



JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 17. april 2018
Kontor: Databeskyttelseskontoret
Sagsbeh: Nanna Due Binø
Sagsnr.: 2017-0037-0005
Dok.: 707107

Hermed sendes besvarelse af spørgsmål nr. 98 vedrørende forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) (L 68) og forslag til lov om ændring af lov om retshåndhævende myndigheders behandling af personoplysninger, lov om massemediers informationsdatabaser og forskellige andre love (Konsekvensændringer som følge af databeskyttelsesloven og databeskyttelsesforordningen samt medieansvarslovens anvendelse på offentligt tilgængelige informationsdatabaser m.v.) (L 69), som Folketingets Retsudvalg efter ønske fra Peter Kofod Poulsen (DF) har stillet til justitsministeren den 9. april 2018.

Søren Pape Poulsen

/

Jakob Lundsager

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 98 fra Folketingets Retsudvalg på vegne af Peter Kofod Poulsen (DF) vedrørende L 68 og L 69:

”Vil ministeren redegøre for, om borgeres dialog med byrådsmedlemmer via email (officiel kommunal mail) vil blive ændret, såfremt den nye databeskyttelseslov vedtages i dens nuværende udformning, og om det vil medføre, at kommunalpolitikere ikke kan besvare borgeres mails direkte, men f.eks. skal sende svar via borgerens e-boks?”

Svar:

1. Reglerne om behandlingssikkerhed, herunder sikkerhed i forbindelse med elektronisk kommunikation, følger efter gældende ret af persondatalovens kapitel 11. Det følger således f.eks. af lovens § 41, stk. 3, at den 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.

Persondatalovens sikkerhedskrav for offentlige myndigheder er nærmere uddybet i sikkerhedsbekendtgørelsen (bekendtgørelse nr. 528 af 15. juni 2000 som ændret ved bekendtgørelse nr. 201 af 22. marts 2001) og i Datatilsynets sikkerhedsvejledning (vejledning nr. 37 af 2. april 2001).

Det følger af sikkerhedsbekendtgørelsens § 14, at der kun må etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger. Det følger uddybende herom af sikkerhedsvejledningen, at der generelt ved transmission af oplysninger over det åbne internet er en risiko for, at oplysningerne undervejs læses og endog ændres af uvedkommende. Det fremgår også af vejledningen, at fortroligheden kan 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.

Der er omvendt ikke et krav om, at almindelige oplysninger, der ikke er af fortrolig eller følsom karakter, krypteres i f.eks. e-mails sendt fra offentlige myndigheder.

Sikkerhedsbekendtgørelsen vil ikke kunne opretholdes, når databeskyttelsesforordningen finder anvendelse fra den 25. maj 2018, jf. betænkning 1565/2017 om databeskyttelsesforordningen, side 484. Det er dog Justitsministeriets vurdering, at databeskyttelsesforordningens artikel 32 om behandlingssikkerhed ikke sænker kravene til behandlingssikkerhed i forhold til gældende ret.

2. Det følger dog af § 8 b i lov om kommunernes styrelse, der blev indført med virkning fra den 1. januar 2018 ved lov nr. 1571 af 19. december 2017, at persondataloven ikke finder anvendelse på behandling af oplysninger, der foretages som led i varetagelsen af et kommunalbestyrelsesmedlems hverv. Ved en ændring af regionsloven er det ved samme lov sikret, at undtagelsen også omfatter regionsrådsmedlemmer.

I ændringsforslag af 18. januar 2018 til L 69 (bilag 16) foreslås det, at § 8 b i lov om kommunernes styrelse konsekvensrettes således, at det herefter fremgår, at databeskyttelsesforordningen og databeskyttelsesloven ikke finder anvendelse på behandling af oplysninger, der foretages som led i varetagelsen af et kommunalbestyrelsesmedlems hverv. Konsekvensændringen omfatter også regionsrådsmedlemmer.

Der er med denne ændring alene tale om en justering af lovteknisk karakter, som ikke ændrer på gældende ret efter lov nr. 1571 af 19. december 2017.

3. Det fremgår af forarbejderne til lov nr. 1571 af 19. december 2017, at undtagelsen i lovens § 8 b omfatter den behandling af oplysninger, der foretages som led i kommunalbestyrelsesmedlemmers hverv, herunder partieller listetilknyttet kommunikation, når medlemmet anvender en kommunikationstjeneste, som medlemmet har fået stillet til rådighed af kommunen. I praksis vil det være den behandling af oplysninger, der foretages af et kommunalbestyrelsesmedlem via en kommunikationstjeneste som f.eks. en mailkonto eller en mobiltelefon, som et kommunalbestyrelsesmedlem får stillet til rådighed som led i varetagelsen af sit hverv.

Det følger endvidere af forarbejderne, at undtagelsen i kommunestyrelseslovens § 8 b fra persondataloven indebærer, at et kommunalbestyrelsesmedlem ved en sådan behandling af oplysninger, ikke er omfattet af bl.a. persondatalovens kapitel 11 om behandlingssikkerhed.

Derudover følger det af de nævnte forarbejder, at en kommune – ligesom i forhold til oplysninger, der udleveres i papirform – fortsat vil have pligt til at sikre, at transmissionen af oplysninger til medlemmet ved anvendelse af en kommunikationstjeneste, som medlemmet har fået stillet til rådighed af kommunen, sker på en forsvarlig og sikker måde, samt at systemet i øvrigt er forsvarligt og sikkert i forhold til den behandling af oplysninger, som foretages, herunder af oplysninger, som måtte tilgå medlemmet fra kommunen som led i medlemmets varetagelse af sit hverv.

Det anføres også i forarbejderne til kommunestyrelseslovens § 8 b, at et kommunalbestyrelsesmedlem fortsat vil være omfattet af reglerne om tavshedspligt i forhold til de oplysninger, som medlemmet modtager i forbindelse med sit hverv. Det forudsættes samtidigt, at kommunalbestyrelsesmedlemmer generelt bliver gjort bekendt med, hvornår en oplysning kan være eller er omfattet af reglerne om tavshedspligt, betydningen heraf og de mulige konsekvenser ved uberettiget videregivelse af sådanne oplysninger.

4. Kommunalbestyrelsesmedlemmer må på den baggrund også i fremtiden kunne føre almindelig korrespondance fra en mailkonto, som medlemmet har fået stillet til rådighed af kommunen, uden i den forbindelse at skulle overveje spørgsmål om kryptering af korrespondancen, så længe kommunalbestyrelsesmedlemmet ikke inkluderer oplysninger af fortrolig eller følsom karakter i e-mailen.

Hvis kommunalbestyrelsesmedlemmet har behov for at inkludere oplysninger af fortrolig eller følsom karakter i en e-mail, må kommunens ovenfor nævnte forpligtelse til at sikre, at systemet er ”forsvarligt og sikkert i forhold til den behandling af oplysninger, som foretages”, indebære, at kommunen skal stille en løsning til rådighed, som sikrer, at kommunalbestyrelsesmedlemmet ikke risikerer at bryde sin tavshedspligt ved at sende ukrypterede e-mails med fortrolige eller følsomme oplysninger. I disse situationer kan det være en mulighed at benytte Digital Post-løsningen, der leveres af e-Boks, eller andre løsninger, der sikrer, at e-mailen ikke i transmissionen læses eller opsnappes af uvedkommende.