Februar 2018

**KOMMENTERET HØRINGSOVERSIGT**
**vedrørende**
**forslag til lov om ændring af lov om Center for Cybersikkerhed**

Et udkast til lovforslag om ændring af lov om Center for Cybersikkerhed har i perioden fra den 13. december 2017 til den 15. januar 2018 været sendt i høring hos:

Advokatrådet, Amnesty International, Danske Advokater, Dansk Energi, Dansk Erhverv, Dansk Industri, Dansk Internet Forum (DIFO), DANSK IT, Danske Regioner, Datatilsynet, Den Danske Dommerforening, DI ITEK, DKCERT, Domstolsstyrelsen, Institut for Menneskerettigheder, ISP Sikkerhedsforum, IT-Branchen, IT-Politisk Forening, Justitia, KL, PROSA, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Rigsombudsmanden i Grønland, Rigsombudsmanden på Færøerne, Rådet for Digital Sikkerhed, samtlige byretspræsidenter, Teleindustrien (TI) og Tilsynet med Efterretningstjenesterne.

Forsvarsministeriet har modtaget høringssvar fra Advokatrådet, Datatilsynet, Det Grønlandske Selvstyre, Færøernes Landstyre, Institut for Menneskerettigheder, IT-Politisk Forening, KL, Præsidenten for Københavns Byret på vegne af byretspræsidenterne, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Rigsombudsmanden i Grønland, Rigsombudsmanden på Færøerne og Tilsynet med Efterretningstjenesterne.

Nedenfor gennemgås og kommenteres de væsentligste bemærkninger fra de hørte parter. Forsvarsministeriets kommentarer til høringssvarene er anført med kursiv.

Det Grønlandske Selvstyre, Færøernes Landstyre, KL, Præsidenten for Københavns Byret på vegne af byretspræsidenterne, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Rigsombudsmanden i Grønland, Rigsombudsmanden på Færøerne og Tilsynet med Efterretningstjenesterne har ikke bemærkninger til lovforslaget.

## 1. Videreførelse af gældende ret

Advokatrådet finder det uhensigtsmæssigt, at Center for Cybersikkerheds behandling af personoplysninger videreføres uændret, selvom der kommer nye databeskyttelsesregler, og persondataloven

ophæves. Advokatrådet anfører, at en sådan ordning kan skabe usikkerhed om retstilstanden, når reglerne skal administreres i overensstemmelse med en ophævet lov. Advokatrådet finder endvidere, at ordningen forekommer ubegrundet og at der er risiko for, at der ikke på sigt i tilstrækkelig grad vil kunne tages højde for den teknologiske udvikling, idet der skal administreres i henhold til ældre praksis, der ikke er opdateret.

*Lovforslaget indebærer, at gældende ret i videst muligt omfang videreføres. Bestemmelserne i kapitel 6 i lov om Center for Cybersikkerhed vedrører centerets behandling af personoplysninger og er baseret på den nuværende persondatalov. Lovforslaget indebærer derfor, at bestemmelserne forstsat vil skulle fortolkes i overensstemmelse med forarbejder og praksis efter persondataloven. Bestemmelserne vil dermed ikke skulle fortolkes i lyset af reglerne i databeskyttelsesforordningen, den nye databeskyttelseslov samt fremtidig praksis herom.*

*Den nuværende regulering af Center for Cybersikkerheds behandling af personoplysninger er et resultat af grundige overvejelser, som blev foretaget i forbindelse med udarbejdelsen af lov om Center for Cybersikkerhed. I den forbindelse blev der foretaget en afvejning af på den ene side hensynet til de særlige forhold, der gør sig gældende for Center for Cybersikkerheds virksomhed, og på den anden side hensynet til at sikre et højt beskyttelsesniveau i forhold til behandlingen af personoplysninger. De kommende ændringer i databeskyttelsesreguleringen fører ikke til en ændret vurdering heraf, hvilket også skal ses i lyset af, at ordningen i de seneste år har vist sig at være hensigtsmæssig og velfungerende.*

**2. Placeringen af civile opgaver under Forsvarets Efterretningstjeneste**

Institut for Menneskerettigheder har ingen bemærkninger til konsekvensrettelserne, men fremhæver det principielt problematiske i, at centrale civile samfundsstrukturer varetages af Forsvarets Efterretningstjeneste med de begrænsninger, det giver i forhold til indsigt og databeskyttelseskrav.

*Lovforslaget indebærer en videreførelse af gældende ret, og der sker ikke med lovforslaget en ændring af de opgaver, som Center for Cybersikkerhed varetager. I forhold til baggrunden for den nuværende ordning henvises til bemærkningerne til det oprindelige forslag til lov om Center for Cybersikkerhed (lovforslag nr. L 192, Folketinget 2013-14, fremsat den 2. maj 2014).*

**3. Korrekt implementering**

IT-Politisk Forening finder ikke, at undtagelsen af efterretningstjenesterne, herunder Center for Cybersikkerhed, fra databeskyttelsesreglerne er en korrekt gennemførelse af de supplerende bestemmelser til databeskyttelsesforordningen, idet samtlige aktiviteter hos Center for Cybersikkerhed ikke kan siges at falde uden for EU-retten. Det gælder ikke mindst, hvis centeret får opgaver i forbindelse med implementeringen af direktiv om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet).

*Da Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, følger det af persondatalovens § 2, stk. 10, at persondataloven ikke gælder for centeret. Behandlingen af personoplysninger vil heller ikke blive omfattet af databeskyttelsesforordningen og den nye databeskyttelseslov. Dette følger af databeskyttelsesforordningens artikel 2, stk. 2, litra a, og af § 3, stk. 2, i den foreslåede nye databeskyttelseslov.*

*Anvendelsesområdet for databeskyttelsesforordningen og den kommende databeskyttelseslov, herunder at efterretningstjenesterne er undtaget fra databeskyttelsesreguleringen, er nærmere beskrevet i bemærkningerne til den foreslåede databeskyttelseslov. Der henvises i den forbindelse til punkt 2.1.3.1 i de almindelige bemærkninger til den foreslåede databeskyttelseslov (lovforslag nr. L 68, Folketinget 2017-18, fremsat den 25. oktober 2017).*

*Med den foreslåede ændring af § 8, stk. 2, i lov om Center for Cybersikkerhed, vil forsvarsministeren kunne bestemme, at dele af databeskyttelsesforordningen og databeskyttelsesloven skal finde anvendelse på centerets behandling af anmodninger om tilslutning til netsikkerhedstjenesten, centerets virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet og centerets personalesager. Det fremgår af bemærkningen til den foreslåede bestemmelse, at det tillige vil være tilfældet for myndighedsopgaver vedrørende informationssikkerhed, som Center for Cybersikkerhed måtte blive tillagt som led i implementeringen af NIS-direktivet.*

**4. Videregivelse af personoplysninger til Center for Cybersikkerhed**

Datatilsynet og IT-Politisk Forening bemærker, at videregivelse af personoplysninger til Center for Cybersikkerhed efter lovens forventede ikrafttræden den 25. maj 2018 kræver en egentlig hjemmel i databeskyttelsesforordningen eller i national lov. IT-Politisk Forening anfører endvidere, at det efter foreningens opfattelse er tvivlsomt, om behandlingsgrundlaget for videregivelse kan udstrækkes til specielt systematisk videregivelse af trafik- og pakkedata til Center for Cybersikkerhed, når der ikke er sikkerhed for, at den videre behandling hos centeret sker i overensstemmelse med databeskyttelsesforordningen.

*Som det fremgår af det oprindelige forslag til lov om Center for Cybersikkerhed (lovforslag nr. L 192, Folketinget 2013-14, fremsat den 2. maj 2014) er videregivelse af personoplysninger til Center for Cybersikkerhed omfattet af persondataloven, uanset at der i sådanne tilfælde er tale om en behandling, som foretages af en efterretningstjeneste.*

*Ligeledes vil videregivelse af personoplysninger til Center for Cybersikkerhed efter den 25. maj 2018 være omfattet af databeskyttelsesforordningen og den kommende databeskyttelseslov, hvorefter der skal foreligge hjemmel i forordningen eller i national lov. En sådan hjemmel vil eksempelvis kunne findes i databeskyttelsesforordningens artikel 6 om lovlig behandling af personoplysninger og artikel 9 om forbud mod behandling af særlige kategorier af personoplysninger. Det bemærkes i den forbindelse, at det af databeskyttelsesforordningens præambelbetragtning 49 fremgår, at behandling af personoplysninger i det omfang, det er strengt nødvendigt og forholdsmæssigt for at sikre net- og informationssikkerheden, der foretages af eksempelvis offentlige myndigheder, Computer Emergency*

*Response Teams (CERT'er) eller Computer Security Incident Response Teams (CSIRT'er), udgør en legitim interesse for den berørte dataansvarlige.*