



Københavns Kommune
Beskæftigelses- og Integrationsforvaltningen
Bernstoffsgade 17
1592 København V

Sendt til: xw53@bif.kk.dk

15. april 2010

Vedrørende Københavns Kommunes forespørgsel vedrørende sms-løsning

Datatilsynet
Borgergade 28, 5.
1300 København K

Ved brev af 2. juli 2009 har Københavns Kommune rettet henvendelse til Datatilsynet med en forespørgsel vedrørende en sms-løsning.

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2009-323-0115
Sagsbehandler

Københavns Kommune har oplyst, at Beskæftigelses- og Integrationsforvaltningen ønsker at indføre en "e-mail og sms"-model, som f.eks. skal anvendes til at erindre borgere om aftaler med forvaltningen. Det fremgår af henvendelsen, at ordningen dels skal varetage hensynet til borgerne dels skal sikre bedre udnyttelse af forvaltningens ressourcer. Det er i første omgang tanken, at ordningen skal omfatte forskellige former for påmindelser til borgerne, men kommunen ønsker på længere sigt, at det bliver muligt at føre en dialog med borgeren via sms.

1. Indledningsvist skal Datatilsynet gøre opmærksom på, at ved iværksættelse af et nyt system, der som det påtænkte indebærer behandling af personoplysninger, har den dataansvarlige myndighed eller virksomhed ansvaret for, at systemet opbygges og indrettes, således at persondataloven¹ iagttages.

2. Persondataloven indeholder i kapitel 11 regler om behandlingssikkerhed. Af persondatalovens § 41, stk. 3, følger, at der skal træffes 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.

Nærmere regler om de i § 41, stk. 3, anførte sikkerhedsforanstaltninger er fastsat af Justitsministeriet i sikkerhedsbekendtgørelsen.² Af sikkerhedsbekendtgørelsens § 14 følger, at der alene må etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

¹ Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.

² Bekendtgørelse nr. 258 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning med senere ændringer.

Kravet i sikkerhedsbekendtgørelsens § 14 er nærmere uddybet i Datatilsynets sikkerhedsvejledning,³ hvor det bl.a. er anført:

”For transmission af personoplysninger over **åbne net** (f.eks. Internet) gælder konkret nedenstående minimumskrav om sikkerhedsforanstaltninger:

Ved transmission af oplysninger over det åbnet 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 sikre ved forsvarlig kryptering af de transmitterede oplysninger. Hvis der er tale om transmission af fortrolige oplysninger, herunder personnummer, skal der som minimum foretages 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 sikre i fornødent omfang ved anvendelse af passende sikkerhedsforanstaltninger, f.eks. elektronisk signatur eller individuelle, fortrolige adgangskoder.”

3. Fremsendelse via sms må efter Datatilsynets opfattelse betragtes som brug af et åbent net. Ved fremsendelse af almindelige sms'er sker der imidlertid ikke kryptering.

Med minimumskravene i sikkerhedsvejledningen er udgangspunktet derfor, at sms'er fra offentlige myndigheder ikke må indeholde fortrolige og følsomme personoplysninger.

Datatilsynet vil være indstillet på at vurdere, om brug af sms til håndtering af fortrolige og følsomme personoplysninger alligevel vil kunne finde sted i et nærmere fastlagt omfang. En sådan fravigelse af Datatilsynets sikkerhedsvejledning vil skulle forelægges for Datarådet.

Hvis kommuner og andre myndigheder ønsker at bruge sms til fremsendelse af fortrolige og følsomme personoplysninger, skal Datatilsynet opfordre til, at konkrete eksempler og forslag til kriterier for brugen fremsendes til Datatilsynet med henblik på en nærmere vurdering.

³ Vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

4. København Kommune har i henvendelsen anført, at kommunen betragter det som berettiget at rette henvendelse til borgerne via sms i tilfælde, hvor borgeren har oplyst deres telefonnummer til forvaltningen, samt i tilfælde, hvor forvaltningens navne- og adresseoplysninger matcher oplysninger, der kan tilgås gennem en oplysningstjeneste (f.eks. TDC).

En tilsvarende problemstilling blev behandlet i den FAQ om Edag2, som er tilgængelig på Finansministeriets hjemmeside. Her fremgår bl.a. følgende:

”Offentlige myndigheder har i dag ikke ret til at kommunikere elektronisk med borgere eller virksomheder, medmindre borgeren eller virksomheden har givet samtykke til denne kommunikationsform. Henviser en borger/virksomhed sig til myndigheden via e-post, er dette at sidestille med et samtykke, og myndigheden kan besvare henvendelsen elektronisk. Er der tale om henvendelser fra virksomheder, antages samtykke til elektronisk kommunikation ligeledes at være givet, blot virksomheden har angivet en e-post adresse på sit brevpapir, hjemmeside eller lignende.

Har borgeren således givet (stiltiende) samtykke til elektronisk kommunikation i forbindelse med et givent sagsforløb, må dette samtykke anses for at kunne udstrækkes til den løbende elektroniske brevveksling i forhold til sagen. Samtykket kan imidlertid ikke umiddelbart udstrækkes til nye/andre sager, og ønsker myndigheden således at kommunikere elektronisk om disse sager også, anbefales det, at borgerens samtykke indhentes på ny. - Enten som stiltiende samtykke, hvor borgeren selv retter henvendelse elektronisk om den nye sag, eller udtrykkeligt samtykke, hvor borgeren svarer bekræftende på myndighedens forslag om at kommunikere elektronisk om den pågældende sag.

Indeholder myndighedens e-post fortrolige eller følsomme personoplysninger eller andre fortrolige oplysninger, er myndigheden forpligtet til at kryptere besvarelsen for at overholde henholdsvis persondataloven og de almindelige regler om tavshedspligt.”⁴

Datatilsynet gør for god ordens skyld opmærksom på, at ovenstående ikke stammer fra Datatilsynets bidrag til Edag2 FAQ'en. Datatilsynet skal derfor henviser til Justitsministeriet for en eventuel afklaring i forhold til sms.

Umiddelbart går Datatilsynet ud fra, at det anførte om e-post også vil være gældende i forhold til sms.

Datatilsynets umiddelbare vurdering er således, at såfremt kommunen ønsker at kommunikere med en borger via sms, skal borgeren give samtykke til anvendelse af denne kommunikationsform.

⁴ Jf. FAQ om Edag2, punkt 3.5,
http://modernisering.dk/da/projekter/edag2/faq_alt_om_edag2/#c7451

Datatilsynet skal i den forbindelse anbefale, at der indgås en klar aftale om, hvilket telefonnummer sms'erne må sendes til. Dette er efter Datatilsynets opfattelse også nødvendigt til opfyldelse af persondatalovens krav om datasikkerhed, jf. persondatalovens § 41, stk. 3.

Datatilsynet skal i øvrigt bemærke, at myndigheden, når borgernes samtykke indhentes, må sikre sig, at det er den rigtige person, som afgiver oplysningerne (herunder telefonnummeret) og samtykket. Dette kan f.eks. ske ved brug af digital signatur eller ved forevisning af legitimation med billede i forbindelse med personligt fremmøde.

5. Ved anvendelse af sms som kommunikationsform må det også tages i betragtning, at mobilnumre skifter ejere. Persondataloven indebærer både krav om datakvalitet (§ 5, stk. 4) og datasikkerhed (§ 41, stk. 3). For at leve op til disse regler må de dataansvarlige for løsningerne efter Datatilsynets opfattelse etablere procedurer til sikring af, at de mobiltelefonnumre, der sendes sms'er til, til stadighed er rigtige.

6. Datatilsynet skal endelig pege på reglerne i telelovgivningen, som eventuelt kan være af betydning. Disse administreres af IT- og Telestyrelsen.⁵

7. Kopi af denne udtalelse vil blive sendt til Kommunernes Landsforening (KL). Datatilsynet vil generelt opfordre myndigheder, der har eksempler og forslag, som kan indgå i Datatilsynets vurdering (jf. punkt 3), om at fremsende disse til tilsynet senest den **20. maj 2010**.

Med venlig hilsen

Lena Andersen
Kontorchef

⁵ Bekendtgørelse af lov om konkurrence- og forbrugerforhold på telemarkedet og bekendtgørelse om udbud af elektroniske kommunikationsnet og – tjenester.