

Fejl! Ukendt betegnelse for dokumentegenskab.

FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE



Folketingets Forsvarsudvalg
Christiansborg

FORSVARSMINISTEREN
Den 6. april 2018

Folketingets Forsvarsudvalg har den 20. marts 2018 stillet følgende spørgsmål nr. 5 vedrørende L 139 til forsvarsministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra ikke-medlem af udvalget (MFU) Lisbeth Bech Poulsen (SF).

Spørgsmål nr. 5:

“Vil ministeren redegøre for, hvilke konsekvenser det vil have, såfremt Center for Cybersikkerheds aktiviteter relateret til NIS-direktivet, underlægges databeskyttelsesforordningen, databeskyttelsesloven, offentlighedsloven og forvaltningsloven?”

Svar:

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, fremsat 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 helbredsmæssige 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. Tilsynet kan hos Center for Cybersikkerhed kræve enhver oplysning og alt materiale, der er af betydning for tilsynets virksomhed. Man kan som borger klage til tilsynet, hvis man

mener, at centeret ulovligt behandler personoplysninger om en. Tilsynet afgiver endvidere hvert år en redegørelse til forsvarsministeren om tilsynets virksomhed i forhold til Center for Cybersikkerhed, og redegørelsen offentliggøres.

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 informationssikkerhed 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. Som beskrevet ovenfor forudsættes Center for Cybersikkerhed i videst muligt omfang at efterleve principperne i offentlighedsloven og forvaltningslovens kapitel 4-6. Dette vil også være gældende for de myndighedsopgaver, som centeret tillægges som led i implementeringen af NIS-direktivet.

På den baggrund vurderes det ikke i praksis at ville indebære væsentlige ændringer, såfremt bemyndigelsen til at sætte offentlighedsloven og forvaltningslovens kapitel 4-6 i kraft for denne del af Center for Cybersikkerheds virksomhed anvendes.

5. Såfremt databeskyttelsesforordningen og den foreslåede databeskyttelseslov helt eller delvist sættes i kraft for de myndighedsopgaver, som Center for Cybersikkerhed tillægges som led i implementeringen af NIS-direktivet, vil det betyde, at der vil blive stillet en række nye – og især formelle – krav til Center for Cybersikkerheds behandling af personoplysninger.

Henset til de regler for behandling af personoplysninger, der allerede i dag gælder for Center for Cybersikkerhed, vurderes det ikke, at de krav, der følger af databeskyttelsesforord-

ningen og den foreslåede databeskyttelseslov, vil medføre en realitetsændring for så vidt angår borgernes retssikkerhed og hensynet til privatlivets fred.

Kravene vil imidlertid have administrative konsekvenser for Center for Cybersikkerhed. Blandt de nye krav, som databeskyttelsesforordningen stiller, kan således fremhæves krav om udpegning af en databeskyttelsesrådgiver, at der skal gennemføres konsekvensanalyser, og at nye it-systemer skal have indbygget databeskyttelse (privacy by design or by default). Såfremt disse krav skal finde anvendelse for Center for Cybersikkerheds myndighedsopgaver efter NIS-direktivet, vil konsekvensen bl.a. være, at centeret vil skulle benytte forskellige it-systemer til de forskellige dele af centerets virksomhed, hvilket vil være forbundet med øgede omkostninger.

Det kan i den forbindelse oplyses, at det er forventningen, at der – i lighed med centerets virksomhed på teleområdet – alene vil blive behandlet ganske få personoplysninger i forbindelse med de myndighedsopgaver, som centeret tillægges som led i implementeringen af NIS-direktivet.

Med venlig hilsen

Claus Hjort Frederiksen