



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: 03-04-2018
Enhed: SUNDOK
Sagsbeh.: DEPMAHA
Sagsnr.: 1706260
Dok. nr.: 572534

Folketingets Sundheds- og Ældreudvalg har den 1. marts 2018 stillet følgende spørgsmål nr. 3 (L 143 – Forslag til lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren) til sundhedsministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra Stine Brix (EL) og Kirsten Normann Andersen (SF).

Spørgsmål nr. nr. 3:

”Ministeren bedes oplyse, om Center for Cybersikkerhed i regi af lovforslaget skal forstås som en forvaltningsmyndighed, jf. forvaltningsloven. Ministeren bedes i forlængelse heraf redegøre for kravene til centerets behandling af personoplysninger. Herunder ønskes oplyst, hvorledes kravene adskiller sig som følge af reglerne i lov om Center for Cybersikkerhed (lov nr. 713 af 25. juni 2014) i forhold til databeskyttelsesforordningen (forordning 2016/679/EU af 27. april 2016 om beskyttelse af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF) og forslaget til databeskyttelseslov (L 68), hvis Forsvarets Efterretningstjeneste ikke er omfattet af lovforslaget og forordningen.”

Svar:

Da Sundheds- og Ældreudvalgets spørgsmål omhandler, hvorvidt Center for Cybersikkerhed er en forvaltningsmyndighed, herunder hvilke krav der gælder for Center for Cybersikkerheds behandling af personoplysninger, har mit ministerium bedt Forsvarsministeriet om bidrag til besvarelsen heraf. Forsvarsministeriet oplyser følgende:

”1. Det følger af § 8 i lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed, at Center for Cybersikkerheds virksomhed er undtaget fra offentlighedsloven (bortset fra lovens § 13 om notatpligt) og forvaltningslovens kapitel 4-6. Dette gælder også for centerets kommende funktioner som nationalt centralt kontaktpunkt og CSIRT efter NIS-direktivet (Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen).

Det fremgår dog af bemærkningerne til forslaget til lov om Center for Cybersikkerhed (L 192, frem-sat 2. maj 2014), at Center for Cybersikkerhed forudsættes i videst muligt omfang at efterleve principperne i offentlighedsloven og forvaltningslovens kapitel 4-6. Det forudsættes således, at centeret – uanset at dets virksomhed er undtaget fra forvaltningslovens bestemmelser på området – i alle afgørelsessager konkret vurderer, om det er muligt at anvende forvaltningslovens principper om partens aktindsigt, partshøring og begrundelse m.v. Tilsvarende forudsættes det, at anmodninger om aktindsigt i videst muligt omfang behandles efter principperne i offentlighedsloven.

Det bemærkes i den forbindelse, at Center for Cybersikkerheds afgørelser i konkrete sager, f.eks. aktindsigtssager, kan påklages til Forsvarsministeriet.

2. Center for Cybersikkerheds virksomhed, herunder centerets kommende funktioner efter NIS-direktivet, er endvidere undtaget fra persondataloven. Denne retstilstand ventes videreført, når persondataloven med virkning fra 25. maj 2018 erstattes af databeskyttelsesforordningen (Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF) og den foreslåede databeskyttelseslov (L 68, fremsat for Folketinget den 25. oktober 2017).

Størstedelen af de centrale principper i persondataloven gælder dog for centeret, jf. kapitel 6 i lov om Center for Cybersikkerhed. Det følger således bl.a. af loven, at centeret kun må indsamle personoplysninger til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål. Endvidere må centeret ikke behandle flere personoplysninger, end hvad der kræves til opfyldelse af formålet med indsamlingen. Der stilles desuden krav om hjemmel til enhver behandling af personoplysninger, ligesom der som udgangspunkt ikke må behandles personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning og fagforeningsmæssige tilhørsforhold samt personoplysninger om helbreds-mæssige og seksuelle forhold. Centeret skal derudover sikre, at der ikke behandles urigtige eller vildledende personoplysninger. Endelig må centeret ikke opbevare indsamlede personoplysninger på en måde, der giver mulighed for at identificere den pågældende person i et længere tidsrum end nødvendigt, og centeret skal træffe passende sikkerhedsforanstaltninger ved behandlingen af personoplysninger.

Visse centrale krav efter persondataloven gælder dog ikke for Center for Cybersikkerhed. Centeret er således undtaget fra kravet om oplysningspligt overfor den registrerede samt kravet om den registreredes indsigts- og indsigelsesret.

Herudover er det Tilsynet med Efterretningstjenesterne – og ikke Datatilsynet – der fører tilsyn med Center for Cybersikkerheds behandling af personoplysninger. Tilsynet med Efterretningstjenesterne er et uafhængigt kontrolorgan, der efter klage eller af egen drift påser, at Center for Cybersikkerhed overholder reglerne vedrørende behandling af personoplysninger.

3. Endvidere følger det af § 8, stk. 2, i lov om Center for Cybersikkerhed, at forsvarsministeren kan bestemme, at kapitel 8-10 i persondataloven, kapitel 4-6 i forvaltningsloven samt offentlighedsloven helt eller delvist skal finde anvendelse for Center for Cybersikkerheds virksomhed som bl.a. myndighed for informationsikkerhed og beredskab på teleområdet.

Der har indtil videre ikke vist sig behov for at anvende denne bemyndigelse, idet der behandles ganske få personoplysninger i forbindelse med centerets virksomhed på teleområdet.

Med lovforslag L 155 om ændring af lov om Center for Cybersikkerhed, der er fremsat for Folketinget den 28. februar 2018, foreslås det bl.a., at den nævnte bemyndigelse tilpasses til den kommende regulering på databeskyttelsesområdet og NIS-området, således at forsvarsministeren vil kunne bestemme, at databeskyttelsesforordningen og den foreslåede databeskyttelseslov også helt eller delvist skal finde anvendelse for

de myndighedsopgaver, som Center for Cybersikkerhed tillægges som led i implementeringen af NIS-direktivet.

4. Blandt de nye krav, som databeskyttelsesforordningen stiller, kan fremhæves krav om udpegelse af en databeskyttelsesrådgiver, at der skal gennemføres konsekvensanalyser, og at nye systemer skal have indbygget databeskyttelse (privacy by design or by default).

For en nærmere gennemgang af forholdet mellem databeskyttelsesforordningen og persondataloven henvises i øvrigt til Justitsministeriets betænkning nr. 1565 om databeskyttelsesforordningen, del I, bind 1.”

Jeg kan henholde mig til Forsvarsministeriets bidrag.

Med venlig hilsen

Ellen Trane Nørby / Maja Holm Andreasen