SUNDHEDS- OG ÆLDREMINISTERIET

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.: 572542

Folketingets Sundheds- og Ældreudvalg har den 1. marts 2018 stillet følgende spørgsmål nr. 1 (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. 1:
"Idet NIS-direktivet bestemmer, at behandlingen af personoplysninger skal ske i overensstemmelse med databeskyttelsesdirektivet, bedes ministeren forklare, hvordan implementeringen af NIS-direktivet i Danmark harmonerer med dette, når Center for Cybersikkerhed, som en del af Forsvarets Efterretningstjeneste, ikke er omfattet af offentlighedsloven, persondataloven og centrale dele af forvaltningsloven."

Svar:

Da Sundheds- og Ældreudvalgets spørgsmål omhandler Center for Cybersikkerheds varetagelse af funktionen som CSIRT og nationalt centralt kontaktpunkt sammenholdt med kravene i databeskyttelsesdirektivet m.v., har mit ministerium bedt Forsvarsministeriet om bidrag til besvarelsen heraf. Forsvarsministeriet oplyser følgende:

"Det følger af artikel 2, stk. 1, i 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), at behandlingen af personoplysninger efter direktivet udføres i overensstemmelse med databeskyttelsesdirektivet (Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger).

Databeskyttelsesdirektivet gælder bl.a. ikke for sådan behandling af personoplysninger, der vedrører statens sikkerhed, jf. direktivets artikel 3, stk. 2. På den baggrund gælder den danske persondatalov – der implementerer databeskyttelsesdirektivet i dansk ret – heller ikke for behandlinger af personoplysninger, der udføres for Forsvarets Efterretningstjeneste, herunder Center for Cybersikkerhed.

En række af de centrale bestemmelser i persondataloven er imidlertid indarbejdet i lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed, der regulerer centerets virksomhed. Endvidere fører Tilsynet med Efterretningstjenesterne, som er et uafhængigt kontrolorgan, tilsyn med Center for Cybersikkerheds 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.

Denne retstilstand videreføres som udgangspunkt, når EU's databeskyttelsesdirektiv fra 25. maj 2018 erstattes af den nye databeskyttelsesforordning (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) samt den foreslåede danske databeskyttelseslov (L 68 fremsat for Folketinget den 25. oktober 2017).

Det bemærkes dog, at der med lovforslag nr. L 155, der konsekvensændrer lov om Center for Cybersikkerhed som følge af den nye regulering på databeskyttelsesområdet, er lagt op til, at forsvarsministeren får hjemmel til helt eller delvist at sætte databeskyttelsesforordningen og databeskyttelsesloven i kraft for dele af Center for Cybersikkerheds virksomhed, herunder centerets virksomhed i medfør af NIS-direktivet. Dette lovforslag blev fremsat den 28. februar 2018 og er fortsat under behandling i Folketinget."

Jeg kan henholde mig til Forsvarsministeriets bidrag.

Det kan endvidere bemærkes, at det ikke er hensigten med det fremsatte lovforslag eller bekendtgørelser, der vil skulle udstedes i medfør af loven, at Sundhedsdatastyrelsen eller Center for Cybersikkerhed vil skulle modtage følsomme personoplysninger, herunder helbredsoplysninger, fra operatører af væsentlige tjenester.

Det forventes, at Sundhedsdatastyrelsen og Center for Cybersikkerhed vil skulle modtage oplysninger om navn og kontaktoplysninger på operatøren af den væsentlige tjeneste, oplysninger om hændelsens årsag, karakter, varighed, forløb og konsekvenser, oplysninger om foranstaltninger, som operatøren har truffet eller foreslår truffet, for at håndtere hændelsen, oplysninger om omfanget af hændelsen og oplysninger om eventuelle grænseoverskridende konsekvenser for hændelsen.

Som det fremgår af besvarelsen af spørgsmål nr. 6 (L 143 – Forslag til lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren), oplyser Forsvarsministeriet følgende:

"Det vil i almindelighed være tilstrækkeligt for at kunne varetage de opgaver, som følger af direktivet, jf. nedenfor, at underretningerne indeholder overordnede oplysninger om hændelsen, herunder om den berørte virksomhed, tidspunktet for og varigheden af hændelsen, beskrivelse af hændelsen og dens konsekvenser samt en vurdering af mulige grænseoverskridende konsekvenser af hændelsen. Underretningerne vil som det helt klare udgangspunkt ikke indeholde personoplysninger, bortset fra eventuelle oplysninger om den medarbejder, som har forestået selve underretningen. Hvis hændelsen er forårsaget af et egentligt angreb, vil det desuden kunne være relevant at anføre IP-adresser, mailadresser mv., som anvendes af den ondsindede aktør. Det vil eksempelvis også kunne være relevant at medtage såkaldte phishing-mails, der har forårsaget en hændelse."

Med venlig hilsen

Ellen Trane Nørby / Maja Holm Andreasen