KØBENHAVNS KOMMUNE
Borgerrådgiveren

Økonomiforvaltningens Direktion
Rådhuspladsen 77
1550 København V

31-07-2012

Sagsnr.
2012-72630

Dokumentnr.
2012-593196

Sendt med e-mail

Sikker e-post, forvaltningens j.nr. 2012-85563

Ved brev af 21. maj 2012 iværksatte jeg en konkret egen driftundersøgelse af, om medarbejderne i Københavns Kommune i tilstrækkeligt omfang er informeret om anvendelsen af sikker e-post af Koncernservice, som leverer rådgivning og administration inden for it til medarbejderne i Københavns Kommune. Koncernservice varetager som led i disse opgaver Kundecenteret, som dels vejleder brugerne ved spørgsmål om it, og dels driver brugerportalen.

Baggrunden for undersøgelsen var en henvendelse hertil fra en borger, som klagede over at have modtaget en e-mail indeholdende personfølsomme oplysninger, uden at reglerne om sikker digital kommunikation var overholdt. Denne klage er fortsat under behandling hos Borgerrådgiveren.

Baggrunden for undersøgelsen var endvidere, at jeg i forbindelse med min besvarelse af borgerens henvendelse ved brug af sikker e-mail blev opmærksom på flere forhold, som gav anledning til bekymring for sikkerheden i anvendelsen af sikker e-post til fremsendelse af personfølsomme oplysninger i Københavns Kommune generelt.

Jeg fandt derfor anledning til at iværksætte nærværende konkrete egen driftsundersøgelse.

I forbindelse med iværksættelsen skrev jeg den 21. maj 2012 blandt andet følgende til forvaltningen:

> ”Det forekommer mig således, i forbindelse med anvendelse af ’Brugervejledning – Sikker e-post (eDag2)’, at brugervejledningen flere steder er uhensigtsmæssigt formuleret, og kan give anledning til misforståelser for brugerne, idet det fremstår som valgfrit om afsendelse af sikker e-post skal ske med digital underskrift og kryptering.
>
> Som eksempel herpå kan der henvises til det indledende afsnit på side 1 i brugervejledningen:
>
> ***’Digital underskrift og kryptering***

Borgerrådgiveren

Vester Voldgade 2A
1552 København V

Telefon
3366 1400

E-mail
borgerraadgiveren@kk.dk

EAN nummer
5798009800053

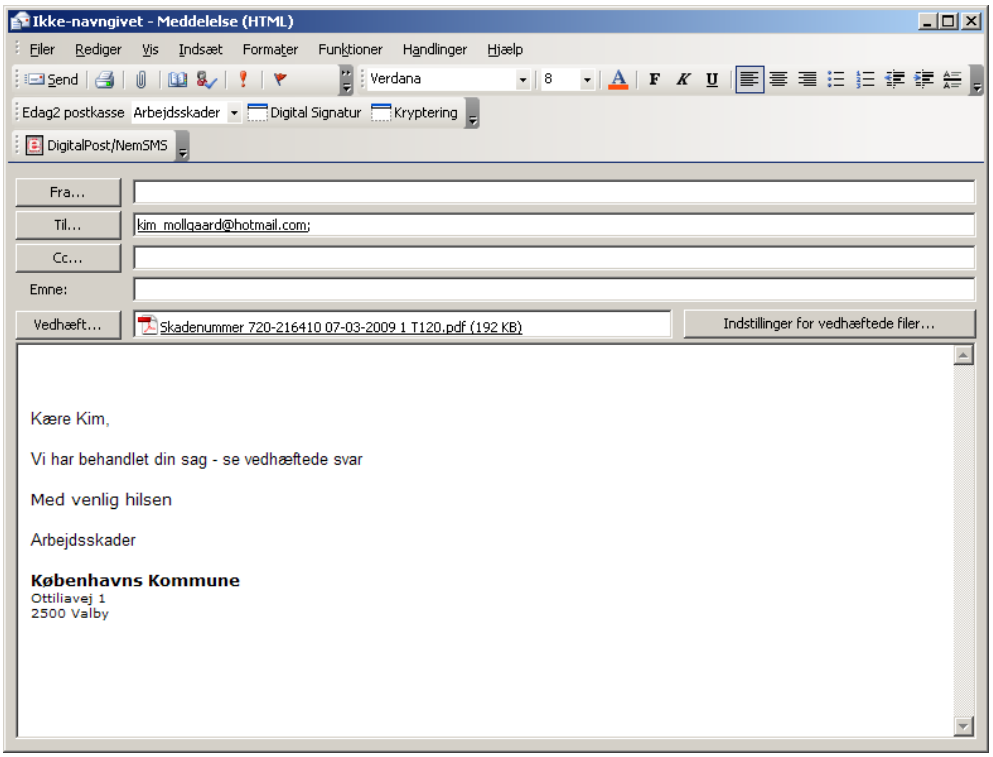
www.borgerraadgiver.kk.dk

Når man anvender certifikater til sikker e-post, er det muligt at vælge, om der kun skal sendes med signatur eller med både digital underskrift og kryptering.
Kun digital underskrift: *Giver modtageren af en meddelelse garanti for, at den kommer fra den person, som påstår at have sendt den (= autenticitet) og sikkerhed for, at en modtaget meddelelse er identisk med den meddelelse, som afsenderen sendte (= integritet).*

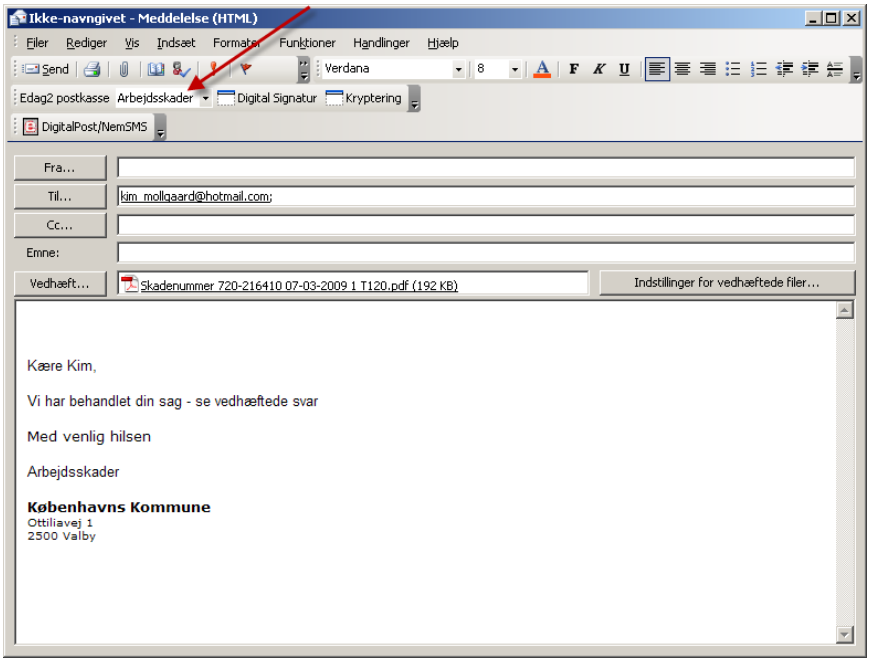
Digital underskrift + kryptering: *Som ovenfor + sikkerhed for, at ingen uvedkommende kan få kendskab til meddelelsens indhold (fortrolighed).'*

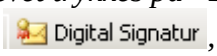
Som eksempel herpå kan der endvidere henvises til side 4 og 5 i brugervejledningen, hvor der fremgår følgende vedrørende fremsendelse af sikker post til borgeren:

'2. Afsendelse af sikker mail fra myndigheden til en borger.

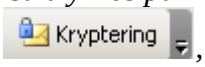


3. Efter at brevet er blevet udarbejdet vælges sikker postkasse i "Drop Down" boksen Edag2 postkasse. Edag2 Postkassen vil være den afsender der fremsender e-posten og der vil blive anvendt det certifikat der er tilknyttet afsenderen til denne e-post.



- *Hvis man ønsker e-post digitalt underskrevet trykkes på "Digital Signatur", Knappen ændrer udseende til* 

, når den er aktiveret.
- *hvis man ønsker e-posten digitalt krypteret dvs. beskyttet så kun modtageren kan læse e-posten så trykkes på "Kryptering".*

  Knappen ændrer udseende til 

, når den er aktiveret. '

Ved anvendelse af sikker post i menuen i Outlook i den af Koncernservice valgte løsning, blev jeg i forbindelse med fremsendelse af sikker e-mail til borgeren endvidere opmærksom på, at menupunktet sikker post og den tilhørende 'Drop Down' boks, hvori det vælges om en meddelelse skal sendes med digital signatur og krypteret, forsvinder efter nogle få minutters forløb. En af mine medarbejdere fik ved telefonisk henvendelse til Koncernservice oplyst, at Koncernservice er opmærksom på fejlen, men at den tidligst vil blive rettet efter sommerferien. Jeg fik endvidere oplyst, at det ikke er muligt at sende en e-mail som sikker post når menupunktet sikker post og 'Drop Down' boksen er forsvundet fra den konkrete mail. Dette er gældende, selv om det *er* valgt at sende e-mailen som sikker post inden menupunktet sikker post og 'Drop Down' boksen forsvinder. Dette indebærer, at e-mailen kun sendes som sikker post, såfremt afsendelse sker inden 'Drop Down' boksen forsvinder og brugere modtager ikke nogen advarsel om at e-mailen ikke længere kan sendes som sikker. "

I forbindelse med iværksættelsen bad jeg særligt forvaltningen om at tage stilling til følgende spørgsmål:

> ”
>
> - Hvor længe har Koncernservice, Københavns Kommune været opmærksom på menupunktet sikker post og ’Drop Down’ boksens delvist manglende funktionalitet?
>
> - Hvad har Koncernservice, Københavns Kommune gjort for at gøre medarbejdere i kommunen opmærksom på problemet?
>
> - Hvad er udsigterne for at problemet afhjælpes?
>
> - Om mine betragtninger om ’Brugervejledning – Sikker e-post (eDag2)’, giver anledning til overvejelser? ”

Jeg modtog ved e-mail af 19. juni 2012 svar fra Økonomiforvaltningen af den 12. juni 2012. Af svaret fremgår blandt andet følgende:

> ”Koncernservice har til ovenstående specifikke spørgsmål, følgende svar:
>
> **Ad 1)** Fejlen er ikke tidligere meldt ind til Koncernservice, men KS Systemejer havde ved et tilfælde, et par dage før fejlen blev indmeldt af Borgerrådgiverens medarbejder i maj 2012, identificeret fejlen.
>
> **Ad 2)** Systemejer i Koncernservice har orienteret forvaltningernes deltagere i Digitalt Kommunikationsforum, samt efter at sagen er rejst af Borgerrådgiveren, indrykket følgende tekst på KKnet siden ’Sikkerpost – DigitalPost – SecureBusinessMail’:
>
> **OBS! Der er konstateret en fejl i ’Sikkerpost’ fanen i Outlook**.
> ’Sikkerpost’ fanen, kan efter en tid med inaktivitet på Outlookklienten forsvinde. Fejlen er bestilt rettet hos leverandøren og forventes rettet og udrullet i august.
> Det er vigtigt, ved afsendelse af sikkerpost, at du sikre dig, at fanen og knapperne er synlige og aktiverede. Er dette ikke tilfældet, er du nødt til at starte forfra.
> Det kan anbefales, at du først aktiverer knapperne umiddelbart inden afsendelse af den sikre post, eller evt. bruger den ’gamle’ metode med #k-koderne# i emnefeltet.
>
> **Ad 3)** Fejlen er meldt til systemleverandøren, og vil efter udbedring og test, blive udrullet på Københavns Kommunes Pc’ere. Dette forventes at kunne ske medio august.

Ad 4) Brugervejledningen der refereres til er udarbejdet af KS systemejer og beskriver systemets funktionaliteter, herunder muligheden for at vælge om forsendelsen skal ske signeret, krypteret eller begge dele. Vejledningen beskriver de muligheder der er i systemet, og har ikke til formål at sætte retningslinjer for hvordan sagsbehandlerne i forvaltningerne overholder gældende lovgivning, kanalstrategi og/eller andre politikker vedr. kommunikation mellem forvaltning og borger.

Indtil eventuelle tværgående fælles standarder for digital kommunikation er implementeret, er det den enkelte forvaltning, som skal udarbejde reglerne for brugen af de værktøjer der stilles til rådighed."

På baggrund af de i undersøgelsen rejste spørgsmål og svaret fra Økonomiforvaltningen forekommer det mig mest hensigtsmæssigt at opdele min undersøgelse i en del om kommunikation vedrørende driftsforstyrrelser, og en del om ansvaret for udarbejdelse af brugervejledninger.

Kommunikation vedrørende driftsforstyrrelser:

Af Økonomiforvaltningens brev af 12. juni 2012 fremgår det, at systemejer har orienteret forvaltningernes deltagere i Digitalt Kommunikationsforum om, at der er konstateret fejl i sikkerpost fanen i Outlook. Af brevet fremgår det endvidere, at der efter min iværksættelse af nærværende undersøgelse er informeret om fejlen på KKnet.

Det er fra Koncernservice oplyst, at Digitalt Kommunikationsforum er et forum nedsat af kommunens itchefer, og at der mindst er tilknyttet én medarbejder fra hver forvaltning. Der findes ikke umiddelbart tilgængelig viden om kommissorium eller sammensætningen af Digitalt Kommunikationsforum på KKnet.

Den overordnede lovgivning vedrørende behandling af personoplysninger findes i persondataloven og sikkerhedsbekendtgørelsen.

De overordnede retningslinjer for varetagelsen af digital sikkerhed i Københavns Kommune findes i "It-sikkerhedspolitik for Københavns Kommune" og "Regulativ for it-sikkerhed i Københavns Kommune" som begge er vedtaget af Borgerrepræsentationen. Spørgsmålet om kommunikation vedrørende driftsforstyrrelser, er ikke reguleret i disse retningslinjer.

Koncernservice har udarbejdet en intern skrivelse om "procedure for information til brugere, bestillere mv. ved nedbrud" som findes på KKnet. Skrivelsen behandler også spørgsmålet om driftsforstyrrelser.

Proceduren er udateret, men må forudsættes at være gældende, da den er tilgængelig på hjemmesiden.

Koncernservice har i skrivelsen opregnet procedurer for kommunikation ved driftsforstyrrelser. Procedurerne indeholder en graduering af alvorligheden af driftsforstyrrelsen, således at procedure 1 anvendes ved de mindst alvorlige driftsforstyrrelse, mens procedure 5 anvendes ved de mest alvorlige driftsforstyrrelser:

> ”
>
> 1. Tekniker fra Servicedesk eller fagenhed lægger besked på Broadcast ved kendskab om driftsnedbrud. Den pågældende tekniker eller Incident manager opdaterer løbende broadcast, typisk med 2 – 4 timers interval.
> 2. Incidentmanager vurderer, om hændelsen er af et sådant omfang, at der skal besked på telefonslusen. Dette gælder typisk hændelser med mange berørte brugere.
> 3. Incidentmanager sender mail til bestillerne hvis hændelsen er længerevarende, kritisk og/eller berører mange brugere. Orientering vil normalt ske ved større nedbrud af kundevendte systemer. Mail kan evt. erstattes med SMS-tjeneste
> 4. Incidentmanager vurderer hvorvidt nyhed / it-driftsstatus skal lægges på kundeportalen[1]. Dette sker typisk ved større nedbrud, der berører mange brugere på tværs af forvaltningerne. Med nyheden sendes et link til bestillerne.
> 5. Ved nyhed på kundeportalen tilgår der mail til forvaltningernes webredaktører med opfordring til at linke til forvaltningernes intranet hvis webredaktørerne skønner at nyheden er relevant.”

Overordnet fremgår det af proceduren, at det er baseret på en individuel vurdering af driftsforstyrrelsens omfang og alvor, herunder hvor mange brugere der er berørt af driftsforstyrrelsen, hvilken konkret procedure der anvendes til kommunikation ved driftsforstyrrelser.

Således som jeg læser brev fra Koncernservice til mig af 12. juni 2012, er ingen af de procedurer for kommunikation ved driftsforstyrrelser, som fremgår af skrivelsen ”Procedurer for information til brugere, bestillere mv. ved nedbrud”, anvendt i forbindelse med Koncernservices konstatering af en, efter min vurdering ganske alvorlig fejl i sikkerheden ved afsendelse af sikker e-post.

Min baggrund for at betragte den aktuelle fejl som en alvorlig fejl er, at fejlen medfører høj risiko for, at der sendes personfølsomme oplysninger fra kommunens medarbejdere uden at reglerne om fortrolig behandling af personoplysninger i persondataloven og sikkerhedsbekendtgørelsen er overholdt.

[1] Jeg lægger til grund, at den omtalte kundeportal, fra den 15. december 2011 er identisk med brugerportalen.

Jeg må således konstatere, at Koncernservice ikke anser fejlen i 'Sikkerpost' fanen i Outlook for omfattet af "Procedurer for information til brugere, bestillere mv. ved nedbrud".

Henset til den forholdsvis vage og uklare definition af begrebet "nedbrud", har jeg ikke fundet fuldt tilstrækkeligt grundlag for at udtalt kritik af dette.

Det er ikke muligt for mig på det foreliggende grundlag at vurdere, hvorvidt de skridt som Koncernservice har iværksat for at informere om fejlen i praksis er tilstrækkelige, herunder fordi det indebærer en nærmere undersøgelse af hvorledes informationen spredes i de enkelte forvaltninger. Jeg må lægge til grund, at Koncernservice på baggrund af samarbejdet med forvaltningerne har skønnet, at det var effektivt, hvorfor jeg ikke har fundet tilstrækkeligt grundlag for at udtale kritik heraf. Jeg må dog indskyde, at jeg har mine tvivl om, hvorvidt informationen er nået ud til alle eller hovedparten af relevante medarbejdere i kommunen.

Det er imidlertid min opfattelse, at Koncernservice straks ved konstateringen af fejlen burde have iværksat skridt til på relevant og effektiv måde at orientere om fejlen. Jeg finder det beklageligt, at det ikke skete straks.

Jeg anbefaler på denne baggrund, at Koncernservice udarbejder retningslinjer for, hvordan sådanne systemfejl, som forøger risikoen for it-sikkerhedsbrud, formidles hurtigt og effektivt.

Jeg beder om underretning om, hvad min anbefaling giver anledning til.

Jeg har ikke bemærkninger i forhold til de skridt, der er taget, i forhold til at afhjælpe den konkrete driftsforstyrrelse, da disse umiddelbart forekommer mig hensigtsmæssige.

Jeg har ikke herved taget stilling til, om Koncernservices skrivelse: "Procedurer for information til brugere, bestillere mv. ved nedbrud" er tilstrækkelig til at sikre tilfredsstillende information til brugerne ved alvorlige driftsforstyrrelser.

Ansvar for at udarbejde korrekte brugervejledninger og den konkrete vejledning

De overordnede retningslinjer for varetagelsen af digital sikkerhed i Københavns Kommune findes, som ovenfor nævnt, i "It-sikkerhedspolitik for Københavns Kommune" og "Regulativ for it-sikkerhed i Københavns Kommune" som begge er vedtaget af Borgerrepræsentationen.

It-sikkerhedspolitik og regulativ for it-sikkerhed i Københavns Kommune fastlægger blandt andet følgende om ansvar og organisering:

- at **It-sikkerhedsfunktionen** fører det daglige tilsyn med overholdelsen af kommunens sikkerhedsbestemmelser og koordinerer kommunens it-sikkerhedsarbejde på vegne af Økonomiudvalget
- at **Direktionen** inden for eget forvaltningsområde har ansvaret for fastlæggelse af it-sikkerhedsniveauet, for gennemførelse af risikovurderinger, og for iværksættelse af foranstaltninger som er nødvendige for at opnå en tilstrækkelig it-sikkerhed
- at Direktionen inden for eget område udpeger en **ledelsesrepræsentant** til at varetage koordineringen med Koncernservice og sikre, at der træffes de nødvendige it-sikkerhedsmæssige beslutninger indenfor området
- at Direktionen indenfor eget område udpeger en **systemejer** samt en stedfortræder for hvert it-system. For de fællessystemer som Koncernservice er ansvarlig for udpeger Direktionen for Koncernservice en systemejer. Systemejeren er ansvarlig for et it-systems funktionalitet, opbygning, anvendelse og sikkerhedsløsning samt for at iværksætte de nødvendige foranstaltninger til beskyttelse af it-systemet og de person- og værdioplysninger der er indeholdt heri. Systemejeren skal endvidere sikre at der udarbejdes procedurer for driftsafviklingen.
- at Direktionen for Koncernservice skal udpege en **it-ansvarlig** og en stedfortræder for denne. Den It-ansvarlige skal sikre, at opbygning og anvendelse af kommunens it-platform, driftsmiljø og kommunikationsforbindelser er i overensstemmelse med de it-sikkerhedsmæssige krav.
- at **Koncernservice** udgør et selvstændigt it-sikkerhedsområde under Økonomiforvaltningen, og at Koncernservice på vegne af forvaltningerne skal varetage systemejerskabet for fællessystemer.
- at der skal etableres et **udvalg for it-sikkerhed** som har til opgave at drøfte it-sikkerhedsmæssige forhold.

Koncernservice er systemejere på Microsoft Exchange, Sikkerpost (SMB) og DigitalPost (DKAL).

Systemejere defineres i ”Regulativ for it-sikkerhed i Københavns Kommune” som ”den medarbejder der har ansvaret for det pågældende it-systems sikkerhedsløsning, opbygning, anvendelse og for beskyttelse af de oplysninger, der indgår i systemet”.

På KKnet findes en ”Opgavebeskrivelse for systemejer” som angiver de vigtigste opgaver, som direkte eller indirekte følger af ”Regulativ for it-sikkerhed i Københavns Kommune”.

Af denne opgavebeskrivelse fremgår det, at systemejeren blandt andet har ansvaret for, at der foreligger skriftlig opdateret brugervejledning. Det fremgår nærmere under bilaget "specifikation af systemdokumentation", at en del af systemdokumentationen er en brugervejledning. Brugervejledningen beskrives som en "skriftlig beskrivelse af, hvordan brugerne betjener systemets forskellige funktioner fra start/inddata til slut/uddata.

Økonomiforvaltningens Direktion har i brev af 12. juni 2012 blandt andet skrevet følgende til mig:

> "**Ad 4)** Brugervejledningen der refereres til er udarbejdet af KS systemejer og beskriver systemets funktionaliteter, herunder muligheden for at vælge om forsendelsen skal ske signeret, krypteret eller begge dele. Vejledningen beskriver de muligheder der er i systemet, og har ikke til formål at sætte retningslinjer for hvordan sagsbehandlerne i forvaltningerne overholder gældende lovgivning, kanalstrategi og/eller andre politikker vedr. kommunikation mellem forvaltning og borger.
>
> Indtil eventuelle tværgående fælles standarder for digital kommunikation er implementeret, er det den enkelte forvaltning, som skal udarbejde reglerne for brugen af de værktøjer der stilles til rådighed."

Jeg forstår indholdet af ovennævnte svar således, at det er forvaltningens opfattelse, at det er den enkelte forvaltnings ansvar at udarbejde vejledninger for lovlig anvendelse af systemer, hvor Koncernservice er systemejer.

Jeg må desuden forstå, at den brugervejledning, som er udarbejdet af Koncernservice, alene er tænkt som en beskrivelse af, hvordan brugerne betjener systemets forskellige (tekniske) funktioner, og at vejledningen ikke har til formål at sætte retningslinjer for, hvordan sagsbehandlerne i forvaltningerne overholder gældende lovgivning, kanalstrategi og/eller andre politikker vedr. kommunikation mellem forvaltning og borger, idet dette efter Koncernservices opfattelse må fastlægges af de enkelte forvaltninger.

Jeg forstår principperne bag denne beskrivelse af opdelingen i Koncernservices hhv. forvaltningernes ansvarsområder (som jeg ikke i denne sammenhæng har bemærkninger til). Uagtet den formelle ansvarsfordeling i kommunen, som den måtte være fastlagt af lovgiver eller Borgerrepræsentationen eller udviklet af forvaltningerne over tid, har jeg imidlertid ikke kendskab til nogen regel, instruks eller lignende, som forhindrer Koncernservice i at indtænke *fælles formål* i en sådan funktionsvejledning, herunder de tværgående gældende rammer som kommunen er underlagt, f.eks. ufravigelige lovgivningsmæssige rammer.

Jeg går da også ud fra, at Økonomiforvaltningen er enig med mig i, at de brugervejledninger, der stilles til rådighed for brugerne af systemerne, naturligvis skal være i overensstemmelse med ufravigelige krav i relevant gældende lovgivning og med Borgerrepræsentation vedtagne politikker, også selv om (hoved)ansvaret for overholdelsen ligger andre steder i kommunen.

Jeg bemærker desuden, at It-sikkerhedsfunktionen, som blandt andet har til opgave at føre tilsyn med it-sikkerheden og at tilrettelægge informations- og uddannelsesaktiviteter for medarbejdere, der varetager kommunens it-sikkerhedsfunktioner, er forankret i netop Koncernservice.

Jeg mener derfor, at det beror på en vildfarelse, at Koncernservice tilsyneladende arbejder ud fra en forestilling om, at ressortfordelingen kan begrunde en ansvarsfralæggelse, når det kommer til korrekt information om it-sikkerhedsspørgsmål. Jeg finder det beklageligt, at Koncernservice og Økonomiforvaltningen har denne opfattelse.

Jeg finder i det konkrete tilfælde, at det er en fejl, når Koncernservice blandt andet har valgt under overskriften "Afsendelse af sikker mail fra myndigheden til en borger" at beskrive tekniske løsninger (f.eks. ukrypteret e-post), som ikke er lovlige i forbindelse med sikker post. Uagtet, at systemet er i stand til at udføre en sådan handling, vil dette nemlig ikke udgøre sikker e-post i sikkerhedsbekendtgørelsens forstand, hvorfor denne løsning ikke må anvendes ved elektronisk forsendelse af personfølsomme oplysninger.

Jeg mener desuden, at det er urealistisk at forvente, at de (formentlig mange) medarbejdere, som gør brug af vejledningen, indser, at den ikke kan anvendes efter sit indhold, men skal suppleres med forvaltningernes egne vejledninger, som måtte eller ikke måtte være udarbejdet. Dette understøttes yderligere af, at der i "Københavns Kommunes e-mail og internetpolitik" henvises til denne vejledning.

Vejledningen er efter min opfattelse vildledende og udgør i sig selv en sikkerhedsrisiko, hvilket jeg finder kritisabelt.

Jeg henstiller på denne baggrund til Koncernservice om at omformulere vejledningen, så den ikke er i risiko for at vildlede brugerne til at anvende usikker post ved elektronisk kommunikation af personfølsomme oplysninger. Jeg henviser til mit brev af 21. maj 2012 og gennemgangen af vejledningen dér.

Jeg beder om underretning om, hvad min henstilling giver anledning til.

Jeg har ved mit brev af dags dato orienteret borgeren, som gav mig anledning til denne undersøgelse, dels om forvaltningens svar og dels om min udtalelse.

Med venlig hilsen

Johan Busse
Borgerrådgiver

/ Rikke Gredal
Jurist