KØBENHAVNS KOMMUNE
Borgerrådgiveren

Socialforvaltningen

Brev er d.d. fremsendt pr. e-mail.

16-11-2012

Sagsnr.
2012-98616

Dokumentnr.
2012-900691

Håndtering af fortrolige og følsomme personoplysninger ved Center for Misbrugsbehandling og Pleje, jf. forvaltningens sagsnummer 2012-119928

Ved brev af 16. august 2012 iværksatte jeg en konkret egen driftundersøgelse vedrørende Center for Misbrugsbehandling og Plejes praksis ved elektronisk kommunikation indeholdende fortrolige og følsomme personoplysninger.

Jeg oplyste blandt andet følgende i mit brev til Socialforvaltningens direktion:

> "…
> En borger rettede ved e-mail af 11. maj 2012 henvendelse til Center for Misbrugsbehandling og Pleje under Socialforvaltningen, da han ønskede at klage over forvaltningen. Samtidig hermed orienterede borgeren Borgerrådgiveren om klagen.
>
> Ved e-mail af 4. juli 2012 modtog Borgerrådgiveren kopi af forvaltningens svar af 5. juni 2012 til borgeren. Jeg går ud fra, at dette er tilstrækkeligt til at identificere sagen. Svaret fra centret, som indeholder fortrolige og følsomme personoplysninger, fremstår sendt pr. e-mail til borgeren, men umiddelbart uden brug af sikker digital kommunikation.
>
> En kopi af svaret er medsendt til forvaltningen i forbindelse med fremsendelsen af dette brev.
>
> Københavns Kommunes udmeldte praksis ved digitale forsendelser er imidlertid at bruge enten digitale postkasser eller signaturbeviser, hvilket vil fremgå af de enkelte e-mails med oplysning om referencekoder eller signaturbeviset.
>
> Ved min gennemgang af forvaltningens svar har jeg dog, som anført, konstateret, at hverken referencekode eller signaturbevis fremgår af de sendte e-mails. Jeg må derfor umiddelbart lægge til grund, at de nævnte e-mails er afsendt uden den fornødne beskyttelse.

Borgerrådgiveren

Vester Voldgade 2A,

Telefon
3366 1400

Telefax
3366 1390

E-mail
borgerraadgiveren@kk.dk

EAN nummer
5798009800053

www.borgerraadgiver.kk.dk

Om den fornødne beskyttelse henviser jeg til følgende retsgrundlag:

Af persondatalovens § 41, stk. 3, jf. lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (med senere ændringer), fremgår, at dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Af sikkerhedsbekendtgørelsens § 14, jf. bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, må der kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

I Datatilsynets sikkerhedsvejledning, jf. vejledning nr. 37 af 2. april 2001, er det nærmere angivet, hvorledes sikkerhedsbekendtgørelsens krav vil kunne opfyldes. Det fremgår blandt andet heraf, at der for transmission af personoplysninger over åbne net (f.eks. Internettet) gælder minimumskrav om sikkerhedsforanstaltninger.

Følgende vedrørende eksterne kommunikationsforbindelser fremgår af vejledningen:

> 'Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.
>
> Bestemmelsen gælder enhver form for telekommunikation i forbindelse med behandling af personoplysninger, f.eks. forsendelse af oplysninger med (…) ekstern e-post (…). De særlige sikkerhedsforanstaltninger skal træffes efter myndighedens vurdering af sikkerhedsrisici i det konkrete tilfælde, herunder med hensyntagen til karakteren af de omhandlede oplysninger.
>
> For at kunne fastlægge sikkerhedsniveauet er det nødvendigt, at den dataansvarlige foretager en samlet risikovurdering, som omfatter alle elementer i kommunikationsforbindelsen.
> (…)

> For transmission af personoplysninger over **åbne net** (f.eks. Internet) gælder konkret nedenstående minimumskrav om sikkerhedsforanstaltninger:
>
> Ved transmission af oplysninger over det åbne Internet er der generelt en risiko for, at oplysningerne undervejs læses og endog ændres af uvedkommende. Derudover er der en risiko for, at parterne i kommunikationen ikke er dem, de udgiver sig for.
>
> Disse risici må vurderes af den dataansvarlige i den konkrete situation, således at der kan træffes de fornødne sikkerhedsforanstaltninger.
>
> Hvad angår fortrolighed kan denne sikres ved forsvarlig kryptering af de transmitterede oplysninger. Hvis der er tale om transmission af fortrolige oplysninger, herunder personnummer, skal der som minimum foretages en kryptering. Hvis de transmitterede oplysninger er af følsom karakter (omfattet af persondatalovens § 7, stk. 1 og § 8, stk. 1), skal der anvendes en stærk kryptering, baseret på en anerkendt algoritme.
>
> Sikkerhed for autenticitet (afsenders og modtagers identitet) og integritet (de transmitterede oplysningers ægthed) må sikres i fornødent omfang ved anvendelse af passende sikkerhedsforanstaltninger, f.eks. elektronisk signatur eller individuelle, fortrolige adgangskoder.'

Endelig fremgår følgende af § 36, stk. 2, i Regulativ for it-sikkerhed i Københavns Kommune:

> 'E-mails der indeholder fortrolige og følsomme personoplysninger eller værdioplysninger, og som sendes over Internettet eller andre åbne netværk, skal altid krypteres med godkendt software. Krypterede e-mails modtages i og afsendes fra sikre e-postkasser i kommunen.'

Jeg har på baggrund af den konkrete sag besluttet at indlede en konkret egen driftundersøgelse af Center for Misbrugsbehandling og Plejes praksis ved elektronisk kommunikation om fortrolige og følsomme personoplysninger.

Jeg beder derfor Socialforvaltningen om at oplyse, hvorledes det i forvaltningen (her Center for Misbrugsbehandling og Pleje) sikres, at de nævnte bestemmelser om forsendelse af e-mails indeholdende fortrolige og følsomme personoplysninger overholdes.

Jeg beder desuden forvaltningen om at oplyse, om der efter forvaltningens vurdering generelt sker overholdelse af de nævnte bestemmelser i forbindelse med behandlingen af konkrete sager."

Den 8. november 2012 modtog jeg følgende besvarelse dateret den 7. november 2012 fra forvaltningen:

"…

Socialforvaltningens bemærkninger

Socialforvaltningen har anmodet Center for Misbrugsbehandling og Pleje om en udtalelse i den konkrete sag. Nedenstående udtalelse er Socialforvaltningens samlede besvarelse.

Ad 1. Hvordan sikres det i forvaltningen (her Center for Misbrugsbehandling og Pleje), at bestemmelserne omkring anvendelse af sikker e-mail overholdes, når e-mailen indeholder fortrolige og personfølsomme oplysninger.

Center for Misbrugsbehandling og Pleje har over for forvaltningen meget beklaget, at de ikke i den konkrete borgersag har sikret sig, at korrespondancen mellem forvaltningen og borgeren skete fra og til en sikker e-mailadresse.

Center for Misbrugsbehandling og Pleje har samtidig oplyst, at der i centret er en klar procedure for håndtering af elektronisk kommunikation. Proceduren blev senest sendt rundt til alle medarbejdere i centret den 8. juni 2012. I proceduren er der et særligt afsnit vedrørende afsendelse af fortrolige oplysninger, jf. vedlagte kopi af proceduren.

Centret er i forbindelse med iværksættelsen af Borgerrådgiverens undersøgelse blevet opmærksom på nødvendigheden af at gentage og indskærpe proceduren for afsendelse af fortrolige og personfølsomme oplysninger.

For fremadrettet at sikre overholdelse af bestemmelserne om forsendelse af e-mails indeholdende fortrolige og personfølsomme oplysninger, vil centret gennemgå proceduren og samtidig indarbejde oplysninger om brugen af Doc2mail i proceduren, se nedenfor under Ad 2. Den reviderede procedure vil herefter blive sendt til alle centrets ledere og medarbejdere.

Der vil også blive taget initiativ til at gennemgå proceduren med forvaltningens Digitaliseringskontor, og få en medarbejder derfra til at komme og præsentere retningslinjer for sikker mail afsendelse - både på Centerledelsesniveau og på afdelingslederniveau.

Herudover har Center for Misbrugsbehandling og Pleje oplyst, at de i 2012 har afholdt 2 introarrangementer for nye medarbejdere, hvor der også er informeret om personfølsomme oplysninger og anvendelsen af sikker e-mail.

Socialforvaltningen er enig med Center for Misbrugsbehandling og Pleje i, at der i den konkrete sag er sket en meget beklageligt fejl, da det ikke er sikret ved fremsendelsen af de fortrolige og personfølsomme oplysninger, at mail-korrespondancen mellem forvaltningen og borgeren skete fra og til en sikker e-mailadresse, ligesom borgeren heller ikke har eller kunne give tilladelse til, at der blev fremsendt fortrolige eller personfølsomme oplysninger via en almindelig (usikker) e-mail. Sådanne oplysninger må — hvis borgeren ikke kan modtage post via sikker e-mail — sendes som almindelig papirpost.

Socialforvaltningen finder på baggrund af tilbagemeldingen fra Center for Misbrugsbehandling og Pleje om de initiativer, som centret iværksætter som følge af den meget beklagelige hændelse, ikke anledning til at foretage videre.

Ad 2. Sker der efter forvaltningens vurdering generelt overholdelse af bestemmelserne om anvendelse af sikker e-mail i forbindelse med behandling af konkrete sager.

Socialforvaltningens opmærksomhed på elektronisk kommunikation og tiltag vedrørende brugen heraf

Socialforvaltningen har siden igangsætning af eDag1 den 1. september 2003 haft opmærksomheden rettet på, at den digitale kommunikation mellem borgeren og forvaltningen skal være sikker, dvs. krypteret og signeret.

Der er i Socialforvaltningen således flere muligheder for at sende sikker post til borgere/virksomheder, nemlig Secure Business Mail, Sikker post via Outlook, Digital post via Doc2mail og selvfølgelig fysiske breve via postvæsnet. Siden 2009 har anbefalingen på tværs af forvaltningerne i Københavns Kommune været at bruge Doc2mail til kommunikation med borgere og eksterne samarbejdspartnere, herunder virksomheder.

Socialforvaltningen har gennemført en række tiltag for at introducere og udbrede viden og læring omkring brugen af elektronisk kommunikation. Det drejer sig blandt andet om følgende:

- Roadshows, hvor den autorisationsansvarlige, lokale koordinatorer m.fl. har informeret om Doc2mail/sikkerpost til ledere/områdeansvarlige i Socialforvaltningen, samt for hele

kontorer, centre m.v., der har meget elektronisk kommunikation
- Informationsmøder om, hvorfor der skal anvendes sikre e-mail, hvad forskellen er på almindelig mail og sikker mail, og hvorledes sikker mail anvendes
- Superbrugere er uddannet til at oplære og igangsætte nye medarbejdere samt supportere medarbejdere i anvendelsen af Doc2mail
- Vejledninger i arbejdsgange og informationer om sikker post og Doc2mail ligger opdaterede på kknet og kk.dk
- Der afholdes hver tredje måned superbrugermøder, hvor superbrugerne opdateres om systemet, lovgivningen og den digitale udvikling i KK
- På baggrund af den nye lov om digital post fra 1. juli 2012 er forvaltningens Digitaliseringskontor i gang med et roadshow rettet til ledelsen og superbrugerne i Socialforvaltningen for at fortælle, om vigtigheden i at bruge Doc2mail i forbindelse med sikkerheden med personfølsomme oplysninger og den nye lovgivning i forbindelse med digitale mail til digitale postkasser.

  Der lægges stor vægt på at informere om, at medarbejderne skal bruge Doc2mail til at besvare borger/virksomheds-henvendelser for at sikre, at personfølsomme oplysninger sendes som sikker kommunikation. I den forbindelse opdateres superbrugerne, vejledninger i arbejdsgange, e-learning og informationskampagner lægges på kknet og kk.dk, der vil være digital post kampagner i form af plakater! brochurer og uddannes digitale ambassadører.

Socialforvaltningens sikre postkasser og brugen af disse

I Socialforvaltningen er der 100 sikre postkasser, som enhederne bruger til at modtage og sende sikker post dagligt til borgere og virksomheder. Antallet af sikre postkasser er inden for de sidste par år blevet næsten femdoblet.

Den autorisationsansvarlige for sikker post i forvaltningen underviser postbestyrere i brugen af de sikre postkasser og lovgivningen om sikker post, og der ligger vejledninger på kknet. Dagligt anvendes de sikre postkasser lokalt af sagsbehandlerne, og almindelig praksis er, at hvis en borger henvender sig via hotmail, f.eks. gmail.com eller andre usikre digitale kanaler, så kan sagsbehandleren i en ny mail via outlook henvise borgeren/virksomheden til Secure Business Mail-system eller Digital post.

Sagsbehandleren svarer herefter borgeren via Doc2mail eller som et fysisk brev, indtil sagsbehandleren modtager en sikker mail fra borgeren/virksomheden. Modtager sagsbehandleren en

sikker mail fra en borger/virksomhed, svarer sagsbehandleren med signering og krypteringskoden i emnefeltet.

Socialforvaltningen ser det stigende antal anmodninger fra forvaltningens enheder om sikre postkasser som et tegn på enhedernes opmærksomhed på afsendelse af sikker post mellem forvaltningen og borgerne/virksomhederne. Oplysninger fra forvaltningens Digitaliseringskontor om, at der i perioden januar 2011 til september 2012 er sendt 62.500 sikre mails (både Secure Business mail og Digital post (sendt med Doc2mail)) viser også, at sikker mail er et kendt værktøj i forvaltningens enheder.

Socialforvaltningen kan desuden afslutningsvis bemærke, at forvaltningen ikke ser indikationer for at antage — feks. via et øget antal henvendelser fra borgerne om forkert brug af mail - at der generelt skulle være et manglende kendskab til brugen af sikker mail blandt forvaltningens medarbejdere."

Jeg er enig med forvaltningen i, at sagsbehandlingen i den konkrete sag er meget beklagelig.

Idet jeg har noteret mig det oplyste om forvaltningens initiativer dels konkret i Center for Misbrugsbehandling og Pleje dels i øvrigt generelt i forvaltningen, foretager jeg ikke ydereligere.

Med venlig hilsen

Johan Busse
Borgerrådgiver

/ Maja Markman
Jurist