

# Personvern ved bruk av sosiale medier



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

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

## Innhold

|           |                                                               |           |
|-----------|---------------------------------------------------------------|-----------|
| <b>1</b>  | <b>Innledning .....</b>                                       | <b>3</b>  |
| <b>2</b>  | <b>Problemstilling, formål og avgrensninger .....</b>         | <b>3</b>  |
| <b>3</b>  | <b>Relevant regelverk .....</b>                               | <b>4</b>  |
| 3.1       | Personvernregelverket .....                                   | 4         |
| 3.2       | Arkivlova .....                                               | 6         |
| 3.3       | Offentleglova .....                                           | 7         |
| 3.4       | Forvaltningsloven .....                                       | 8         |
| <b>4</b>  | <b>Behandlingsansvar .....</b>                                | <b>8</b>  |
| <b>5</b>  | <b>Behandlingsgrunnlag .....</b>                              | <b>11</b> |
| 5.1       | Utøvelse av offentlig myndighet som behandlingsgrunnlag ..... | 12        |
| 5.2       | Berettiget interesse som behandlingsgrunnlag .....            | 14        |
| <b>6</b>  | <b>De grunnleggende personvernprinsippene .....</b>           | <b>16</b> |
| 6.1       | Lovlighet, rettferdighet og åpenhet .....                     | 17        |
| 6.2       | Formålsbegrensning .....                                      | 19        |
| 6.3       | Dataminimering .....                                          | 19        |
| 6.4       | Riktighet .....                                               | 20        |
| 6.5       | Lagringsbegrensning .....                                     | 21        |
| 6.6       | Integritet og konfidensialitet .....                          | 21        |
| 6.7       | Ansvarlighet .....                                            | 22        |
| <b>7</b>  | <b>Ivaretagelse av de registrertes rettigheter .....</b>      | <b>23</b> |
| 7.1       | Rett til informasjon .....                                    | 23        |
| 7.2       | Rett til innsyn .....                                         | 24        |
| 7.3       | Rett til retting .....                                        | 24        |
| 7.4       | Rett til sletting .....                                       | 25        |
| 7.5       | Rett til å protestere .....                                   | 26        |
| <b>8</b>  | <b>Risikovurderinger .....</b>                                | <b>27</b> |
| <b>9</b>  | <b>Andre vurderingsmomenter .....</b>                         | <b>27</b> |
| 9.1       | Etiske og andre vurderinger .....                             | 27        |
| 9.2       | Overføring til utlandet .....                                 | 28        |
| 9.3       | Andre dokumentasjonskrav .....                                | 29        |
| <b>10</b> | <b>Oppsummering .....</b>                                     | <b>30</b> |

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](mailto: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 adresseres 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 personvern vurderinger som er påkrevd å gjennomføre i Oslo kommune ved all behandling av personopplysninger (Innledende personvern vurdering (IP), Personvernkonsekvensvurdering ved lav/middel risiko (PLM) eller Personvernkonsekvensvurdering ved høy risiko (DPIA)). Denne vurderingen erstatter ikke disse personvern vurderingene.

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 personvern vurderinger.

## 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 verdi 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 offentliglova<sup>1</sup>.

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

---

<sup>1</sup>[https://www.regjeringen.no/contentassets/3a11886db3604e9d9a049e872564467d/rettleiar\\_offentleglova.pdf](https://www.regjeringen.no/contentassets/3a11886db3604e9d9a049e872564467d/rettleiar_offentleglova.pdf)

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 regnes 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, rettfærdig 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 personvern vurderingene (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 behandlingsansvarlige 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.

Interesseavveilingen 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 tilføy egnede tiltak slik som å begrense 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:

- ▶ Opptre 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 opptre i samsvar med reglene?

Tiltak:

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

## 7 Ivaretagelse 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 ivaretagelse 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 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?

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 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?

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 virksomheten 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 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?

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 personvern vurdering (IP), før virksomheten enten gjennomfører en personvern vurdering av lav/middels risiko (PLM) eller en personvernkonsekvensvurdering ved høy risiko (DPIA).

Som en del av personvern vurdering 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 personvern vurderinger 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 personvern vurdering med lav/middels risiko (PLM) og personvern vurdering ved høy risiko (DPIA).

## 9 Andre vurderingsmomenter

### 9.1 Etske 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 ytterligere 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)