



Holbergsgade 6
DK-1057 København K

T +45 7226 9000
F +45 7226 9001
M sum@sum.dk
W sum.dk

Folketingets Sundheds- og Ældreudvalg

Dato: 17-01-2017
Enhed: Sundhedsjura og Psykiatri
Sagsbeh.: DEPTBH
Sagsnr.: 1611478
Dok. nr.: 265307

Folketingets Sundheds- og Ældreudvalg har den 20. december 2016 stillet følgende spørgsmål nr. 311 (Alm. del) til sundhedsministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra Liselott Blixt (DF).

Spørgsmål nr. 311:

”Ministeren bedes redegøre for retningslinjerne for at anvende it-eksperter, der skal arbejde med sundhedsvæsnets databaser. Ministeren bedes samtidig redegøre for, hvilke godkendelser m.v. der skal foreligge inden it-eksperter kan få adgang til at arbejde med sundhedsvæsnets databaser?”

Svar:

En IT-eksperts uberettigede videregivelse af personfølsomme oplysninger vil kunne indebære en overtrædelse af straffelovens § 152 a, hvorefter straffelovens § 152 om offentligt ansattes uberettigede videregivelse af fortrolige oplysninger vil finde tilsvarende anvendelse bl.a. på den, som er eller har været beskæftiget med opgaver, der udføres efter aftale med en offentlig myndighed. Overtrædelse af straffelovens § 152 a, jf. § 152, kan straffes med bøde eller fængsel indtil 6 måneder.

Endvidere følger det af persondatalovens § 41, stk. 1, at personer, virksomheder m.v., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

Kravet om, at vedkommende person m.v. kun må behandle oplysninger i overensstemmelse med instruks fra den dataansvarlige, indebærer bl.a., at personen m.v. ikke må behandle oplysninger til andre formål end dem, som den dataansvarlige har fastsat - herunder til egne formål - samt at vedkommende ikke må behandle oplysninger efter instruks fra andre end den dataansvarlige.

Jeg kan oplyse, at de overordnede krav til datasikkerhed følger af persondatalovens § 41, stk. 3, hvorefter en dataansvarlig myndighed skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Jeg kan endvidere oplyse, at sikkerhedsbekendtgørelsen, som er udstedt i medfør af persondatalovens § 41, stk. 5, opstiller en række nærmere krav til sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. Sikkerhedsbekendtgørelsen pålægger den dataansvarlige myndighed at fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der fremgår af sikkerhedsbekendtgørelsen. Sikkerhedsbekendtgørelsen indeholder desuden nærmere regler om bl.a. autorisation og adgangskontrol, kontrol med afviste adgangsforsøg og logning.

Derudover kan jeg oplyse, at it-sikkerhed er en hel central prioritet for regeringen. Som ligeledes oplyst i min svar på spørgsmål 308 (Alm. del), så indledte regeringen i december 2016 arbejdet med en ny strategi for cyber- og informationssikkerhed, som skal gøre danske myndigheder og private aktører inden for centrale sektorer, herunder sundhedssektoren, bedre rustet til at beskytte den danske digitale infrastruktur. Det er for mig som sundhedsminister selvfølgelig afgørende, at der er sikkerhed om og tillid til, at sundhedsdata og dermed relevante it-systemer, sikkerhedsprocedurer mv. fungerer betryggende i hele sundhedssektoren. I ØA 2016 aftalte regionerne og regeringen at styrke informationssikkerheden i regionerne ved at sikre fælles obligatoriske retningslinjer og krav til informationssikkerhed, risikostyring og kontroller.

Med venlig hilsen

Ellen Trane Nørby / Trine Berner Hansen