

Vurderingsmomenter ved bruk av sosiale medier

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

Tabellen kan brukes ved gjennomføring av personvern vurderinger (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? <u>Nærmere om nødvendighet</u> - 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?