

Praktiske retningslinjer for bruk av sosiale medier



Dette dokumentet skal gi ansatte og ledere i Oslo kommune praktiske retningslinjer og faglige råd for bruk av sosiale medier.

Praktiske retningslinjer ved bruk av sosiale medier

Dette dokumentet skal gi ansatte og ledere i Oslo kommune praktiske retningslinjer og faglige råd for bruk av sosiale medier. Virksomheter i Oslo kommune kan ha ulike behov og ulikt utgangspunkt for å vurdere bruk av sosiale medier. Virksomhetene må selv gjøre de nødvendige vurderingene i forhold til denne behandlingen, for eksempel personvern vurderinger og risiko- og sårbarhetsanalyse (ROS).

Det anbefales å sette seg inn i og bruke disse retningslinjene sammen med dokumentet «Personvern ved virksomheters bruk av sosiale medier i Oslo kommune – en juridisk vurdering med veiledning».

Med sosiale medier menes nettsider og apper som brukes som en plattform til å skape, dele og viderele innhold, i tillegg til at det tilrettelegges for samhandling i sosiale nettverk. Sosiale medier leveres av eksterne og gjerne internasjonale leverandører.

1 Om formålsbeskrivelse

Virksomheten må ha et spesifikt, uttrykkelig angitt og berettiget formål med all sin behandling av personopplysninger i sosiale medier, og virksomhetens formål må dekke den behandlingen av personopplysninger de planlegger å bruke det sosiale mediet til. Virksomheten må vurdere formålet før sosiale medier tas i bruk.

Virksomheten må ha oversikt over egne formål og leverandørens formål, blant annet som et ledd i å avklare behandlingsansvaret. Virksomheten må også finne ut hvem leverandøren deler personopplysninger med, slik at personopplysningene ikke behandles til ulovlige formål.

2 Behandlingsgrunnlag

Virksomheten må ha et behandlingsgrunnlag for all sin behandling av personopplysninger i sosiale medier. Virksomheten må finne ut hvilket behandlingsgrunnlag leverandøren har. For en beskrivelse av hvilke behandlingsgrunnlag som vanligvis brukes i denne sammenheng, se juridisk vurdering.

3 Personvern vurderinger

Det skal alltid gjennomføres personvern vurderinger før virksomheten behandler personopplysninger i sosiale medier. Dette innebærer alltid en innledende personvern vurdering (IP) og i tillegg enten personvern vurdering ved lav/middels risiko (PLM) eller personvern vurdering ved høy risiko (DPIA). Se maler for personvern vurderinger og veileder.

Virksomheten må gjøre personvern vurderinger av all sin planlagte bruk av sosiale medier, og må avklare hvilke behandlinger de må gjøre personvern vurderinger av.

4 Behandling av særlige kategorier av personopplysninger

Det er i utgangspunktet forbudt å behandle særlige kategorier personopplysninger (f. eks helseopplysninger), og behandling av denne typen personopplysninger krever et særskilt behandlingsgrunnlag.

Virksomhetene må derfor sørge for å ha på plass tiltak som sikrer at de ikke samler inn særlige kategorier personopplysninger, og må ha rutiner som ivaretar sletting hvis det likevel skjer.

5 Spesielle utfordringer knyttet til prinsipper for behandling av personopplysninger

Prinsippet om dataminimering

Virksomhetene må ha tiltak på plass som ivaretar kravet til dataminimering, dvs. at det ikke samles inn flere personopplysninger enn det som er relevant og nødvendig for formålet. Virksomhetene bør sørge for at det ikke samles inn overskuddsinformasjon.

Prinsippet om lagringsbegrensning

Virksomheten må ha kontroll på at personopplysninger ikke lagres lenger enn til formålet med behandlingen er oppnådd. Se også rett til sletting nedenfor.

Prinsippet om ansvarlighet

Bruk av sosiale medier vil vanligvis innebære at virksomheten blir felles behandlingsansvarlig med leverandøren for deler av behandlingen som skjer. Virksomheten 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. Dette er blant annet nødvendig for å vite ansvarsfordelingen, hvem som skal gjennomføre personvern vurderinger og hvem som skal ivareta øvrige plikter etter regelverket. Virksomheten må også følge opp hvis det skjer endringer som påvirker den registrertes personvern eller avtaleforholdet mellom de behandlingsansvarlige.

6 Spesielle utfordringer knyttet til den registrertes rettigheter

Rett til informasjon

Virksomheten må gi den registrerte informasjon tilpasset brukergruppen, og informasjonen bør inneholde en tydelig ramme for behandlingen og hvordan den

registrerte kan utøve sine rettigheter. Vanligvis vil det ikke være tilstrekkelig å henvise til leverandørens personvernerklæring.

Når leverandøren gjør oppdateringer som påvirker den registrertes personvern, må virksomheten sørge for at informasjon til den registrerte oppdateres, f. eks i personvernerklæringen.

Rett til sletting

Virksomhetene må undersøke om leverandøren ivaretar kravet til sletting.

Virksomheten må i tillegg selv ha rutiner for sletting. I sosiale medier vil virksomheten og leverandøren behandle de samme personopplysningene for ulike formål, og det kan dermed være ulike frister for sletting som den registrerte bør informeres om.

Retten til å protestere

Virksomhetene må sørge for å ha rutiner for ivareta den registrertes rett til å protestere mot behandlingen, særlig når behandlingen igangsettes uten den registrertes medvirkning.

7 Dokumentasjon

Virksomhetene må ha følgende dokumentasjon:

- Personvern vurderinger og ROS
- Databehandleravtaler (hvis relevant)
- Involvering av Personvernombudet dersom det er snakk om DPIA:
- Ledelsesinvolvering og forankring
- Registrering i virksomhetens behandlingsoversikt

8 Overføring til utlandet

Mange leverandører av sosiale medier er aktører i tredjeland. I slike tilfeller vil behandling av personopplysninger i sosiale medier medføre overføring av personopplysninger til tredjeland, noe som gir økt risiko for personvernet og virksomhetene. Virksomheten må være særlig oppmerksom på at det kan være behov for DPIA.

Dersom det viser seg at personopplysninger overføres til utlandet i forbindelse med bruk av sosiale medier, må det sikres følgende:

- Det finnes nødvendig overføringsgrunnlaget
- Det finnes ytterligere tiltak dersom det er snakk om overføring til tredjeland (land utenfor EU/EØS)
- Ledelsesinvolvering og forankring

9 Andre forhold

Personverninnstillinger

Virksomheten bør bruke de mest personvernvennlige innstillinger som tilbys i sosiale medier.

Avtaleforhold

Virksomheten må sette seg inn i avtalen med leverandøren, dette gjelder også bruksvilkårene eller avtalen leverandøren har med den registrerte. Dette er nødvendig for å kartlegge risikoen for bruken av det sosiale mediet.

Relevante dokumenter:

- ▶ Personvern ved virksomheters bruk av sosiale medier i Oslo kommune – En Juridisk vurdering med veiledning, FIN/ISI.