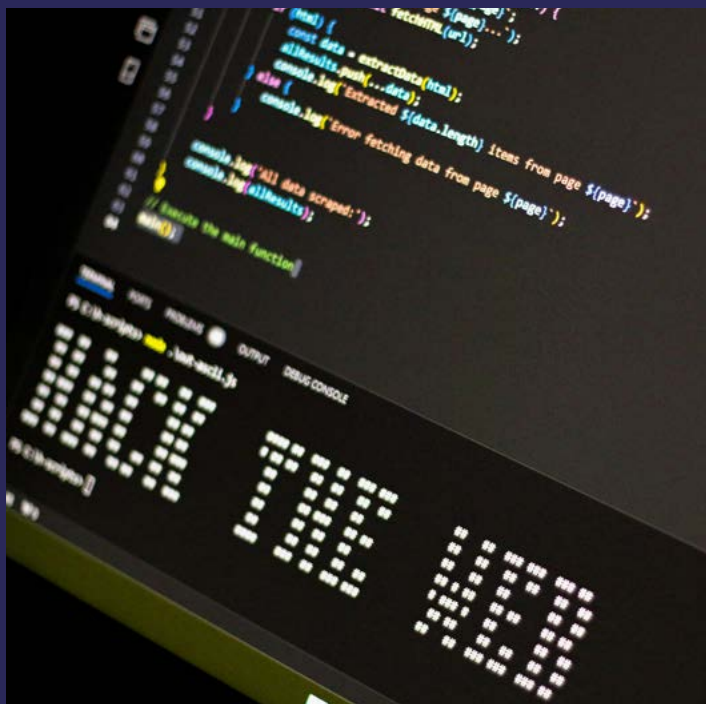




Oslo

Der unge er bør også kommunalt ansatte være

Digitalt feltarbeid, kartlegging og observasjon



SALTO

SAMMEN LAGER VI ET TRYGT OSLO

1 Vurderinger i forkant av kommunens tilstedeværelse på nett

I tillegg til å sette seg inn i relevante lovverk er det flere vurderinger som må gjøres i forkant av tilstedeværelse på nett. En av vurderingene er tilknyttet personopplysningsloven.

Personvern vurderinger

Den kommunale virksomheten er ansvarlig (se boksen om «Behandlingsansvar» under) for at behandlingen av personopplysninger i tilstedeværelsen på nett etterlever personopplysningsloven (Kommunesektorens Organisasjon, 2022). Hver bydel har ansatt en personvern - og informasjonskoordinator som kan kontaktes for råd og veiledning. I forkant av tilstedeværelse på gamingplattformer og behandling av personopplysninger må virksomheten derfor gjennomføre vurderinger av personvern, også når det er usikkert om det er nødvendig. Vurderingene kan bidra til at virksomheten kan dokumentere at den etterlever personopplysningsloven (Kommunesektorens Organisasjon, 2022).

Behandlingsansvar

En behandlingsansvarlig er ethvert organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger, samt hvilke midler som skal benyttes.

Det er ofte leverandørene av plattformene som har behandlingsansvar for store deler av behandlingen, basert på egne formål. Virksomhetene vil imidlertid etter avtale med leverandørene kunne ta i bruk plattformene for egne formål. Ettersom at formålene ofte innebærer behandling av personopplysninger, medfører dette at også virksomhetene har behandlingsansvar.

Den behandlingsansvarlige har ansvar for at:

1. Behandlingen av personopplysninger etterlever personopplysningsloven.

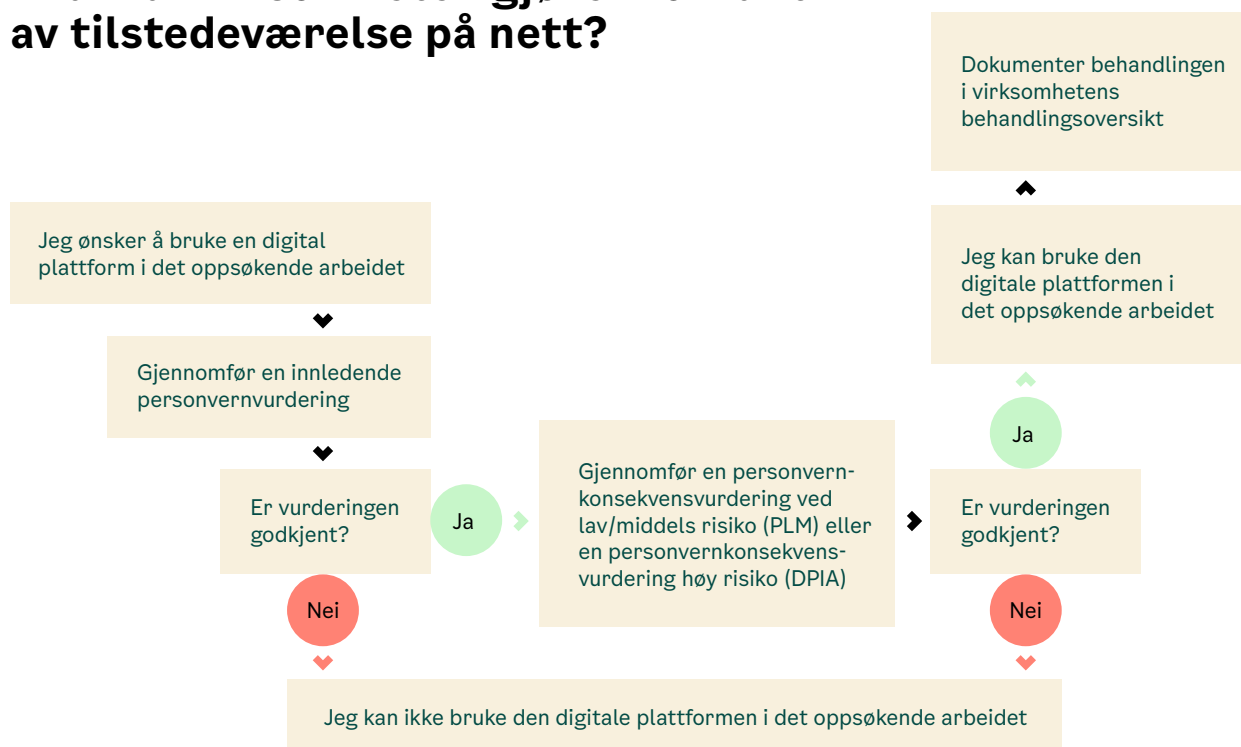
Det er den behandlingsansvarlige som har det overordnede ansvaret for at behandlingen etterlever personopplysningsloven, herunder personvernprinsipper og de registrertes rettigheter.

2. Behandlingen av personopplysninger har et behandlingsgrunnlag.

Det er den behandlingsansvarlige som har ansvaret for at behandlingen har et behandlingsgrunnlag. For oppsøkende arbeid på digitale plattformer er det særlig to aktuelle behandlingsgrunnlag, henholdsvis utøvelse av offentlig myndighet og berettiget interesse.

Dersom leverandøren av plattformen tilhører et land utenfor EU/EØS som ikke er på EU's liste over godkjente land, må virksomheten i tillegg til et behandlingsgrunnlag også ha et overføringsgrunnlag. Virksomheten bør også forsikre seg om at det ikke finnes lover eller praksiser i det aktuelle landet som til tross for et overføringsgrunnlag vil medføre at personvernloven ikke etterleves i praksis.

Hva må virksomheten gjøre i forkant av tilstedeværelse på nett?



Modellen er utarbeidet etter inspirasjon fra [modellen til KS \(som du finner på denne lenken\)](#).

Først må virksomheten gjennomføre en [Innledende personvern-vurdering \(IP\)](#). Vurderingen kartlegger informasjon om en behandling av personopplysninger, og vurderer på bakgrunn av informasjonen risikoen for den registrerte som virksomheten behandler opplysninger om. Risikovurderingen omfatter risiko knyttet til [personvernprinsippene](#) og den registrertes [rettigheter](#) (Kommune-sektorens Organisasjon, 2022).

Vurderingen av personvernkonsekvenser bør gjennomføres av en gruppe personer med ulike fagbakgrunn. I spørsmål som omhandler sosiale medie- og gamingplattformer kan ansatte i kommunikasjonsfaget vært nyttige samarbeidspartnere.



På bakgrunn av risikovurderingen i en Innledende personvern vurdering (IP), må virksomheten gjennomføre en [Personvernkonsekvensvurdering ved lav/middel risiko \(PLM\)](#) eller en [Personvernkonsekvensvurdering ved høy risiko \(DPIA\)](#).

Antakelig vil tilstedeværelse på nett medføre en høy risiko for personvernprinsipper og rettigheter, men virksomheten må likevel vurdere hvert enkelt tilfelle konkret. Risikoen kan nemlig tenkes å variere mellom de ulike måtene å være til stede på nett (Kommunesektorens Organisasjon, 2022). Dersom det er behov for råd og veiledning med utfylling av DPIA kan bydelens personvern og informasjonsskordinator kontaktes.

En vurdering av personvernkonsekvenser (enten en PLM eller en DPIA), og konklusjonen av denne vurderingen, skal forankres i ledelsen i den kommunale virksomheten. Det vil si at ledelsen beslutter og begrunner ett av de følgende alternativene:

1. **Godkjenning.** Vurderingen av personvernkonsekvenser er godkjent. Virksomheten kan ta i bruk digitale plattformer i oppsøkende arbeid på nett.
2. **Betinget godkjenning.** Vurderingen av personvernkonsekvenser godkjennes under forutsetning av følgende forbedringer... (beskriv forbedringene). Revidert vurdering av personvernkonsekvenser skal fremlegges for ledelsen på nytt.
3. **Ikke godkjent.** Vurderingen av personvernkonsekvenser er ikke godkjent. Virksomheten kan ikke ta i bruk digitale plattformer i oppsøkende arbeid på nett.

Før virksomheten kan behandle personopplysninger, må behandlingen dokumenteres i virksomhetens behandlingsoversikt (Kommunesektorens Organisasjon, 2022). Oslo kommune har et felles system (se [Behandlingsoversikten](#)) for å dokumentere alle behandlinger av personopplysninger.

Sikkerhet

Ved opprettelse av en sosial mediekonto bør virksomheten foreta grundige vurderinger knyttet til sikkerhet.

To-trinnsertifisering og sterke passord bør benyttes.

Anbefalinger for sikring av konto og passord kan eksempelvis finnes hos NSM¹ og Nettvett². Flere enheter kan som regel legges til med MFA (multi factor authentication) på samme bruker dersom det er behov for at flere personer har tilgang til brukeren. Generelt sett anbefales det å ikke dele fellespassord over «klare» kanaler, som Teams, E-post og lignende. Bruk av passordvelv³ eller andre krypterte kanaler anbefales.

[1] <https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord>

[2] <https://nettvett.no/passord/>

[3] <https://bitwarden.com/>

Ansettelse av ungdom for å produsere innhold på sosiale medier krever gode vurderinger

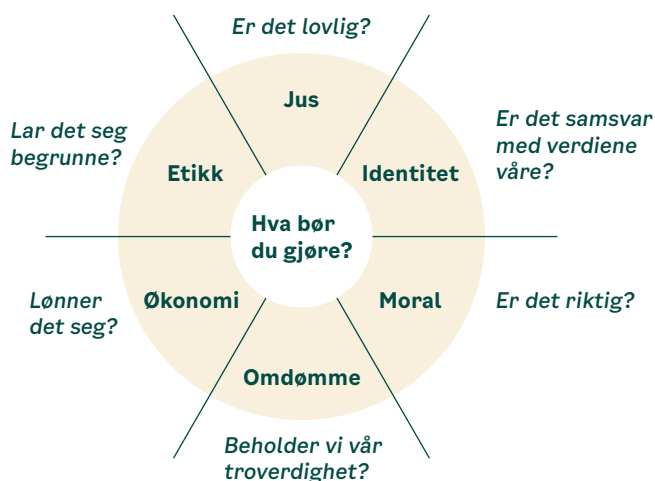
I Oslo kommune ansettes ungdom blant annet for å produsere innhold for de kommunale tjenestene. Det anbefales at det tas en grundig vurdering om deres tilgang til konto og innhold kan være en risiko for deling av taushetsbelagt informasjon. Det kan f.eks være at andre ungdommer/innbyggere tar kontakt via SOME. Det er vesentlig at det foretas vurderinger av dette i forkant. En ansatt i bydel bør ha det overordnede ansvaret for innholdsproduksjon, publisering og personvernmessige forhold dersom ungdom gis tilgang til publisering via SOME konto tilknyttet kommunen.



Etiske vurderinger

«Når kommunen vurderer å bli en aktør i sosiale medier, må en være bevisst på utfordringene og foreta en etisk vurdering av de ulike dilemmaene som oppstår ved eventuell tilstedeværelse i sosiale medier og alternativt om man skal la være. Dersom kommunen beslutter at en ønsker å være til stede på sosiale media-plattformer, bør kommunen også gjøre en vurdering av hvilke aktiviteter en ønsker å fremme på plattformen/bruke plattformen til» (KS -Veileder for sosiale medier kommunen).

Selv om vurderingen av personvernkonsekvenser er godkjent, kan det være relevant å gjennomføre en etisk vurdering av dilemmaene som likevel kan oppstå ved tilstedeværelse på digitale plattformer. Dersom tjenesten velger å ta i bruk sosiale medier bør det avsettes ressurser og tid i tjenestens etablerte struktur for å vurdere dette. Einar Øverenget og Øyvind Kvalnes (referert i Kommunesektorens Organisasjon, 2022) har utviklet et verktøy for å gjennomføre en slik etisk vurdering. Navigasjonshjulet består av seks ulike tema med tilhørende spørsmål, som kan veilede den kommunale virksomheten eller de kommunalt ansatte gjennom en etisk vurderingsprosess. Tanken er at dersom virksomheter eller ansatte står overfor et valg mellom ulike handlinger, vil temaene og spørsmålene kunne veilede dem til å foreta en beslutning som er basert på en gjennomvurdert begrunnelse.



Hvordan kan navigasjonshjulet brukes i praksis?

Utekontakten er ute og jobber oppsøkende i nærmiljøet. De møter en gruppe jenter som er kjent for dem fra tidligere. Jentene går på en videregående skole i bydelen. Praten går og temaet dreier over til festkultur og rus. «Slik er det overalt!» En av jentene viser frem en screenshot fra Instagram. Bildet ser ut til å være fra en fest. På et bord ligger det masse konanter og et knokjern ved siden av en hånd som med et bankkort skrapet sammen hvitt pulver til en «linje».

Utekontakten kan via screenshoten se brukernavnet på profilen. Brukeren har satt personverninnstillingene til «privat». Det er kun de vedkommende aksepterer som følgere som har tilgang til poster fra kontoen.

Situasjonen blir drøftet på utekontaktens teammøte. En av de ansatte mener man bør ta opp bildet på Instagram med brukeren som viser seg å være en ungdom i bydelen. En kollega er uenig. Hun argumenterer for at det er en privat konto og at de ikke kan vite hvem det er tatt bilde av.

Hva ville dere gjort i en slik situasjon sett opp mot navigasjonshjulet?

Målgruppe

Oppsøkende arbeid er en kontaktskapende og ressursformidlende sosial aktivitet som rettes mot grupper som ofte er vanskelig å nå med andre virkemidler. Nettet har et utvidet potensial i det oppsøkende arbeidet. I tillegg kan sosiale medier være viktig for å styrke informasjonsarbeidet ut mot innbyggere og øke oppslutningen om de tjenester kommunen tilbyr.

Formål og målgruppen for kommunal tilstedeværelse på nett er:

- › Informasjon om kommunens tjenestetilbud
- › Ungdom man søker å nå ved oppsøkende arbeid på gaten.
- › Ungdom som er lite ute i det offentlige rom, og som man derfor ikke når ved oppsøkende arbeid på gaten.

Rolle

Gjennom tilstedeværelse på nett kan kommunalt ansatte innta en mer eller mindre uformell rolle i møte med ungdom. Dette blant annet på grunn av fokuset på etablering av kontakt og relasjon med ungdom gjennom interaksjon på internett (se kapittel 2) «Kommunalt ansattes tilstedeværelse på nett». En uformell rolle kan skille seg fra politiets og nettpatruljens rolle, som gjennom forebyggende arbeid på nett er mer eller mindre formell. En uformell rolle kan tenkes å skape tillit hos ungdom, og med dette mulighet for å hjelpe og støtte målgruppen av ungdom med (forhøyet risiko for) sosiale og helsemessige utfordringer.

Tillit hos ungdom forutsetter at man er tydelig i rollen som kommunalt ansatt. Når man arbeider oppsøkende på gaten har den ansatte stort sett en tydelig rolle. Dette er ikke alltid tilfellet på nett. Ungdommene som oppholder seg mye på sosiale medie plattformer er ikke nødvendigvis vant til å møte på sosialarbeidere eller andre kommunalt ansatte på disse plattformene. Når man er til stede på nettet er det derfor viktig at man er tydelig i rollen som kommunalt ansatt.

Hvordan synliggjøre kommunalt ansatte sin rolle:

- › Ikke bruke private profiler.
- › Tydelig avsender: Bruke profiler med navn tilknyttet den kommunale virksomheten man representerer (for eksempel «Utekontakten Bydel XX»), og med kommunevåpen som profilbilde. På den måten signaliseres tydelig at man representerer en kommunal virksomhet.
- › Gjøre ungdom kjent med hvem man er, hvilke hensikter man har med arbeidet og ikke minst hvilke regler (herunder informasjon om for eksempel taushetsplikt, avvergingsplikt og opplysningsplikt) som ligger til grunn for arbeidet.
- › Synliggjøre hvem i virksomheten som er pålogget på den aktuelle plattformen, samt kontaktinformasjon til virksomheten.
- › Reflekter over hvordan man benytter emojis og memer i dialog med ungdomsmiljøet og hvordan det kan fortolkes av mottaker.
- › Legg inn autosvar ved henvendelser på chat/melding om åpningstider i tidsrom plattformen ikke er betjent med kontaktinformasjon til andre akutte tjenester.

Det har vært uroligheter i et ungdomsmiljø, og Elias og Eva i Utekontakten ønsker derfor innpass i miljøet. Elias og Eva legger ut en story på Snapchat-kontoen til Utekontakten. I storyen presenterer de seg selv som utekontakter. De forteller deretter at de har kjennskap til uroligheter i ungdomsmiljøet, og at de derfor vil være ekstra til stede både på nettet og på gaten fremover. Til slutt ber de ungdommene å ta kontakt med dem dersom de ønsker å snakke, og informerer i den sammenheng om taushetsplikten de har som utekontakter.

Tillit hos ungdom forutsetter også at kommunalt ansatte avklarer rollen sin med ungdommene. Det er viktig at ungdommene får komme med innspill om hvordan de ønsker at kommunalt ansatte skal være til stede på nett. Innspillene kan optimalisere arbeidet og fordi innspillene kan tilrettelegge for arbeidet og videre tillit mellom kommunalt ansatte og ungdom. Dialog med ungdommen vil kunne optimalisere det oppsøkende arbeidet ytterligere ved at tjenesten oppleves relevant og aktuell.

Plattform(er)

Det finnes mange plattformer å velge mellom når man skal informere ungdom om kommunens tjenestetilbud:

- › Finn ut hvilke(n) plattform(er) ungdommene er på.
- › Bestemmer seg for en plattform man ønsker å arbeide oppsøkende på (man kan arbeide på flere eller andre plattformer etter hvert).
- › Setter seg inn i plattformen, som for eksempel hvem som bruker den, hvordan den fungerer og ikke minst hvilke regler som finnes for bruk av den (dette er viktig for å vurdere om det er en plattform man kan arbeide oppsøkende på).

Forankring

Det er viktig at tilstedeværelse på nett ikke blir et personlig ansvar liggende utenfor den kommunale virksomhetens ordinære arbeid. Før virksomheten starter tilstedeværelsen på nett bør man:

- › **Forankre arbeidet**
Den kommunale virksomheten bør forankre arbeidet på nett hos nærmeste leder. Forankringen gir legitimiteten som er nødvendig for arbeidet.
- › **Involvere samarbeidspartnere i arbeidet**
Den kommunale virksomheten bør involvere samarbeidspartnere i det kommunens tilstedeværelse på nett. Ofte fører arbeidet til avdekking av behov for ulike tiltak, og økonomien og ansvaret for tiltakene kan være hos samarbeidspartnere. For å ansvarliggjøre samarbeidspartnere kan den kommunale virksomheten opprette en referansegruppe som møtes jevnlig. Da kan samarbeidspartnere få et større eierforhold til tilstedeværelsen på nett, og dermed et større ansvar for eventuelle tiltak.

Forankring er også viktig i andre deler av tilstedeværelsen på nett. Se kapittel 3 om «Vurderinger i forkant av kommunens tilstedeværelse på nett» for viktigheten av å forankre en vurdering av personvernkonsekvenser i ledelsen.

I forkant av tilstedeværelse på sosiale medie- og gamingplattformer og behandling av personopplysninger må virksomheten gjennomføre vurderinger av personvern, også når det er usikkert om det er nødvendig.



2 Kontaktetablering og relasjonsarbeid på nett

Kommunalt ansatte er dyktige på oppsøkende arbeid. Tilstedeværelse på nett har, som nevnt tidligere, mange likhetstrekk med tradisjonelt oppsøkende arbeid på gaten. Arbeidsmetodene er mer eller mindre de samme. Når man skal være til stede på nett, er det viktig at den kommunale virksomheten arbeider med å kartlegge hensiktsmessige plattformer for å nå ungdom i den respektive bydelen. Kjennskap til ungdomsmiljøene er viktig når man skal arbeide oppsøkende, både på gaten og på nettet (Oslo kommune, 2020). Veilederen anerkjenner kunnskapen som kommunalt ansatte har i arbeid med å etablere kontakt og relasjon med ungdom på disse plattformene. Den vil derfor ikke gå i dybden på de ulike arbeidsmetodene, men heller fokusere på de ulike utfordringene som kan oppstå i forbindelse med kommunal tilstedeværelse på nett.

Etablere kontakt med ungdom

Vurdering før kontaktetablering

Etter at bruk av sosiale medier er forankret i ledelsen og det gjennomført DPIA knyttet til den eller de plattformene som skal benyttes man har kartlagt plattformene, bør man foreta en vurdering knyttet til kontaktetablering.

Hvorvidt man skal forsøke å etablere kontakt med ungdom, avhenger av formålet med det oppsøkende arbeidet. Er målet å informere eller å kommunisere med ungdommene? Eller er målet å oppnå kontakt og en videre relasjon med ungdommene? Man bør også foreta en vurdering om forsøket på å etablere kontakt kan avskrekke eller provosere ungdommene (Oslo kommune, 2020).

Kontaktetablering

Når man skal forsøke å etablere kontakt med ungdom på nett, må man som på gaten prøve ut ulike fremgangsmåter. En av måtene er å være til stede over tid på de plattformene som ungdommer bruker. I tillegg til kjennskap til ungdomsmiljøene er også innpass i miljøene viktig når man skal arbeide oppsøkende. At de samme ansatte er til stede på de samme plattformene over tid, er derfor viktig for å etablere kontakt med ungdom på nett. Å gjøre den kommunale virksomheten kjent og tilgjengelig er nødvendig for å etablere kontakt med ungdom på nett. Dette kan for eksempel innebære en bevisst bruk av navn og logo som er tilknyttet den virksomheten eller bydelen man representerer (Oslo kommune, 2020).



Når man skal etablere kontakt med ungdom på nett, vil man bevege seg inn på en arena ungdommene kan oppfatte som «sin». Derfor vil det være hensiktsmessig å diskutere med ungdommene hva de synes om fremgangsmåten man har for å etablere kontakt. Da kan man få innspill som kan brukes for å bedre kontaktetableringen og dermed også den kommunale tilstedeværelsen på nett.



Man kan oppleve at man ikke klarer å etablere kontakt med ungdom, men likevel gjøre viktige observasjoner. Å beskrive det man observerer i et ungdomsmiljø, i dette tilfellet på en digital plattform, er også en viktig oppgave i det forebyggende arbeidet. Beskrivelsene kan brukes til å «ta pulsen» på ungdomsmiljøet (Oslo kommune, 2020). En viktig presisering er at kommunalt ansatte jobber i åpne kilder og sammenfatter kunnskap fra den informasjonen som ligger offentlig tilgjengelig på nettet.

Etablere relasjon med ungdom

Etter at man har etablert kontakt med ungdom, kan man bruke nettet til å vedlikeholde kontakten. Gjennom en videre og regelmessig kontakt med ungdom, kan kommunalt ansatte bli enda bedre kjent med ungdommene og dermed også bedre vurdere eventuelle hjelpetilbud.

Når man går fra en uregelmessig til en regelmessig kontakt med ungdommene, må man vurdere hvor denne kontakten skal foregå. Som kommunalt ansatt har man et ansvar for å ivareta ungdommenes personvern, se kapittel 3 og 7. Av den grunn bør man etterstrebe videre kontakt med ungdommene på fysiske heller enn på digitale arenaer. Som hovedregel bør ikke personsensitive opplysninger deles via sosiale medier.

Datatilsynet definerer personsensitive opplysninger som opplysninger knyttet til personnummer, etnisitet, seksuell legning, helseforhold, genetiske opplysninger mm. For uttømmende oversikt se: [Personopplysninger](#) | [Datatilsynet](#)

Utfordringer med tilstedeværelse på nett

Tilstedeværelse på nett, både ved kartlegging av ungdomsmiljøer og ved etablering av kontakt og relasjon med ungdommer, kan ha visse utfordringer. Det er viktig at offentlige ansatte er bevisst de utfordringer som ligger i oppsøkende arbeid på nett.

Anonymitet

Mulighet for anonymitet kan for mange ungdommer medføre lavere terskel for å etablere kontakt med kommunalt ansatte. Når det er sagt kan anonymitet også medføre flere utfordringer. Gjennom oppsøkende arbeid kan man få informasjon som bekymrer. Et eksempel kan være at du som kommunalt ansatt blir bekymret for en ungdom som på en av plattformene kommuniserer at han eller hun vil begå selvmord. Utfordringen oppstår dersom denne ungdommen er anonym, ettersom man da har få eller ingen opplysninger som kan identifisere vedkommende. Dersom man kommuniserer med en anonym ungdom og det fremkommer informasjon som innebærer akutt fare for liv eller helse, er politiet den aktøren man skal ta kontakt med. Politiet har større mulighet enn kommunalt ansatte til å identifisere og hjelpe ungdommen.

Usikkerhet rundt hvem vi snakker med

I forbindelse med anonymitet er det relevant å nevne at kommunalt ansatte aldri kan vite helt sikkert hvem de kommuniserer med på nett. Det samme er tilfellet for ungdommene. En mulighet for å sikre kommunikasjonen mellom partene, er at man avtaler et passord eller en kode som bare den kommunalt ansatte og den aktuelle ungdommen kjenner til. Da kan partene, i større grad, være sikre på at de kommuniserer med rett person.

Ikke dele sensitiv informasjon

En annen mulighet for å sikre kommunikasjonen mellom partene, er at man ikke deler sensitiv informasjon på nett. Kommunalt ansatte bør oppfordre ungdommene til det samme. Også når man er sikker på hvem man kommuniserer med, er det viktig at man ikke deler sensitiv informasjon. Dette fordi andre parter, som for eksempel eier av plattformene, kan få tilgang til den informasjonen som kommuniseres mellom den kommunalt ansatte og den aktuelle ungdommen.

Vurdering av informasjon

Nettet kan gi et feilaktig bilde av virkeligheten, og dermed også et feilaktig bilde av ungdom og ungdomsmiljøer. Fremveksten av kunstig intelligente systemer, som for eksempel ChatGPT, gjør at kommunalt ansatte bør være ekstra påpasselig på dette. Slike systemer kan overøse nettet med informasjon i form av eksempelvis bilder, videoer, lyd og tekst (Bogen, 2023).

Begrenset mulighet for digital deltakelse

Noen ungdommer opplever begrenset mulighet for digital deltakelse (se rapporten til Redd Barna for mer informasjon). Dette på grunn av barrierer som for eksempel dårlig tilgang på nett og digitale tjenester, manglende foreldrestøtte, mobbing og hatprat på nett samt levekår og boforhold (Redd Barna, 2022). Som følge av slike barrierer finnes det noen ungdommer man ikke vil nå gjennom tilstedeværelse på nettet, og som man derfor må fortsette å søke og nå gjennom oppsøkende arbeid på gaten.

Begrenset tilgjengelighet

Kommunalt ansatte er ikke tilgjengelige hele døgnet. Dette gjør at ungdom kan befinne seg i situasjoner uten tilgang til hjelp og støtte fra kommunalt ansatte. I slike situasjoner er det viktig at ungdom er informert om andre hjelpe-tjenester som de kan kontakte i stedet. Ikke minst er det viktig at ungdom i slike situasjoner er informert om når kommunalt ansatte faktisk er tilgjengelige, slik at ungdommene vet når de kan kontaktes og ikke. En måte å gjøre dette på er å tydeliggjøre åpningstiden til den kommunale virksomheten på de sosiale medie- og gamingplattformene som virksomheten bruker.

Sikkerhet

Selv om tjenesten følger sikkerhetsmessige råd vil det alltid være et rom for at en konto kan bli hacket eller informasjon kommer på avveie. Det er derfor nødvendig å minimere risiko for dette så langt det lar seg gjøre.

To-trinnsertifisering og sterke passord bør benyttes

3 Hva gjør jeg dersom jeg avdekker noe bekymringsfullt på nett?

Når man arbeider på digitale plattformer, kan man avdekke bekymringsfull atferd. I slike tilfeller kan man ha en plikt til å avverge atferden og/eller en plikt til å opplyse om atferden.

Avvergingsplikt

Kommunalt ansatte har en plikt til å avverge lovbrudd (straffeloven, 2005, § 196).

Avvergingsplikten (strl. § 196)

Med bot eller fengsel inntil 1 år straffes den som unnlater å anmelde til politiet eller på annen måte å søke å avverge et lovbrudd eller følgene av det, på et tidspunkt da dette fortsatt er mulig, og det fremstår som sikkert eller mest sannsynlig at lovbruddet er eller vil bli begått. Avvergelsesplikten gjelder uten hensyn til taushetsplikt og innebærer en plikt til å avverge en rekke lovbrudd. Se [strl. § 196](#) for mer informasjon.



Utekontakten avdekker bilde av våpen – hva bør de gjøre?

Utekontakten scroller gjennom feeden på Snapchat. Der dukker det opp et bilde av en ungdom med balaklava som holder et håndvåpen rettet mot kamera. På bildet står det “SNiTChes get StiTChes!”. Utekontakten tar screenshot av bildet og tar opp posten med de andre på teamet. De er kjent med at den aktuelle ungdommen har en pågående konflikt med ungdom fra andre bydeler. Han har tidligere blitt dømt for grov vold og er involvert i narkotikaomsetning.

Utekontakten velger i første omgang å drøfte saken anonymt med bydelens nærpolti.

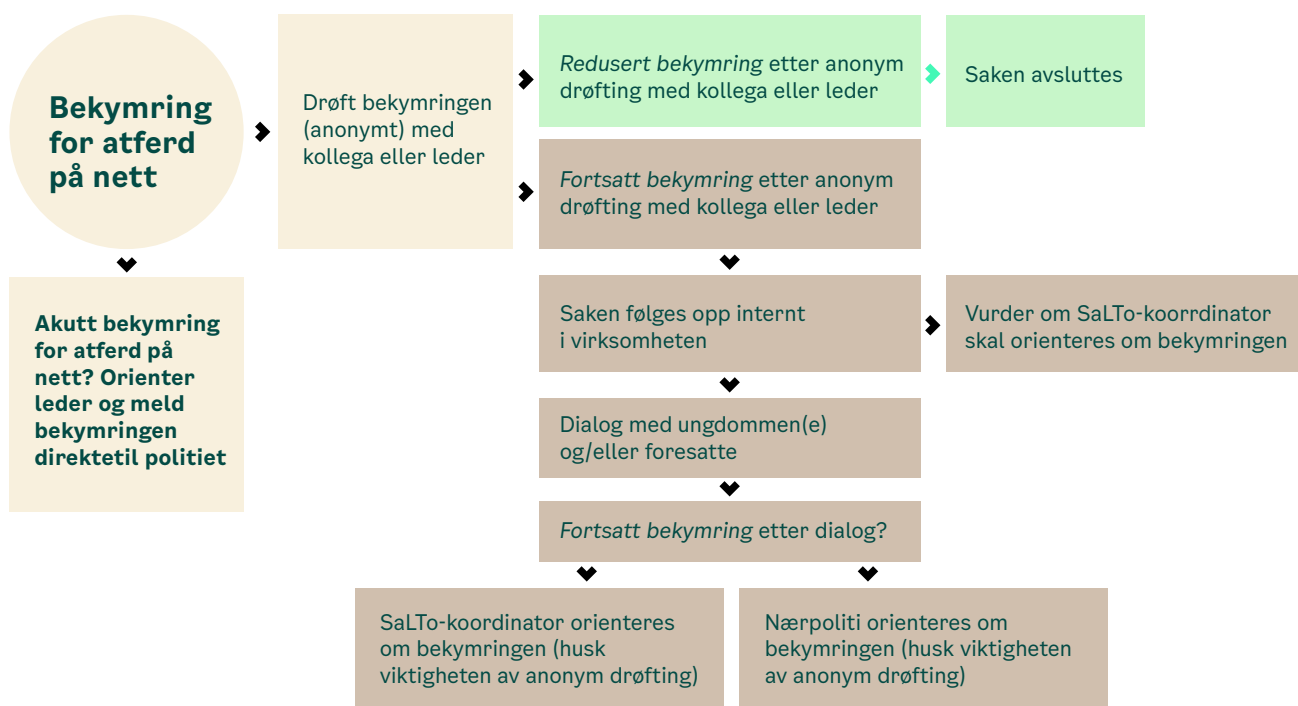
Hvordan ville du løst det?

Hvilke rutiner har din virksomhet for å løse tilsvarende utfordring?

Hvordan kan kommunalt ansatte gå frem dersom de er bekymret?

Under følger to modeller for hvordan kommunalt ansatte kan gå frem dersom de er bekymret for atferd på nett.

Trinnvis modell ved bekymringsfull atferd på nett



Med bekymring for atferd henspeiler veilederen til atferd som ikke utgjør en fare for liv og helse, og som derfor kan håndteres over tid. Med akutt bekymring for atferd henspeiler derimot veilederen til atferd som kan utgjøre en fare for liv og helse, og som derfor må håndteres akutt.

Er du bekymret for fare for liv og helse: Ring politi: 112 eller medisinsk nødhjelp: 113.



Trinnvis modell for å tipse politiet ved bekymringsfull atferd på nett



En av fordelene med å tipse politiet er at det da er politiet som tar en vurdering av atferden man opplever som bekymringsfull.

Opplysningsplikt

Foruten en plikt til å avverge kan kommunalt ansatte også ha en plikt til å opplyse om bekymringsfull atferd. Når man arbeider på nett, både når man kartlegger ungdomsmiljøer og når man etablerer kontakt og relasjon med ungdom i miljøene, kan man avdekke bekymringsfull atferd som utløser en plikt til å opplyse for eksempel foreldre (se [forvaltningsloven](#)) eller barnevern-tjenesten (se [barnevernsloven](#)).

Avdekker et bilde på Snapchat – vil opplysningsplikten inntreffe?

Utekontakten kommer over et bilde i stories på Snapchat. En kjent ungdom – Emilie (14 år) har lagt ut et «før/etter» bilde hvor hun i det første bildet holder en rosa pille foran kamera og etterbilde som viser hun livløs i en sofa. «Fjeeeeeeeern ass!!» er plassert inn som en snakkeboble over «etterbildet».

Utekontakten har tidligere fulgt opp bekymring rundt Emilie. Hun har hatt aktiv barnevernssak som nå er avsluttet. På teammøtet drøftet utekontakten hvorvidt summen av tidligere oppfølging og story på Snap utløser opplysningsplikten.

Vil utekontakten ha en plikt til å opplyse om Emilie sin atferd, og hvilke tjenester bør eventuelt informeres?

4 Dokumentasjon

Kunnskap om det forebyggende arbeidet bør systematisk nedtegnes. Når man jobber på nett, kartlegger ungdomsmiljøer (det vil si plattformer) eller etablerer kontakt og relasjon med ungdommer, bør kunnskapen som opparbeides dokumenteres. Når det kommer til dokumentasjon bør kommunalt ansatte bør fokusere på tre områder: registrering, journalføring og rapportering.

Registrering

Kommunalt ansatte bør registrere virksomhetens tilstedeværelse på nett.

Virksomheten bør ta utgangspunkt i målsetningen med tilstedeværelsen.

For å sikre at man registrerer den informasjonen som ønskes er det avgjørende å definere hva man vil oppnå med registreringen og hva rapporten skal brukes til. Virksomheten kan utarbeide standardiserte skjemaer med eksempelvis avkrysningsfelt og plass til notater for de ulike variablene. Skjemaene vil inneholde anonymisert kunnskap som kan brukes for å synliggjøre arbeidet og videreformidle kunnskapen som erverves. Kunnskapen kan synliggjøre arbeidet som virksomheten gjør på nettet, men også et utgangspunkt for en videreutvikling av arbeidet.

Journalføring

Digitaliseringsdirektoratet viser til tre kriterier som må være oppfylte for at et dokument skal være journalføringspliktig:

1. Det må være et saksdokument for organet.
2. Det må enten ha kommet inn til eller blitt sendt ut fra organet.
3. Dokumentet må både være gjenstand for saksbehandling og ha verdi som dokumentasjon.

I tillegg til å registrere tilstedeværelse på nett, har kommunalt ansatte både rett og plikt til å oppbevare og journalføre opplysninger om en ungdom når:

- › Ungdommen mottar individuell oppfølging.
- › Man har samtykke fra ungdommen/foresatte til ungdommen.
- › Opplysningene om ungdommen synes så alvorlige at de kan utløse en melding til barnevernstjenesten.
- › Det foreligger en så alvorlig situasjon at nødrett utløses (det vil si en situasjon hvor liv og helse avhenger av inngripen fra den kommunalt ansatte).

Dersom man oppbevarer og journalfører opplysninger om en ungdom, må ungdommen informeres om dette. Det er vedkommende eller foresatte til vedkommende som eier opplysningene, og man må derfor informere om hvilke opplysninger som lagres, samt hvilke regler og retningslinjer som gjelder for lagringen av opplysningene (se kapittel 3 og 7), for henholdsvis lover og vurderinger knyttet til lagring av personopplysninger).

Når man skal oppbevare og journalføre opplysninger om ungdom, må man følge visse regler. Om arkivering knyttet til sosiale medier sier Digitaliseringsdirektoratet følgende:

«Det finst ingen løysingar for journalføring av kommunikasjon i sosiale medium mellom offentleg forvaltning og innbyggjarane. Ingen av sak-/arkivsystema som er godkjente for Noark 5, har i dag støtte for arkivering av innhald frå sosiale medium.

Den praktiske løysinga som ofte blir brukt for arkivering fra sosiale medium i dag, er å lagre eit skjermbilete av kommunikasjonen og arkivere det som ei bildefil».

- Arkivering av journaler som inneholder opplysninger som er underlagt taushetsplikt, skal oppbevares på en sikker måte. Arkiveringen krever rutiner og utstyr som gjør at opplysningene ikke er tilgjengelige for andre, og den bør derfor gjøres i samarbeid med datateknisk personell i kommunen.
- Kommunalt ansatte som oppbevarer og journalfører opplysninger etter lov om sosiale tjenester kapittel 3 plikter å melde fra om at de har et personopplysningsregister til Datatilsynet. Kommunalt ansatte som ikke oppbevarer og journalfører opplysninger etter disse lovene, må søke om konsesjon for et slikt register til Datatilsynet.

Den kommunale virksomheten bør, i tillegg til de ovennevnte reglene, lage interne retningslinjer for oppbevaring og journalføring av opplysninger om ungdom. Slike retningslinjer kan for eksempel være:

- Opplysninger som kommunalt ansatte får gjennom tilstedeværelse på nett skal oppbevares og journalføres ut fra de samme prinsippene som ved oppsøkende arbeid.
- Ungdom som gir uttrykk for et ønske om hjelp og støtte fra kommunalt ansatte, skal ha en journal. Opplysninger skal oppbevares og journalføres i de samme programmene som man bruker i oppsøkende arbeid.
- Ungdom som ikke gir uttrykk for et ønske om hjelp og støtte fra kommunalt ansatte, skal ikke ha en journal. Opplysninger skal da kun registreres som anonyme data, jf. punktet om registrering.
- Ungdom skal informeres om at opplysninger oppbevares og journalføres.
- Opplysninger om en ungdom skal lagres i journalen umiddelbart etter kontakten på nett. Alternativt skal loggen fra kontakten med ungdommen innlemmes i journalen.
- Opplysninger om en ungdom fra andre enn ungdommen selv, skal ikke inngå i journalen.
- Dersom man får opplysninger og bekymringer om en ungdom fra andre enn ungdommen selv, bør disse drøftes med ungdommen utenfor nettet. Dersom opplysningene gjelder en ungdom man bare har møtt på nettet, og som man derfor ikke kjenner, bør man motivere ungdommen til å møtes utenfor nettet.

- Dersom man får opplysninger og bekymringer om en ungdom man ikke kjenner, og man mener det er riktig at man oppbevarer og journalfører kontakten (med bakgrunn i bekymring som kan utløse melding til barneverntjenesten), skal man journalføre ungdommen på en måte som er gjenkjennelig (for eksempel med skole, alder osv.) Dette kan danne grunnlag for kontakt med ungdommen når man senere arbeider oppsøkende på gaten. Dersom man ikke oppnår kontakt etter den tiden som loven gir, skal opplysningene slettes.

Hvorfor skal man journalføre?

Journalføring er viktig blant annet fordi:

1. Ungdommen kan ha nytte av journalføringen som dokumentasjon for senere å kunne oppnå rettigheter i for eksempel skole og barnevern.
2. Kontakten med ungdommen kan bli gjenstand for en senere melding til barneverntjenesten.
3. Det bidrar til kvalitet og kontinuitet i det oppsøkende arbeidet med ungdommen.

Rapportering

Den informasjonen som kommunalt ansatte får om ungdomsmiljøer og ungdommer gjennom tilstedeværelse på nett, kan utløse tiltak overfor både miljøene og ungdommene. Rapportering er derfor en naturlig forlengelse av registrering og journalføring.

Tiltak for ungdom og ungdomsmiljøer

Dersom man har klarete kanaler å rapportere gjennom (som for eksempel en teamleder), øker sjansen for at rapporteringen når frem til beslutningstakere som kan iverksette tiltak. Sjansen for at tiltak iverksettes øker også dersom man i tillegg har etablerte referansegrupper med samarbeidspartnere.

Skriftlig eller muntlig rapportering?

For at informasjonen som kommunalt ansatte får om ungdomsmiljøer og ungdommer skal kunne utløse tiltak, må den tolkes og formidles gjennom en skriftlig rapportering. Skriftligheten er viktig ettersom man da kan etterprøve eller stille spørsmål ved informasjonen. I tillegg kan skriftlig tolkning og formidling sikre at vellykket tilstedeværelse på nett kan benyttes også av andre kommunalt ansatte eller av andre kommunale virksomheter.

I forkant av den skriftlige rapporteringen er det viktig å avklare hvem mottakeren er. Dette spesielt med tanke på rapportens omfang og språk. Det er viktig at språket er konkret og forståelig slik at mottakeren kan iverksette tiltak overfor ungdomsmiljøene og ungdommene.

5 Lover som regulerer kommunal tilstedeværelse på nett

Når man har tilstedeværelse på nett, uavhengig av om man kartlegger, etablerer kontakt og relasjon eller dokumenterer, må man forholde seg til flere lover og reguleringer. Det er viktig at kommunalt ansatte setter seg inn i lovene som er aktuelle for det arbeidet som de skal gjøre på nett.

Relevante lover

Tilstedeværelse på nett reguleres av lovverket som den kommunale virksomheten ellers reguleres av. Ettersom ulike virksomheter reguleres av ulike lovverk, er det viktig at man setter seg inn i dette i forkant av tilstedeværelse på nett. Ikke minst er det viktig at man setter seg inn i hvordan lovverket legger føringer for arbeidet. Under følger en oversikt over relevante lovverk.

Lov om arkiv ([arkivlova](#)).

Loven trykker arkiv som har en kulturell eller forskningsmessig verdi eller som inneholder rettslig eller viktig forvaltningsmessig dokumentasjon, slik at disse kan tas vare på og gjøres tilgjengelige for ettertiden.

Lov om rett til innsyn i dokument i offentlig verksemd ([offentleglova](#)).

Formålet med loven er å regulere innsyn i dokumenter i offentlige virksomheter. Saksdokumenter som beror hos en offentlig myndighet, skal som hovedregel være fritt tilgjengelig for enhver som ønsker å gjøre seg kjent med dem.

Lov om behandlingsmåten i forvaltningssaker ([forvaltningsloven](#)).

Loven gjelder regulerer blant annet habilitet, taushetsplikt og vedtak. I tillegg til forvaltningsloven er det også andre lover (eksempelvis sosialtjenesteloven) som regulerer taushetsplikten i det oppsøkende arbeidet. Se [Utenfor boksen – innenfor lovverket: Veileder for god informasjonsflyt](#) (Oslo kommune og Oslo politidistrikt, 2021) for mer informasjon om taushetsplikten til kommunalt ansatte.

Lov om behandling av personopplysninger ([personopplysningsloven](#)).

Formålet med loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.

Lov om sosiale tjenester i arbeids- og velferdsforvaltningen ([sosialtjenesteloven](#)).

Formålet med loven er blant annet å forebygge sosiale problemer og bidra til at utsatte barn og unge og deres familier får et helhetlig og samordnet tjenestetilbud.

Lov om straff ([straffeloven](#)).

Loven regulerer straff, straffereaksjoner og straffbare handlinger.

Personopplysningsloven

Når man arbeider oppsøkende på nett, stilles det særlige krav til behandling av personopplysninger. Dette gjør personopplysningsloven relevant. Loven består av nasjonale regler og EUs personvernforordning, også kalt GDPR – General Data Protection Regulation, som er et sett av regler som gjelder for alle EU/EØS-land (Datatilsynet, 2023).

Personopplysningsloven gjelder når kommunalt ansatte:

- › Helt eller delvis foretar en automatisk (typisk elektronisk) behandling av personopplysninger (Datatilsynet, 2023). Med behandling menes all bruk av personopplysninger, som innsamling, registrering, sammenstilling, lagring og utlevering.
- › Foretar en ikke-automatisk behandling av personopplysninger, men opplysningene skal inngå i et strukturert register (Datatilsynet, 2023).

Personopplysninger er opplysninger og vurderinger som kan knyttes til en enkeltperson, for eksempel navn, adresse, telefonnummer, fødselsnummer (Datatilsynet, 2023).

Sensitive personopplysninger er opplysninger om a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, b) genetikk og biometri med det formål å identifisere noen, c) helseforhold, d) seksuelle forhold og seksuell legning og e) medlemskap i fagforeninger (Datatilsynet, 2023). De fleste opplysninger som kommunalt ansatte behandler i forbindelse med tilstedeværelse på nett, kan være sensitive.

Innhenting av samtykke for behandling av personopplysninger

I forkant av behandling av personopplysninger må kommunalt ansatte som hovedregel innhente samtykke fra den personen som opplysningene gjelder. Et samtykke er kun gyldig dersom det er:

- › Frivillig
- › Spesifikt
- › Informert
- › Utvetydig
- › Gitt gjennom en aktiv handling
- › Dokumenterbart
- › Mulig å trekke tilbake like lett som det ble gitt

Samtykke og publisering av bilder og videoer

Reglene er strenge for publisering av bilder og videoer. Dette er relevant i saker der ungdom publiserer bilder eller videoer av hverandre uten samtykke, men det er også relevant i saker der kommunalt ansatte publiserer bilder eller videoer av ungdom på sine plattformer. Det kan være vanskelig for ungdom å ha oversikt over konsekvensene som publiseringen kan få. Derfor bør kommunalt ansatte som en hovedregel ikke publisere bilder eller videoer fra egen virksomhet der ungdom vises eller kan identifiseres, selv om man har samtykke fra ungdommen.

Innhenting av samtykke fra mindreårige

Ungdom kan samtykke til behandling av personopplysninger når de er over 18 år (Datatilsynet, 2022). Når de er under 18 år, må foreldre eller den/de med foreldreansvar samtykke på ungdommenes vegne (Datatilsynet, 2022).



Barn og unge har rett til økt selv- og medbestemmelse med alderen (Datatilsynet, 2022). Foreldre eller den/de med foreldreansvar bør derfor høre med ungdommene før de samtykker på deres vegne.

I noen tilfeller kan ungdom, dersom de er i stand til det, samtykke til behandling av personopplysninger selv om de er under 18 år (Datatilsynet, 2022). Hvorvidt en ungdom er i stand til det, må vurderes blant annet etter ungdommens modenhet og om informasjonen som gis er tilpasset ungdommens alder og evne til å forstå hva den samtykker til. En tommelfingerregel kan uansett være at jo større personvernkonsekvenser (se kapittel 1 om Vurderinger i forkant av kommunens tilstedeværelse på nett for mer informasjon om personvernkonsekvenser) som behandlingen av personopplysninger kan ha, desto høyere terskel bør det være for at en ungdom som er under 18 år kan samtykke uten foreldre eller den/de med foreldreansvar (Datatilsynet, 2022).



Flere plattformer har egne regler for når en ungdom under 18 år kan samtykke (Datatilsynet, 2022). Eksempelvis kan ungdom på plattformer som Instagram, TikTok og Snapchat samtykke fra de er 13 år. For ungdom som er under 13 år, må foreldre eller den/de med foreldreansvar samtykke på vegne av ungdommene (Datatilsynet, 2022).

Rutiner for innhenting av samtykke

Den kommunale virksomheten bør utvikle rutiner for innhenting av samtykke ved oppsøkende arbeid på nett. På de aller fleste plattformer publiseres alltid noen personopplysninger om brukerne. Innhenting av samtykke, og rutiner for dette, er derfor en nødvendighet for å kunne arbeide oppsøkende på plattformene. At ungdommene legger til kommunale virksomheter og kommunalt ansatte på plattformer som Snapchat, Instagram og Discord, er ikke nok til å være et uttrykkelig og informert samtykke.

**Kreves det samtykke for å benytte Snapmap?**

Elias og Eva i Utekontakten har startet å bruke Snapchat som en plattform i det oppsøkende arbeidet, og flere ungdommer har lagt dem til som venn. I et møte med politiet får de vite at ungdommer, deriblant flere av ungdommene de har som venner på Snapchat, møtes for å slåss ulike steder i bydelen de arbeider i. Fordi slåsskampene foregår ulike steder hver gang, opplever Elias og Eva det som vanskelig å vite hvor de skal arbeide oppsøkende.

Elias får en idé om å bruke Snap Map for å lokalisere ungdommene, og lager sammen med Eva en standardmelding de sender til samtlige som har lagt dem til eller som eventuelt legger dem til på Snapchat. At ungdommene har lagt til Utekontakten på Snapchat, er nemlig ikke ensbetydende med at de har samtykket til at Elias og Eva kan bruke posisjonen deres på Snap Map i det oppsøkende arbeidet. I meldingen informerer de derfor ungdommene om hva det innebærer å dele posisjon med Utekontakten på Snap Map, og ber også ungdommene om å svare på meldingen med en bekreftelse på at de har forstått informasjonen. Elias og Eva opplever at noen av ungdommene fjerner dem som venn når de får meldingen tilsendt, men majoriteten bekrefter meldingen og beholder dem som venn.

Spørsmålet er om det holder at Elias og Eva innhenter samtykke for å bruke Snap Map i det oppsøkende arbeidet?

I tillegg til å innhente samtykke, bør kommunalt ansatte gjøre etiske vurderinger før de behandler ungdommers personopplysninger (se [kapittel 1 Vurdering i forkant av kommunens tilstedeværelse på nett](#)).

At Elias og Eva behandler personopplysninger om ungdommene de har på Snap Map lovlig på grunn av samtykke, er for eksempel ikke ensbetydende med at det er riktig å gjøre det.

