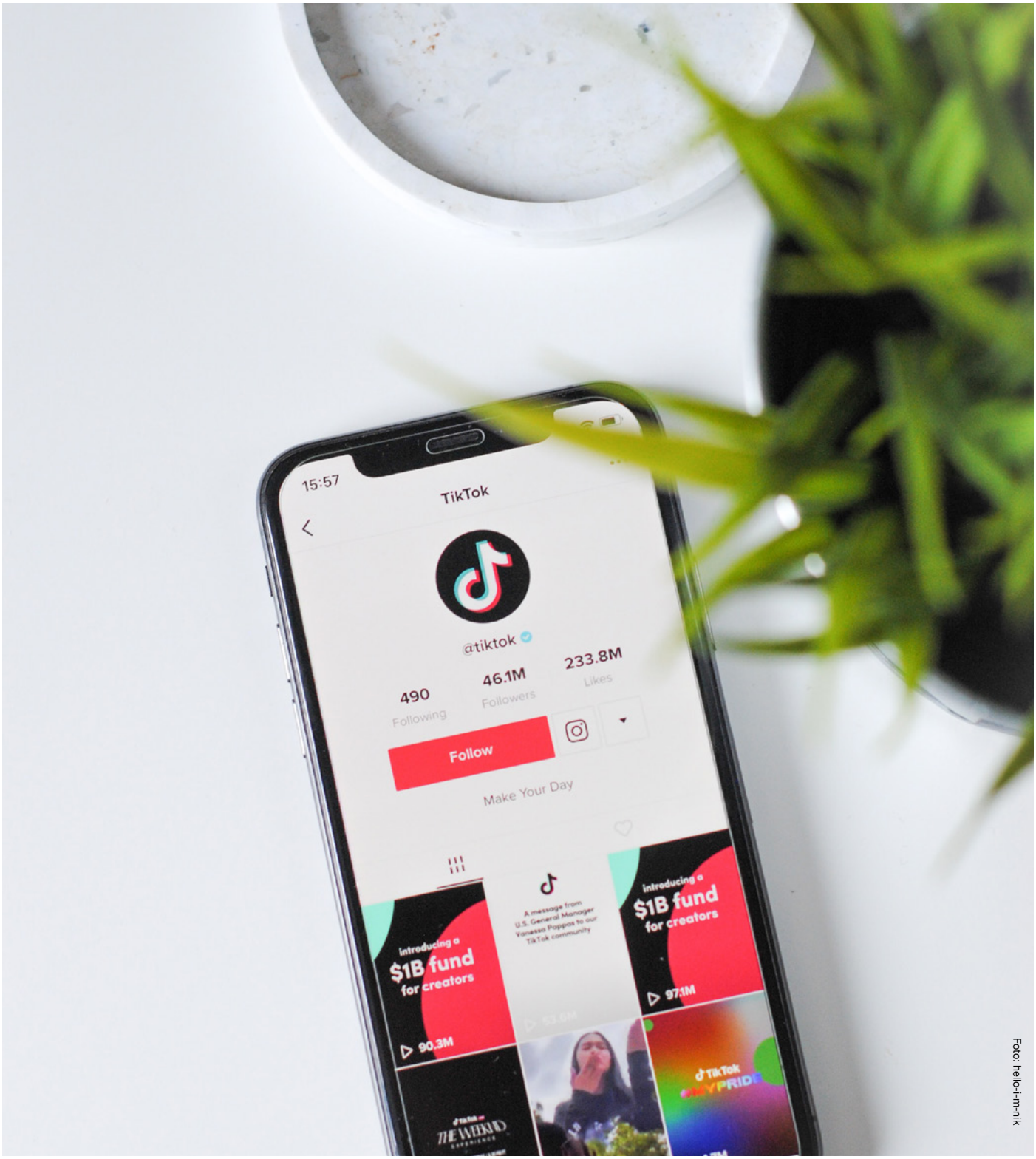

Foto: hello-i-m-nik


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

Oslo

Byrådsavdeling for finans

Personvern ved bruk av sosiale medier

En juridisk vurdering med veiledning om virksomheters bruk av sosiale medier i Oslo kommune.

Foto: Will Francis on Unsplash

Personvern ved virksomheters bruk av sosiale medier i Oslo kommune - En juridisk vurdering med veiledning

Innhold

Vedlegg: Vurderingsmomenter ved bruk av sosiale medier (ikke en del av dette dokumentet)

1 Innledning

Oslo kommune bruker flere sosiale medier rettet mot innbyggere og andre brukere. For virksomhetene i Oslo kommune gir sosiale medier mange muligheter, men også noen utfordringer sett i et personvernperspektiv. Dette er bakgrunnen for vurderingen.

Denne vurderingen er utført av Byrådsavdeling for finans ved Seksjon for informasjonssikkerhet og IKT (FIN/ISI).

Nye opplysninger vil kunne føre til endringer i vurderingen.

Eventuelle spørsmål knyttet til vurderingen sendes til fagsjef for personvern i Oslo kommune: maryke.nuth@byr.oslo.kommune.no.

2 Problemstilling, formål og avgrensninger

Denne vurderingen vil behandle prinsipielle problemstillinger ved bruk av sosiale medier sett fra et personvernperspektiv og relevant regelverk. Vurderingen og veiledningen er gjort generisk for å kunne brukes uavhengig av hvilke sosiale medier det er snakk om. Som et ledd i arbeidet med vurderingen, er det på forhånd gjort en kartlegging av noen av de mest brukte sosiale medier i Oslo kommune med hensikten å finne felles utfordringer som kan adresses i vurderingen. Facebook og TikTok er blant de sosiale mediene som er kartlagt. Kartleggingen er ikke en del av den endelige vurderingen og vurderingen henviser heller ikke direkte til konkrete sosiale medier.

Formålet med vurderingen er å bidra til at

- alle virksomheter i Oslo kommune skal forstå hva som skal vurderes i et personvernperspektiv før sosiale medier lovlig kan tas i bruk.
- personvernregelverket etterleves i all bruk av sosiale medier i Oslo kommune til enhver tid.

Begrepet sosiale medier favner bredt og det finnes mange ulike plattformer enten via en app eller et nettsted. Denne vurderingen vil ta for seg sosiale medier som

- brukes som en kommunikasjonskanal rettet mot innbyggere,
- brukes for å nå virksomhetens definerte formål og
- er eid og driftet av en tredjepart (utenfor Oslo kommune).

I vurderingen brukes begrepet kommunikasjonskanal og sosiale medier om hverandre, fordi det kun er bruksmåten (som kommunikasjonskanal) og ikke sosiale medier som sådan som vurderes. De registrerte omtales som innbyggere, og begrepet virksomhet brukes om alle former for etater, byrådsavdelinger, bydeler og andre virksomheter i Oslo kommune.

Vurderingen knytter seg ikke til noen spesifikk plattform eller tjeneste, men gjelder overordnet, uavhengig av om innbyggeren må logge seg inn eller ikke.

Selv om vurderingene i hovedsak gjelder personvern, vil noen andre rettsområder også omfattes, slik som andre relevante regelverk. Vurderingen tar for seg de mest aktuelle av den registrertes rettigheter, men den registrertes friheter behandles ikke utover omtalen av den etiske siden i vurderingen.

Vurderingen avgrenses mot ansattes egen bruk av sosiale medier. Utover dette avgrenses det også mot føringer knyttet til kommunikasjonsstrategi herunder hvem som skal uttale seg og administrere innlegg, hvordan kommunikasjonen skal foregå, prioritering og valg av kommunikasjonskanaler eller håndtering av krisekommunikasjon.

Vurderingen er ikke personvernvurderinger som er påkrevd å gjennomføre i Oslo kommune ved all behandling av personopplysninger (Innledende personvernvurdering (IP), Personvernkonsekvensvurdering ved lav/middel risiko (PLM) eller Personvernkonsekvensvurdering ved høy risiko (DPIA)). Denne vurderingen erstatter ikke disse personvernvurderingene.

Virksomheter i Oslo kommune vil ha ulike behov og ulikt utgangspunkt for å vurdere om og hvordan de vil ta i bruk sosiale medier. Vurderingen vil derfor ikke besvare konkrete problemstillinger knyttet til de enkelte sosiale medier for alle virksomheter. Denne vurderingen er ment som hjelp og veiledning i gjennomføringen av virksomhetenes egne personvernvurderinger.

3 Relevant regelverk

Nedenfor følger en redegjørelse av regelverket som er relevant ved vurdering av om virksomhetene kan bruke en kommunikasjonskanal, samt hvilke bestemmelser i de aktuelle regelverkene som er relevant eller må etterleves. Gjennomgangen gjelder fire sentrale lover på området som ofte kan ha stor betydning i praksis.

3.1 Personvernregelverket

Personvernregelverket regulerer ikke bruk av sosiale medier spesifikt, men de generelle reglene for behandling av personopplysninger gjelder også ved bruk av sosiale medier når det mulig å identifisere enkeltpersoner, enten direkte eller indirekte.

Personopplysningsloven av 2018, som gjør EUs personvernforordning (General Data Protection Regulation – GDPR) til norsk lov, regulerer all behandling av personopplysninger. Formålet med personvernregelverket er å sikre «vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger», jf. GDPR art. 1 nr. 2.

Personvernregelverket omfatter all behandling av personopplysninger som utføres av blant annet offentlige myndigheter, uavhengig av hvilket formål personopplysningene behandles for.

Enhver behandling av personopplysninger må behandles i tråd med de grunnleggende personvernprinsippene, jf. GDPR art. 5. I henhold til bestemmelsen skal personopplysninger:

- Behandles på en lovlig, rettferdig og åpen måte

- Samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene
- Være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for
- Være korrekte og om nødvendig oppdaterte
- Ikke lagres lenger enn det som er nødvendig for formålene som personopplysningene behandles for
- Behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysninger ved bruk av egnede tekniske eller organisatoriske tiltak

Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at de ovennevnte personvernprinsippene overholdes. I tillegg har behandlingsansvarlig plikt til å tilrettelegge for og ivareta den registrertes rettigheter etter GDPR art. 12-22.

Videre må all behandling av personopplysninger ha et rettslig grunnlag for å være lov, jf. GDPR art. 6. Det innebærer at behandlingsansvarlig må ha identifisert om det finnes et behandlingsgrunnlag før en behandling av personopplysningene starter.

Enhver behandling av personopplysninger må også skje i henhold til Grunnloven § 102 som verner om retten til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Bestemmelsen lyder:

> «*Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.*
> *Statens myndigheter skal sikre et vern om den personlige integritet*».

Grunnloven § 102 har klare likhetstrekk med Den europeiske menneskerettskonvensjon (EMK) art. 8 og må tolkes i lys av denne. EMK er gjort til norsk lov gjennom menneskerettsloven av 1999.

EMK art. 8 verner om respekten for familie- og privatliv, hjem og korrespondanse, og den norske oversettelsen lyder som følgende:

> «1. *Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.*
> 2. *Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.»*

Et inngrep i retten etter EMK art. 8 nr. 1 må kunne rettferdiggjøres etter EMK art. 8 nr. 2. Dette innebærer at inngrepet må ivareta et legitimt formål og være forholdsmessig. Kravet om at inngrepet må være «i samsvar med loven» innebærer at inngrepet må ha et rettslig grunnlag i norsk rett.

Ved motstrid skal EMK gå foran bestemmelser i norsk lovgivning, jf. menneskerettsloven § 3.

Hva betyr dette for Oslo kommune?
Personvernregelverket gjelder for all behandling av personopplysninger. Når virksomheter i Oslo kommune bruker sosiale medier som kommunikasjonskanal, må virksomhetene som bruker sosiale medier som kommunikasjonskanal, sikre at regelverket etterleves.

Virksomhetene må i tråd med rutiner i Oslo kommune, gjennomføre en innledende personvernvurdering (IP), etterfulgt av enten en personvernvurdering for lav/middels risiko (PLM) eller en personvernkonsekvensvurdering ved høy risiko (DPIA). Trolig vil bruk av sosiale medier som kommunikasjonskanal medføre en høy risiko for den registrertes rettigheter og friheter, men virksomhetene må vurdere hvert enkelt tilfelle konkret, blant annet basert på formål, behandlingens art og behandlingens omfang.

Vurderingene som gjøres vil bidra til at virksomhetene dokumenterer etterlevelse av personvernregelverket.

3.2 Arkivlova

Kommunale og fylkeskommunale virksomheter er underlagt arkivplikt etter arkivlova. Formålet med loven fremgår av § 1 og lyder som følger:

> «*Føremålet med denne lova er å tryggja arkiv som har monaleg kulturelt eller forskingsmessig verde eller som inneheld rettsleg eller viktig forvaltningsmessig dokumentasjon, slik at desse kan verta tekne vare på og gjorde tilgjengelege for ettertida*»

I forskrift om offentlige arkiv stilles det nærmere krav til journalføring, registrering av dokument, kassasjon mm. I § 9 om journalføring fremgår følgende:

> *«Eit offentleg organ skal ha ein eller fleire journalar for registrering av dokument i dei sakene organet opprettar. I journalen skal ein registrere alle inngåande og utgåande dokument som etter offentleglova § 4 må reknast som saksdokument for organet, dersom dei er eller blir saksbehandla og har verdi som dokumentasjon. Organinterne dokument etter offentleglova § 14 skal organet registrere i journalen så langt organet finn det tenleg. Desse organinterne dokumenta skal likevel alltid journalførast:*
>
> *a) dokument som er omtalte i offentleglova § 14 andre ledd*
> *b) dokument som er omtalte i offentleglova § 16 første ledd bokstav a til d, § 16 andre ledd og § 16 tredje ledd første punktum*
> *c) dokument som er omtalte i offentlegforskrifta § 8.*
>
> *Dokument i saker om innsyn er ikkje omfatta av journalføringsplikta, med mindre dokumenta gjeld eller inneheld ei nærmare grunngjeving, ein klage, eit krav om betaling for innsyn eller eit spørsmål om korleis innsyn skal givast*»

For dokumenter som er gjenstand for saksbehandling eller har dokumentasjonsverdi, foreligger det en arkivplikt.

Dokumentdefinisjonen i arkivlova er teknologinøytral og svært vid. Et dokument blir definert som en logisk avgrenset informasjonsmengde som er lagret på et medium for senere lesing, lytting, visning eller overføring. Definisjonen er tolket til å omfatte kommunikasjon i sosiale medier, uavhengig av utforming eller format på mediet.

Hva betyr dette for Oslo kommune?
Det er materialets innhold, uavhengig av hvor materialet produseres, som styrer om arkivlova kommer til anvendelse eller ikke. Den enkelte saksbehandler og virksomhet må derfor selv vurdere innholdets arkivverdighet basert på hva som produseres av innhold.

Kort sagt er det tre punkter som må vurderes for å avgjøre om virksomhetene skal journalføre noe:

- Er dokumentet et saksdokument?
- Er det sendt inn eller ut av virksomheten?
- Blir det saksbehandlet og har verdi som dokumentasjon?

Hvis det kan svares ja på alle tre spørsmålene, skal dokumentet journalføres. Hvordan journalføringen skal gjennomføres i praksis, må virksomhetene vurdere konkret blant annet ut fra typer og mengde av personopplysninger, krav til dokumentasjon osv. Et eksempel på journalføring av kommunikasjon i sosiale medier er lagring av skjermbilde av kommunikasjonen og arkivering som en bildefil.

3.3 Offentleglova

Offentleglovas bestemmelser henger sammen med reglene i arkivlova og forvaltningsloven. Offentleglova skal blant annet legge til rette for åpenhet og kontroll av det forvaltningen bruker sine ressurser på, og hvordan de arbeider.

Loven stiller blant annet krav til å gi innsyn, og § 3 angir følgende hovedregel:

> «*Saksdokument, journalar og liknande register for organet er opne for innsyn dersom ikkje anna følgjer av lov eller forskrift med heimel i lov. Alle kan krevje innsyn i saksdokument, journalar og liknande register til organet hos vedkommande organ*»

Hva som regnes som dokument i lovens forstand fremgår av § 4 og lyder som følger:

> «*Med dokument er meint ei logisk avgrensa informasjonsmengd som er lagra på eit medium for seinare lesing, lytting, framsyning, overføring eller liknande.*
> *Saksdokument for organet er dokument som er komne inn til eller lagde fram for eit organ, eller som organet sjølv har oppretta, og som gjeld ansvarsområdet eller verksemda til organet. Eit dokument er oppretta når det er sendt ut av organet. Dersom dette ikkje skjer, skal dokumentet reknast som oppretta når det er ferdigstilt.* […]»

For tolkning av regelverket og merknader til bestemmelsene, vises det til Rettleier til offentleglova[1].

Hva betyr dette for Oslo kommune?
Hvorvidt innholdet som skapes i sosiale medier anses som saksdokument, journaler eller lignende register, må vurderes konkret av virksomheten basert på materialets innhold. Vurderingen av om

[1] https://www.regjeringen.no/contentassets/3a11886db3604e9d9a049e872564467d/rettleiar_offentleglova.pdf

det som behandles er et saksdokument, får betydning for plikten til å journalføre, arkivere og evt. gjøre tilgjengelig for offentlig innsyn.

Når et dokument anses som et saksdokument etter offentleglova utløses dette en rekke krav til åpenhet og forsvarlig behandling av dokumentet. Dette vil si at virksomheter må være bevisste på når informasjon som utveksles i sosiale medier utgjør et saksdokument og etablere rutiner for å ivareta dette.

3.4 Forvaltningsloven

Forvaltningsloven inneholder generelle regler om behandlingsmåten i den offentlige forvaltning. Loven regulerer saksbehandlingen når det treffes avgjørelser, og særlig partenes rettigheter under saksbehandlingen.

Forvaltningsloven regulerer også sentrale bestemmelser knyttet til behandling av blant annet personopplysninger, herunder § 13 om taushetsplikt. Bestemmelsen lyder som følger:

> *«Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om:*
> *1. noens personlige forhold, eller […]*
>
> *Som personlige forhold regnes ikke fødested, fødselsdato og personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted, med mindre slike opplysninger røper et klientforhold eller andre forhold som må anses som personlige. Kongen kan ellers gi nærmere forskrifter om hvilke opplysninger som skal reknes som personlige, om hvilke organer som kan gi privatpersoner opplysninger som nevnt i punktumet foran og opplysninger om den enkeltes personlige status for øvrig, samt om vilkårene for å gi slike opplysninger. […]»*

Hva betyr dette for Oslo kommune?
Forvaltningslovens regler gjelder uavhengig av hvilken kommunikasjonskanal eller plattform kommunen bruker til å produsere innhold. Det betyr at forvaltningslovens regler dermed kan gjelde dersom det f.eks. foregår saksbehandling i kommunikasjonskanalen.

På samme måte som for arkivlova, styres vurderingen av om forvaltningslovens anvendelse av innholdet i materialet som produseres og ikke av typer av kommunikasjonskanal. Virksomhetene må vurdere om kommunikasjonskanalen brukes på en måte som kan omfattes av forvaltningslovens regler, og bør i så fall etablere rutiner i tråd med dette. Samtidig bør virksomhetene være oppmerksom på utfordringer knyttet til dialog med innbyggere i slike kommunikasjonskanaler, der det f. eks kan være vanskelig å sikre konfidensialitet og overholde eventuell taushetsplikt.

4 Behandlingsansvar

Når en virksomhet ønsker å ta i bruk en kommunikasjonskanal, er det viktig å ta stilling til hvilken rolle virksomheten har og om det foreligger et behandlingsansvar for virksomheten.

GDPR art. 4 nr. 7 definerer behandlingsansvarlig som en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre

bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

GDPR art. 5 nr. 2. fastslår at det er den behandlingsansvarlige som har det overordnede ansvaret for å overholde personvernprinsippene og regelverket. I praksis innebærer dette at den behandlingsansvarlige har ansvaret for at personopplysningene behandles på en lovlig, rettferdig og åpen måte. I dette ansvaret ligger det også et krav om at den behandlingsansvarlige skal ha full oversikt over sin behandling av personopplysninger, og iverksette eventuelle tekniske og organisatoriske tiltak som kreves for å etterleve loven. Det er også den behandlingsansvarlige som må se til at det finnes et lovlig behandlingsgrunnlag for behandlingen, og som må sikre at den registrerte kan utøve rettighetene sine. Dette betyr at den behandlingsansvarlige må gjøre mange viktige vurderinger før behandlingen av personopplysninger starter.

I følge EUs Artikkel 29-gruppen for beskyttelse av personopplysninger inneholder definisjonen av behandlingsansvarlig tre hovedelementer:

- Det personlige aspektet (den fysiske eller juridiske personen, en offentlig myndighet eller ethvert annet organ)
- Muligheten for kontroll (alene eller sammen med andre)
- De essensielle elementene for å skille behandlingsansvarlig fra andre aktører (bestemmer formålet med behandlingen og hvilke midler som skal benyttes)

Når det gjelder sosiale medier konkret, så kan punktene som Artikkel 29-gruppen nevner i mange situasjoner treffe både den kommunale virksomheten og leverandøren av kommunikasjonsplattformen. En kommunikasjonskanal vil i denne sammenhengen være eid av en tredjepart utenfor Oslo kommune, enten nasjonal eller internasjonal. I praksis vil det ofte være leverandøren av kommunikasjonskanalen som har behandlingsansvar for store deler av behandlingen som skjer, basert på egne definerte formål. Kommunen har vanligvis ikke noen innflytelse på de generelle delene av kommunikasjonskanalen.

Som oftest er det leverandøren som har inngått en avtale med innbyggerne, eller som har innhentet samtykke for bruk av deres personopplysninger mot at de får bruke kommunikasjonskanalen. Dette vil si at innbyggere allerede er brukere av kommunikasjonskanalen som kommunen tenker å ta i bruk. Kommunene vil etter avtale med leverandør kunne ta i bruk kommunikasjonskanalen for egne formål. Dette vil typisk være de tilfellene der kommunen bruker kommunikasjonskanalen aktivt til å nå ut til innbyggerne. I de tilfellene vil det ofte bli produsert nytt innhold som innebærer behandling av personopplysninger, og som medfører at også kommunen blir behandlingsansvarlig.

GDPR art. 26 åpner for at behandlingsansvaret kan være felles. Dette må avgjøres på bakgrunn av de faktiske (og ikke formelle) omstendighetene rundt behandlingen. Hvis to eller flere aktører sammen har bestemt eller hatt avgjørende påvirkning på formål og valg av midler, kan det være snakk om felles behandlingsansvar. Praksis viser at listen synes å være nokså lav før et felles behandlingsansvar foreligger.

Ved felles behandlingsansvar er det krav om at det inngås en avtale mellom de behandlingsansvarlige, der det blant annet skal fremgå hvem som skal ivareta den registrertes rettigheter mv. Et felles behandlingsansvar vil i så måte kreve mer av de behandlingsansvarlige fordi det må avklares hvem som skal ivareta hvilke forpliktelser etter regelverket, og i tillegg vil det kreve oppfølging når det skjer endringer som påvirker den registrertes personvern eller avtaleforholdet mellom de behandlingsansvarlige.

Utgangspunktet for denne vurderingen er at kommunen og eieren/leverandøren av kommunikasjonskanalen har felles behandlingsansvar. Dette er i tråd med praksis fra EU-domstolen. Felles behandlingsansvar krever at den enkelte kommune må være proaktiv 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, må imidlertid den enkelte virksomhet kartlegge hvordan personopplysningene sikres, hva leverandøren gjør for å etterleve og ivareta personvernprinsippene, og hvordan den enkelte registrertes rettigheter og friheter ivaretas av leverandøren.

I tillegg vil et felles behandlingsansvar kreve at virksomhetene må finne ut hvor grensen går for hvilken behandling av personopplysninger som omfattes av det felles behandlingsansvaret og hvilken behandling som er innenfor virksomhetens eget behandlingsansvar. Vurderingen av hvor denne grensen går knytter seg til hva som er virksomhetens egne formål og hva som er leverandørens formål.

Det kan være utfordrende å få kunnskap om behandling som skjer med innbyggernes personopplysninger som er under eieren/leverandørens behandlingsansvar. Denne utfordringen bør være en del av risikovurderingen når virksomheten skal ta i bruk en kommunikasjonskanal.

Avtaleforhold og behandlingsansvar
Virksomhetene må sikre at det foreligger en avtale med eieren/leverandøren av sosiale medier som regulerer ansvarsforholdene. Avtalen bør regulere om det foreligger felles behandlingsansvar, og eventuelt hvem som er ansvarlig for hvilke deler av behandlingen som skjer. For de fleste kommunikasjonskanaler er ikke avtalen en forhandlingssak, men noe virksomheten må akseptere ved å ta i bruk kanalen f. eks. gjennom standardvilkår for bruk. Dette er en risiko ved bruk av sosiale medier som virksomheter må ta stilling til.

Hva betyr dette for Oslo kommune?
Dersom det er snakk om felles behandlingsansvar må virksomheten sikre at det foreligger en avtale med leverandøren av kommunikasjonskanalen, som regulerer ansvarsforholdene rundt det felles behandlingsansvaret.

Det bør fremgå tydelig av avtalen hvem som er ansvarlig for hvilke deler av behandlingen som skjer. Dersom det er snakk om at virksomheten må akseptere standardvilkår for bruk, må

risikoen dette innebærer tas med i personvernvurderingene (PLM og DPIA) og i eventuell ROS før virksomheten beslutter om det sosiale mediet skal tas i bruk.

Virksomheten bør blant annet vurdere følgende punkter knyttet til ansvarsfordeling før kommunikasjonskanalen tas i bruk:

- Har kommunen eller virksomheten innflytelse på behandlingen som skjer i kommunikasjonskanalen, eller må avtalevilkårene aksepteres uten mulighet for endring?
- Er det inngått en avtale om felles behandlingsansvar med eier/leverandør av kommunikasjonskanalen?
- For hvilke deler av tjenesten er virksomhetene å betrakte som behandlingsansvarlig, og er dette klart for virksomheten? Fremgår det noe om dette i avtalen mellom virksomheten og eier/leverandør av sosiale medier?

5 Behandlingsgrunnlag

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

Selv om brukeren av sosiale medier har inngått en avtale med eier/leverandør av kommunikasjonskanalen, er dette i utgangspunktet ikke å regne som virksomhetens behandlingsgrunnlag. Oslo kommune må ha et behandlingsgrunnlag for de delene av behandlingen som omfattes av eget behandlingsansvar. Virksomhetene bør imidlertid gjøre seg kjent med avtalens innhold, og vurdere om avtalen berører behandlingen som ligger under virksomhetens behandlingsansvar. Det er derfor viktig å avklare dette ansvarsforholdet først i tråd med det som fremgår under punkt 4 i denne vurderingen.

Denne vurderingen tar kun for seg de to aktuelle behandlingsgrunnlagene for sosiale medier:

(i) utøvelse av offentlig myndighet som en kommune er pålagt etter GDPR art. 6 nr. 1 bokstav e). Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.
(ii) berettiget interesse etter GDPR art. 6 nr. 1 bokstav f).

Et annet behandlingsgrunnlag som kan være aktuelt er rettslig forpliktelse i GDPR art. 6 nr. 1 bokstav c), som i likhet med behandlingsgrunnlag om utøvelse av offentlig myndighet, krever et supplerende rettsgrunnlag i nasjonal rett. Som oftest vil et supplerende rettsgrunnlag etter denne bestemmelsen kreve en tydelig formulert og mer konkret forpliktelse for kommunen for eksempel gjennom en uttrykkelig lovbestemmelse. På bakgrunn av erfaringer fra konkrete saker i sentralt fagmiljø for personvern i Oslo kommune, har det så langt ikke vært tilfeller der dette behandlingsgrunnlaget har vært aktuelt. Derfor går ikke vurderingen nærmere inn på rettslig forpliktelse som behandlingsgrunnlag, og vurderingen vil kun fokusere på de to ovenstående behandlingsgrunnlagene.

Behandlingsgrunnlagene må vurderes konkret av den enkelte virksomhet, og det gjøres oppmerksom på at andre behandlingsgrunnlag også kan være aktuelle avhengig av de faktiske omstendighetene.

Vurderingen tar ikke spesifikt for seg behandling av særlige kategorier av personopplysninger, men viser til at behandling av disse vil i tillegg kreve et eget behandlingsgrunnlag i GDPR art. 9. For nærmere informasjon om behandlingsgrunnlag, se Veileder for behandlingsgrunnlag på felles intranett.

5.1 Utøvelse av offentlig myndighet som behandlingsgrunnlag

Et aktuelt behandlingsgrunnlag for behandling av personopplysninger i forbindelse med bruk av sosiale medier er GDPR art. 6 nr. 1 bokstav e). Bestemmelsen sier 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*»

Videre fremgår det av art. 6 nr. 3 at

> *«Grunnlaget for behandlingen nevnt i nr. 1 bokstav c) og e) skal fastsettes i*
> *a) unionsretten eller*
> *b) medlemsstatens nasjonale rett som den behandlingsansvarlige er underlagt.*
> *Formålet med behandlingen skal være fastsatt i nevnte rettslige grunnlag eller, når det gjelder behandlingen nevnt i nr. 1 bokstav e), være nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt. Nevnte rettslige grunnlag kan inneholde særlige bestemmelser for å tilpasse anvendelsen av reglene i denne forordning, blant annet de generelle vilkårene som skal gjelde for lovligheten av den behandlingsansvarliges behandling, hvilken type opplysninger som skal behandles, berørte registrerte, enhetene som personopplysningene kan utleveres til, og formålene med dette, formålsbegrensning, lagringsperioder samt behandlingsaktiviteter og framgangsmåter for behandling, herunder tiltak for å sikre lovlig og rettferdig behandling, slik som dem fastsatt med henblikk på andre særlige behandlingssituasjoner som nevnt i* kapittel IX. *[...]*»

Dette behandlingsgrunnlaget (utøvelse av offentlig myndighet) krever et supplerende rettsgrunnlag, og i praksis vil nasjonal særlovgivning kunne være aktuelt.

Et eksempel på supplerende rettsgrunnlag er kommuneloven, dersom virksomheter tar i bruk sosiale medier som et ledd i utøvelsen av offentlig myndighet.

Formålet virksomhetene har for å bruke en kommunikasjonsplattform, kan vurderes opp mot kommuneloven § 4-1 som omhandler informasjon og dialog. Bestemmelsen lyder som følger:

> *«Kommuner og fylkeskommuner skal aktivt informere om egen virksomhet og om virksomhet som andre rettssubjekter utfører på vegne av kommuner og fylkeskommuner. De skal også legge til rette for at alle kan få tilgang til slik informasjon»*

I Prop.46 L (2017-2018) omtales bestemmelsen nærmere under kapittel 30. Her fremgår blant annet følgende:

> *«Etter første punktum plikter kommuner og fylkeskommuner å informere om egen virksomhet. Dette kravet knytter seg til virksomhet som foregår i kommunen eller fylkeskommunen som rettssubjekt.*
>
> *Videre plikter kommuner og fylkeskommuner å informere om virksomhet som foregår i et annet rettssubjekt, når dette utfører oppgaver for kommunen eller fylkeskommunen. [...]*
>
> *Plikten er kun knyttet til de oppgavene eller liknende andre rettssubjekter utfører for kommunen eller fylkeskommunen. Dette vil for eksempel kunne være å informere om aktiviteter og*

liknende som andre rettssubjekter utfører for kommuner og fylkeskommuner, og som har direkte innvirkning på innbyggerne i kommunen eller fylkeskommunen. Selve plikten til å informere om forhold i det eksterne rettssubjektet påligger kommunen og fylkeskommunen og ikke det eksterne rettssubjektet som sådan.
Kommuner og fylkeskommuner plikter etter andre punktum å legge til rette for at alle kan få tilgang til den informasjonen kommunene eller fylkeskommunene gir. Dette kan innebære både tiltak for å tilpasse informasjonen til mottakerne og tiltak for å gjøre informasjonen fysisk eller elektronisk tilgjengelig. Forpliktelsen etter andre punktum innebærer at kommunen skal bruke et klart språk som er tilpasset de forskjellige brukergruppene.

Verken første eller andre punktum regulerer nærmere hvilke konkrete forhold det skal informeres om, hvor mye det skal informeres, hvordan det skal informeres, eller til hvem det skal informeres. Det er i utgangspunktet opp til kommunen og fylkeskommunen selv å vurdere disse spørsmålene ut fra lokale behov og tilgjengelige ressurser. Det vil likevel være i strid med bestemmelsen helt å unnlate å informere eller å informere i svært liten grad. Bestemmelsen gir kommuner og fylkeskommuner frihet til å fylle informasjonsplikten med innhold. Dette innebærer at innbyggere, presse eller andre ikke kan bruke denne bestemmelsen til å påberope seg at kommunen eller fylkeskommunen ikke har gitt dem den nødvendige informasjonen»

Betraktninger om grensegangen mellom «rettslig forpliktelse» og «utøvelse av offentlig myndighet»

Selv om både «rettslig forpliktelse» etter GDPR art. 6 nr. 1 bokstav c) og «utøvelse av offentlig myndighet» etter GDPR art. 6 nr. 1 bokstav e) antagelig kan brukes som behandlingsgrunnlag for kommunenes behandling av personopplysninger i sosiale medier, viser erfaringen så langt, utfra saker der det sentrale fagmiljøet for personvern i Oslo kommune har vært involvert, at «utøvelse av offentlig myndighet» er det som i praksis kan brukes som behandlingsgrunnlag for behandling av personopplysninger i sosiale medier.

I denne vurderingen ansees «rettslig forpliktelse» som et mer snevert behandlingsgrunnlag enn «utøvelse av offentlig myndighet», fordi det betyr at kommunen må være forpliktet til å behandle personopplysningene det er snakk om. I en rettslig forpliktelse ligger det at formålet ikke kan oppnås uten at personopplysningene behandles, og behandlingen i sosiale medier må være nødvendig for å oppnå dette formålet. Dette vil begrense når kommunen kan bruke dette behandlingsgrunnlaget i praksis. Det er videre et krav at formålet med behandlingen fremgår av det supplerende rettsgrunnlaget, noe som betyr at formålet er definert av lovgiver gjennom en demokratisk prosess. Det supplerende rettsgrunnlaget trenger ikke regulere behandlingen i seg selv, men må gi den registrerte forutsigbarhet knyttet til behandlingen. «Rettslig forpliktelse» som behandlingsgrunnlag vil ikke bli omtalt videre i denne juridiske vurderingen, selv om det i spesielle tilfeller kan være et aktuelt behandlingsgrunnlag når kommunen skal behandle personopplysninger i sosiale medier.

«Utøvelse av offentlig myndighet» krever også et supplerende rettsgrunnlag i nasjonal rett, men det stilles ikke de samme kravene til det supplerende rettsgrunnlaget som for «rettslig forpliktelse». Formålet trenger ikke fremgå av det supplerende rettsgrunnlaget, og dette åpner for at behandlingsansvarlig selv kan definere formålet. Kravene til det supplerende rettsgrunnlaget er dermed ikke like omfattende som for «rettslig forpliktelse», og det er tilstrekkelig at det supplerende rettsgrunnlaget gir grunnlag for å utøve offentlig myndighet og at det er nødvendig for den behandlingsnansvarlige å behandle personopplysninger for å utøve

den offentlige myndigheten. Mer om utøvelse av offentlig myndighet som behandlingsgrunnlag nedenfor.

Det er likevel ikke helt klare grenser for når noe er en rettslig forpliktelse som er pålagt kommunen og når kommunen utøver offentlig myndighet. Det må derfor gjøres konkrete vurderinger av hvilken behandling som skal gjennomføres og av ordlyden i det supplerende rettsgrunnlaget, for å bestemme hvilket behandlingsgrunnlag som er riktig i det enkelte tilfelle.

Hva betyr dette for Oslo kommune?
Virksomhetene bør være varsomme med å legge til grunn utøvelse av offentlig myndighet som behandlingsgrunnlag, og det må i så fall vurderes konkret. Ikke alle kommunes aktiviteter kan regnes som utøvelse av myndighet, f. eks. vil kommunen i rollen som arbeidsgiver ikke kunne sies å utøve offentlig myndighet.

I tråd med beskrivelsen over, må det sikres at det supplerende rettsgrunnlaget som brukes er tydelig nok til å kunne begrunne behandlingen, og videre at bruken av sosiale medier er nødvendig for å oppnå virksomhetens formål med behandlingen.

I vurderingen av om utøvelse av offentlig myndighet kan legges til grunn som behandlingsgrunnlag, kan virksomheten stille følgende kontrollspørsmål:

- Er behandlingen av personopplysninger nødvendig for å utøve offentlig myndighet som virksomheten er pålagt?
- Har virksomheten et supplerende rettsgrunnlag som begrunner behandlingen?

5.2 Berettiget interesse som behandlingsgrunnlag

Et aktuelt behandlingsgrunnlag er GDPR art. 6 nr. 1 bokstav f). Bestemmelsen sier at behandlingen av personopplysninger er lovlig dersom

> «*behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.*»

Det er viktig å merke seg at dette behandlingsgrunnlaget ikke får anvendelse på behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver.

For dette behandlingsgrunnlaget kreves det at virksomheten må gjennomføre en interesseavveining mellom virksomhetens berettigede interesse og den registrertes interesser, grunnleggende rettigheter og friheter, og særlig når det er snakk om barn. I interesseavveiningen skal det tas hensyn til om den registrerte med rimelighet kan forvente at personopplysningene blir anvendt til det aktuelle formålet mv, jf. GDPR fortalepunkt 47.

GDPR angir ikke hvilke momenter som skal vurderes i en slik interesseavveining. Virksomheten må veie sin egen interesse i behandlingen opp mot personvernkonsekvensene for den registrerte. Hvis virksomheten ikke har en tungtveiende interesse, kan behandlingen bare skje hvis personvernkonsekvensene for de berørte er små. Jo større personvernulempene er, desto tyngre må virksomhetens interesse veie for å kunne lande på at det er snakk om en berettiget interesse. Virksomheten kan iverksette tiltak som reduserer personvernkonsekvensene.

Tre vilkår må alle være oppfylt for å kunne benytte GDPR art. 6 nr. 1 bokstav f berettiget interesse som behandlingsgrunnlag:

1. Virksomheten må ha en saklig berettiget interesse
2. Behandlingen av personopplysninger må være nødvendig for å oppnå formålet knyttet til den berettigede interessen
3. Den berettigede interessen må veie tyngre enn de registrertes rett til personvern

I tråd med slike føringer, skal det vurderes om den planlagte behandlingen er av en så inngripende art at virksomheten ikke kan legitimere interessen.

Nærmere om berettiget interesse i Oslo kommune

For å lovlig kunne bruke dette behandlingsgrunnlaget må det foreligge en berettiget interesse. Interessen ses i lys av formålet med behandlingen, dvs. hva virksomhetene ønsker å oppnå. At noe er berettiget må vurderes konkret, og følgende kontrollspørsmål kan brukes:

- Hvorfor skal virksomheten behandle opplysningene i kommunikasjonskanalen?
- Hvor viktig er det å behandle opplysningene gjennom bruk av en kommunikasjonskanal?
- Hva skjer hvis virksomheten lar være å bruke kommunikasjonskanalen?
- Er behandlingen av personopplysninger i kommunikasjonskanalen uetisk på noen måte?

Virksomheten må beskrive den berettigede interessen, og formålet med bruken av sosiale medier som tiltak må knytte seg til denne. En berettiget interesse for å bruke en kommunikasjonsplattform kan f.eks. ha følgende formål:

- å nå ut til flest mulig av kommunens innbyggere med innhold virksomheten publiserer (det vil si å være på flere enn en flate)
- å stimulere til dialog eller debatt om temaene virksomheten arbeider med, både mellom virksomheten og innbyggerne og mellom innbyggerne. På den måten kan virksomhetene få innspill til forbedring av sine tjenester
- å nå ut til en spesifikk målgruppe med informasjon for å oppfylle formål om åpenhet i forvaltningen
- å innhente data og statistikk og bruke denne til å nå ut med virksomhetens budskap på en mer treffende måte

Formålet virksomhetene har knyttet til bruk av kommunikasjonskanalen, vil sette rammene for hva som lovlig kan behandles i kanalen og hvordan behandlingen kan foregå.

Nærmere om nødvendighet i Oslo kommune

For å kunne benytte berettiget interesse må behandlingen være «nødvendig». Det må altså være en sammenheng mellom behandlingen i kommunikasjonskanalen og virksomhetens interesse. Dette innebærer at en ikke med rimelighet kan oppnå det samme formålet på en annen måte som er mindre inngripende for innbyggerens rettigheter og friheter.

Dersom formålet kan løses eller risikoen minimeres gjennom andre egnede, men mindre inngripende tiltak, skal en ikke bruke den spesifikke kommunikasjonskanalen.
Kontrollspørsmål kan være:

- Er det mulig å oppnå det samme formålet uten å ta i bruk kommunikasjonskanalen?

- Er det mulig å oppnå formålet på en mindre inngripende måte?

Nærmere om interesseavveining i Oslo kommune

I en interesseavveining skal virksomheten på den ene siden se hen til innbyggerens rett til privatliv og deres interesse i ikke å bli overvåket eller etterlate seg spor. På den andre siden ser virksomheten på sin egen interesse i å behandle personopplysninger basert på sitt formål.

Interesseavveiingen må dokumenteres, og i avveiningen kan flere momenter vurderes konkret. Vurderingen må være helhetlig og ta for seg alle relevante vurderingsmomenter for den aktuelle behandlingen. Nedenfor gis det noen eksempler på vurderingsmomenter som er relevante i en interesseavveining.

Svarer virksomheten ja på spørsmål nedenfor, er det i virksomhetens favør i avveiningen. Jo flere spørsmål virksomheten svarer ja på nedenfor, desto mer i virksomhetens favør i avveiningen.

- Er det mulig for innbyggeren å protestere på hele eller deler av behandlingen før den starter?
- Er det valgfrihet knyttet til ulike behandlinger i kommunikasjonskanalen?
- Regner innbyggeren med at deres personopplysninger blir behandlet av virksomheten ved å ta i bruk kommunikasjonskanalen?
- Vil innbyggeren ha fordeler av at virksomheten tar i bruk kommunikasjonskanalen?
- Er behandlingen som skjer i kommunikasjonskanalen i innbyggerens interesse?
- Har virksomheten og innbyggeren samme interesse i å ta kommunikasjonskanalen i bruk?
- Er det et gjensidig forhold mellom virksomheten og innbyggeren?
- Gir virksomheten god informasjon til innbyggeren om behandlingen?
- Er det enkelt for innbyggeren å kontakte virksomheten for å kontrollere behandlingen?

Svarer virksomheten ja på spørsmål nedenfor, er det i virksomhetens disfavør i avveiningen:

- Vil innbyggeren bli overrasket over virksomhetens behandling av sine opplysninger i kommunikasjonskanalen?
- Vil innbyggeren kunne oppfatte behandlingen som negativ?
- Kan innbyggeren oppfatte behandlingen som upassende – basert på forholdet mellom virksomheten og innbyggeren?
- Vil det bli behandlet mange personopplysninger om innbyggeren?
- Vil behandlingen av personopplysninger i kommunikasjonskanalen være av sensitiv art?

Det er ikke slik at kontrollspørsmålene er uttømmende eller har samme vekt. Dette må vurderes konkret av den enkelte virksomhet.

Dersom virksomheten etter en avveining av de ulike interessene kommer til at innbyggerens grunnleggende personverninteresser veier tyngre enn virksomhetens interesse i å behandle opplysningene, kan ikke dette behandlingsgrunnlaget benyttes.

6 De grunnleggende personvernprinsippene

Enhver behandling av personopplysninger må være i tråd med de grunnleggende personvernprinsippene i GDPR art. 5. Prinsippene gir på ulike måter uttrykk for at behandling av personopplysninger skal skje på en måte som i størst mulig grad sikrer forutsigbarhet og forholdsmessighet for enkeltmennesket.

Nedenfor følger en redegjørelse av de ulike prinsippene og hvilken betydning de har dersom virksomhetene velger å ta i bruk sosiale medier.

Det stilles også en del kontrollspørsmål og gis eksempler på tiltak som kan iverksettes for å sikre at behandlingen ivaretar hvert av prinsippene. Redegjørelsen inneholder ingen uttømmende oversikt over aktuelle tiltak.

6.1 Lovlighet, rettferdighet og åpenhet

At behandlingen av personopplysninger må være lovlig innebærer først og fremst at det må finnes et rettslig grunnlag for en planlagt behandling av personopplysninger.

At behandlingen av personopplysninger må skje rettferdig betyr at den skal gjøres i respekt for de registrertes interesser og rimelige forventninger. Behandlingen skal være forståelig for de registrerte og ikke foregå på skjulte eller manipulerende måter.

Åpenhet betyr i denne sammenheng at bruken av personopplysninger skal være oversiktlig og forutsigbar for den opplysningene gjelder. Personer det behandles opplysninger om, skal være informert om behandlingen. Åpenhet bidrar til å skape tillit og det setter enkeltpersonen i stand til å bruke sine rettigheter og ivareta sine interesser.

Hva betyr dette for Oslo kommune?
Lovlighet
Virksomhetene må sikre at det foreligger et behandlingsgrunnlag før kommunikasjonskanalen tas i bruk. Det er redegjort for behandlingsgrunnlag i kapittel 5.

Under dette prinsippet kan virksomheten generelt vurdere:

- Finnes det et rettslig grunnlag for den planlagte behandlingen av personopplysningene?
- Er det skille mellom hvilke opplysninger som er nødvendig å behandle for å levere tjenesten, og hvilke andre opplysninger det kan være valgfritt å oppgi for å få tilgang til utvidede tjenester?

Tiltak:

- Gjøre en grundig vurdering av aktuelle behandlingsgrunnlag og dokumentere vurderingen.

Rettferdighet
Bruk av en kommunikasjonsplattform må skje med respekt for de registrertes interesser og rimelige forventninger. Behandlingen av personopplysninger som skjer på plattformen må være

forståelig for innbyggerne som tar kanalen i bruk. Behandlingen skal ikke foregå på manipulerende måter.

Under dette prinsippet kan virksomheten vurdere:

- Gjøres behandlingen av personopplysningene i respekt for de registrertes interesser og rimelige forventninger?
- Er behandlingen åpen og forståelig for de registrerte (den skal ikke foregå på fordekte eller manipulerende måter)?
- Hva skjer med opplysningene som genereres ved å bruke virksomhetens del av kommunikasjonskanalen?
- Genereres det ny informasjon som brukes til andre formål enn virksomhetens formål?
- Hvem andre har tilgang til å bruke informasjonen som behandles av virksomhetene?
- Er dataflyten kjent for virksomheten?

Tiltak:

- Sikre at virksomheten forstår hvordan personopplysninger blir behandlet og hvordan dataflyten foregår
- Gi god informasjon til innbyggerne om behandlingen
- Sikre at det gjennomføres personvernkonsekvensvurdering der virksomhet involverer ulike interessenter i vurderingsprosessen (f.eks. tillitsvalgte, personvernombudet osv.).
- Sikre at kommunikasjonskanalen har personvernvennlige innstillinger, eller tilføye egne tiltak slik som å begrene innsamlingen av overskuddsdata

Åpenhet

For å ivareta prinsippet om åpenhet, må det gis god informasjon til innbyggerne om behandlingen av personopplysninger og hva det innebærer når vedkommende bruker virksomhetens del av kommunikasjonskanalen. Dette vil gi innbyggere anledning til å protestere på behandlingen (se nærmere om retten til å protestere under).

Det vil ikke være tilstrekkelig å vise til eierens/leverandørens personvernerklæring alene, da denne ikke vil gi innbyggeren konkret informasjon om virksomhetens behandling av deres personopplysninger.

Under dette prinsippet kan virksomheten vurdere:

- Er bruken av personopplysningene oversiktlig og forutsigbar for de opplysningene gjelder?
- Har virksomheten funksjonalitet for å gi informasjon om hvilke opplysninger som behandles, hva de brukes til og mulighet for de registrerte til å gjøre seg kjent med sine rettigheter og hvordan de skal utøve disse?
- Har virksomheten en personvernerklæring på virksomhetens nettsider med generell informasjon om hvordan virksomheten behandler personopplysninger?

Tiltak:

- Gi informasjon om behandlingen i virksomhetens tilpassede personvernerklæring.
- Ha en tydelig tekst synlig på kommunikasjonsplattformen der det beskrives vilkår og retningslinjer som gjelder for virksomhetens bruk av kommunikasjonskanalen/er.

6.2 Formålsbegrensning

Prinsippet innebærer at personopplysninger kun skal behandles for spesifikke, uttrykkelige, angitte og legitime formål. Det betyr at ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist, og alle formål skal være forklart på en måte som gjør at alle berørte har samme forståelse av hva personopplysningene skal brukes til.

At formålet skal være legitimt innebærer at det i tillegg til å ha et rettslig grunnlag også skal være i samsvar med øvrige etiske og rettslige samfunnsnormer. Personopplysninger kan ikke gjenbrukes til formål som er uforenlig med det opprinnelige formålet.

Hva betyr dette for Oslo kommune?
Virksomhetene må definere hva som er formålet eller formålene med bruk av sosiale medier. Det er gitt eksempler på dette under kapittel 5.2 om berettiget interesse. Hvordan formålet defineres, vil være viktig for den videre behandlingen, og er en forutsetning for å vurdere om behandlingen er lovlig og hva som er riktig behandlingsgrunnlag.

Når formålet skal beskrives, er det viktig at beskrivelsen dekker det virksomheten planlegger å bruke kommunikasjonsplattformen til, slik at formålet er tydelig for innbygger. Det er også viktig å beskrive de overordnede formålene med bruk av kommunikasjonskanalen, for eksempel å nå ut til flest mulig, nå ut til en konkret brukergruppe, kommunisere på tvers av plattformer osv. Det kan også være lurt å definere målgruppen først, og deretter bestemme formålet i lys av målgruppen.

Under dette prinsippet kan virksomheten vurdere:

- Er ethvert formål med behandling av personopplysninger identifisert og presist beskrevet for alle berørte?
- Har formålet med behandlingen et rettslig grunnlag?
- Hvis personopplysninger skal gjenbrukes, er behandlingen lovfestet eller er det innhentet nytt samtykke?

Tiltak:

- Etablere rutiner for hvordan plattformen kan brukes, f.eks. hvordan personopplysningene håndteres ved innsyn og utlevering.
- Danne seg et bilde av hvilken type opplysninger som faktisk behandles, for eksempel ytringer, informasjon om hvordan kanalen brukes, tegn for å beskrive reaksjon på noe (smilefjes, like osv.), kontaktopplysninger, preferanser m.m.
- Klargjøre om personopplysningene også vil viderebehandles av eieren/leverandøren av kommunikasjonskanalen til andre formål enn det virksomheten har lagt til grunn.

6.3 Dataminimering

Prinsippet om dataminimering innebærer å begrense behandling av personopplysninger til det som er nødvendig for å realisere formålet med innsamlingen. For å oppfylle prinsippet om dataminimering må det iverksettes tiltak som sikrer adekvans og relevans i behandlingen knyttet til formålet.

Hva betyr dette for Oslo kommune?
Det er trolig store forskjeller på hvor mye informasjon som samles inn og behandles om innbyggere i de ulike kommunikasjonskanalene. Når virksomheten er behandlingsansvarlig, skal formålet sette rammene for hva som skal samles inn og hvor lenge personopplysningene lagres.

Virksomheter som velger ulike kommunikasjonskanaler med innbyggere, har et ansvar for å unngå å skape situasjoner som kan føre til at personvernet til innbyggeren blir svekket. Virksomheten må derfor legge til rette for at innbyggeren ikke deler personopplysninger om seg selv eller andre utover det som er nødvendig og innenfor det definerte formålet.

Under dette prinsippet kan virksomheten vurdere:

- Er alle personopplysningene som behandles relevante og nødvendige for å realisere formålet med behandlingen?
- Kan formålet med behandlingen med rimelighet oppfylles på annen måte enn å behandle personopplysninger? (I så fall skal det ikke innhentes personopplysninger).
- Innhentes det personopplysninger om flere personer enn nødvendig?

Virksomheten må også tilrettelegge for at bruker ikke deler taushetsbelagt informasjon om seg selv eller andre. Følgende punkter kan vurderes:

- Er det mulig for virksomheten å rette eller slette opplysninger, f. eks. hvis det blir registrert særlige kategorier av personopplysninger?
- Kan slettingen i tilfelle oppleves som sensur, dersom kommentaren ikke inneholder personangrep, navngir tredjepersoner eller er i strid med norsk lov?

Tiltak:

- Etablere rutiner for å fjerne overskuddsinformasjon som publiseres
- Kontrollere om det er mulig å fjerne eller minimere bruk av fritekstfelt
- Gi tydelig informasjon om publiseringsregler og konsekvenser ved å publisere noe utenfor reglene
- Sette i verk tiltak som sikrer at innbyggere ikke publiserer personopplysninger om andre når dette er utenfor formålet med behandlingen

6.4 Riktighet

Prinsippet innebærer at personopplysninger som behandles skal være korrekte, og skal om nødvendig oppdateres. Dette betyr at den behandlingsansvarlige må sørge for å straks slette eller rette personopplysninger som er uriktige.

Hva betyr dette for Oslo kommune?
Når det gjelder opplysninger om en person som produseres av den enkelte, er det som oftest ikke en utfordring at personopplysningene ikke er riktige. Det kan imidlertid oppstå en situasjon der en person publiserer uriktige personopplysninger om andre, eller at kommunikasjonskanalens eier/leverandør generer informasjon som er feil.

Under dette prinsippet kan virksomheten vurdere:

- Er det iverksatt tiltak som sørger for at personopplysningene er korrekte og oppdaterte (f. eks. tekniske tiltak)?
- Er det iverksatt tiltak som sikrer at personopplysninger som er uriktige med hensyn til formålene de behandles for, straks slettes eller korrigeres?

Tiltak:

- Virksomheten må ha rutiner som sikrer at personopplysninger kan rettes dersom de er uriktige, enten av virksomheten selv, innbyggeren eller av eieren/leverandøren.

6.5 Lagringsbegrensning

Prinsippet om lagringsbegrensning innebærer at personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.

Se for øvrig punktene om arkivlova og forvaltningsloven. Det kan også være annet regelverk som begrenser plikten til å slette personopplysninger.

Hva betyr dette for Oslo kommune?
Virksomheten må gjøre en konkret vurdering av hvor lenge personopplysningene som genereres på plattformen skal lagres, basert på formålet og om det finnes særlovgivning som regulerer lagringstiden. Dersom behandlingen av personopplysninger skjer på en plattform med felles behandlingsansvar, er det ikke sikkert at virksomheten gis mulighet til å slette personopplysninger i den grad som er ønskelig.

Under dette prinsippet kan virksomheten vurdere:

- Gir kommunikasjonskanalen mulighet for at opplysninger skal slettes når formålet er oppnådd? Reguleres dette av kommunikasjonskanalens avtale med virksomheten og/eller med innbyggeren?
- Dersom virksomheten mener at opplysningene skal slettes, men innbyggeren frivillig har lagt opplysningene inn, kan virksomheten faktisk slette, eller går dette på bekostning av ytringsfriheten?

Tiltak:

- Virksomheten må ha rutiner som sikrer at personopplysninger kan slettes i tråd med personvernforordningen.

6.6 Integritet og konfidensialitet

Personopplysninger skal behandles slik at opplysningenes integritet, konfidensialitet og tilgjengelighet beskyttes. Det må iverksettes tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger.

Hva betyr dette for Oslo kommune?
I kommunikasjonskanaler som omtales i denne vurderingen, vil det i de fleste sammenhenger være snakk om personopplysninger som er offentlig tilgjengelig som registreres. Det må likevel gjøres konkrete vurderinger av om det er personopplysninger som bør vernes, selv om

informasjonen i utgangspunktet er offentlig tilgjengelig.

For å sikre at det vurderes og eventuelt iverksettes tiltak for å sikre konfidensialitet og integritet, må det gjennomføres en risikovurdering. Avtalevilkårene eller andre dokumenter som beskriver tjenesten bør undersøkes for å kunne danne et bilde av risikoen i den bestemte kommunikasjonskanalen.

Under dette prinsippet kan virksomheten vurdere:

- Har virksomheten tiltak mot uautorisert utlevering og tilgang til personopplysninger?
- Har virksomheten som standard å sørge for at personopplysninger ikke gjøres tilgjengelig for et ubegrenset antall mennesker uten den berørte personens medvirkning?
- Har virksomheten tiltak for å sikre at systemene som behandler personopplysninger er robuste mot for eksempel sårbarheter, angrep og uhell?

Tiltak:

- Gjennomføre opplæring av ansatte som skal behandle personopplysninger i kommunikasjonskanalen
- Iverksette monitorering av informasjon som blir behandlet i kommunikasjonskanalen
- Etablere sletterutiner
- Sikre at det er gitt tilstrekkelig informasjon til innbyggeren slik at de ikke publiserer innhold som er sensitiv eller taushetsbelagt
- Sette i verk tiltak som hindrer uautorisert utlevering av innbyggerens personopplysninger, f. eks. gjennom å etablere rutiner for innsyn og utlevering

6.7 Ansvarlighet

Prinsippet om ansvarlighet understreker ansvaret for å opptre i samsvar med reglene for behandling av personopplysninger. I Oslo kommune har den enkelte virksomheten behandlingsansvaret for egen behandling av personopplysninger i virksomheten.

Se for øvrig kapittel 4 om behandlingsansvarlig.

Hva betyr dette for Oslo kommune?
Virksomheten må opptre proaktivt og etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid.

Under dette prinsippet kan virksomheten vurdere:

- Opptrer virksomheten proaktivt?
- Har virksomheten etablert alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid?
- Er det dokumentert at virksomheten faktisk opptrer i samsvar med reglene?

Tiltak:

- Dokumentere at virksomheten har gjennomført tiltak for å etterleve personvernregelverket.

7 Ivaretakelse av de registrertes rettigheter

Personvernregelverket skal sikre vern av den enkeltes personopplysninger, jf. GDPR art. 1 nr. 2. Hver enkelt virksomhet i Oslo kommune har en plikt til å ivareta de registrertes rettigheter når virksomheten samler inn og bruker personopplysninger om enkeltpersoner. Disse rettighetene må, så langt de rekker, også ivaretas dersom den enkelte virksomhet velger å ta i bruk en kommunikasjonsplattform.

Under følger en redegjørelse for de registrertes rettigheter, sammen med eksempler på tiltak for ivaretakelse av disse.

7.1 Rett til informasjon

Virksomhetenes plikt til å gi informasjon til den registrerte ved behandling av personopplysninger følger av GDPR art. 12-14.

Det stilles også krav til hvordan de kommuniserer med enkeltpersoner. Regelverket krever at virksomheten skal kommunisere på en kortfattet, åpen, forståelig og lett tilgjengelig måte. Språket skal være klart og enkelt, særlig når informasjonen er spesifikt rettet mot barn.

Når en virksomhet velger å ta i bruk sosiale medier som kommunikasjonskanal, vil retten til informasjon også gjelde for virksomhetens behandling av personopplysninger som skjer i kommunikasjonskanalen.

Hva betyr dette for Oslo kommune?
Virksomheten må utarbeide informasjon om sin bruk av den konkrete kommunikasjonskanalen. Her er det viktig å oppgi korrekt informasjon, og særlig informasjon om hvilke personopplysninger som vil kunne bli behandlet.

Av informasjonen bør det også fremgå hva bruk av kommunikasjonskanalen innebærer, for eksempel at andre kan se den registrertes personopplysninger, og at ansvaret for behandlingen er delt mellom ulike aktører. Videre bør det informeres om hvilke tekniske tiltak som er iverksatt for å ivareta hensynet til personvernet, evt. hvor vedkommende kan finne slik informasjon.

Under denne rettigheten kan virksomheten vurdere:

- Har virksomheten informert de registrerte om at det behandles personopplysninger om dem?
- Har virksomheten informert om hva bruk av kommunikasjonskanalen innebærer for den registrerte?
- Har virksomheten tilpasset informasjonen til målgruppen og tatt hensyn til at informasjonen eventuelt er rettet mot barn?

Tiltak:

- Etablere en personvernerklæring tilpasset virksomhetens bruk av hver enkelt kommunikasjonskanal.

7.2 Rett til innsyn

I henhold til GDPR art. 15 har den registrerte rett til innsyn i egne personopplysninger. Bestemmelsens bokstav a-h angir hvilken informasjon den registrerte skal gis ved krav om innsyn.

Når en virksomhet velger å ta i bruk sosiale medier som kommunikasjonskanal, vil retten til innsyn også gjelde for personopplysninger som behandles i kommunikasjonskanalen.

Hva betyr dette for Oslo kommune?
Virksomheten bør undersøke om og i hvilken grad retten til innsyn ivaretas av kommunikasjonskanalens eier/leverandør. Dersom retten ivaretas i løsningen, må virksomheten sikre at det foreligger rutiner som har tatt høyde for hvordan et innsynskrav skal behandles. Videre må virksomheten vurdere om det er deler av innsynsretten som likevel ikke er tilstrekkelig ivaretatt, og denne vurderingen må tas før virksomheten velger å ta i bruk kommunikasjonskanalen.

Under denne rettigheten kan virksomheten vurdere:

- Er det bekreftet at eieren/leverandøren av kommunikasjonskanalanen skal ivareta deler av retten til innsyn? Hvis ja, i hvilken grad?
- Er det etablert rutiner for håndtering av krav om innsyn fra den registrerte?
- Besvares et krav om innsyn i egne personopplysninger med informasjon om hvilke konkrete personopplysninger virksomheten behandler om den registrerte, hvordan personopplysningene om den registrerte behandles og hvor opplysningene er hentet fra?

Tiltak:

- Etablere rutiner for hvordan virksomheten skal gå frem ved et innsynskrav.

7.3 Rett til retting

I henhold til GDPR art. 16 har den registrertes rett til retting av uriktige personopplysninger om seg selv, og rett til å få ufullstendige personopplysninger om seg komplettert, herunder ved å fremlegge en supplerende erklæring.

Når en virksomhet velger å ta i bruk sosiale medier som kommunikasjonskanal, vil retten til retting også gjelde for personopplysninger som behandles i kommunikasjonskanalen.

Hva betyr dette for Oslo kommune?
Virksomheten bør undersøke om og i hvilken grad retten til retting ivaretas av kommunikasjonskanalens eier/leverandør. Videre må virksomheten vurdere om retten til retting likevel ikke er tilstrekkelig ivaretatt, og denne vurderingen må tas før virksomheten velger å ta i bruk kommunikasjonskanalen.

Virksomheten må sikre at det foreligger rutiner knyttet til krav om retting fra den registrerte. Rutinene må si noe om hvordan krav om retting fra den registrerte skal behandles, i hvilke tilfeller virksomheten selv kan rette opplysninger og hvordan retting skal skje.

Under denne rettigheten kan virksomheten vurdere:

- Er det bekreftet at eieren/leverandøren av kommunikasjonskanalanen skal ivareta retten til retting? Hvis ja, i hvilken grad?
- Er det etablert rutiner for håndtering av krav om retting fra den registrerte?
- Er det lagt til rette for at den registrerte kan kreve at uriktige opplysninger om seg rettes og at den registrerte kan kreve at ufullstendige opplysninger om seg suppleres?

Tiltak:

- Etablere rutiner for hvordan virksomheten skal gå frem ved et krav om retting.

7.4 Rett til sletting

Det følger av GDPR art. 17 at de registrerte i enkelte tilfeller kan kreve at egne personopplysninger slettes. Denne retten til sletting kalles også noen ganger «retten til å bli glemt».

De registrertes rett til sletting gjelder imidlertid ikke dersom lagring av opplysningene er nødvendig:

- For å utøve retten til ytrings- og informasjonsfrihet
- For å oppfylle en rettslig forpliktelse som Oslo kommune er underlagt, eller for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet
- For visse typer bruk innen helsetjenester
- For arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål
- For å fastsette, gjøre gjeldende eller forsvare rettskrav

Virksomheten må være bevisst på at personopplysninger skal slettes dersom det ikke lenger er et nødvendig grunnlag for å lagre opplysningene. Dette skal virksomheten vurdere av eget tiltak eller dersom den registrerte ber om sletting.

Når en virksomhet velger å ta i bruk sosiale medier som kommunikasjonskanal, vil retten til sletting også gjelde for personopplysninger som behandles i kommunikasjonskanalen.

Hva betyr dette for Oslo kommune?
Virksomheten bør undersøke om og i hvilken grad retten til retting ivaretas av kommunikasjonskanalens eier/leverandør. Videre må virksomheten vurdere om retten til sletting likevel ikke er tilstrekkelig ivaretatt, og denne vurderingen må tas før virksomheter velger å ta i bruk kommunikasjonskanalen.

Virksomheten må sikre at det foreligger rutiner knyttet til krav om sletting fra den registrerte. Rutinene må si noe om hvordan krav om sletting fra den registrerte skal behandles og hvordan sletting skal skje.

Under denne rettigheten kan virksomheten vurdere:

- Er det bekreftet at eieren/leverandøren av kommunikasjonskanalanen skal ivareta retten til sletting? Hvis ja, i hvilken grad?

- Er det lagt til rette for at den registrerte kan kreve at personopplysninger om seg slettes?
- Er det lagt til rette for at virksomheten sletter personopplysninger dersom det ikke lenger er et nødvendig grunnlag for å lagre opplysningene?

Tiltak:

- Etablere rutiner for hvordan virksomheten skal gå frem ved et krav om sletting.

7.5 Rett til å protestere

Den registrertes rett til å protestere følger av GDPR art. 21. Retten til å protestere innebærer at den registrerte i noen tilfeller kan protestere mot at egne personopplysninger behandles.

Virksomheten må gjøre en konkret avveining dersom den registrerte protesterer på behandlingen, men gjelder ikke i dersom en virksomhet kan påvise at det foreligger tvingende berettigede grunner:

- for behandling av personopplysninger som går foran den registrertes interesser, rettigheter og friheter, eller
- for å fastsette, gjøre gjeldende eller forsvare rettskrav.

Når en virksomhet velger å ta i bruk sosiale medier som kommunikasjonskanal, vil retten til protestere også gjelde for virksomhetens behandling av personopplysninger som skjer i kommunikasjonskanalen.

Hva betyr dette for Oslo kommune?
Det fremgår av GDPR art. 21 nr. 1 at den registrerte til enhver tid har rett til å protestere mot behandling av personopplysninger om seg som har grunnlag i blant annet GDPR art. 6 nr. 1 bokstav f (berettigede interesse).

Den registrertes rett til å protestere knytter seg til selve behandlingen av sine opplysninger, i motsetning til rett til innsyn, retting og sletting hvor den registrertes rett knytter seg til de konkrete personopplysningene. Virksomheten skal ikke lenger behandle personopplysninger med mindre virksomheten kan påvise at det foreligger tungtveiende grunner som går foran en protest.

Under denne rettigheten kan virksomheten vurdere:

- Er det etablert gode rutiner for å håndtere protest mot behandling av personopplysningene fra den registrerte?
- Er det lagt til rette for at den registrerte alltid kan protestere dersom formålet med personopplysningene er direkte eller tilpasset markedsføring?

Tiltak:

- Etablere rutiner for hvordan virksomheten skal gå frem ved protest fra innbyggeren.

8 Risikovurderinger

Før behandlingen av personopplysninger iverksettes, skal det gjøres en vurdering av personvernkonsekvenser. I Oslo kommune starter dette med utfylling av innledende personvernvurdering (IP), før virksomheten enten gjennomfører en personvernvurdering av lav/middels risiko (PLM) eller en personvernkonsekvensvurdering ved høy risiko (DPIA).

Som en del av personvernvurdering av lav/middels risiko (PLM) og personvernkonsekvensvurdering ved høy risiko (DPIA) må det gjennomføres en risikovurdering som omfatter:

- risiko knyttet til personvernprinsippene
- risiko knyttet til den registrertes rettigheter
- risiko knyttet til den registrertes friheter

I tillegg skal det gjennomføres en risikovurdering av personopplysningssikkerhetsrisiko. På felles intranett ligger det utfyllende informasjon om og maler for personvernvurderinger og risikovurdering.

Risikovurderingen gjelder primært for den delen av behandlingen som virksomheten er behandlingsansvarlig for, men det kan være hensiktsmessig og også se på den generelle behandlingen av personopplysninger i kommunikasjonskanalen.

Vurderingene som gjøres må dokumenteres, og det anbefales å bruke kommunens risikomatrise som følger som vedlegg til malene for personvernvurdering med lav/middels risiko (PLM) og personvernvurdering ved høy risiko (DPIA).

9 Andre vurderingsmomenter

9.1 Etiske og andre vurderinger

Et sentralt prinsipp i GDPR art. 5 bokstav a, er at behandlingen av personopplysninger skal foregå på en rettferdig måte. Selv om virksomhetenes behandling er vurdert å være rettferdig, kan det også være relevant å gjøre en overordnet etisk vurdering av om virksomheten skal være på den konkrete kommunikasjonsplattformen. Dette kan både handle om signaleffekten knyttet til om en står inne for behandlinger som eier av kanalen gjør, og det kan også handle om virksomheten utelukker eller forskjellsbehandler innbyggere.

Hva betyr dette for Oslo kommune?
For virksomhetene i kommunen innebærer dette i praksis at det må gjøres en selvstendig og konkret vurdering av den etiske siden ved bruken av den aktuelle kommunikasjonskanalen.

Relevante kontrollspørsmål eller vurderingsmomenter kan være:

- Vil bruk av kommunikasjonskanalen kunne innebære en urimelig forskjellsbehandling?
- Er det rimelig at målgruppen må ha en bruker på kommunikasjonsplattformen for å motta informasjonen, eller har de samme mulighetene for kommunikasjon andre steder?
- Finnes de samme mulighetene for de som ikke ønsker å være i sosiale medier?

- Skjer det en forskjellsbehandling, f.eks. at innbyggere får raskere informasjon, raskere svar osv. i kommunikasjonskanalen?
- Er det noe ved kommunikasjonskanalen generelt som innebærer en uforutsigbarhet for innbyggeren, eller urimelig behandling av deres personopplysninger?
- Deles personopplysninger virksomheten genererer med andre kommersielle aktører?
- Tjener evt. disse aktørene penger på innhold som virksomheten produserer?
- Kan eieren av kommunikasjonskanalen stå for holdninger virksomheten ikke står inne for, og som kan få betydning for virksomhetens omdømme?
- Ved at virksomheten bruker kommunikasjonskanalen, kan innbyggerne få inntrykk av kommunen går god for måten personopplysningene blir behandlet på generelt?
- Dersom Oslo kommune har liten grad av kontroll eller kunnskap knyttet til hvordan personopplysningene behandles i løsningen, er det riktig at virksomheten legger til rette for at innbyggere skal bruke tjenestene?
- Kan kommunikasjonskanalen som benyttes ha innhold som oppleves krenkende for innbyggere?
- Oppfyller virksomheten krav til tilgjengelighet eller universell utforming ved bruk av kommunikasjonskanalen?
- Oppfyller virksomheten krav til språkbruk (nynorsk), eller utelukkes fremmedspråklige som virksomheten har krav om å nå ut til?

9.2 Overføring til utlandet

De fleste aktørene som står bak ulike sosiale medier er utenlandske og befinner seg utenfor EU/EØS, og er ofte amerikanske eller kinesiske. Disse aktørene forholder seg derfor i liten grad til norsk eller europeisk personvernlovgivning. Dette utløser flere personvernrettslige problemstillinger.

Dersom det er en utenlandsk aktør som står bak det sosiale mediet virksomheten ønsker å ta i bruk, må virksomheten først finne ut om aktøren er hjemmehørende i EU/EØS eller om den tilhører et tredjeland. Innad i EU/EØS kan personopplysninger overføres fritt, da alle land i EU/EØS er underlagt det samme lovverket. For land utenfor EU/EØS gjelder ikke nødvendigvis tilsvarende strenge regler, og det kan innebære stor risiko å overføre personopplysninger til aktører i disse landene. Dersom aktøren tilhører et tredjeland som ikke er på EUs liste over godkjente land, er det et krav om at virksomheten har et gyldig overføringsgrunnlag. Kravet om gyldig overføringsgrunnlag gjelder fordi beskyttelsesnivået i disse landene ikke anses like høyt som i EU/EØS. Virksomheten må 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.

Dersom landet aktøren tilhører, er oppført på EU-kommisjonens liste over godkjente tredjeland, er det ikke behov for overføringsgrunnlag. At et land er oppført på listen over godkjente tredjeland, innebærer at EU-kommisjonen har vurdert beskyttelsesnivået til å være på samme nivå som for EU/EØS-landene. Det vil heller ikke være behov for å treffe ytterliggere tiltak.

Mer informasjon om overføring til tredjeland ligger på felles intranett, og vurderingsmomenter ved overføring til utlandet er en del av maler for PLM/DPIA med veileder.

Hva betyr dette for Oslo kommune?
For virksomhetene i kommunen innebærer dette i praksis at man må kontakte den aktuelle aktøren og be om informasjon om hvilke tiltak som er gjort for å sikre at personvernet er ivaretatt. Eksempel på slike tiltak kan være tekniske tiltak som kryptering, eller organisatoriske tiltak som internkontroll for virksomheten, selv om slik informasjon ofte er vanskelig å få fra selskapene som står bak de store sosiale mediene.

Det vil alltid innebære en risiko å overføre personopplysninger til et tredjeland. Det er også mye usikkerhet rundt overføring til utlandet etter Schrems II-dommen. Dette må virksomhetene særlig være oppmerksomme på og ta med i personvern- og risikovurderingene som gjøres før sosiale medier tas i bruk som kommunikasjonskanal.

Det er opp til hver enkelt virksomhet å forsikre seg om at det foreligger et gyldig overføringsgrunnlag før det skjer overføring av personopplysninger til tredjeland.

Dersom det er avklart at aktøren bak det sosiale mediet er utenlandsk kan virksomheter vurdere følgende punkter:

- Innebærer behandlingen av personopplysninger en overføring til utlandet og til et land utenfor EU/EØS?
- Hvis ja, har virksomheten kontrollert om landet er oppført på EU-kommisjonens liste over godkjente tredjeland?
- Dersom landet ikke er oppført på listen over godkjente tredjeland:
  - har virksomheten sikret at det finnes et gyldig overføringsgrunnlag for overføringen?
  - har virksomheten vurdert hvilke ytterligere tiltak som må iverksettes for å sikre samme beskyttelsesnivå som i EU/EØS?
  - har virksomheten kontrollert at aktøren bak det sosiale mediet har gitt nødvendige garantier?

9.3 Andre dokumentasjonskrav

Før virksomheten kan sette i gang behandling av personopplysninger på en kommunikasjonsplattform, stilles det krav til at behandlingen er dokumentert i virksomhetens behandlingsoversikt. Felles system for å dokumentere alle behandlinger av personopplysninger i Oslo kommune («Behandlingsoversikten») er tilgjengelig fra januar 2023. Veileder for behandlingsoversikt ligger på felles intranett for Oslo kommune.

10 Oppsummering

Følgende er en oppsummering av ovenstående vurdering og avsluttende bemerkninger:

- Virksomhetene må være bevisste på at det er flere regelverk i tillegg til personvernregelverket som kan komme til anvendelse ved bruk av sosiale medier, f. eks. arkivlova, offentleglova og forvaltningsloven.
- Før virksomhetene tar i bruk en kommunikasjonskanal bør det gjøres en innledende personvernvurdering (IP) og enten en personvernvurdering med lav/middels risiko (PLM) eller en personvernvurdering ved høy risiko (DPIA). Disse vurderingene må blant annet vise til hvordan den registrertes rettigheter og friheter ivaretas ved bruk av den aktuelle kommunikasjonskanal.
- For å sikre at alle plikter etter personvernlovgivningen etterleves, skal virksomheter som tar i bruk sosiale medier som kommunikasjonskanaler kartlegge ansvarsforholdene.
- Som behandlingsgrunnlag for bruk av sosiale medier i Oslo kommune kan virksomhetene vurdere følgende behandlingsgrunnlag i GDPR:
    a. utøvelse av offentlig myndighet som en kommune er pålagt (GDPR art. 6 nr. 1 bokstav e). Dette behandlingsgrunnlaget krever supplerende rettsgrunnlag i nasjonal rett.
    b. berettiget interesse (GDPR art. 6 nr. 1 bokstav f)

Virksomheten må sørge for at kravene i GDPR for bruk av disse behandlingsgrunnlagene er oppfylt.

• ▪ • ▪ • ▪ •

Vedlegg: Vurderingsmomenter ved bruk av sosiale medier (ikke en del av dette dokumentet)

Asker kommune

Vurdering av personvernkonsekvenser: **Asker kommunes side på Facebook**

2021/22

Asker kommune

Innhold

Vurdering av personvernkonsekvenser: Asker kommunes side på Facebook

1. Oppsummering

I kjølvannet av offentliggjøringen av Datatilsynets kritiske rapport – som i korte trekk sier at de ikke skal være på Facebook - oppstod det en offentlig debatt om hvorvidt andre aktører – og spesielt offentlige instanser- skal være på Facebook.

I Asker kommune etablerte vi raskt et tverrfaglig team, bestående av ressurser fra informasjonssikkerhet, personvern og kommunikasjon, for å vurdere om vi har en berettiget interesse av å bruke Facebook som kommunikasjonsplattform, og hvordan vi eventuelt kan være til stede på en forsvarlig måte som ivaretar personvernperspektivet.

Gjennom grundige vurderinger har teamet kommet frem til at vi fortsetter å bruke Facebook, men på en mer restriktiv og bevisst måte. Ved å iverksette tiltak som er egnet til å redusere risikoen for at innbyggerne ikke skal ha sine rettigheter i medhold av personvernregelverket i behold, mener vi at opprettholdelsen av Asker kommunes side på Facebook er lovlig og forsvarlig.

2. Innledning

Asker kommune legger som premiss at kommunens bruk av sosiale medier generelt, og Facebook (og Meta sine andre plattformer) spesielt, vil innebære behandling av personopplysninger. Dette betyr at vi er ansvarlig for at dette skjer i samsvar med personvernregelverket.

I de tilfellene hvor Asker kommune initierer en behandling av personopplysninger som innebærer en *høy risiko for de registrertes rettigheter og friheter* så er vi forpliktet til å gjennomføre en vurdering av personvernkonsekvenser i tråd med krav i personvernforordningen[1].

For vurderingen av hvorvidt bruken av Facebook innebærer en høy risiko for de registrertes rettigheter og friheter kan vi enten ta stilling til hvordan vår bruk samsvarer med kriteriene i

[1] Plikten til å gjennomføre en vurdering av personvernkonsekvenser følger av personvernforordningen artikkel 35. I den engelske utgaven av forordningen kalles prosessen for «data protection impact assessment, derav forkortelsen «DPIA» som mange omtaler den som.

personvernforordningen artikkel 35 nr. 1[2], eller ta stilling til om behandlingen faller innenfor noen av de behandlingene som Datatilsynet i sin liste over aktiviteter som alltid vil kreve en vurdering av personvernkonsekvenser[3].

Når det gjelder Datatilsynets liste så kan det ikke utelukkes at det å etablere en side på Facebook vil kunne falle inn under aktiviteten som er beskrevet som følger:

«Behandling av personopplysninger der formålet er å tilby en tjeneste eller utvikle produkter for kommersiell bruk som involverer å forutsi jobbprestasjoner, økonomi, helse, personlige preferanser eller interesser, pålitelighet, adferd, lokasjon eller bevegelsesmønster. (Særlige kategorier av personopplysninger eller svært personlige opplysninger og evaluering/poengsetting).»

Vi tenker oss at det da særlig er tale om å forutsi personlige preferanser og interesser i forbindelse med tjenestene «sideinnsikt» og «annonsering».

I tråd med Datatilsynets anbefaling om å gjøre en vurdering av personvernkonsekvenser i de tilfellene der det er usikkert om det er nødvendig, så gjør vi det fordi det er et nyttig verktøy for å sikre at personvernforordningen følges.

En vurdering av personvernkonsekvenser er en prosess ment for å beskrive aktiviteten som skal gjennomføres, vurdere om den er nødvendig og proporsjonal, og håndtere de risikoer som oppstår gjennom å vurdere dem og å finne tiltak egnet til å redusere risiko.

Vurderingen skal iht. GDPR art. 35 (7) minst inneholde:

a) en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen, herunder, dersom det er relevant, den berettigede interessen som forfølges av den behandlingsansvarlige

b) en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene

c) en vurdering av risikoene for de registrertes rettigheter og friheter

d) de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise at denne forordning

[2] Personvernforordningen artikkel 35 nr. 1 omtaler spesifikt «ny teknologi» og at det skal tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i.

[3] Se Datatilsynets hjemmesider på nett; https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/

overholdes, idet det tas hensyn til de registrertes og andre berørte personers rettigheter og berettigede interesser.

I det følgende vil vi beskrive Asker kommunes bruk av Facebook og gjøre en vurdering av personvernkonsekvensene av dette.

3. Systematisk beskrivelse av behandlingen

3.1 Hva skal beskrives

Det som skal beskrives er de planlagte behandlingsaktivitetene og formålene med dem, herunder den berettigede interessen som forfølges av den behandlingsansvarlige.

3.2 Formål

Asker kommune har siden 2010 hatt en side på Facebook som ble etablert som supplement til kommunens hovedinformasjonskanal, hjemmesiden asker.kommune.no.

Hovedformålet med Facebook-siden er å innfri vår lovfestede plikt til å aktivt informere våre innbyggere (kommuneloven paragraf 4-1), og sørge for at de både har og finner den informasjonen de skal.

3.3 Art, omfang og sammenheng

Art

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

Asker kommune bruker «like-», engasjements-, publiserings- og annonseringsfunksjonaliteten i Facebook, kommentarfelt, meldinger, «Sideinnsikt» og Meta Business Suite. Gjennom kommunikasjon på Facebook-siden behandles derfor personopplysninger når profiler (registrerte) «liker» eller engasjerer seg ved organiske og sponsede poster, ved arrangementer eller skriver kommentarer. I tillegg samler Facebook informasjon om den registrertes bruk av sidene (såkalt observert bruk), noe som danner grunnlaget for Facebook sin tjeneste «Sideinnsikt» og annonseplattform. Dette er nærmere beskrevet i Facebook sine retningslinjer for behandlingen av personopplysninger.

«Sideinnsikt» styres i sin helhet av Facebook, og resultatet presenteres for Asker kommune som aggregert statistikk om de registrertes bruk av Asker kommune sine Facebook-sider. Facebook sin beskrivelse av behandlingen er som følger:

«Sideinnsikt» er aggregert statistikk som lages på bakgrunn av et utvalg handlinger som gjøres av brukeren/profilen av Facebook. Handlinger logges av Facebook-serverne når folk samhandler med sider og innhold tilknyttet dem. Eksempler på handlinger er:

- visning av en side, et innlegg, en video, en historie eller annet innhold tilknyttet en side
- samhandling med en historie

- følge eller slutte å følge en side
- like eller slutte å like en side eller et innlegg
- anbefale en side i et innlegg eller en kommentar
- kommentere, dele eller reagere på et sideinnlegg (inkludert type reaksjon)
- skjule et sideinnlegg eller rapportere det som spam
- hold pekeren over en lenke til en side eller navnet eller profilbildet til en side for å se en forhåndsvisning av sidens innhold
- klikke på knappene for nettsted, telefonnummer, få veibeskrivelse eller en annen knapp på en side
- visning av en sides arrangement på skjermen, svar på et arrangement, deriblant type reaksjon, klikk på en lenke for arrangementsbilletter
- starte Messenger-kommunikasjon med siden
- se eller klikke på elementer i sidens butikk

Informasjon som dette om handlingen, personen som utfører handlingen, og nettleseren/appen som brukes:

- dato og tid for handlingen
- land/by (anslått fra IP-adresse eller importert fra brukerprofilen for innloggede brukere)
- språkkode (fra nettleserens http-topptekst og/eller språkinnstilling)
  alders-/kjønnsgruppe (fra brukerprofilen bare for innloggede brukere)
  tidligere besøkt nettsted (fra nettleserens http-topptekst)
- om handlingen ble utført fra en datamaskin eller mobilenhet (fra nettleserens brukeragent eller appegenskaper)
- FB-bruker-ID (bare for innloggede brukere)

Facebook bruker informasjonskapsler for å finne ut hvorvidt en person er en innlogget Facebook-bruker. Denne behandlingen er beskrevet i et dokument som heter «Retningslinjer for informasjonskapsler».

Det behandles personopplysninger også om personer som ikke er logget inn i Facebook. Om disse personene lagres det besøk på side, klikk på et bilde eller video i et innlegg for å se det.

Asker kommune har ikke tilgang til personopplysningene som behandles som en del av hendelsene, men bare til den aggregerte sideinnsikten. Hendelser som brukes til å opprette sideinnsikt, lagrer ikke IP-adresser, nettkapsel-ID-er eller andre identifikatorer som er knyttet til personer eller enhetene deres, men derimot FB-brukerID-en til personer som er logget inn på Facebook. Hendelsene som logges av Facebook for å opprette sideinnsikt, er helt og fullt definert av Facebook og kan ikke angis, endres eller på annen måte påvirkes av kommunen.

Oppsummert gir «Sideinnsikt» Asker kommune informasjon om hvor mange som har sett og respondert på innlegg/poster (rekkevidde og engasjement, hvem som har likt, delt og kommentert, hvordan brukerne reagerer på innlegg) demografiske data, og hvor mange som ser sidene, følger/liker sidene og slutter å følge/ slutter å like sidene. Asker kommune samler ikke inn ytterligere opplysninger via Facebook enn det som gjøres gjennom bruk av Sideinnsikt.

Omfang

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

Antall registrerte som omfattes av behandlingen avhenger av hvor mange som besøker og eventuelt samhandler med Asker kommunes sider. Pr mai 2022 har Asker kommune ca. 31 000 personer som følger siden, hvorav ca. halvparten er i primærmålgruppen fra 35-54 år. Totalt er det ca. 27 000 innbyggere som er i denne aldersgruppen i Asker, og ca. 15 000 av disse følger oss på Facebook. Dette betyr at vi har et potensiale til å nå en stor andel innbyggere via Facebook. I tillegg er det en høy andel av brukerne som bruker plattformen daglig.

Personopplysningene som behandles som følge av at Asker kommune har en side på Facebook er av ulik karakter. Den mest åpenbare behandlingen er at det er synlig hvem som har en interesse i å følge/like Asker kommune, hva og hvordan disse personene eventuelt har engasjert seg i, eksempelvis trykket «liker» på av innlegg, eventuelle kommentarer de skriver selv eller delinger.

Asker kommune har ingen intensjon om å samle inn særlige kategorier av personopplysninger, men vi kan ikke garantere at ikke de som følger oss selv publiserer informasjon om seg selv som direkte eller indirekte sier noe om helse, politisk oppfatning etc. Erfaringsmessig er ikke risikoen for dette høy. Asker kommune oppfordrer i «om-feltet» og i enkelte innlegg om at privat informasjon ikke skal deles. Kommunen har også etablert en moderatorrolle som skal følge med på aktiviteten på nettsidene og slette innlegg som er støtende eller avslører for mye om enkeltpersoner. Vi kan likevel ikke forhindre at denne informasjonen fanges opp av Facebook, og har ikke noen garanti for at informasjonen slettes hos dem.

Tjenesten «Sideinnsikt» samler demografisk informasjon om enkeltpersoner (kjønn, alder, bosted), hvilke innlegg vedkommende har sett, likt, mislikt, delt, samt informasjon lagt ut i kommentarfeltet. Denne behandlingen av personopplysninger er systematisk og kontinuerlig.

Asker kommune har en stor andel av sine innbyggere som følgere på Facebook, og omfanget i prosent kan dermed sies å være stort. Detaljgraden av informasjon om den enkelte følger vil avhenge av hvor aktiv den enkelte er med hensyn til å lese innlegg, like og kommentere/engasjere seg. Potensielt vil det være et visst omfang i informasjonen som samles, og ved å publisere saker som engasjerer vil omfanget øke.

På den annen side er den type informasjon som publiseres fra Asker kommune sin side av en slik karakter at informasjonen likevel vil være begrenset. Når kommunen bruker Facebook til å øke spredningen av informasjon er det hovedsakelig positivt vinklede saker som det høstes positive tilbakemeldinger på. Dersom kommunen skulle brukt Facebook til å skape engasjement rundt kontroversielle saker for å få treff og «likes» eller «dislikes» ville omfanget av privat og avslørende informasjon om den enkelte vært større.

Samlet sett mener vi at behandlingen av personopplysninger er moderat sammenlignet med hva plattformen har potensiale til å behandle.

Sammenheng

Med sammenhengen opplysningene behandles menes hva slags relasjon har man til personene det behandles opplysninger om, og hva slags forventninger de vil ha med hensyn til hvordan opplysningene om dem vil bli behandlet.

I en vurdering av personvernkonsekvenser er det viktig å tydeliggjøre sammenhengen 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 Facebook aktualiseres spørsmålet om ny eller innovativ teknologi. Dette fordi det er kjent at Facebook bruker og utvikler algoritmer for å analysere informasjon om brukerne, og for å stadig vinne ny innsikt om disse brukerne som kan være nyttig i et kommersielt perspektiv.

Facebook-sider, og tilhørende bruk av Sideinnsikt, har vært i bruk siden Facebooks oppstart i 2004, og nettsamfunnet har flere enn 1,7 milliarder aktive brukere hver måned på verdensbasis (juni 2016).

Tjenestene er dynamisk i sin natur, og personvernkonsekvensene ved bruk kan derfor utvikle seg over tid. Eksempler som bruk av Facebook for manipulering av valgene i USA og Myanmar er eksempler på uforutsette konsekvenser som også har hatt betydning for personvernet til befolkningen i disse områdene. Denne type hendelser har, sammen med påtrykk for endring fra EU, blant annet resultert i endring av tjenestevilkårene som følge av praksis fra EU-domstolen.

Erkjennelsen av at Facebook gjør bruk av kompleks teknologi gjør at vi må gjøre grundige og gode vurderinger med hensyn til hvorvidt vi kan si at behandlingen av personopplysninger som skjer ved å bruke Facebook-sider og Sideinnsikt er kjent for innbyggerne i Asker kommune som bruker Facebook.

Asker kommunes relasjon til brukerne er som leverandør av kommunale tjenester, og videreformidler av statlige og frivillige tjenester. Den typiske bruker av Asker kommunes Facebook-sider vil være en innbygger i kommunen i alderen 35-54 år.

Asker kommune erfarer at innbyggerne forventer at de får informasjon og kan nå kommunen via Facebook. Når en innbygger oppretter en Facebook-profil/bruker blir det innhentet et samtykke. Brukeren får også informasjon om Facebooks personvernerklæring, innstillinger og muligheter til å endre innstillinger. Dette er et forhold mellom brukeren og Facebook.

Vi legger til grunn at ingen brukere er på Facebook utelukkende for å kommunisere med Asker kommune. Å være på Facebook er heller ingen nødvendig betingelse for å kommunisere med kommunen, da informasjon alltid vil være tilgjengelig via andre kanaler i tillegg.

Det vi skal vurdere er den eventuelle negative personvernkonsekvensen av at kommunen har egne Facebook-sider, og den ytterligere behandling av brukernes personopplysninger som dette innebærer.

Kilden til informasjonen som samles inn via Facebook-sidene, sideinnsikt og annonseplattform er brukerne selv og det de foretar seg der, samt de analyser som Facebook gjør og presenterer for Asker kommune gjennom Sideinnsikt og annonseplattform. Et viktig unntak er hvis en bruker har blitt tagget av andre i et innlegg/story eller lignende. I et slikt tilfelle har ikke bruker samme mulighet til å styre kilden.

Til tross for den nevnte kompleksiteten mener vi at behandlingen av personopplysninger som skjer som konsekvens av Asker kommunes sider på Facebook er nokså forutsigbar for brukeren. Dette fordi at Facebook er en etablert kanal, den har eksistert i Norge siden 2007, over 82 % av innbyggere i Norge over 18 år har en Facebook profil, og 67% av disse brukerne bruker kanalen daglig (IPSOS SoMetracker Q1-22). Det er grunn til å tro at denne trenden også gjelder for innbyggere i Asker, og at den typiske Facebook-brukeren antas å ha kompetansen som skal til for å finne frem til den informasjonen som Facebook gjør tilgjengelig om behandlingen.

3.4 Informasjonssikkerhet

Informasjonssikkerheten ved behandlingen ivaretas i all hovedsak av Facebook, noe som også kommer frem av plattformen Meta Business Suite. Plattformen Meta Business Suite gir behandleransvarlig et samlet sted/tilgang til verktøy de trenger for å holde i organisasjonens/bedriftens tilstedeværelse på Meta sine kanaler (Facebook og Instagram). Som eksempel publisering og oppfølging av innlegg/stories/kommentarer/annonser, se aktivitet/innsikt, brukeradministrasjon og organisering av konto, informasjonssikkerhet, opplæring og testing, sårbarhetshåndtering og håndtering av sikkerhetshendelser.

Facebook overfører personopplysninger til egne datasentre både innenfor og utenfor EU/EØS. Overføringen av data mellom datasentrene skjer, ifølge Facebook, etter Standard Contractual Clauses med nødvendige tilpasninger i samsvar med Personvernrådets veiledning etter EU-domstolens *Schrems II*-dom.

Facebook sier at de årlig har en tredjepart SOC 2 type II-revisjon relatert til databehandlingstjenestene, og annen revisjon etter bransjestandard som anses passende av Facebook som del av Facebooks revisjonsprogrammer.

Asker kommune ivaretar informasjonssikkerheten for sin egen behandling, særlig gjennom, opplæring av ansatte med tjenstlig behov, samt tilgangsstyring når det gjelder muligheten for å administrere sidene. Målsettingen er at alle sider i regi av Asker kommune, altså undersider, skal inn i Meta Business Suite, med tilgangsstyring derfra.

3.5 Ansvarsforhold

Med ansvarsforhold menes hvilke aktører er involvert i behandlingen av personopplysninger og hvordan ansvarsforholdene er. Relevant informasjon her er hvilke

kilder man har til opplysningene, hvem som er mottagere, hvem som er behandlingsansvarlig, databehandler evt. delt behandlingsansvar.

Datatilsynet har i sin rapport skissert ansvarsforholdene mellom Facebook og en virksomhet som har en side på Facebook. Vi har i stor grad basert oss på de samme vurderingene med hensyn til fordeling av ansvar for de ulike aktivitetene. I dette ligger at vi aksepterer at det foreligger et felles ansvar mellom Facebook og Asker kommune når det gjelder de opplysningene som behandles som en konsekvens av at Asker kommune har en side på Facebook.

Felles behandlingsansvar oppstår når to eller flere behandlingsansvarlige «i fellesskap fastsetter formålene med og midlene for behandlingene»[4]. 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 gitt ut retningslinjer om behandlingsansvarlige og databehandlere. Der presiseres det at begge de behandlingsansvarlige har et overordnet ansvar for behandlingen i helhet, selv om de har fordelt ansvar 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/har ansvaret for[5].

I henhold til personvernforordningen artikkel 26 skal det være «en ordning» mellom partene. 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.

Asker kommune legger til grunn at det viktigste med den eventuelle ordningen 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 en tjeneste som innebærer et delt ansvar så er det ikke noe i art 26 som hindrer kommunen i å ta et større ansvar enn vår andel i tjenesten skulle tilsi. Det vil si at mer av informasjonsplikten faller på oss og at vi stekker oss langt for å opplyse våre innbyggere om hva som er de problematiske sidene ved Facebooks forretningsmodell, og f.eks. gi tips om hvordan man kan tilpasse sin bruk for å redusere risikoen for å bli profilert på en uheldig måte.

[4] Personvernforordningen artikkel 26

[5] EU-domstolens avgjørelse i C-210/16 Wirtschaftsakademie og EU-domstolens avgjørelse C-40/17 Fashion ID

Ved kombinasjonen av å ha en beskrivelse av behandlingsaktiviteten(e) som kommunen og Meta får felles behandlingsansvar for, Metas avtale om felles behandlingsansvar og Asker kommunes ekstra tiltak med hensyn til å informere innbyggerne om alle sider ved behandlingen av personopplysninger som en Facebook-side innebærer, mener vi at vilkårene i personvernforordningen artikkel 26 er oppfylt.

4. Nødvendighet og proporsjonalitet

Asker kommune mener at behandlingsgrunnlaget for å ta i bruk Facebook som kommunikasjonskanal er en interesseavveining i henhold til personvernforordningen artikkel 6 nr. 1 bokstav f.

Det er problematisert hvorvidt kommunen kan anvende dette rettslige grunnlaget overhodet da det følger av forordningen at dette rettslige grunnlaget ikke får anvendelse på en behandling *som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver.*

I forordningens fortalepunkt 47 finner vi noe veiledning med hensyn til begrunnelsen for denne begrensningen. Her står det at:

«Ettersom det er opp til lovgiveren ved lov å fastsette det rettslige grunnlaget for offentlige myndigheters behandling av personopplysninger, bør nevnte rettslige grunnlag ikke gjelde for behandling som offentlige myndigheter utfører i forbindelse med utførelse av de oppgavene de er tillagt.»

I forarbeidene til personopplysningsloven legger departementet til grunn at ettersom unntaket fra artikkel 6 nr. 1 bokstav f bare retter seg mot «offentlige myndigheter» og «deres oppgaver», så gjelder unntaket som utgangspunkt bare behandling av personopplysninger i forbindelse med utøvelse av offentlig myndighet.

Departementet legger videre til grunn at det offentlige følgelig må ha samme adgang som private behandlingsansvarlige til å benytte artikkel 6 nr. 1 bokstav f i for eksempel kommersiell virksomhet eller i egenskap av å være arbeidsgiver.

Departementet føyes dessuten til at rekkevidden av unntaket og de grensedragningsspørsmålene som oppstår, må få sin avklaring gjennom praksis.

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

Med dette skal Asker kommune kunne underbygge at behandlingen av personopplysninger som skjer ved at vi har en side på Facebook er nødvendig for å vareta en berettiget interesse som veier tyngre enn hensynet til den enkeltes personvern.

Asker kommunes 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.

I den sammenheng er det er viktig å presisere at Facebook ikke er en nødvendighet for kommunens informasjonsarbeid. Hovedkanal for kommunikasjon av viktig informasjon er kommunens hjemmeside (asker.kommune.no), førstelinje veiledning på telefon og e-post og selvsagt saksbehandlere og rådgivere tilhørende de enkelte tjenesteområdene. Facebook er kun et supplement til informasjonsformidling.

Det som imidlertid gjør Facebook til en unik plattform er evnen til å skape engasjement og sørge for rask og stor rekkevidde.

Datatilsynet har i sin interesseavveiing stilt spørsmålet; kan vi oppnå det samme uten Facebook, for eksempel ved å benytte oss av andre kommunikasjonskanaler? Dette har også Asker gjort.

Asker kommune har en overordnet kommunikasjonsstrategi, og også en delstrategi for bruk av sosiale medier. Disse strategiene sier noe om hvem vi treffer via Facebook, og viktigheten for oss i å komme i kontakt med nettopp disse. Følgende momenter er vektlagt i kommunikasjonsstrategien i vurderingen av bruk av Facebook:

- Som kommune har vi en informasjonsplikt som går utover det å passivt tilgjengeliggjøre informasjon. Vi skal aktivt informere om egen virksomhet, og virksomhet som utføres av andre aktører på vegne av kommunen. Vi skal også legge til rette for at alle kan få tilgang på informasjon. Dette er lovfestet og regulert gjennom kommuneloven paragraf 4-1.

- Kommunen skal legge til rette for lokaldemokrati, skape samfunnsengasjement med aktiv innbyggerdeltagelse.
- Kommunikasjon er avgjørende for å sikre at alle innbyggerne kjenner til, og har tilgang til informasjon om våre tjenester. Kommunen må derfor skaffe seg kunnskap om hvor innbyggere rent faktisk tilegner seg informasjon og tilpasse seg dette.
- En stor andel av våre innbyggere er brukere av Facebook.

Det å basere seg på det rettslige grunnlaget «berettiget interesse» forutsetter at man klarer å balansere interessen man har i å behandle personopplysningene mot de registrertes personopplysningsvern. Dette er en konkret avveiing som hver kommune må gjøre, men likt for alle kommuner er at personopplysningene ikke behandlers for kommersielle hensyn. Dette mener vi har betydning for balansetesten. Interessen vi har i å bruke enhver kommunikasjonskanal er å komme ut til innbyggerne med relevant informasjon.

Vi gjør dessuten tiltak for å ivareta personverninteressen – herunder dataminimeringstiltak ved å unngå funksjonalitet som legger til rette for høsting av informasjon fra tredjeparter, forsterkede informasjonstiltak for å gjøre våre følgere bevisst på de personvernrisikoene som eksisterer ved bruk av Facebook.

Samlet sett mener vi at vi har dekning i artikkel 6 nr. 1 bokstav f («berettiget interesse») for bruk av Facebook som kommunikasjonskanal.

5. Risiko for de registreres rettigheter

I en vurdering av personvernkonsekvenser er det særlig elementene av **medbestemmelse, åpenhet og forutsigbarhet** som skal sikres for de som er registrert. For å få til dette må v i evne å ta hensyn til hvilke rimelige forventninger våre innbyggere har til beskyttelse av sine personopplysninger.

Det er viktig å gå inn i prosessen med en grunnleggende respekt for innbyggernes rettigheter og friheter.

Når det gjelder **medbestemmelse** så er det viktig å erkjenne det faktum at brukere av Facebook mest sannsynlig ikke har full kontroll over de personopplysningene som tilfaller tjenesteleverandøren. På den annen side har det betydning at ingen trenger å være på Facebook for å motta viktig informasjon fra kommunen, og at de som er på Facebook og velger å følge kommunen har tatt et selvstendig valg om dette.

Videre kan manglene knyttet til rettigheter kompenseres ved å gi brukerne nok informasjon til å gjøre valg utfra sin situasjon, og samtidig legge til rette for at følgere kan justere sin bruk utfra det de vet om hvordan sosiale medier behandler informasjon om dem.

Når det gjelder **åpenhet** så er det viktig å erkjenne at informasjonen omkring hvordan enkelte sosiale medier sine algoritmer fungerer kan være utfordrende å kommunisere tydelig og forståelig.

På den annen side er verdt å merke seg at det har skjedd utvikling også i måten Facebook informerer og bevisstgjør om rettigheter (in-app informasjon knyttet til personverninnstillinger og hva som skjer når man utfører ulike handlinger, slik som liker en post, tagger noen etc.).

Det er også mulig for kommunen å kompensere mangelfull åpenhet fra Facebook med å ta mer av ansvaret for å informere våre brukere om de underliggende risikoene ved å bruke Facebook.

Når det gjelder **forutsigbarhet** så er det av relevans hvor godt kjent Facebook er blant befolkningen. Facebook har eksistert i snart 20 år. I den tiden har det også med jevne mellomrom vært diskusjoner omkring deres forretningsmodell, og det kan dermed være grunn til å tro at innbyggere får med seg slike diskusjoner og tar sine valg basert på dette.

For kommuner kan det også være relevant å vektlegge potensialet for involvering og lokaldemokrati som sosiale medier muliggjør. Kommunene har som samfunnsoppdrag å legge til rette for lokaldemokrati, og kan derfor vektlegge innbyggerkommunikasjon tyngre enn andre myndighetsorganer.

Prosessen for vurdering av personvernkonsekvenser er en nyttig øvelse for å gjøre kommuner mer bevisst med hensyn til personvernperspektivet, og det at kommunens tilstedeværelse på Facebook medfører risiko for brukers rettigheter. Vi må ta tak i dette ved å se på hvordan vi kan redusere risiko.

Asker kommune reduserer denne risikoen på følgende måter:

- Ved å ha en sentral redaksjon, som jobber med alt fra strategi, konsept-planer, publisering/administrasjon, rutiner, moderering av kommentarfelt, kursing, oppfølging og samarbeid med alle redaktører for Facebook-sider i regi av kommunen.
- Samle alle Facebook-sider og annonsekontoer i regi av kommunen i Meta Business Suite – en plattform som samler alle verktøy og gjør det mulig på et overordnet nivå å ha kontroll over sider etablert av ulike tjenesteområder.
- Pålegge multifaktor autentisering ved innlogging til brukerne i Meta Business Suite.
- Bevissthet omkring hvilke tema det publiseres informasjon om, og hvordan dette påvirker engasjement hos innbyggere.
- Bevissthet om balansegangen mellom kommunens behov og plikt til å informere om noe og personvernperspektivet..
- Bevissthet om *hvordan* vi velger å informere, format, vinkling, ordlyd og andre virkemidler
- Sørge for å ha rett beredskap for ulike type innhold – A, B, C – poster/kategorier.
- Styre publiseringene, og komme med anbefalinger for når ulike ting skal publiseres, og på hvilken måte.
- Tar en større del av ansvaret for å beskrive personvernkonsekvenser, håndtering av data og hva en bruker kan forvente ved å interagere med Facebook, ved å informere om dette i «om-oss» feltet i Facebook og ved å feste en post på toppen av egen side som tar opp dette temaet, og/eller lenker til en nettside med utdypende informasjon eller en erklæring.
- Gjøre konkrete vurderinger av hvilken funksjonalitet i Facebook som vi skal ta i bruk, med tanke på å minimere innsamlingen av personopplysninger. Eksempler her er Facebook pixel og speilpublikum.
- På sikt, involvere innbyggerne ved å spørre et utvalg av dem til råds ved bruk av Facebook/Meta/SoMe.

Personvernrådet har en veileder ute på høring som omhandler hvordan man kan oppdage og motvirke såkalte «dark patterns» ved sosiale media, som f.eks. manipulerende design[6]. Når denne veiledningen er endelig vil vi ta en ny vurdering av om det er flere tiltak vi kan iverksette for å sikre at innbyggerne i Asker har sine rettigheter i behold.

6. Konklusjon

I en prosess hvor vi skal gjøre en vurdering av personvernkonsekvenser er kunsten å få til å ta i betraktning den konkrete situasjonen til den registrerte i vurderingen av om behandlingen er forenelig med forordningens krav. Vi som kommune må ta hensyn til hvilke rimelige forventninger våre innbyggere har til beskyttelsen av sine personopplysninger, samt eventuell makt-ubalanse mellom innbyggerne og kommunen.

Vi har gått inn i prosessen med en grunnleggende respekt for innbyggernes rettigheter og friheter og sett på behandlingens bredere etiske problemstillinger som også er belyst i Datatilsynets rapport.

Vår konklusjon er:

For å innfri vår lovfestede plikt til å aktivt informere våre innbyggere, og sørge for at de både har og finner den informasjonen de skal, vil vi fortsette å bruke Facebook som informasjonskanal. Kanalen blir et supplement til hovedkanalen, hjemmesiden vår, og et verktøy for å nå raskt og bredt ut med informasjon til en stor andel av innbyggerne våre. Kanalen har vist seg svært effektivt i krisekommunikasjon, eksempelvis under koronaperioden, hvor vi hadde et behov for å raskt formidle nye tiltak og regler til innbyggere, skoler, medier og lokalsamfunnet generelt.

Allikevel, som belyst gjennom denne vurderingen, er det flere hensyn å ta når vi velger å være til stede på en plattform som Facebook - med de risikoene det medfølger. Vi må vekte informasjonsplikten opp mot personopplysningsvern og informasjonssikkerhet, og finne den riktige balansen. Bruken av plattformen skal administreres på en ansvarlig måte slik at vi ivaretar våre forpliktelser etter personvernregelverket.

Vi skal fremover bruke Facebook på en mer restriktiv og bevisst måte ved å iverksette risikoreduserende tiltak (nevnt tidligere). Videre bruk av kanalen forutsetter at det faktisk settes av de nødvendige ressursene til å følge opp de risikoreduserende tiltakene vi har identifisert.

Dette blir en kontinuerlig prosess, og vi må med jevne mellomrom ta en gjennomgang og evaluere risikobildet. Dette kan settes opp som en rutine i februar, hvor det tas et sporadisk utvalg stikkprøver rundt i organisasjonen.

Den samme prosessen vil måtte gjennomføres også for andre sosiale mediekanaler. Vi anbefaler at også fremtidige vurderinger av personvernkonsekvenser gjøres av en tverrfaglig gruppe slik at risikoer blir belyst fra ulike perspektiver.

7. Forankring av beslutningen i ledelsen

Den 2. juni 2022 presenterte personvernombud og digital kommunikasjonsrådgiver vurderingen av personvernkonsekvenser av kommunens bruk av Facebook i organisasjonsdirektørens ledergruppe, og fikk tilslutning til arbeidet og konklusjonen. En slik forankring og støtte fra ledelsen er avgjørende for at kommunen kan fortsette å være på Facebook.

Foto: Charles Deluvio

Etiske vurderinger ved bruk av sosiale medier

Hvorfor er vi opptatt av at vi må vurdere de etiske sidene ved å ta i bruk sosiale medier? I omtalen av Shoshana Zuboffs bok «Overvåkningskapitalismens tidsalder» beskrives en del av utfordringsbildet som følger:

«Med sine «gratis» tjenester har giganter som Google og Facebook gitt oss et tilbud vi ikke kunne takke nei til. Til gjengjeld forsyner de seg med enorme mengder data om vår oppførsel og preferanser, som de ganske uforstyrret selger videre til høystbydende. Det er dette Shoshana Zuboff kaller overvåkningskapitalisme, et fenomen som truer med å omforme samfunnet like mye som den industrielle revolusjonen gjorde på 1800-tallet. I overvåkningskapitalismens tid er vi ikke bare konsumenter, vi utgjør selve råvaren. Den skjulte og stadig mer sofistikerte bruken av dataene om oss bidrar ikke bare til å gi oss skreddersydd innhold og reklame. Den er blitt et verktøy til å forutsi og påvirke vår atferd, både som kunder, borgere og som velgere.»

En organisasjon som vurderer å være en aktør i sosiale medier står overfor valget mellom å lansere en profil i ett eller flere sosiale medier eller å la være. Organisasjonen står dermed i en valgsituasjon. Et dilemma er en situasjon hvor du står overfor to relevante alternativer som har mer eller mindre samme moralske eller etiske verdi (Kvalnes, 2020, s.7). Når vi befinner oss i en situasjon hvor vi har identifisert to relevante alternativer må vi begrunne valget av det ene alternativet fremfor det andre.

I et velfungerende samfunn lar mennesker seg styre utenfra gjennom lover, regler og sanksjoner. Vi mennesker har også frihet i en rekke forhold og her lar vi oss styre innenfra gjennom etisk refleksjon og holdninger. Vi bruker gjerne uttrykket moral når vi snakker om holdninger og vår oppfatning av hva som er rett og galt. Vi bør kunne begrunne våre valg gjennom etisk refleksjon. For å kunne gjøre dette må vi ha en forståelse av innholdet i begrepene etikk og moral.

Øverenget (2013) beskriver forskjellen mellom etikk og moral på følgende måte:

> *Moral handler om de oppfatningene mennesker har om rett og galt, om karaktertrekk, idealer, holdninger og handlingsmønstre – om hvordan vi faktisk er mot hverandre, og hva vi faktisk gjør. Etikk dreier seg om å reflektere over disse oppfatningene for å finne frem til hva man bør gjøre. Etikk handler om å forsøke å begrunne sine oppfatninger på en saklig måte.*

Oppfatningen av hva som er moralsk kan variere fra samfunn til samfunn, mellom regioner, selskaper, offentlige organisasjoner, foreninger og familier for å nevne noen.

I det følgende presenteres et eksempel på et dilemma, som vil bli benyttet under presentasjonen av Navigasjonshjulet. Dilemmaet er hentet fra tunnel eksempelet Kvalnes presenterer i boken Digital Dilemmas (2020), men historien er tilpasset for å gjøre den mer relevant for kommunesektoren.

Eksempelsituasjon

I Solvik kommune skal det bygges et kombinert kommunehus og kultursenter. Kommunedirektøren er opptatt av åpenhet og ønsker at både innbyggere og ansatte skal kunne følge med i den pågående byggeprosessen. Byggeleder har derfor fått i oppgave å ta bilder underveis i byggeprosessen. Bildene oversendes sammen med en kort tekst til Kari i HR avdelingen, som publisere saker på kommunens kommunikasjonsplattformer og i sosiale medier. Kari ser gjennom sakene før de publiseres, men på grunn av høy arbeidsbelastning har hun lite tid til å arbeide med sakene før publisering. På slutten av dagen mottar Kari et bilde fra byggeleder med teksten «Endelig er stillasene oppe». Kari ser kjapt på den mottatte saken og legger den ut på kommunens Facebook-profil.

Morgenen etter sjekker Kari som vanlig profilene kommunen har i ulike sosial medier. Hun oppdager en rekke sinte kommentarer om HMS avvik på kommunens byggeplass. Byggeleder er også blitt oppmerksom på det som skjer i sakens kommentarfelt og har følgelig sett på saken med «nye» øyne. Det viser seg at bildet avdekker et klart brudd på HMS rutinene. På bildet kan en se to usikrede montører som monterer opp det øverste nivået i det seks etasjes høye stillaset. Byggelederen er bekymret for at saken vil føre til negativ publisitet rundt byggeprosjektet og ha en negativ innvirkning på kommunens omdømme. Hun ber derfor Kari om å slette saken umiddelbart.

Kari er usikker på om det er klokt å bare slette saken eller om de først bør gi en begrunnelse for hvorfor de har besluttet å fjerne saken, for deretter å slette den. Byggeleder insisterer imidlertid på at saken skal slettes og Kari velger å følge å følge byggeleders ønske og sletter saken.

I denne situasjonen tar Kari en avgjørelse basert på en rask og impulsive vurdering - det Kahneman (2013) kaller system 1 tenkning. Etisk refleksjon er en saktere og mer analytisk tankeprosess – det Kahneman (2013) benevner som system 2 tenkning. Dialogen i sosiale medier går raskt. I en pågående dialog vil det være begrenset tid til etisk refleksjon (system 2) og mange av beslutningene baserer seg på raske og impulsive beslutninger (system 1). Når man står i en situasjon hvor beslutningene må tas veldig raskt, vil forberedelser i forkant og evaluering av håndteringen i etterkant føre til en bedre håndtering av den aktuelle situasjon.

Navigasjonshjulet

Navigasjonshjulet (Kvalnes, 2017) som presenteres nedenfor er et hjelpemiddel som kan benyttes ved etisk refleksjon når en står overfor ulike dilemma. Navigasjonshjulet guider oss gjennom ulike tema av relevans for en beslutning basert på etisk refleksjon. Det er ingen regel for hvor en skal starte i navigasjonshjulet. (Kvalnes, 2020.) Refleksjon rundt de ulike temaene og spørsmål i Navigasjonshjulet skal guide oss frem til en helhetsvurdering vi kan begrunne vår beslutning med.

Jus – Er det lovlig?

Kari står overfor valget mellom å slette saken uten videre bemerkninger eller å responder på kommentarene før sletting. Begge de to handlingsalternativene er juridisk akseptable. Dersom et av alternativene hadde vært ulovlig ville dette i seg selv være grunnlag for å avstå fra handlingen, men om et handlingsalternativ er lovlig vil ikke dette alene kunne begrunne valget av ett av handlingsalternativene. Enkeltindividers moraloppfatning samsvarer ikke alltid med gjeldende rett eller med en organisasjons verdier. Arbeidstakeren skylder imidlertid uansett sin arbeidsgiver å overholde reglene.

Selv om en handling er lovlig, kan den allikevel anes å være kritikkverdig. Foreligger det f.eks. en skult agenda. Dersom Kari velger å slette saken uten å respondere på kommentarene, kan omgivelsene oppfatte dette som et forøk på å skjule HMS avvikene. Dersom Kari i stedet velger å respondere før hun sletter saken og forklarer at bedriften sletter saken da de ikke aksepterer avvikene som har funnet sted vil slettingen kunne oppfattes mindre kritikkverdig.

Identitet – Er det i samsvar med våre verdier?

Under dette punktet skal en vurdere om de ulike handlingsalternativene er i tråd med organisasjonens kjerneverdier og eventuelle profesjonsverdier. Åpenhet, sannferdig, gjennomsiktighet, tillitsvekkende, fleksibel er eksempler på kjerneverdier en organisasjon kan ha besluttet å følge og som i så fall vil være retningsgivende når en står overfor valget mellom to mulige alternativer. Kjerneverdier det er besluttet at en skal følge kan komme til uttrykk i overordnede planer, prinsipper, organisasjonspolitikken med videre. I vårt eksempel har vi ikke informasjon om organisasjonenes verdier, men om en av verdiene er gjennomsiktighet vil dette klart trekke i retning av at Kari bør respondere før hun sletter saken.

Moral – Er det riktig?

Moral er som nevnt et uttrykk for våre oppfatninger og holdninger. Hvordan vi oppfatter skillet mellom rett og galt. Dette er oppfatninger som er innebygd i mennesket og formet gjennom påvirkning fra omgivelsene. Det vil også ofte finnes en felles oppfatning av hva som er rett og galt i en organisasjon. Under dette punktet reflekterer vi dermed over egne holdninger og oppfatninger av hva som er rett og galt og hvilken felles oppfatning av rett og galt som er etablert i organisasjonen, profesjonen eller regionen osv.

Dersom Kari sletter saken uten videre kommentar, vil det bli oppfattet som moralsk akseptabelt?

Omdømme – Beholder vi vår troverdighet?

Hvordan vil ulike interessenter respondere på handlingen dersom de blir kjent med den? Hvis beslutningen blir kjent, er vi da villig til å forsvare den offentlig? Hva om pressen får kjennskap til beslutningen? Vil vi være bekvemme med at vår historie ender opp som ett førstesideoppslag i Aftenposten, VG eller Dagbladet?

Dersom eventuell offentlighet rundt beslutningen føles ubehagelig, kan dette være tegn på at en står i fare for å ta en uklok beslutning og derfor bør foreta en revurdering.

I eksemplet vårt vet Kari at beslutningen om å slette saken vil bli kjent blant flere av interessentene på Facebook. Hvordan vil de oppfatte en beslutning om å slette saken uten videre kommentar? HMS avvik er alvorlig og i dette tilfellet kan avviket i verste fall føre til fatale konsekvenser for montørene. Dersom Kari sletter saken uten å kommentere på alvoret knyttet til denne type avvik, vil interessentene i så fall oppfatte situasjonen dithen at kommunen ikke tar avvikene på alvor eller forsøker å legge lokk på alvorlige avvik?

I en situasjon hvor beslutningene må tas i raskt tempo, kan det være vanskelig å hensynta alle mulige utfall. Det kan derfor være fornuftig å gjennomføre en debrifing i etterkant for å legge til rette for gode beslutninger i fremtiden.

Økonomi – Lønner det seg?

Ulike handlingsalternativer kan sette økonomiske vurderinger opp mot etiske. Vi kan tenke oss at en av kommunens kjerneverdier er at all databehandling skal skje på en så sikker måte som overhodet mulig. Kommunen har vurdert to ulike it-systemer, hvorav det ene kommer med en vesentlig lavere kostnad enn det andre. Sikkerhetsmessig tilfredsstiller begge systemer minimumskravene til sikkerhet, men systemet med den høyeste kostnaden kommer med den ypperste informasjonssikkerhets-løsningen som er tilgjengelig. Kommunen har dårlig økonomi og økonomien er forverret som følge av investeringen i nytt kommunehus. I dette tilfellet oppstår det et dilemma mellom kommunens økonomiske situasjon og kjerneverdien om at all databehandling skal skje på en så sikker måte som overhodet mulig.

I vårt gjennomgående eksempel om avsløring av HMS avvik på byggeplassen, er ikke økonomi videre relevant som vurderingstema. I et slikt tilfellet vil en bare kunne konstatere at temaet ikke relevant for valg av handlingsalternativ og hoppe videre til neste vurderingstema i navigasjonshjulet.

Etikk – Lar det seg begrunne?

Her vil fokuset rettes mot samtlige dimensjoner i navigasjonshjulet, og vi vurdere her spenningen som oppstår mellom to eller flere av spørsmålene i hjulet. Målet er å komme frem til rasjonelle begrunnelser for våre valg og prioriteringer. (Kvalnes, 2017.) Når du benytter navigasjonshjulet har du som beslutningstaker et verktøy som hjelper deg i din analyse av mulige handlingsalternativer, samt med å holde oversikt over hensyn av betydning for beslutningen. Under punktet etikk vurderes alternativene opp mot de ulike spørsmålene i navigasjonshjulet og ulike hensyn veies opp mot hverandre. Vi ønsker å finne ut hvem som berøres av de ulike alternativene, hvordan disse berøres, hvor sannsynlig det er at utfallet blir slik eller slik og hvilke hensyn som taler for og imot de ulike alternativene. (Kvalnes, 2017.)

De ulike alternativene vurderes også i forhold til etisk teori. Det foretas en sammenlignende analyse av tilgjengelige alternativer ut fra et utilitaristisk og pliktetisk perspektiv, samt likebehandlingsprinsippet og offentlighetsprinsippet.

Ifølge utilitarismen, som senere er videreutviklet i konsekvensetikken, er en handling «moralsk riktig å utføre hvis den fører til de beste samlede konsekvensene for de berørte partene, sammenlignet med mulige alternativer. (Kvalnes 2017, s. 53.)

Utfordringen med konsekvensetikken er at den kun legger vekt på utfallet og at dette er viktigere enn å handle rett. Det negative ved en handling kan etter denne teorien oppveies av det samlede utbytte for flertallet, dvs. at en kan ofre enkeltindividet dersom dette gir størst nytte for flertallet. Vi må følgelig også vurdere alternativene i forhold til pliktetikken.

Pliktetikken prioriterer riktig oppførsel og handling foran resultatet. Ifølge pliktetikken er hensyn som menneskeverd, respekt og integritet viktigere en å velge handlingen som gir størst mulig nytte.

Alternativene vurderes også i forhold til likhetsprinsippet. Likhetsprinsippet handler om å behandle like tilfeller likt og at tilfeller hvor det foreligger relevante forskjeller vil kunne kreve ulik behandling.

Offentlighetsprinsippet handler som nevnt om vår villighet til å forvare våre beslutninger offentlig. Se ovenfor under omdømme.

Eksempler på dilemmaer ved bruk av sosiale medier

I boken «Digital Dilemmas – Exploring Social Media Ethics in Organizations» (2020) presenterer Øyvind Kvalnes ulike dilemmaer som er relevante for aktører i sosiale medier. Nedenfor er det hentet inn en oversikt fra ovennevnte bok over de dilemmaene Kvalnes har identifiser gjennom sin forskning. Boken er tilgjengelig som en open access bok og lisensiert med Creative Commons Attribution 4.0, se referanseliste nedenfor.

Eksempel på ulike dilemmaer en vil stå overfor som aktør i ulike sosiale medier.

Role dilemmas	Who is the agent in social media? Professional, employee, friend, owner, politician, private individual or more than one of these at the same time?
Tempo dilemmas	What kind of information and opinions do we spread with the touch of a finger? What do we miss out on if we slow down and are more thoughtful?
Integrity dilemmas	To what extent should we downplay our own principles and values to gain or keep friends, followers and clients and get more likes?
Speech dilemmas	What kinds of opinions is it acceptable to express in social media? Where do we draw the line of free speech in the processes of expressing disagreement and defending ourselves against what we perceive to be unreasonable criticism?
Competence dilemmas	To what extent is it acceptable for professionals to exploit the gaps in social media competence in their own favor?

Kvalnes, 2020.

Kahneman, D. (2011). Thinking Fast and Slow. Farrar, Straus and Giroux, 1. utgave 2011.

Kvalnes, Ø. (2017). Se Gorillaen, Etikk i arbeid. Universitetsforlaget, 3. utgave 2017.

Kvalnes, Ø. (2020). Digital Dilemmas, Exploring Social Media Ethics in Organizations. Palgrave MacMillan. https://doi.org/10.1007/978-3-030-45927-7 Http://creativecommons.org/licenses/by/4.0/

Øverenget, E. (2013). Helstøpt. H. Aschehoug & Co. W. Nygaard), Oslo

Foto: Brooke Cagle

Vurderingsmomenter ved bruk av sosiale medier

Denne tabellen er utarbeidet i sammenheng med «Personvern ved bruk av sosiale medier – En Juridisk vurdering med veiledning om virksomheters bruk av sosiale medier i Oslo kommune»

Tabellen kan brukes ved gjennomføring av personvernvurderinger (inkl. DPIA).

Områder	**Vurderingsmomenter**
Behandlingsansvar	
	• Har kommunen eller virksomheten innflytelse på behandlingen som skjer i kommunikasjonskanalen, eller må avtalevilkårene aksepteres uten mulighet for endring? • Er det inngått en avtale om felles behandlingsansvar med eier/leverandør av kommunikasjonskanalen? • For hvilke deler av tjenesten er virksomhetene å betrakte som behandlingsansvarlig, og er dette klart for virksomheten? Fremgår det noe om dette i tjenesteavtalen mellom virksomheten og eier/leverandør av sosiale medier?
Behandlingsgrunnlag **(disse er kun eksempler)**	
Utøvelse av offentlig myndighet	
Berettiget interesse	• Hvorfor skal virksomheten behandle opplysningene i kommunikasjonskanalen? • Hvor viktig er det å behandle opplysningene gjennom bruk av en kommunikasjonskanal? • Hva skjer hvis virksomheten lar være å bruke kommunikasjonskanalen? • Er behandlingen av personopplysninger i kommunikasjonskanalen uetisk på noen måte? **Nærmere om nødvendighet** • Er det mulig å oppnå det samme formålet uten å ta i bruk kommunikasjonskanalen?

	• Er det mulig å oppnå formålet på en mindre inngripende måte? **<u>Nærmere om interesseavveining</u>** • Er det mulig for innbyggeren å protestere på hele eller deler av behandlingen før den starter? • Er det valgfrihet knyttet til ulike behandlinger i kommunikasjonskanalen? • Regner innbyggeren med at deres personopplysninger blir behandlet av virksomheten ved å ta i bruk kommunikasjonskanalen? • Vil innbyggeren ha fordeler av at virksomheten tar i bruk kommunikasjonskanalen? • Er behandlingen som skjer i kommunikasjonskanalen i innbyggerens interesse? • Har virksomheten og innbyggeren samme interesse i å ta kommunikasjonskanalen i bruk? • Er det et gjensidig forhold mellom virksomheten og innbyggeren? • Gir virksomheten god informasjon til innbyggeren om behandlingen? • Er det enkelt for innbyggeren å kontakte virksomheten for å kontrollere behandlingen? Svarer virksomheten ja på spørsmål nedenfor, er det i virksomhetens disfavør i avveiningen: • Vil innbyggeren bli overrasket over virksomhetens behandling av sine opplysninger i kommunikasjonskanalen? • Vil innbyggeren kunne oppfatte behandlingen som negativ? • Kan innbyggeren oppfatte behandlingen som upassende – basert på forholdet mellom virksomheten og innbyggeren? • Vil det bli behandlet mange personopplysninger om innbyggeren? • Vil behandlingen av personopplysninger i kommunikasjonskanalen være av sensitiv art?
Prinsipper	
Lovlighet	• Finnes det et rettslig grunnlag for den planlagte behandlingen av personopplysningene?

	• Er det skille mellom hvilke opplysninger som er nødvendig å behandle for å levere tjenesten, og hvilke andre opplysninger det kan være valgfritt å oppgi for å få tilgang til utvidede tjenester?
Rettferdighet	• Gjøres behandlingen av personopplysningene i respekt for de registrertes interesser og rimelige forventninger? • Er behandlingen åpen og forståelig for de registrerte (den skal ikke foregå på fordekte eller manipulerende måter)? • Hva skjer med opplysningene som genereres ved å bruke virksomhetens del av kommunikasjonskanalen? • Genereres det ny informasjon som brukes til andre formål enn virksomhetens formål? • Hvem andre har tilgang til å bruke informasjonen som behandles av virksomhetene? • Er dataflyten kjent for virksomheten?
Åpenhet	• Er bruken av personopplysningene oversiktlig og forutsigbar for de opplysningene gjelder? • Har virksomheten funksjonalitet for å gi informasjon om hvilke opplysninger som behandles, hva de brukes til og mulighet for de registrerte til å gjøre seg kjent med sine rettigheter og hvordan de skal utøve disse? • Har virksomheten en personvernerklæring på virksomhetens nettsider med generell informasjon om hvordan virksomheten behandler personopplysninger?
Formålsbegrensning	• Er ethvert formål med behandling av personopplysninger identifisert og presist beskrevet for alle berørte? • Har formålet med behandlingen et rettslig grunnlag? • Hvis personopplysninger skal gjenbrukes, er behandlingen lovfestet eller er det innhentet nytt samtykke?
Dataminimering	• Er alle personopplysningene som behandles relevante og nødvendige for å realisere formålet med behandlingen? • Kan formålet med behandlingen med rimelighet oppfylles på annen måte enn å behandle personopplysninger? (I så fall skal det ikke innhentes personopplysninger). • Innhentes det personopplysninger om flere personer enn nødvendig? • Er det mulig for virksomheten å rette eller slette opplysninger, for eksempel hvis det blir registrert særlige kategorier av personopplysninger? • Kan slettingen i tilfelle oppleves som sensur, dersom kommentaren ikke inneholder personangrep, angir tredjepersoner eller er i strid med norsk lov?

Riktighet	• Er det iverksatt tiltak som sørger for at personopplysningene er korrekte og oppdaterte (f. eks. tekniske tiltak)? • Er det iverksatt tiltak som sikrer at personopplysninger som er uriktige med hensyn til formålene de behandles for, straks slettes eller korrigeres?
Lagringsbegrensning	• Gir kommunikasjonskanalen mulighet for at opplysninger skal slettes når formålet er oppnådd? Reguleres dette av kommunikasjonskanalens avtale med virksomheten og/eller med innbyggeren? • Dersom virksomheten mener at opplysningene skal slettes, men innbyggeren frivillig har lagt opplysningene inn, kan virksomheten faktisk slette, eller går dette på bekostning av ytringsfriheten?
Integritet og konfidensialitet	• Har virksomheten tiltak mot uautorisert utlevering og tilgang til personopplysninger? • Har virksomheten som standard å sørge for at personopplysninger ikke gjøres tilgjengelig for et ubegrenset antall mennesker uten den berørte personens medvirkning? • Har virksomheten tiltak for å sikre at systemene som behandler personopplysninger er robuste mot for eksempel sårbarheter, angrep og uhell?
Ansvarlighet	• Opptrer virksomheten proaktivt? • Har virksomheten etablert alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid? • Er det dokumentert at virksomheten faktisk opptrer i samsvar med reglene?
Den registrertes rettigheter	
Rett til informasjon	• Har virksomheten informert de registrerte om at det behandles personopplysninger om dem? • Har virksomheten informert om hva bruk av kommunikasjonskanalen innebærer for den registrerte? • Har virksomheten tilpasset informasjonen til målgruppen og tatt hensyn til at informasjonen eventuelt er rettet mot barn?
Rett til innsyn	• Er det bekreftet at eieren/leverandøren av kommunikasjonskanalen skal ivareta deler av retten til innsyn? Hvis ja, i hvilken grad?

	• Er det etablert rutiner for håndtering av krav om innsyn fra den registrerte? • Besvares et krav om innsyn i egne personopplysninger med informasjon om hvilke konkrete personopplysninger virksomheten behandler om den registrerte, hvordan personopplysningene om den registrerte behandles og hvor opplysningene er hentet fra? •
Rett til retting	• Er det bekreftet at eieren/leverandøren av kommunikasjonskanalen skal ivareta retten til retting? Hvis ja, i hvilken grad? • Er det etablert rutiner for håndtering av krav om retting fra den registrerte? • Er det lagt til rette for at den registrerte kan kreve at uriktige opplysninger om seg rettes og at den registrerte kan kreve at ufullstendige opplysninger om seg suppleres? •
Rett til sletting	• Er det bekreftet at eieren/leverandøren av kommunikasjonskanalen skal ivareta retten til sletting? Hvis ja, i hvilken grad? • Er det etablert rutiner for håndtering av krav om sletting? • Er det lagt til rette for at den registrerte kan kreve at personopplysninger om seg slettes? • Er det lagt til rette for at virksomheten sletter personopplysninger dersom det ikke lenger er et nødvendig grunnlag for å lagre opplysningene? •
Rett til å protestere	• Er det etablert gode rutiner for å håndtere protest mot behandling av personopplysningene fra den registrerte? • Er det lagt til rette for at den registrerte alltid kan protestere dersom formålet med personopplysningene er direkte eller tilpasset markedsføring? •
Friheter for den registrerte, etiske og andre vurderinger	
	• Vil bruk av kommunikasjonskanalen kunne innebære en urimelig forskjellsbehandling? • Er det rimelig at målgruppen må ha en bruker på kommunikasjonsplattformen for å motta informasjonen, eller har de samme mulighetene for kommunikasjon andre steder?

	• Finnes de samme mulighetene for de som ikke ønsker å være i sosiale medier? • Skjer det en forskjellsbehandling, f.eks. at innbyggere får raskere informasjon, raskere svar osv. i kommunikasjonskanalen? • Er det noe ved kommunikasjonskanalen generelt som innebærer en uforutsigbarhet for innbyggeren, eller urimelig behandling av deres personopplysninger? • Deles personopplysninger virksomheten genererer med andre kommersielle aktører? • Tjener evt. disse aktørene penger på innhold som virksomheten produserer? • Kan eieren av kommunikasjonskanalen stå for holdninger virksomheten ikke står inne for, og som kan få betydning for virksomhetens omdømme? • Ved at virksomheten bruker kommunikasjonskanalen, kan innbyggerne få inntrykk av kommunen går god for måten personopplysningene blir behandlet på generelt? • Dersom kommune har liten grad av kontroll eller kunnskap knyttet til hvordan personopplysningene behandles i løsningen, er det riktig at virksomheten legger til rette for at innbyggere skal bruke tjenestene? • Kan kommunikasjonskanalen som benyttes ha innhold som oppleves krenkende for innbyggere? • Oppfyller virksomheten krav til tilgjengelighet eller universell utforming ved bruk av kommunikasjonskanalen? • Oppfyller virksomheten krav til språkbruk (nynorsk), eller utelukkes fremmedspråklige som virksomheten har krav om å nå ut til?
Overføring til utlandet	

	• Innebærer behandlingen av personopplysninger en overføring til utlandet og til et land utenfor EU/EØS?
	• Hvis ja, har virksomheten kontrollert om landet er oppført på EU-kommisjonens liste over godkjente tredjeland?
	• Dersom landet ikke er oppført på listen over godkjente tredjeland:
	  ▪ Har virksomheten sikret at det finnes et gyldig overføringsgrunnlag for overføringen?
	  ▪ Har virksomheten vurdert hvilke ytterligere tiltak som må iverksettes for å sikre samme beskyttelsesnivå som i EU/EØS?
	  ▪ Har virksomheten kontrollert at aktøren bak det sosiale mediet har gitt nødvendige garantier?

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

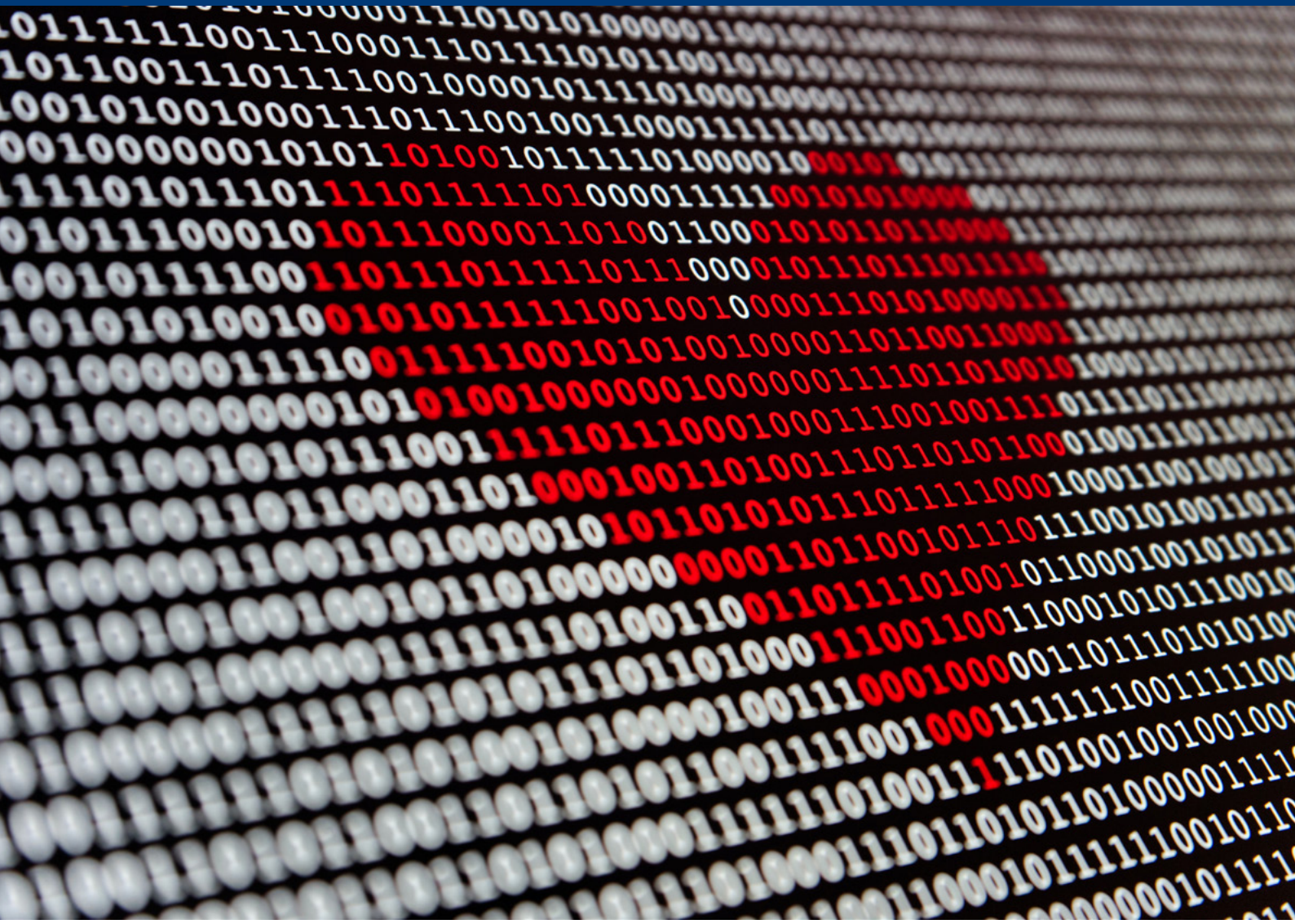

Foto: Xxxxxxxxxxxxx