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.

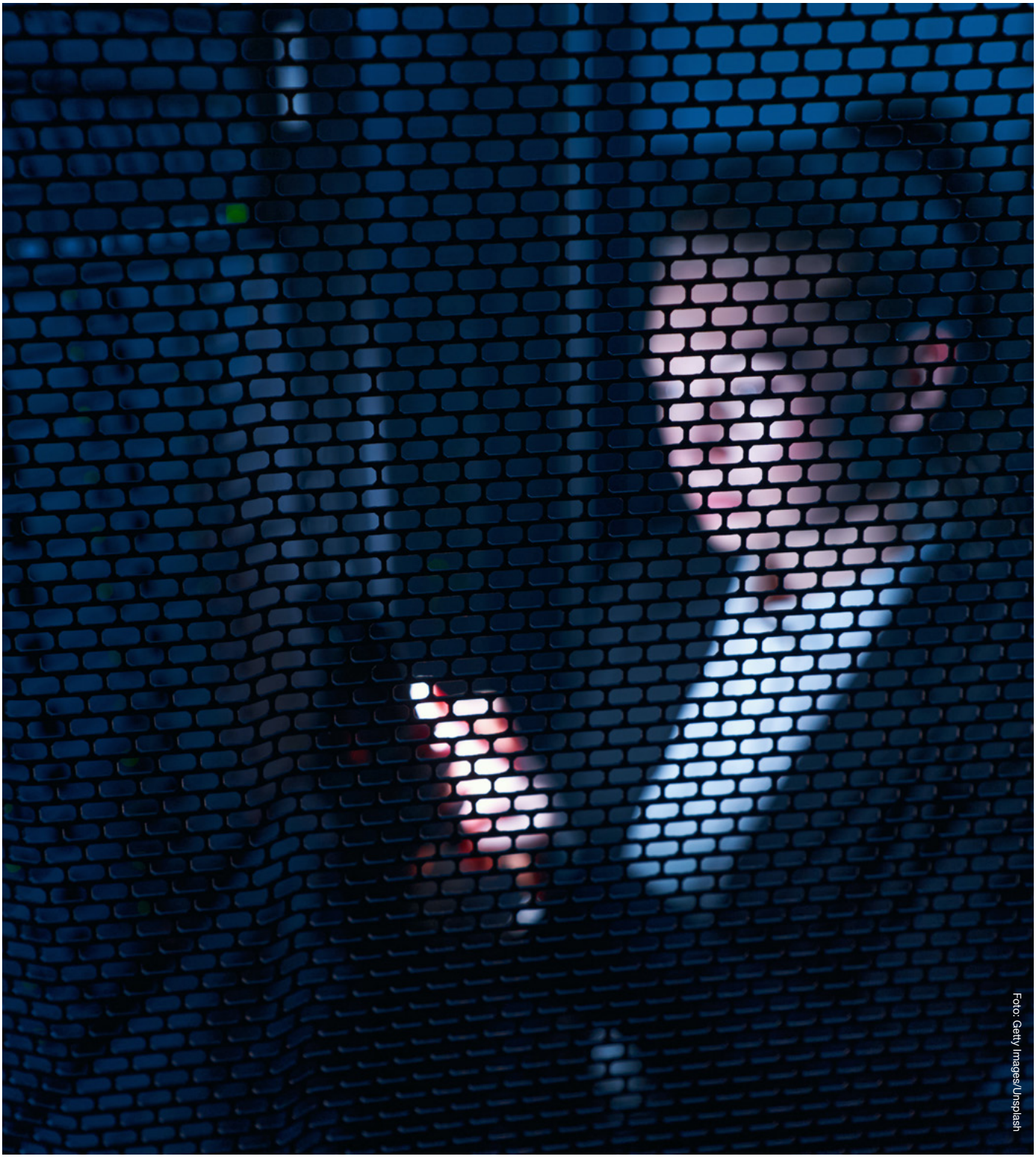

Foto: Getty Images/Unsplash

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.

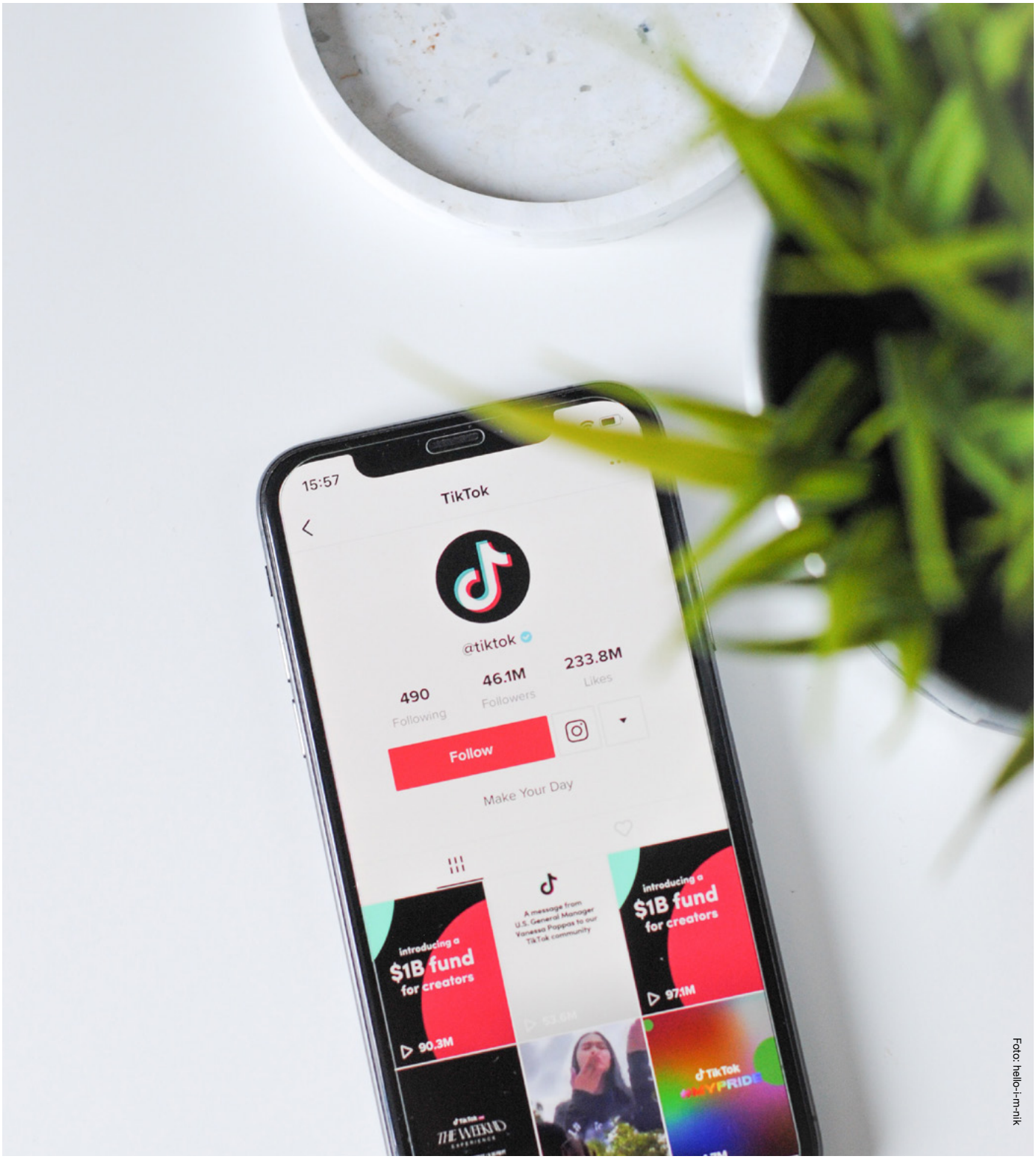

Foto: hello-i-m-nik


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.

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

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

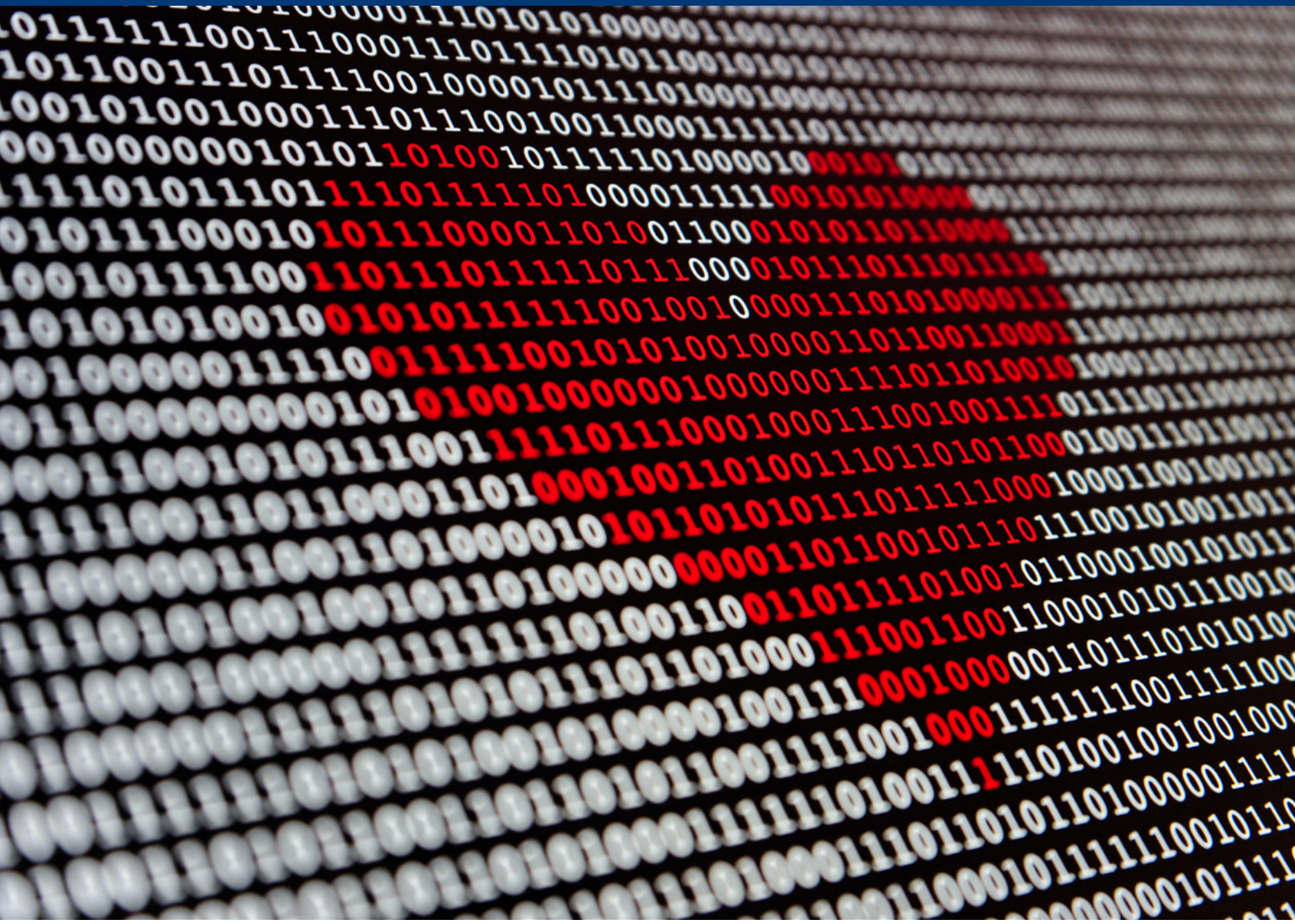

Foto: Xxxxxxxxxxxxx