Retningslinjer for sikker kommunikation

Revisionshistorik

Version	Dato	Beskrivelse af ændringer	Udført af	Godkendt af
2.1	01-03-2023	Tilføjelse og gennemgang af flere afsnit	Sikkerhedsrådgiver	Sikkerhedsteam
2.2	12-04-2024	Ændringer i afsnittet 'Sociale medier'	Sikkerhedsrådgiver	Sikkerhedsteam
3.0	05-01-2026	Tilføjelse af flere afsnit, og derudover er retningslinjerne samlet med retningslinjer for billeder og video	Sikkerhedsrådgiver	Sikkerhedsteam

Indhold

Indledning

Disse retningslinjer har til formål at fastlægge et regelsæt for en sikker og lovmedholdelig kommunikation i kommunen. Det er vigtigt, at retningslinjerne overholdes for at undgå, at der gennem kommunikationen sker utilsigtede fejl, som medfører brud på databeskyttelsesreglerne fx ved uretmæssig adgang til personoplysninger. Ledere i Jammerbugt Kommune har ansvaret for, at retningslinjerne efterleves af medarbejderne i den pågældende afdeling.

Mail, kalender og drev

Ansatte må aldrig bruge deres arbejdsmail til private formål, da dette øger sikkerhedsrisici for phishing-mails o.l. Benyt derfor kun arbejdsmail til arbejdsrelaterede formål.

Forsendelse af mails

Hvis det er muligt at undgå, bør ansatte ikke sende mails med personoplysninger til andre ansatte i kommunen. Det er vigtigt, at afsenderen altid tager stilling til, om det er relevant for modtageren at få oplyst fx CPR-nummer på en borger, eller om det er muligt for afsenderen at forholde sig til sagen uden at få indsigt i personoplysninger.

Når medarbejdere sender mails internt fra x@jammerbugt.dk til y@jammerbugt.dk, er det automatisk en sikker forsendelse. Ansatte må derfor sende alle typer oplysninger via mails til Jammerbugt-e-mailadresser, så længe modtageren har lov til at behandle, herunder at modtage oplysningerne.

Mails indeholdende følsomme og fortrolige personoplysninger eller forretningsoplysninger til eksterne modtagere som fx borgere, virksomheder eller andre myndigheder må aldrig sendes usikkert, hvilket vil sige udenom fx Sikker Mail eller OneTooX -funktionerne. Hvis disse typer af oplysninger sendes usikkert, vil der være tale om et sikkerhedsbrud.

Det anbefales, at man undlader at notere følsomme eller fortrolige personoplysninger i en mails emnefelt for at minimere risikoen for, at uvedkommende ser oplysningerne.

Medarbejdere bør så vidt muligt anvende fagsystemer og Sikker Mail-funktionen i Outlook til at sende personoplysninger sikkert, uanset at der kun er tale om almindelige personoplysninger. Det er dog tilladt for medarbejdere at sende mails, der alene indeholder almindelige (og ikke-fortrolige) personoplysninger, eller som slet ikke indeholder personoplysninger, til borgere eller andre eksterne aktører til deres private mail. Det anbefales dog, at der foretages en vurdering i den enkelte afdeling, som indfører og nedskriver en procedure for, hvilken type borgerkommunikation der gerne må foregå udenom de sikre kanaler. Her er der mulighed for at tage højde for den praksis, det enkelte fagområde har – fx hvilken kommunikationsform passer til os?

Det er ikke tilladt at oprette regler for automatisk videresendelse af mails i Outlook. Det skyldes, at risikoen for sikkerhedsbrud er stor, idet oplysninger nemt kan havne hos en modtager, som ikke har hjemmel eller et arbejdsbetinget behov for at tilgå oplysningerne. Der kan være enkelte undtagelser til denne regel, men afvigelser herfra kræver en begrundelse og en tilladelse fra en afdelingschef eller direktør, og der vil kun være tale om en tidsbegrænset periode.

Kommunen kan kun modtage digital post sikkert, hvis afsenderen har mulighed for at sende sikkert. Det gør afsenderen sandsynligvis ikke, hvis de sender fra deres private Hotmail, iCloud, Outlook eller Gmail. Kommunen kan ikke garantere, at alle eksterne parter sender sikkert til Jammerbugt Kommune, men som offentlig myndighed har kommunen en etisk forpligtelse for at vejlede eller i nogle tilfælde kræve, at følsomme og fortrolige oplysninger håndteres forsvarligt. Hvis en fast leverandør eller samarbejdspartner gentagende gange sender følsomme borgeroplysninger til kommunen, bør medarbejdere undersøge, om den digitale post sendes sikkert.

Det er vigtigt, at medarbejdere aldrig opfordrer borgere til at sende følsomme eller fortrolige oplysninger til deres jammerbugt-mailadresse eller direkte til en fællespostpasse. En borger vil typisk ikke have mulighed for at sende sikkert direkte fra egen e-mailkonto til fx jobcenter@jammerbugt.dk, ppr@jammerbugt.dk eller industri@jammerbugt.dk, hvorfor borgeren i stedet skal opfordres til at anvende Sikker Post-funktionerne via kommunens hjemmeside eller Digital Post / eBoks, hvor de i menuen kan vælge, hvilken afdeling de ønsker at sende til i Jammerbugt Kommune. Hvis ansatte jævnligt modtagere almindelige personoplysninger via usikre mails, skal det indskærpes overfor alle i afdelingen, at medarbejderne aldrig må besvare mailen direkte i tilfælde af, at en borger sender følsomme eller fortrolige personoplysninger i en usikker mail til en medarbejder hos kommunen. Medarbejderen skal i stedet oprette en ny mailtråd, hvor vedkommende svarer borgeren. Det anbefales, at medarbejderen informerer borgeren om, at følsomme og fortrolige oplysninger ikke er sikre at sende via mailforbindelse. Hvis korrespondancen kræver udveksling af yderligere følsomme eller fortrolige personoplysninger, skal medarbejderen fortsætte kommunikationen via en sikker linje fx ved telefonopkald eller Digital Post.

Det er ikke muligt at sende Digital Post til personer, medmindre de har dansk cpr.nr. og er oprettet med MitID. For denne modtagergruppe anbefales det, at man i stedet sender fysisk post. Dog kan man i særlige tilfælde sende en zip-fil til en usikker mail, hvorefter man fremsender en kode over usikker SMS eller ved telefonopkald, som gør, at borger derefter kan åbne filen.

Sletning af mails og filer

Alle medarbejdere, der har fået tildelt en e-mailadresse, er forpligtet til at tjekke postkassen jævnligt. Alle ansatte er desuden forpligtede til løbende at slette mails i overensstemmelse med nedenstående regler.

Mails med **personoplysninger** skal slettes fra mailboksen, når der ikke længere er et legitimt formål med opbevaringen.

Mails med **følsomme eller fortrolige personoplysninger** skal slettes fra mailboksen senest 30 dage efter modtagelse/afsendelse. Er du afsender af en mail med **følsomme eller fortrolige personoplysninger**, skal du slette mailen i mappen 'Sendt post'. Alt indhold i mappen 'Slettet post' bliver automatisk slettet efter 30 dage.

Samme regler for opbevaringsbegrænsning på maksimalt 30 dage gælder for følsomme og fortrolige personoplysninger opbevaret som filer, fx dokumenter, på andre midlertidige placeringer som drev, OneDrive, Teams og SharePoint. Almindelige personoplysninger må opbevares udenfor fagsystemer, indtil der ikke længere er aktuelt eller relevant at gemme på den midlertidige filplacering.

Kalender

Mødebookninger i Outlook-kalenderen skal være anonymiseret, så det ikke er muligt for udefrakommende at aflæse personoplysninger ved at kigge i kalenderen. Hvis en ansat har et møde med en borger, skal man undlade at skrive borgerens navn, adresse eller cpr-nummer i kalenderen. Det er tilladt at notere journal- eller sagsnumre samt borgers initialer. I de tilfælde, hvor man skal indkalde en borger til et møde, enten fysisk eller virtuelt, er det tilladt at notere en privat mailadresse i deltager-feltet. Man bør dog undlade at notere øvrige oplysninger, som kan afsløre oplysninger om mødets karakter og indhold. Det vil ikke være tilstrækkeligt at gøre mødet 'privat', da personoplysninger som udgangspunkt ikke må opbevares i Outlook-kalenderen, medmindre der foreligger tungtvejende hensyn.

Det er et krav, at samtlige kalendere er åbne, hvilket vil sige, at alle i organisationen kan se indholdet i mødeindkaldelser. Den enkelte medarbejder skal således være opmærksom på at overholde reglen om ikke at lægge personoplysninger – hverken almindelige, følsomme eller fortrolige - ind i sin kalender, og den nærmeste leder har ansvaret for at sikre, at reglen overholdes lokalt.

Delte postkasser

Delte postkasser skal have mindst to brugere tilkoblet. Dette er for at undgå, at digital post strander i delte postkasser, hvis kun en bruger har adgang, som af en eller anden årsag ikke tjekker den delte postkasse ofte nok, eller som er fraværende.

Nærmeste ledere af de afdelinger, som har oprettet delte postkasser, er ansvarlige for at sikre, at der til enhver tid er tildelt korrekte adgange, samt at mindst to brugere er tilkoblet postkasserne. Ledere er desuden årligt på foranledning fra Digitalisering, IT og Borgerservice forpligtet til at kontrollere adgange til delte postkasser samt at give Servicedesk besked om eventuelle ændringer.

Alle bestillinger af nye delte postkasser kræver ledelsesgodkendelse, og nærmeste leder beslutter, hvem der skal tildeles adgang hertil. Der må ikke oprettes delte postkasser med det formål at håndtere fortrolige eller følsomme personaleoplysninger (HR-afdelingen undtages herfor).

Ledere er desuden ansvarlige for, at der udpeges en primær ansvarlig blandt de tilkoblede brugere på de delte postkasser, som får ansvaret for dagligt at videresende

Kommunalbestyrelsens brug af jammerbugt-mail til politiske møder o.l.

Oplysninger om personers politiske overbevisning, herunder oplysning om medlemskaber af politiske partier, kategoriseres i databeskyttelseslovgivningen som værende følsomme personoplysninger. Det betyder, at disse oplysninger skal beskyttes på lige fod med fx sundhedsoplysninger eller CPR-numre. Alle deltagere i mødeindkaldelser, som foretages via jammerbugt-mail, er som udgangspunkt synlige i Outlook og Teams for samtlige ansatte i Jammerbugt Kommune, og da offentliggørelse af politisk tilhørsforhold gennem en mødeindkaldelse, ikke har arbejdsmæssig relevans for ansatte i Jammerbugt Kommune, kan det derfor blive vurderet som et alvorligt sikkerhedsbrud.

Af sikkerhedsmæssige årsager kræves derfor særlig opmærksomhed, hvis man anvender sin jammerbugt-mail til indkaldelser til partipolitiske møder, og det anbefales ikke, at anvende sin jammerbugt-mail til mødeindkaldelser i større politiske forsamlinger. Hvis dette gøres, skal det sikres, at alle mødedeltagere i forvejen offentligt har tilkendegivet medlemskab af et givent parti (fx som kandidat). Er man i tvivl, kan mødeindkaldelsen i Outlook sættes som ”privat”, hvorved listen af mødedeltagere udelukkende er tilgængelig for de deltagere, der er indkaldt til det aktuelle møde.

Deling af dokumenter via OneDrive eller Teams/SharePoint

I Microsoft 365 er det muligt at dele dokumenter via OneDrive eller Teams/SharePoint med interne såvel som eksterne brugere. For at minimere risikoen for sikkerhedsbrud har kommunen besluttet nedenstående regelsæt:

- Filer indeholdende personoplysninger, herunder både almindelige, fortrolige og følsomme oplysninger, må kun deles internt, hvis du har hjemmel hertil (fx lovhjemmel eller samtykke). Du kan altid spørge en af kommunens jurister, hvis du er i tvivl, om du har hjemmel til at dele oplysninger internt.
  OBS. deling af dokumenter indeholdende personoplysninger med eksterne personer er ikke tilladt.
- Filer indeholdende forretningsoplysninger (fx fortrolige interne oplysninger og offentlige oplysninger) må deles internt og eksternt, hvis det er relevant for modtagerne.

SMS

SMS vurderes som værende en usikker kommunikationsform, og kommunikation via SMS skal derfor begrænses til at give borgere påmindelser og kortere servicebeskeder[1], og SMS-kommunikation bør aldrig anvendes til sagsbehandling.

I nogle særlige tilfælde kan SMS'er med følsomt eller fortroligt indhold accepteres som kommunikationsform grundet tungtvejende hensyn til borgeren fx baseret på socialfaglige eller lægelige skøn, hvilket skal kunne dokumenteres.

Hvis en afdeling vurderer, at SMS er en nødvendig kommunikationsform, skal nedstående krav overholdes:

Undgå brug af privat telefon

Personoplysninger bør så vidt muligt kun ligge på arbejdstelefoner og ikke på private telefoner. Det er vigtigt at undgå at blande private kontaktoplysninger med arbejdsrelaterede oplysninger. Hvis medarbejdere anvender privattelefoner til borgerkommunikation, bør den pågældende afdeling tage en dialog om dette, herunder hvilke procedurer der er for sletning af SMS'er med personoplysninger, og hvem i medarbejderens husstand har eventuelt adgang til borgeres personoplysninger gennem den private telefon.

Kun forsendelse af almindelige oplysninger

En ansat må aldrig sende følsomme eller fortrolige personoplysninger (fx sundhedsoplysninger eller børns personoplysninger) pr. SMS.

Skriv kun det mest nødvendige

Man bør begrænse mængden af personoplysninger, som sendes via SMS mest muligt. Det gælder også servicebeskeder, hvor der kun bør anføres det absolut mest nødvendige, fx '*Husk din aftale [dato/kl.] hos tandlæge [X], [adresse]. Evt. afbud på [tlf.nr./e-mailadresse].'*

I telefonens kontaktliste skal den ansatte begrænse personoplysningerne mest muligt, fx ved at notere 'Jens' eller 'JJ' fremfor 'Jens Jensen, Torvegade 16' osv. Der må aldrig noteres følsomme eller fortrolige oplysninger i kontaktlisten.

Hvis borgeren uden opfordring deler følsomme eller fortrolige oplysninger (fx 'jeg kommer ikke til mødet i morgen, fordi jeg har rygsmerter'), anbefales det, at medarbejderen orienterer borgeren, at SMS ikke er en sikker kommunikationsform til den type oplysning, og hvis det vurderes, at det er nødvendigt at udveksle yderligere følsomme eller fortrolige oplysninger,

[1] I Social-, Sundhed- og Beskæftigelsesforvaltningen anvendes et system, som i daglig omtale benævnes som 'Sikker SMS'. Der er i praksis ikke tale om egentlig SMS-kommunikation, men derimod en applikation, som har til formål at sikre nem og sikker kommunikation med borgere. Dette system er derfor ikke en del af dette afsnits regler i forhold til brug af SMS.

skal medarbejderen fortsætte dialogen over en anden kanal, fx telefonopkald eller Digital Post.

Overholdelse af journalpligt og sletning
Ansatte skal huske at overholde notat- og journaliseringspligten, hvis SMS anvendes som kommunikationsform.

Den ansatte har selv ansvaret for at slette personoplysninger på den telefon, som vedkommende har anvendt i sit arbejde, efter evt. relevant journalisering er foretaget. Medarbejderen kan fx hver tredje måned sørge for at slette SMS-beskeder eller noter. Det er vigtigt, at denne regel overholdes, og nærmeste leder bør jævnligt indskærpe dette over for medarbejderne. Desuden bør lederen løbende føre kontrol med, at reglen i praksis overholdes.

SMS til udsatte borgere
Udsatte borgere har de samme datarettigheder som alle andre, men hensynet til databeskyttelse kan i en konkret sag veje mindre end hensynet til den udsatte borgers liv og helbred. I nogle særlige tilfælde må kravene til databeskyttelse derfor vige for mere tungtvejende hensyn til borgeren baseret på socialfaglige eller lægelige skøn.

Er en sms til en borger fx den eneste måde at imødekomme en borgers rettigheder efter serviceloven, skal der foretages en afvejning i forhold til databeskyttelsesreglerne. Overvejelserne for afvigelsen af databeskyttelsesreglerne skal være dokumenteret. Det er et krav, at man ikke kan komme i kontakt med borgeren på anden vis. Uanset at man i den konkrete situation kan begrunde kommunikation med SMS, skal der fortsat tænkes i dataminimering.

Følgende eksempler kan bruges til begrundelse for kommunikation via SMS med følsomt indhold: Kognitiv funktionsnedsættelse, mental udvikling, fysisk funktionsnedsættelse og nødvendig for personens vitale interesse

Lokal procedure for brug af SMS
Balancen for, hvornår SMS er tilladt, og hvornår det ikke er, er hårfin, og det kan være svært som medarbejder at navigere i. Derfor er det et krav, at afdelinger, som anvender SMS som kommunikationsform, udarbejder en lokal, skriftlig procedure. Det gælder dog kun de afdelinger, hvor der føres SMS-korrespondancer med borgere eller andre eksterne parter, og hvor der naturligt vil blive udvekslet personoplysninger via korrespondancerne. Det vil sige, at kravet om procedure ikke gælder for afdelinger, som udelukkende anvender SMS som automatiske servicemeddelelser, hvor der ikke indgår personhenførbare oplysninger i teksten.

Nærmeste leder har ansvaret for, at medarbejderne klædes på til en forsvarlig og sikker brug af SMS samt udarbejdelse af den lokale skriftlige procedure. Proceduren skal indeholde følgende overvejelser:

- Hvorfor er der et behov for at anvende SMS som kommunikationsform, og hvilke overvejelser har afdelingen gjort sig i forhold til at begrænse brugen?
- Hvorfor er det ikke muligt at bruge en anden og mere sikker kommunikationsform?
- I hvilke konkrete sammenhænge må SMS anvendes som kommunikationsform, fx 'kun i forbindelse med praktisk information vedrørende møder'?
- Hvilke oplysninger må medarbejderne sende via SMS?
- Hvordan det sikres, at journaliseringspligten overholdes?
- Hvornår og af hvem skal SMS'er slettes?

Proceduren skal jævnligt genopfriskes for medarbejderne, og nye medarbejdere skal introduceres til proceduren. Der bør også løbende føres kontrol med, at proceduren overholdes af medarbejderne.

Telefonopkald

Det er altid sikkert at ringe til en borger og have en fortrolig samtale, hvor der udveksles følsomme personoplysninger. Det er dog vigtigt, at den ansatte sikrer sig, at der ikke er andre i nærheden, som kan risikere at overhøre samtalen. Undgå derfor at tale offentlige steder, hvor andre kan overhøre samtalen eller steder/situationer, hvor man har sværere ved at vurdere risikoen. Hvis den ansatte arbejder tæt op ad andre fx i storrumskontorer, bør man undersøge, om der findes nogle lokaler på arbejdspladsen, som er tilstrækkeligt lydisoleret. Emnet kan med fordel tages op på et personalemøde, hvor afdelingen kan drøfte, hvordan man bedst muligt undgår at overhøre hinandens fortrolige samtaler.

Videomøder

Herunder oplistes de mest almindelige videomødeløsninger, og hvorvidt de er sikkerhedsgodkendte.

Microsoft Teams

Videoopkald gennem Microsoft Teams er altid sikre, og det er muligt at dele alle typer personoplysninger på et videomøde. Teams er godkendt som en sikker kommunikationsplatform, og ansatte må derfor godt sende personoplysninger i beskeder til kolleger. Dog skal den ansatte være opmærksom på, at man ikke sender til andre kolleger end dem, der har lov til at behandle den pågældende persondata. Det vil sige, at hvis det kun er en enkelt kollega, der skal have borgerens personoplysninger, skal man sende det via Chat. Hvis en hel gruppe skal have oplysningerne, vil det være acceptabelt at sende det via Teams-grupperne. Den ansatte skal huske at slette beskeder i Teams med almindelige personoplysninger, når behandlingen ikke længere er relevant, eller sagen er afsluttet. Hvis der er tale om følsomme eller fortrolige personoplysninger, skal beskeden slettes efter

maksimalt 30 dage. Det samme gælder for fildeling. Ledere har ansvaret for at føre kontrol med, at ovennævnte procedure følges, hvis afdelingen vælger at anvende Teams til opbevaring af personoplysninger. Eventuelt kan lederen udpege en medarbejder, der får til opgave at sikre løbende sletning mv.

Medarbejdere må gerne benytte Teams til at holde møder med eksterne som fx borgere eller samarbejdspartnere. Det er således tilladt at sende videomødeinvitationer til private mailadresser. Man skal blot være opmærksom på ikke at sende følsomme eller fortrolige personoplysninger via indkaldelsen, hvilket vil sige, at man ikke må skrive 'Genoptræning efter rygskade' i emnefeltet på mødeindkaldelsen. Mens videomødet afholdes, må man dele alle typer personoplysninger. Alle mødedeltagere bør være opmærksomme på, at de befinder sig et fortroligt sted, hvor deres samtale ikke kan overhøres af uvedkommende.

Medarbejdere må gerne benytte Teams på private enheder, men kun igennem browseren og ikke gennem en app/program, som er installeret på den private enhed. Her skal man være opmærksom på, at man ikke gemmer sine loginoplysninger på browseren.

Google Meet
Google Meet er tilladt til videomøder på skoleområdet. Ovennævnte regler for Teams gælder også for brug af Google Meet.

Andre videomødeplatforme
Ansatte kan blive inviteret til videomøder af eksterne parter via andre udbydere end Microsoft Teams, fx Zoom. Der er i så fald nogle ting, der skal være på plads, inden man deltager i sådanne møder:

1. Ansatte må gerne deltage i sådanne videomøder, hvis mødeindkalderen har en fuldt licenseret version af programmet. Som regel vil uddannelsesinstitutioner, KL og andre større organisationer have en betalingsversion af programmerne. Er man i tvivl, skal man kontakte mødeindkalderen og forhøre sig ad. Det er ikke tilladt at deltage i møder via gratisversioner af fx Zoom og Skype, ligesom det heller ikke under nogen omstændighed er tilladt at deltage i videomøder via Messenger, FaceTime eller lignende tjenester. Det skyldes, at gratisversionerne af videomødeplatforme generelt har et meget lavt sikkerhedsniveau og ikke er blevet risikovurderet af kommunen.
2. Hvis den ansatte forventer at skulle drøfte eller på anden vis dele følsomme eller fortrolige personoplysninger på mødet, må man ikke deltage.
3. Ansatte i kommunen må aldrig selv invitere til videomøder via andre programmer end Teams og Google Meet.

Diktafon og oversættelsesprogrammer
Der kan opstå situationer, hvor ansatte har brug for at kommunikere med borgere, som ikke taler et sprog, som den ansatte forstår, og hvor det ikke er muligt eller relevant at skaffe en

tolk. I disse tilfælde skal den ansatte være opmærksom på, at det ikke er tilladt at anvende ikke-godkendte, gratis oversættelsesprogrammer som fx apps.

På samme måde kan ordblinde ansatte have behov for et hjælpemiddel i form af en diktafon. Her gælder de samme krav om, at det ikke er tilladt at anvende ikke-godkendte, gratis diktafon-løsninger. De ansatte skal desuden være opmærksom på, at det ikke er tilladt at bruge Siri eller de indbyggede diktafonløsninger på kommunens it-udstyr (fx iPads og smartphones) til at diktere personoplysninger – hverken almindelige, fortrolige eller følsomme oplysninger.

Ønsker man at anvende en it-løsning til diktering eller oversættelse, skal lederen sende en anmodning herom via kommunens ServiceDesk. Kommunens sikkerhedsrådgiver vil derefter undersøge og evt. godkende brugen af et program, herunder sikre indgåelse af en databehandleraftale.

Kontaktlister over medarbejderes pårørende

Visse afdelinger ønsker at udarbejde kontaktlister over pårørende til medarbejdere, så det er muligt at kontakte medarbejderens nærmeste pårørende i tilfælde af nødsituationer, pludseligt opstået uheld eller sygdom o.l. Det er tilladt at ophænge lister over kontaktoplysninger i kommunens lokaler. Det er dog en forudsætning at nedenstående krav overholdes:

- Det skal være frivilligt for medarbejdere at afgive oplysninger på pårørende, og medarbejdere skal altid have mulighed for at få tilrettet eller slettet oplysningerne igen.
- Listen over kontaktoplysninger skal kun indeholde oplysninger på nuværende ansattes pårørende, og det er derfor nødvendigt at opdatere listen, hver gang en medarbejder fratræder sin stilling.
- Listen må kun hænges op i lokaler/områder, hvor kun personale har adgang til. Det kan være fysisk i et aflåst personalerum eller digitalt i en mappe, hvor kun relevante ansatte i den pågældende afdeling har adgang til. Det kan alternativt med fordel drøftes i personalegruppen, om det kun er lederen af den pågældende afdeling, som skal have adgang til listen.

Billede og video

Et billede af en genkendelig/identificerbar person udgør en personoplysning. En tommelfingerregel er, at hvis nogen (fx personen selv eller dennes pårørende) kan identificere den pågældende person ud fra billedet, så er der tale om en personoplysning. Et billede af en hånd er som udgangspunkt ikke mulig at identificere en person ud fra, men hvis hånden bærer unikke kendetegn, fx særlige ar, smykker, tatoveringer, vil billedet udgøre en personoplysning.

Intern brug af billede og video
Billeder, som ikke offentliggøres, men som udelukkende er til intern brug, kan i de fleste tilfælde behandles med hjemmel i kommunens myndighedsudøvelse, hvorfor der ikke er behov for indhentelse af samtykke eller indgåelse af kontrakt. Kommunen skal dog have en saglig begrundelse for at behandle billedet.

Det er et krav, at interne billeder og video slettes, når de ikke længere har et formål, og derudover skal borgeren informeres om, hvad billedet skal anvendes til mv., inden billedet tages. Lederen af den afdeling, hvori billedbehandlingen foregår, er ansvarlig for at sikre, at disse krav overholdes, og er forpligtet til at kontrollere, at medarbejderne efterlever reglerne.

Eksempler på legitime formål til intern brug af billeder kan være:

- Lærervikarers brug af billeder af skoleelever som forberedelse, når de skal undervise en ny klasse for første gang.
- Socialpædagogers/SOSU-personales brug af videooptagelser af handicappede borgere som et led i kompetenceudvikling/levering af en offentlig ydelse (fx 'denne borger skal løftes op ad sin kørestol på denne måde').

Offentliggørelse af billede og video
Inden et billede/video offentliggøres, er medarbejderen forpligtet til at foretage en konkret vurdering af, hvorvidt man må offentliggøre det pågældende billede/video på internettet, fx på kommunens hjemmeside eller et socialt medie. Man må fx ikke dele et billede, hvis den afbildede person kan føle sig krænket over billedet.

Medarbejderen, som ønsker at offentliggøre et billede/video, skal også vurdere hjemmelsgrundlaget:

- Samtykke:
    - Samtykke skal anvendes i de tilfælde, hvor der portrætteres en specifik person, fx i et interview, hvor der også offentliggøres andre personoplysninger om vedkommende. Et eksempel herpå er et opslag på Facebook, hvor kommunen ønsker at fortælle den gode historie om den motionist, som vandt det lokale halvmaratonløb. I den forbindelse deler man navn, alder og billede af vedkommende på kommunens Facebook-side, hvorfor der forinden skal indhentes samtykke hos vedkommende.
    - Når der offentliggøres billede/video af sårbare personer, herunder børn, og hvor billede/video er taget i forbindelse med kommunens myndighedsudøvelse, skal der indhentes samtykke hos den afbildede person. Dette gælder fx, når skoleelever deltager i et arrangement, hvor der er mødepligt/undervisningspligt, og en lærer efterfølgende ønsker at lægge billeder fra arrangementet ud på skolens Facebook-side. Det kan også være plejehjemsbeboere til en intern fastelavnsfest, hvor en SOSU'er ønsker at lægge billeder ud på egen hjemmeside.

- Kontrakt: Hvis kommunen ønsker at bruge billeder af borgere eller medarbejdere i markedsføringsmateriale, fx trykte foldere [1], der beskriver kommunens tilbud, anbefales det, at man indgår kontrakt med de afbildede personer. Dette skyldes, at kommunen skal trække markedsføringsmaterialet tilbage, hvis personen vælger at trække sit samtykke tilbage. Det er vigtigt, at personen økonomisk kompenseres for sin ydelse i markedsføringsmaterialet, da der ellers kan sættes spørgsmålstegn ved kontraktens gyldighed.
- Øvrige billeder/videoer, som ikke falder inden for ovenstående kategorier, vil kunne offentliggøres uden hverken kontrakt eller samtykke.

Hvis den person, der fremgår af billedet, er utilfreds med offentliggørelsen, har vedkommende ret til at gøre indsigelse, hvorefter kommunen er forpligtet til at fjerne billedet.

I retningslinjer for samtykke som behandlingsgrundlag beskrives der krav til samtykkes udformning mv. På Tryk findes desuden en række skabeloner til samtykkeerklæringer.

Oplysningspligt ved brug af billede/video
Kommunen skal give en oplysningspligt til de afbillede personer, inden et billede/video tages. Det kan fx ske gennem allerede eksisterende oplysningsbreve eller som et separat oplysningsbrev, som udarbejdes særligt til billed- og videobehandlingen.

I nogle tilfælde kan det være svært at opfylde oplysningspligten, fx til offentlige arrangementer, hvor der er mange mennesker til stede. I så fald skal man i almindelighed sørge for, at personen, der er på billedet, er informeret om, at man har tænkt sig at offentliggøre billedet, så personen har mulighed for at reagere, f.eks. gøre indsigelse imod det. Man kan også i nogle tilfælde overveje muligheden af at oplyse herom i invitationer, markedsføringsmateriale mv.

Kommunen skal også overholde oplysningspligten, hvis man tillader en ekstern part at komme ind på kommunens arealer for at tage billeder/video. Det kan være en børnehave, som tillader, at en journalist kommer ind i institutionen for at lave optagelser af børnene eller personalet. GDPR-koordinatorerne i de respektive forvaltninger er ansvarlige for at bistå med udformning af oplysningsbrevene.

Hvis en ekstern part, fx en journalist, ønsker at lave optagelser eller at tage billeder i forbindelse med kommunale arrangementer med offentlig adgang, og kommunen ikke selv har et formål med dette, er den eksterne part dataansvarlig og har pligt til at oplyse de registrerede om databehandlingen. Det vil dog være god skik, at kommunen orienterer de

[1] Definition af markedsføring: I en kommunal kontekst forstås *markedsføringsformål* som aktiviteter, hvor kommunen aktivt promoverer sine tilbud, services, arrangementer eller generelle image med henblik på at skabe opmærksomhed, engagement eller deltagelse blandt borgere og interessenter. Dette kan ske via kommunens hjemmeside, sociale medier, trykte materialer, kampagner og events.

registrerede, fx ansatte og beboere på et plejehjem, i god tid om, at der vil ske optagelser eller fotografering.

Sletning af offentliggjorte billeder af genkendelige personer
Der skal slettes billeder og øvrige personoplysninger fra opslag på det sociale medie senest 2 måneder efter, at opslaget er lavet. Nærmeste leder er ansvarlig for at sikre, at relevante medarbejdere er instrueret heri samt at føre kontrol med, at sletningen foretages.

Personer med adressebeskyttelse

For adressebeskyttede borgere eller borgere, som befinder sig i særligt kritiske situationer, fx er gået under jorden, skal kommunen ved indhentning af samtykke til brug af billed- og videomateriale gøre borgere opmærksomme på, at de selv skal vurdere risici forbundet med samtykkeafgivelsen. Det er således borgernes ansvar at tage en vurdering af risici forbundet ved fx offentliggørelse af de pågældende billeder på internettet. I de tilfælde, hvor samtykket er irrelevant, er der ikke behov for, at kommunen indfører særlige sikkerhedsforanstaltninger for at beskytte borgere med adressebeskyttelse. Det skyldes, at risikoen forbundet med de ovennævnte tilfælde vurderes som værende minimale.

Den eneste situation, hvor kommunen vurderer, at der kunne være en mindre risiko for borgere med adressebeskyttelse, er situationsbilleder på internettet uden vidende/aftale. Det kan fx være, at en børnehave går på offentlig gade, og at TV2 Nord vælger at optage børnene uden at spørge om lov. I det tilfælde vurderer kommunen, at det næsten er umuligt for kommunens personale at undgå offentliggørelsen. Helt lavpraktisk kan det være svært at 'gemme' det pågældende barn væk fra kameraet, eller at konfrontere journalister med krav om ikke at anvende optagelse, eller simpelthen på stående fod at have overblik over, hvilke af børnene der er adressebeskyttede. Dette sammenholdt med, at der generelt set vil være en minimal risiko for borger ved offentliggørelse betyder, at kommunen ikke vil foretage sig yderligere i de pågældende situationer.

Optagelse af borgermøder
Det er ikke tilladt at lave optagelser af borgermøder fx i forbindelse med høring af en lokalplan. Dette er begrundet i, at det formål, man gerne vil opnå med optagelsen (fx gennemsigtighed og mulighed for deltagelse for dem, der ikke kan deltage i arrangementet, så det er muligt at høre, præcis hvad der er sagt) kan opnås ved mindre indgribende foranstaltninger, nemlig et skriftligt referat, der kan offentliggøres efterfølgende. Der er altså tale om en ikke-proportional handling.

Kommunen kan i særlige tilfælde vælge at afvige fra denne retningslinje. I så fald skal beslutningen nedfældes i et notat, og der stilles en række krav til kommunen i forhold til at oplyse deltagerne på borgermødet om optagelserne.

Notatet skal indeholde:

- Gode argumenter for, hvorfor det er nødvendigt at optage
- Argumentation i forhold til hvordan formålet med behandlingen er proportionelt
- Hjemlen (ofte databeskyttelsesforordningens art. 6, litra e – myndighedsudøvelse)
- Overvejelser i forhold til, hvor optagelsen efterfølgende placeres/udstilles, og hvor længe det så vil være nødvendigt at have det gemt og udstillet

Derudover skal kommunen:

- Overveje, hvordan kameraet skal vende (fx kun op mod en scene og ikke mod publikum)
- Oplyse borgeren om, at der optages, både ved tilmelding og igen ved starten af mødet
- Overveje, at det faktum, at der optages, måske medfører, at nogle ikke har lyst til at deltage

Borgeres private brug af billeder

Ansatte kan opleve situationer, hvor borgere som privatpersoner tager billeder eller optager video af andre borgere i kommunalt regi, fx til et arrangement på en kommunal institution. I så fald har de personer, som tager et billede eller laver en optagelse, ansvaret for data. Det betyder, at kommunen således ikke har et dataansvar for billed- og videomaterialet.

Det anbefales, at institutioner, som ofte oplever disse situationer, har interne aftaler og regler om, hvordan man bedst muligt kan tage hensyn til de andre borgere.

Eksempler på situationer:

- Mor henter billeder fra AULA af andres børn til brug til en børnefødselsdag.
- Far optager en teaterforestilling på sit kamera.
- Beboer tager billeder fra et arrangement på et plejecenter og lægger det på sin Facebook-profil.

Billeder af ansatte

Kommunen må gerne uden den ansattes samtykke lægge portrætbilleder af de ansatte i interne systemer, fx intranettet TRYK, med henblik på, at de ansatte kan sætte ansigt på kolleger, de har kontakt med.

Hvis det er nødvendigt af hensyn til arbejdets karakter, har kommunen mulighed for gennem ansættelseskontrakten at betinge sig, at der sker offentliggørelse af nødvendige (arbejdsrelaterede) oplysninger om den ansatte på kommunens hjemmeside, herunder portrætbilleder. Dette vil kunne være tilfældet, hvis der er tale om stillinger, hvor den pågældendes person er i centrum for arbejdet, eller hvor den ansatte har funktioner særligt rettet mod offentligheden.

Nogle ansatte besidder desuden offentlige embeder, hvor det er en naturlig del af stillingen at være kendt udadtil for borgere og i nogle tilfælde være kontaktperson for borgere. Det kan

fx være databeskyttelsesrådgiver, borgerrådgiver, ledere eller kommunalbestyrelsesmedlemmer. I disse tilfælde har kommunen hjemmel til offentliggørelse, men kommunen sikrer, at den pågældende person får mulighed for godkende, at der lægges oplysninger frem om vedkommende.

Hvis kommunen ønsker at anvende billede/video af ansatte i markedsføringssammenhænge, fx i informationsfoldere eller rekrutteringsvideoer, anvendes samtykke som hjemmel, og her er det vigtigt, at de ansatte aktivt tilvælger deltagelsen uden at blive spurgt direkte. Fx kan man sende en mail til en afdeling, hvori man bredt efterspørger deltagere til en rekrutteringsvideo fremfor at spørge enkelte medarbejdere direkte. Dette skyldes, at der via ansættelsesforholdet er et iboende magtforhold, som bevirker, at de ansatte ved direkte forespørgsel kan føle sig forpligtet til at deltage.

Sociale medier

I Jammerbugt Kommune er det kun tilladt at bruge følgende sociale medier: Facebook, Instagram, YouTube, Twitter og LinkedIn. Hvis en afdeling ønsker at oprette en profil på et andet socialt medie, skal afdelingen først kontakte Sikkerhedsrådgiveren på sikkerhed@jammerbugt.dk for at sikre sig, at det kan sikkerhedsgodkendes.

Det skal understreges, at retningslinjerne kun gælder for medarbejderes brug af sociale medier i arbejdsmedfør. Retningslinjerne omhandler således ikke de ansattes egne (private) ytringer og indlæg på sociale medier.

Overvej nødvendigheden

Ønsker man at oprette en ny side eller gruppe på et socialt medie, skal man altid overveje, om man kan nå ud med det samme budskab via en anden kommunikationskanal. Når man deler billeder, video eller oplysninger på sociale medier, bliver det som udgangspunkt gjort offentligt tilgængeligt for alle brugere på det sociale medie. Det er derfor vigtigt at være opmærksom på, hvad formålet med delingen er og dernæst at overveje, om dette formål kan opnås på andre kommunikationsplatforme. Hvis man fx vil orientere om noget, der som udgangspunkt kun er relevant at vide for et begrænset antal modtagere, kan dette med fordel gøres i et nyhedsbrev eller pr. mail. Ønsker man derimod at orientere om noget, der kan være relevant for den bredere offentlighed, kan det være fint at dele på et socialt medie, hvor det kan nå bredt ud.

Sociale medier må som udgangspunkt ikke bruges til at kommunikere med andre ansatte i kommunen eller samarbejdspartnere fra fx andre kommuner eller leverandører. Her er det et krav, at afdelingen anvender Teams eller andre indkøbte løsninger som kommunikationskanal.

Udarbejd en procedurebeskrivelse

Alle afdelinger med sider eller grupper på sociale medier skal udarbejde skriftlig dokumentation, hvori overvejelserne for, hvordan man vil overholde retningslinjerne, dokumenteres. Til dette formål findes en skabelon på Tryk, som skal udfyldes og journaliseres i SBSYS: 'Skabelon - Procedure for sider og grupper på sociale medier'.

Brug ikke sociale medier til sagsbehandling
Kommunen må aldrig sagsbehandle på sociale medier. Det skyldes, at sociale medier som udgangspunkt er usikre kommunikationskanaler, og derfor må kommunen aldrig opfordre eller invitere borgerne til at sende personhenførbare beskeder eller information via disse kanaler.

Hvis borgere stiller spørgsmål, der kan være personhenførbare, skal man henvise til en sikker kommunikationskanal som fx Digital Post eller telefonisk kontakt. Hvis en borger deler følsomme eller fortrolige oplysninger på kommunens sider eller grupper, fx i et kommentarspor, skal administratoren slette det fra opslaget hurtigst muligt og derefter skrive en kommentar til borgeren om, at vedkommende i stedet skal benytte en sikker forbindelse.

Hvis borgere kontakter en ansat via den ansattes private profil på et socialt medie, er den ansatte ikke forpligtet til at besvare henvendelsen. Hvis den ansatte selv ønsker det, kan vedkommende besvare borgers henvendelse med følgende besked: *"Hej xx. Du har kontaktet mig på min private profil, og vi må ikke sagsbehandle på Facebook. Du kan i stedet ringe til kommunens omstilling på tlf. 7257 7777."*

Kontrollér administratorroller
Af forretningsmæssige og sikkerhedsmæssige årsager er det et krav, at der minimum er to administratorroller tilkoblet alle sider og grupper. Den nærmeste leder, hvis afdeling har oprettet en side eller en gruppe, har ansvaret for, at der indføres en lokal procedure for, hvordan man tildeler og nedlægger administratorrollerne. Derudover skal lederen sikre, at der mindst to gange årligt føres kontrol af brugere på den pågældende side eller gruppe. Proceduren og resultater af kontrollerne anføres i skabelonen 'Procedure for brug af Facebook'.

Oplys om brug af cookies
På alle sider og -grupper skal der så vidt muligt oplyses om det sociale medies brug af cookies og linkes til deres cookiepolitik. På en Facebook-side kan man fx benytte følgende tekst: *"Når du færdes på vores Facebook-side, registrerer Facebook din færden ved hjælp af cookies. Det betyder bl.a., at vi kan få statistik over vores besøgende, ligesom Facebook bruger oplysningerne til at målrette indhold til dig. Læs mere om Facebooks brug af cookies."*

Slå sikkerhedsindstillinger til
En medarbejder, som administrerer en side eller gruppe på vegne af Jammerbugt Kommune, er ofte nødt til at have sin private profil tilkoblet siden eller gruppen. Ofte vil

sociale medier ikke tillade, at man opretter mere end én personlig profil eller opretter en "falsk" profil for at administrere en side eller gruppe. Det er derfor nødvendigt, at medarbejderens private profil tilknyttes Jammerbugt Kommunes sider og grupper. Som medarbejder skal man derfor være opmærksom på at skifte mellem sin private profil og virksomhedsprofilen for at beskytte sin egen identitet og separere arbejdsrelateret og privat indhold.

Kommunen ønsker at minimere brugernes mulighed for deling af personoplysninger ved at slå følgende sikkerhedsindstillinger til for henholdsvis sider og grupper. Der tages udgangspunkt i Facebook, men samme foranstaltninger skal så vidt muligt bruges på alle sociale medier.

For Facebook-sider:

- Indstillingen "Opslag fra besøgende" skal være deaktiveret.
- Indstillingen "Beskeder" skal være slået fra. Indstillingen resulterer i, at besøgende ikke kan komme i kontakt med Facebook-sidens administratorer. Der skal i stedet være en henvisning til Jammerbugt Kommunes hovednummer, hjemmeside og mailadresse.
- Messenger-funktionen, som automatisk er tilgængelig på alle Facebook-sider, skal deaktiveres. Man må ikke besvare direkte beskeder fra borgere via Messenger-funktionen, da kommunikation med borgere skal ske gennem sikre kanaler. Du kan sende borger sikkert videre med følgende besked:

  "Når du vil sende en mail til Jammerbugt Kommune med fortrolige og følsomme oplysninger, skal du benytte en "sikker forbindelse". Du vil blive bedt om at logge på med dit MitID. Send sikker post for borger (indsæt link)[1] eller Send sikker post for virksomheder (indsæt link)[2]."

For Facebook-grupper:

- Indstillingen "Hvem kan lave opslag?" skal sættes til 'Kun administratorer'.
- Indstillingen "Hvem kan godkende medlemsanmodninger?" skal sættes til 'Kun administrator og ordstyrer'.

[1] *post.borger.dk/send/ce71360c-06c8-4477-a4a4-222e8334b853/a307e17f-5695-4928-8ddd-76eb 58170d3a/*
[2] *virk.dk/digitalpost/new/ce71360c-06c8-4477-a4a4-222e8334b853/a307e17f-5695-4928-8ddd-76 eb58170d3a/*

Deling af andre brugeres opslag
Man må gerne dele opslag fra andre sider og grupper, som Jammerbugt Kommune er ansvarlig for. Den pågældende afdeling i Jammerbugt Kommune, som oprindeligt lavede opslaget, har ansvaret for at sikre, at kommunens regler er overholdt, herunder at vurdere, hvorvidt der skulle indhentes samtykke til offentliggørelse af billeder.

Deling af opslag fra pressen er også tilladt, og her behøver medarbejderne ikke at foretage sig noget, inden delingen foretages.

Deling af andre brugeres opslag, fx en forælder til en skoleelev eller en virksomheds opslag, frarådes som udgangspunkt. Hvis man alligevel ønsker at dele et konkret opslag, skal man sikre sig, at den bruger, som oprindeligt lavede opslaget, har indhentet samtykke, hvis kommunens regler vurderer dette som værende nødvendigt.

Særligt for Facebook: Brug kun lukkede grupper
En gruppe kan være offentlig eller lukket, og der må kun anvendes lukkede grupper, da alternativet til en offentlig gruppe er en side. I en offentlig gruppe kan alle blive medlem uden administrators godkendelse og kan bruges til branding/markedsføring, og denne mulighed anbefales ikke, da en offentlig Facebook-side kan bruges til samme formål og i højere grad lever op ovennævnte sikkerhedskriterier. En lukket gruppe kræver administrators godkendelse, før brugere kan blive medlem, og indholdet i gruppen er kun tilgængeligt for gruppemedlemmer.