Socialforvaltningens vejledning i

Sikker Digital Kommunikation

SOCIALFORVALTNINGEN

I denne vejledning kan du læse om, hvad sikker digital kommunikation er, og hvorfor vi skal være opmærksomme på, ikke at sende personoplysninger og værdidata til borgere og virksomheder på usikre digital måder.

På side 5 i vejledningen kan du også læse om, hvilke sikre digitale kanaler vi i SOF kan bruge, når vi kommunikerer med eksterne parter, eksempelvis borgere og virksomheder.

FORMÅL

Hovedformålet med denne oversigt er at skabe et overblik over, hvordan vi som ansatte i SOF kan kommunikere digitalt med borgere og virksomheden inden for de juridiske og it-sikkerhedsmæssige rammer.

Vejledningen er udarbejdet ud fra forskellige lovgrundlag, herunder Serviceloven, Lov om Digital Post og Persondatalovgivningen samt ud fra Københavns Kommunes it-sikkerhedspolitik, og giver en samlet it-sikkerhedsstatus på de digitale kanaler og de underliggende teknologier, som ansatte i SOF kan anvende til daglig kommunikation med borgere og virksomheder.

Vejledningen dækker over de digitale kommunikationskanaler, som vi bruger i den daglige kommunikation og sagsbehandling med borgere og virksomheder. Vejledningen afdækker også hvordan vi som ansatte i SOF skal sikre en god tone i kommunikationen.

HVAD ER SIKKER DIGITAL KOMMUNIKATION?

Ved sikker digital kommunikation forstås de sikre digitale kanaler, som ansatte i SOF kan benytte i den daglige kontakt med eksterne parter: Borgere, samarbejdspartnere, myndigheder, virksomheder, foreninger osv.

En kanal er sikker, hvis den er blevet sikkerhedsgodkendt af it-sikkerhed i KIT, hvilket betyder, at kanalen kan anvendes af ansatte til kommunikation med borgere og virksomheder, hvor der indgår følsomme persondata og værdidata.

Udbuddet af digitale kanaler er omfangsrige for borgere og virksomheder, men antallet af kanaler, der indeholder følsomme persondata og værdidata, som forvaltningen må anvende til kommunikation er begrænsede. Derfor er det vigtigt at vide, at vi som borgere kan anvende digitale kanaler mere frit, end hvis vi er ansat i en offentlig myndighed eller virksomhed.

ROLLER OG ANSVAR?

Når du som ansat i Københavns Kommune går på arbejde, er der forskellige regler for, hvordan du må bruge digitale kanaler til kommunikation, end hvis du benytter disse kanaler som privat person.

Som privat person/borger, er der ikke særlige regler for, hvordan man kommunikerer og sender følsomme data til andre. Som borger skal man selv sikre sig, at man benytter sikre kommunikationskanaler, hvis man vil undgå at følsomme data kommer til uvedkommendes kendskab eller bliver misbrugt.

Som ansat i KK er der nogle generelle it-sikkerhedsregler, som gælder for hele kommunen og som skal overholdes af alle, der er ansat i kommunen eller har driftsaftaler med kommunen. Der er regler for, hvordan vi bl.a. passer på borgernes oplysninger omkring sociale forhold, helbredsoplysninger, økonomi, sagsbehandling, pårørende, CPR-numre. Reglerne sikrer, at disse data ikke falder i de forkerte hænder og bliver misbrugt. Der er også regler for, hvordan vi sikrer en god forvaltningsskik i vores kommunikation med hinanden.

Det er lederens ansvar at sikre, at it-sikkerheden overholdes på alle niveauer

---

HVAD ER PERSONFØLSOMME DATA / VÆRDIDATA?

For at sikre, at borgernes og virksomhedernes data i Danmark ikke bliver misbrugt, har vi Datatilsynet, som overvåger persondatalovgivningen, og som sikrer, at borgere og virksomheders følsomme oplysninger samt deres retssikkerhed ikke bliver misbrugt.

Der opereres med følsomme persondata og personhenførbare data samt værdidata.

Oplysninger, der omhandler blot et af forholdende nævnt i ovenstående skema, og som indgår i samtaler, skriftlige korrespondancer og anden kommunikation med borgere eller virksomheder uden for kommunens it-netværk, skal foregå sikkert.

Personfølsomme data er blandt andet	Personhenførbare data er blandt andet	Værdidata er blandt andet
Racemæssige/etniske forhold	Alle oplysninger om en identificeret eller identificerbar fysisk person. Det vil sige alle oplysninger, som både direkte eller indirekte kan identificere en person ved et eller flere elementer. En personoplysning kan derfor også være en oplysning, der når den kombineres med andre oplysninger, kan henføre til en fysisk person. Personhenførbare oplysninger kan bl.a. være:	Økonomi
Fagforeningsmæssige forhold		It-infrastruktur
Politiske tilhørsforhold		Forretningsplaner
Helbredsforhold		Udbudsmateriale
Seksuelle forhold		Kontrakter
Religiøse / filosofiske overbevisninger		
Strafbare forhold		
Væsentlige sociale problemer, fx arbejdsløshed, misbrug mm.		
Interne familieforhold og stridigheder	Personlighedstests	
Selvmord og selvmordsforsøg	Økonomiske forhold	
Ulykkestilfælde	IP-adresse	
Bortvisning af medarbejdere	Billeder	

SIKKERHED

Københavns Kommune har en fælles it-sikkerhedspolitik, der skal sikre, at vi arbejder ensartet med it-sikkerhed i kommunen, og at vi ikke overtræder persondatalovgivningen. It-sikkerhed handler ikke kun om den bagvedliggende teknik, men lige så meget om, hvordan vi bruger teknologien, altså hvilke arbejdsgange vi skal bruge.

Hvis vi bruger teknologien forkert risikerer vi at sende følsomme persondata usikkert.

Kommunen har mange data liggende – både følsomme og værdidata – og det kan få alvorlige konsekvenser for borgerne eller kommunen, hvis disse oplysninger bliver ændret og misbrugt af uvedkommende.

Når vi kommunikerer med eksterne parter uden for vores eget it-netværk, sender vi data om borgere og virksomheder ud på servere, som alle i princippet kan få adgang til.

Mange af de digitale kommunikationskanaler vi bruger sender data ud på Internettet på serverer rundt omkring i verden, som bliver ejet af udenlandske virksomheder. Data, der ligger på "fremmede" servere er ikke sikre, og kan hackes af kriminelle. Derfor er det vigtigt, at vi som ansatte i en myndighed før vores yderste for at følsomme data om borgere og virksomheder ikke falder i de forkerte hænder, og det kan vi ved at anvende sikkerhedsgodkendte kommunikationskanaler.

I det følgende kan du læse om, hvilke sikre digitale kanaler vi i SOF kan bruge, når vi kommunikerer med eksterne parter, eksempelvis borgere og virksomheder.

TELEFONI

TELEFON: Vi må gerne ringe og have personfølsomme samtaler med en borger / virksomhed – som ansat i KK har vi tavshedspligt og skal sikre os at andre uvedkommende ikke kan overhøre samtalen.

BESKEDER PÅ TELEFONSVARER: Vi må gerne lægge en meget kort og nøgtern besked uden personfølsomme oplysninger på modtagerens telefonsvarer.

Eksempelvis: *"Hej, det er Helle Hansen fra Borgercenter Handicap. Jeg har prøvet at ringe til dig, og vil gerne tale med dig, så kan du ringe på tlf. nr. 33 33 33 17 når du har tid?"*

SMS-KOMMUNIKATION: Vi må ikke sende sms'er til borgere med personfølsomt indhold, hverken fra arbejdstelefonen eller en privat mobiltelefon – Alene det forhold, at vi sender en sms fra en socialmyndighed kan tolkes, som om borgeren har en relation til / en sag i Socialforvaltningen, og det er en personfølsom oplysning.

Hvis sms-kommunikationen skal praktiseres, anbefales det af datatilsynet, at vi bruger et særskilt it-system, eksempelvis NemSMS, der kan sende nøgterne beskeder fra en PC, og at vi har fået skriftligt samtykke til at sende en sms-besked til modtageren.

Eksempelvis fra NemSMS: *"Husk fin tid på afdeling Q på Hvidovre Hospital kl. 15, de. 3. januar 2017. Mvh Hvidovre Hospital."*

Læs mere om NemSMS

SKÆRMKOMMUNIKATION

SKYPE FOR BUSINESS: I dag anvender vi skærmkommunikationsløsningen "Skype for Business" fra en PC eller mobile enheder til at kommunikere med borgere og samarbejdspartnere – det sparer transporttid og er god service.

Medarbejdere skal huske at dokumentere samtalen (som ved telefonopkald) i form af et notat, hvori det fremgår hvilken medarbejder, der har foretaget opkaldet, hvornår opkaldet er foretaget samt hvilken borger, det er foretaget til. Der skal ske journalisering i et fagsystem.

Læs mere om skærmkommunikation

SRIFTLIG KOMMUNIKATION

DIGITAL POST TIL BORGERE: Vi må gerne sende Digital Post til borgernes digitale postkasse på borger.dk / e-boks.dk. Faktisk er det lovbestemt, at det offentlige skal sende deres skriftlige meddelelser med Digital Post. I KK bruger vi it-systemet Doc2mail, der er integreret i både CSC Social og e-Doc. Hvis en borger er fritaget for Digital Post, sender Doc2mail i stedet et fysisk brev. '

Link til sådan gør du

DIGITAL POST TIL VIRKSOMHEDER: Alle virksomheder har en digital postkasse på virk.dk, som vi kan sende digital post til via Doc2mail. Det er virksomhedens CVR-nummer, der skal bruges for at sende digitalt. Vi kan også sende et fysisk brev gennem Doc2mail.

Link til sådan gør du

"SIKKER POST" TIL MYNDIGHEDER: De fleste myndigheder i Danmark er på en fælles sikker løsning, der gør det muligt for ansatte i det offentlige at sende direkte til en medarbejders e-mailadresse sikkert. I Outlook har vi "send sikkert"-knappen, som sørger for at sende din mail sikkert. "Send sikkert"-knappen kan også fortælle om den offentlige mailadresse er sikker eller ej.

Link til sådan gør du

"SIKKER POST" TIL BORGERE OG VIRKSOMHEDER: I Outlook kan vi sende til virksomheder og borgeres digitale postkasser på borger.dk / e-boks.dk og virk.dk med "send sikkert"-knappen. Men der er nogle ekstra arbejdsgange, som vi SKAL udføre, for at sikre, at juridiske krav til den efterfølgende journalisering er overholdt.

Link til sådan gør du

SOCIALE MEDIER

Facebook og andre sociale medier er blevet en del af vores privat- og arbejdsliv. Derfor er Facebook også blevet en platform, hvor arbejde og privatliv nemt flyder sammen. Måske er vi venner med chefen og kolleger, som kigger med, når vennerne kommenterer på vores privatliv. Når arbejds- og privatliv smelter sammen, er det godt at vide, hvad vi må og ikke må, når vi bruger de sociale platforme – og hvordan vi sikrer en god tone på Internettet.

Københavns Kommune brander sig og kommunikerer på flere sociale medier, eksempelvis på Facebook, Twitter og Snapchat. Læs mere her http://kff.kkintra.kk.dk/indhold/kender-du-kks-sociale-medier.

De sociale platforme anvendes fortrinsvist til at sprede viden og nyheder til borgerne i København, og for mange borgere er det en god måde at få information om kommunens nyheder på. MEN platformene er ikke sikre, og der må ikke forekomme nogen form for korrespondance med borgerne, der direkte eller indirekte kan vise, at borgeren eller andre har en sag i kommunen (overtrædelse af persondataloven.)

I det følgende finder du et udpluk af regler for god brug af internettet som ansat i Københavns Kommune.

SOM ANSAT

KOMMUNIKATION OM INTERNE FORHOLD: Det er vigtigt, at vi holder en god tone på Internettet og husker, at vi ikke må udtale os ærekrænkende, urimeligt groft eller give urigtige oplysninger om væsentlige forholde inden for vores arbejdsområde. Det kan få personalemæssige konsekvenser.

DELTAGE I DAGLIGE DEBATTER/YTRINGSFRIHED: Som offentligt ansat kan vi på egne vegne fremsætte personlige meninger om alle emner – også emner om vores eget arbejdsområde. MEN som offentligt ansat skal vi præcisere, at vi udtaler os på egne vegne, hvis der er risiko for, at en udtalelse kan opfattes som et udtryk for arbejdsgiverens (kommunens/institutionens) synspunkter – uden at være det.

VENNEANMODNINGER: Online venskaber med borgere eller pårørende er som udgangspunkt en dårlig idé, da der er en risiko for at skabe forventninger om, at vi altid er "på", eller risiko for at få negative kommentarer, vi ikke ønsker, skal blandes ind i vores privatsfære. Der vil også kunne opstå situationer, hvor dialogen tager karakter af sagsbehandling, og det er hverken foreneligt med persondataloven eller kommunens internet- og e-mailpolitik.

KOMMUNEIKATION MED BORGER / VIRKSOMHED / SAMARBEJDSPARTNER: Det kan være problematisk at kommunikere med borgere/samarbejdspartnere/virksomheder på Twitter, Snapchat, LinkedIn, Facebook osv. fra sin private profilside eller på/fra andres sider eller via lukkede grupper, som har forbindelse eller relation til arbejdet eller kommunen. Det er derfor besluttet, at indbakkefunktionen på kommunens Facebook-sider skal være inaktiv. Vi kan meget let overtræde persondatalovgivningen og tavshedspligten, hvis vi fører samtaler via de sociale platforme. Data på de sociale medier eges af private firmaer, og kan misbruges af firmaerne til eksempelvis videresalg til medicinalfirmaer, reklamebureauer mv.

BRUG AF BILLEDER / VIDEOER: Det er ikke tilladt at lægge billeder/videoer ud af genkendelige personer på de sociale medier UDEN at have fået deres skriftlige samtykke. For mindre børn og borgere uden mulighed for at give samtykke kan forældrene eller påførende/værge give samtykke.

Link til samtykkeerklæring på kk.dk

NYHEDER: Nyheder, der ikke henviser til borgere eller indeholder personfølsomme oplysninger, må gerne offentliggøres.

Eksempelvis: "Der afholdes fest på Bostedet Falken for beboere og familie/pårørende d. 12. april 2016".

Link til brug af sociale medier og offentligt ansattes ytringsfrihed

LOKAL SOCIAL MEDIE-POLITIK: Det kan give god mening at få drøftet spillereglerne for brug af Facebook og de andre sociale platforme ved hjælp af en lokal socialmedie-politik. Den kan hjælpe arbejdspladsen og den enkelte til at finde ud af, hvordan man kan håndtere brugen af eksempelvis Facebook i relation til arbejdet, og hvad vi kan forvente af hinanden.

- Må vi bruge Facebook i arbejdstiden på samme måde, som hvis det var en telefon?
- Hvem skal vi spørge, om vi må lægge billeder fra faglige eller sociale arrangementer eller papirer fra arbejdspladsen på Facebook?
- Hvordan kan vi holde en god omgangstone medarbejdere imellem på Facebook?
- Kan ledelsen være "venner" med medarbejderne på sociale medier?
- Må vi hjælpe beboerne med at offentliggøre billeder og tekster på deres profiler?

SOM ENHED/TILBUD I KOMMUNEN

Et botilbud eller en særlig enhed i forvaltningen må gerne oprette en Facebook-side om enhedens tilbyd/services, men skal være opmærksom på, hvorledes der kommunikeres med ord og billeder. Denne type side er den mest anvendelige i forhold til borgerrettet kommunikation. Her "liker" folk siden. Man vælger selv, om man vil godkende medlemmer, eller om alle kan blive medlem.

På denne type side har vi også mulighed for at angive "spilleregler" for siden, angive kontaktdetaljer på stedet, poste indlæg og beskrive, hvornår vi fjerne anstødelige indlæg mv. Vær dog opmærksom på, at sætte tid og ressourcer af til at overvåge og skrive historier til profilen så vi opfanger spørgsmål og kommentarer i tide. Det kan være en god idé at udpege en eller flere administratorer til at sikre, at reglerne for Facebook-siden overholdes.

Link til sådan gør du

NÅR BORGEREN SKRIVER PÅ ENHEDENS FACEBOOK-SIDE: Der gælder de samme regler for indlæg på nettet, som for andre typer af henvendelser. De sociale medier egner sig imidlertid ikke til behandling af enkelt- og personsager.
Bliver der skrevet om personsager, skal vi:

- Fjerne indlægget
- Sørge for, at der bliver oprettet en administrativ sag
- Behandle sagen som enhver anden henvendelse
- Give borgeren besked om, at indlægget er slettet, og hvorfor det er slettet.

Indlæg på en offentlig Facebook-side skal betragtes som en borgerhenvendelse. Som ansvarlig for profilen har vi som enhed eller center ansvar for at journalisere efter reglerne.

Det betyder, at:

- Indlæg om konkrete sager skal journaliseres
- Generelle henvendelser og spørgsmål skal besvares inde på siden.

Vi har pligt til at vejlede og pligt til at besvare henvendelser, også på Facebook. Vi har også pligt til at videresende indlæg til den rette enhed.

Det betyder, at:

- Hvis vi får et spørgsmål, der ligger uden for jeres område, men inden for kommunens område, har vi pligt til at henvise vedkommende til, hvordan de kan få besvaret deres spørgsmål.
- Vi har også pligt til at videresende henvendelsen til rette enhed.

Reglerne om tavshedspligt og videregivelse af oplysninger gælder også på de sociale medier.