FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

April 2014

KOMMENTERET HØRINGSOVERSIGT
vedrørende
forslag til lov om Center for Cybersikkerhed
(Lovforslag L 192)

Et udkast til lovforslag har i perioden 4. februar 2014 til 4. marts 2014 været sendt i høring hos:

Advokatrådet, Amnesty International, Brancheorganisation for Den Danske Vejgodstransport (ITD), Danmarks Rederiforening, Dansk Energi, Dansk Erhverv, Dansk Industri (DI), Dansk Internet Forum (DIFO), DANSK IT, Danske Advokater, Danske Regioner, Datatilsynet, Den Danske Dommerforening, DI ITEK, DKCERT, Domstolsstyrelsen, Finansrådet, Foreningen Danske Olieberedskabslagre, Foreningen af Open Source Leverandører, Foreningen af Vandværker i Danmark, Færøernes Landsstyre, Grønlands Selvstyre, Institut for Menneskerettigheder, ISP Sikkerhedsforum, IT-Branchen, IT-Politisk Forening, Kommunernes Landsforening (KL), Landbrug & Fødevarer, Lægemiddelindustriforeningen (LIF), Procesindustriens Brancheforening, PROSA, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Retssikkerhedsfonden, Rigsadvokaten, Rigspolitichefen, Rigsrevisionen, Rådet for Digital Sikkerhed, Statens IT-projektråd, Teleindustrien (TI) og The Open Web Application Security Project (OWASP Danmark).

Heraf har Forsvarsministeriet modtaget høringsudtalelse fra følgende:

Advokatrådet, **Dansk Energi**, **Dansk Erhverv**, **Dansk Industri (DI)**, **Datatilsynet**, **Den Danske Dommerforening**, **DI ITEK**, **DKCERT**, **Domstolsstyrelsen**, **Finansrådet**, **Institut for Menneskerettigheder**, **IT-Branchen**, **IT-Politisk Forening**, **Præsidenten for Vestre Landsret**, **Præsidenten for Østre Landsret**, **Retspolitisk Forening**, **Rigsadvokaten**, **Rigspolitichefen**, **Rigsrevisionen**, **Rådet for Digital Sikkerhed og Teleindustrien (TI)**.

Forsvarsministeriet har endvidere modtaget høringsudtalelse fra **Branchefællesskab for Intelligent Energi** og **Forbrugerrådet Tænk.**

HOLMENS KANAL 42
1060 KØBENHAVN K
TELEFON: 33 92 33 20
TELEFAX: 33 32 06 55
MAIL: FMN@FMN.DK
WEB: www.FMN.DK
CVR: 25-77-56-35
EAN: 5798000201200

Branchefællesskab for Intelligent Energi, **Dansk Energi**, **Datatilsynet**, **Den Danske Dommerforening, Domstolsstyrelsen**, **Præsidenten for Vestre Landsret**, **Præsidenten for Østre Landsret** og **Rigsrevisionen** har ikke fremsat bemærkninger til lovforslaget.

Nedenfor gennemgås og kommenteres de væsentligste bemærkninger fra de hørte parter til de enkelte emner i lovforslaget. Forsvarsministeriets kommentarer til høringsudtalelserne er anført med kursiv.

Enkelte høringsudtalelser indeholder bemærkninger og opfordringer til initiativer, som ikke vedrører lovudkastet. Disse omtales ikke nærmere.

De modtagne høringsudtalelser vedlægges.

1. Generelle bemærkninger

Advokatrådet anerkender behovet for Center for Cybersikkerheds arbejde og funktioner, og rådet finder det hensigtsmæssigt at samle lovgrundlaget for centerets organisation og funktioner. Advokatrådet udtaler, at udkastet overordnet er gennemarbejdet og velbegrundet.

Dansk Erhverv bakker op om lovforslagets intention om at styrke it-sikkerheden i Danmark gennem en professionel, offentlig indsats i regi af Center for Cybersikkerhed. Dansk Erhverv mener, at Center for Cybersikkerhed kan give et reelt og vigtigt bidrag til it-sikkerheden i et samfund, der til stadighed bliver mere afhængigt af en robust it-infrastruktur.

Dansk Industri (DI), **DI ITEK, Teleindustrien (TI)**, **Rådet for Digital Sikkerhed, Forbrugerrådet Tænk og Institut for Menneskerettigheder** finder det positivt, at der etableres et lovgrundlag for Center for Cybersikkerhed, herunder for GovCERT's[1] og MILCERT's[2] virke.

[1] Governmental Computer Emergency Response Team - Den statslige varslingstjeneste for internettrusler mod statslige myndigheder samt virksomheder.
[2] Military Computer Emergency Response Team - Den statslige varslingstjeneste for internettrusler på Forsvarsministeriets område.

Dansk Industri (DI), **DI ITEK** og **Teleindustrien (TI)** er endvidere tilfredse med, at væsentlige dele af reguleringen af Center for Cybersikkerheds virke tager udgangspunkt i og viderefører en række principper fra den gældende lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v. (GovCERT-loven[3]). Organisationerne anfører desuden, at de er tilfredse med, at analyse af pakkedata kun må finde sted ved begrundet mistanke om en sikkerhedshændelse og kun i det omfang, at det er nødvendigt for afklaring af forhold vedrørende hændelsen, idet dette giver en fornuftig begrænsning i forhold til behandling af personoplysninger.

DKCERT ser positivt på lovforslaget. DKCERT finder, at lovforslaget i højere grad afspejler den nye virkelighed, og at lovforslaget er et skridt på vejen mod en mere effektiv behandling af sikkerhedshændelser.

Finansrådet bifalder beslutningen om at etablere et statsligt Center for Cybersikkerhed i Danmark. Rådet finder det endvidere positivt, at der kommer et øget fokus på it-sikkerhed i Danmark i takt med, at internettet spiller en stadig større rolle i samfundet.

IT-Branchen bakker generelt op om lovforslaget og finder det i udgangspunktet positivt, at der i lovforslaget angives klare regler for dataindsamlingens formål samt tidsgrænser for opbevaring og for sletning af indsamlede data og metadata.

IT-Politisk Forening anfører, at it-sikkerhed er en væsentlig samfundsmæssig opgave, og at det uden tvivl er hensigtsmæssigt at samle ansvaret for cybersikkerheden på statens område i én enkelt enhed.

2. Center for Cybersikkerheds organisatoriske placering og forholdet til persondataloven, offentlighedsloven og forvaltningsloven

Dansk Erhverv finder, at der ligger nogle indbyggede udfordringer i, at arbejdet med at sikre civil infrastruktur placeres i regi af Forsvarets Efterretningstjeneste. Organisationen anfører, at det er afgørende, at der ikke kan drages tvivl om centerets formål, og at principper om demokratisk kontrol, oplyste samtykker og gennemsigtighed derfor skal være gennemgående for centerets virke. Organisationen opfordrer desuden til, at forsvarsministeren benytter muligheden i lovforslagets § 8, stk. 2, til at definere klare reg-

[3] Lov nr. 596 af 14. juni 2011 om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v.

ler for håndtering af persondata, der så vidt muligt afspejler praksis i andre offentlige myndigheder.

Dansk Industri (DI), DI ITEK og **Teleindustrien (TI)** anfører, at det er et positivt skridt, at Center for Cybersikkerhed skal følge persondataloven på væsentlige punkter. Organisationerne mener endvidere, at det er naturligt, at visse dele af persondataloven ikke finder anvendelse for Center for Cybersikkerhed. Organisationerne opfordrer imidlertid til, at der i lovforslaget indføres en bestemmelse, som svarer til persondatalovens § 41, stk. 4. Herudover opfordrer organisationerne til, at Tilsynet med Efterretningstjenesterne spørges eller orienteres i principielle sager, hvor der behandles personoplysninger, svarende til bestemmelsen i persondatalovens § 7, stk. 7. Desuden opfordrer organisationerne til, at forsvarsministeren anvender sin mulighed efter lovforslagets § 8, stk. 2, til at tildele borgere og virksomheder et minimum af rettigheder.

Institut for Menneskerettigheder anbefaler, at GovCERT omfattes af persondataloven, offentlighedsloven og forvaltningsloven, for eksempel gennem en ændret organisatorisk placering af GovCERT.

IT-Politisk Forening anfører, at beskyttelsen af personoplysninger i lovforslagets kapitel 6, som formelt svarer til persondatalovens regler om behandling af personoplysninger, ikke er reel, idet beskyttelsen i lovforslagets §§ 10-12 ikke omfatter personoplysninger, som i medfør af lovforslagets kapitel 4 behandles på baggrund af indgreb i meddelelseshemmeligheden. Foreningen antager i den forbindelse, at Center for Cybersikkerheds netsikkerhedstjeneste primært behandler personoplysninger på baggrund af indgreb i meddelelseshemmeligheden.

Retspolitisk Forening finder, at begrundelsen i lovforslaget for placeringen af Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste ikke forekommer overbevisende, idet det er foreningens opfattelse, at lovforslaget i alt væsentligt omhandler civile sikkerhedsopgaver. Foreningen anfører, at såfremt GovCERT's opgaver skal forblive under Forsvarets Efterretningstjeneste, bør dette ske i form af en særlig civil it-sikkerhedsafdeling, der er underlagt persondataloven med de modifikationer, som følger af et administrativt fællesskab med en efterretningstjeneste.

Rådet for Digital Sikkerhed og **Forbrugerrådet Tænk** opfordrer til, at Center for Cybersikkerhed i det hele adskilles fra Forsvarets Efterretningstjenestes funktionsområde og henlægges til en forvaltningsmyndighed, der er omfattet af persondataloven. Rådene

finder endvidere, at forvaltningsmyndigheden, der får til opgave at undersøge og forebygge cyberangreb, skal være underlagt almindelige forvaltningsretlige principper for åbenhed, kontrol og indsigt samt retsplejelovens krav om retskendelse ved indgreb i meddelelseshemmeligheden.

Center for Cybersikkerhed blev oprettet i december 2012 som en del af Forsvarets Efterretningstjeneste. Det skal således understreges, at lovforslaget ikke indebærer, at der sker en ændring af Center for Cybersikkerheds organisatoriske placering, idet centeret siden oprettelsen har været en del af Forsvarets Efterretningstjeneste.

Med oprettelsen af Center for Cybersikkerhed i 2012 blev flere forskellige myndigheders indsats på cybersikkerhedsområdet samlet i én myndighed. Center for Cybersikkerhed varetager i dag en række forskellige opgaver på informationssikkerhedsområdet, hvor centeret er national it-sikkerhedsmyndighed og myndighed for informationssikkerhed og beredskab på teleområdet. Centeret omfatter ligeledes de to varslingstjenester for internettrusler GovCERT og MILCERT. MILCERT er varslingstjeneste på Forsvarsministeriets område og har siden oprettelsen i 2010 været en del af Forsvarets Efterretningstjeneste. GovCERT er den statslige varslingstjeneste for internettrusler på det civile område og var indtil oktober 2011 en del af IT- og Telestyrelsen.

Center for Cybersikkerhed blev placeret ved Forsvarets Efterretningstjeneste for at opnå synergieffekter gennem udnyttelse af Forsvarets Efterretningstjenestes erfaringer inden for it-sikkerhedsområdet, viden om det internationale trusselsbillede og særlige adgang til oplysninger fra udlandet om cybertrusler. Som det fremgår af evalueringen af GovCERT-loven, har placeringen ved Forsvarets Efterretningstjeneste betydet, at Center for Cybersikkerhed har fået adgang til flere oplysninger om cybertrusler fra internationale partnere. En række af disse oplysninger har konkret kunnet omsættes i en styrkelse af it-sikkerheden for danske myndigheder og virksomheder.

I overensstemmelse med hensigten bag samlingen af myndighedernes indsats i Center for Cybersikkerhed vil der kunne ske en bedre udnyttelse af de samlede ressourcer, såfremt de to CERT'er (der grundlæggende udfører de samme opgaver i forhold til henholdsvis civile aktører og myndigheder på Forsvarsministeriets område) ses som én samlet netsikkerhedstjeneste, der varetager statens samlede CERT-funktion. Dermed vil der kunne opnås yderligere synergieffekter, ligesom den samlede kapacitet, som kan indsættes ved større cyberangreb, vil blive væsentligt større. Et centralt formål med lovforslaget er at etablere denne netsikkerhedstjeneste.

Formålet med lovforslaget er endvidere at etablere et samlet lovgrundlag for Center for Cybersikkerhed, herunder at styrke centerets muligheder for at undersøge og forebygge cyberangreb, samt at regulere centerets behandling af personoplysninger. Center for Cybersikkerheds arbejde skal fortsat ske med respekt for borgernes retssikkerhed og den personlige frihed, og dette er et centralt tema i lovforslaget.

Det fremgår udtrykkeligt af lovforslagets almindelige bemærkninger, at Center for Cybersikkerhed i videst muligt omfang skal 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. Ved modtagelse af anmodninger om aktindsigt vil Center for Cybersikkerhed i praksis foretage en søgning i centerets elektroniske sags- og dokumenthåndteringssystem. Såfremt der i den forbindelse lokaliseres dokumenter, der er omfattet af aktindsigtsanmodningen, vil disse dokumenter blive behandlet efter principperne i offentlighedsloven. Derimod vil centeret bl.a. ikke foretage en søgning i de store mængder data, som centerets netsikkerhedstjeneste til enhver tid opbevarer.

Det følger herudover af lovforslaget, at persondatalovens principper for, hvornår der må ske behandling af personoplysninger, i vidt omfang skal gælde for Center for Cybersikkerhed. Som supplement hertil indeholder lovforslaget særlige regler om analyse, videregivelse og sletning af data, der behandles på baggrund af indgreb i meddelelseshemmeligheden. Disse regler er generelt mere detaljerede og restriktive end de tilsvarende regler i persondataloven.

Et krav om, at persondatalovens bestemmelser om indsigtsret og oplysningspligt skal finde anvendelse på data, som indsamles af netsikkerhedstjenesten, vil imidlertid ikke være hensigtsmæssigt. Netsikkerhedstjenesten behandler i overensstemmelse med sit formål store mængder data, hvor behandlingens fokus er på oplysninger af rent teknisk karakter. De store mængder data indsamles af netsikkerhedstjenestens alarmenheder og benyttes bl.a. til at tegne et normalbillede af netværkskommunikationen hos de tilsluttede myndigheder og virksomheder. Det er kun i tilfælde af, at der er begrundet mistanke om en sikkerhedshændelse, at netsikkerhedstjenesten konkret analyserer disse data. Langt de fleste data, herunder e-mails, vil således aldrig blive åbnet eller læst af netsikkerhedstjenestens personale. Det vil endvidere kun være i meget sjældne

tilfælde, at netsikkerhedstjenesten vil have behov for at analysere og anvende oplysninger om fysiske og juridiske personer m.v., som er indeholdt i de behandlede data.

Såfremt netsikkerhedstjenesten eksempelvis var omfattet af kravet i persondatalovens § 28, stk. 1, hvorefter en myndighed ved indsamling af oplysninger hos den registrerede bl.a. skal give den registrerede meddelelse om formålene med behandlingen af oplysningerne, vil dette have som konsekvens, at netsikkerhedstjenesten vil skulle gennemse samtlige opbevarede data med henblik på at konstatere, om de indeholder personoplysninger. Denne gennemgang vil indebære en højere grad af indgreb i den personlige frihed, idet indholdet af e-mails, som ikke er knyttet til en sikkerhedshændelse, vil skulle åbnes og gennemses. Hertil kommer, at krav om sådanne gennemgange vil indebære et så stort ressourceforbrug, at det i praksis vil gøre det umuligt at drive netsikkerhedstjenesten.

Med den foreslåede model er der således opnået en hensigtsmæssig balance mellem på den ene side hensynet til borgernes retssikkerhed og den personlige frihed og på den anden side hensynet til de særlige forhold, som gør sig gældende for Center for Cybersikkerheds aktiviteter.

Det bemærkes i øvrigt, at persondatalovens bestemmelser om indsigts- og indsigelsesret heller ikke efter gældende ret finder anvendelse på GovCERT's aktiviteter.

Det følger af lovforslagets § 8, stk. 2, at forsvarsministeren kan bestemme, at kapitel 8-10 i persondataloven, offentlighedsloven samt forvaltningslovens kapitel 4-6 helt eller delvis skal finde anvendelse for dele af Center for Cybersikkerheds aktiviteter. Forsvarsministeriet vil løbende vurdere, om der er behov for at anvende denne hjemmel.

På baggrund af høringsudtalelserne er der i lovforslagets § 18, stk. 2, indsat en bestemmelse svarende til persondatalovens § 41, stk. 4, hvorefter der for oplysninger af særlig interesse for fremmede magter skal træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

Derimod finder Forsvarsministeriet ikke anledning til at tilføje en bestemmelse svarende til persondatalovens § 7, stk. 7. Den pågældende bestemmelse giver mulighed for at gøre undtagelse fra persondatalovens bestemmelse om, at der ikke må behandles

oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold. Forsvarsministeriet finder ikke, at der i forhold til Center for Cybersikkerheds virksomhed er behov for en sådan undtagelse.

3. Kredsen af virksomheder, der kan tilsluttes Center for Cybersikkerheds netsikkerhedstjeneste, og konsekvenserne for private sikkerhedsleverandører

Dansk Erhverv anfører, at det bør tydeliggøres, at tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste altid er frivillig og aldrig sker uden oplyst samtykke fra virksomhederne.

Dansk Industri (DI), DI ITEK og **Teleindustrien (TI)** finder, at den foreslåede udvidelse af Center for Cybersikkerheds arbejdsområde vil kunne medføre, at Center for Cybersikkerhed vil komme til at konkurrere med private udbydere af sammenlignelige services. Organisationerne mener derfor, at det i lovforslagets bemærkninger bør præciseres, at Center for Cybersikkerheds aktiviteter bør tilrettelægges således, at netsikkerhedstjenesten i mindst muligt omfang konkurrerer med private udbydere af sammenlignelige services. Organisationerne peger på, at Center for Cybersikkerhed efter lovforslagets §§ 6 og 7 træffer afgørelse om, hvorvidt en anmodning om tilslutning eller bistand kan imødekommes. Organisationerne anfører i den forbindelse, at de virksomheder, der tilsluttes netsikkerhedstjenesten, bliver bedre stillet end de virksomheder, der får afslag på en tilslutning. Desuden anfører organisationerne, at det ikke fremgår af lovforslaget, om den midlertidige tilslutning og analyse af data efter lovforslagets §§ 6 og 7 er frivillig.

DKCERT finder, at udvidelsen af dækningsområdet og introduktionen af midlertidigt tilsluttede virksomheder og myndigheder principielt set er begrundet.

Finansrådet påpeger, at segmentet af virksomheder, som ikke er kritiske for Danmarks infrastruktur, men hvor sikkerheden alligevel kan være afgørende, mangler et sted, hvor disse virksomheder kan henvende sig og få råd og vejledning.

IT-Branchen opfordrer til, at det i lovforslaget tydeliggøres, at Center for Cybersikkerheds virke i videst mulig udstrækning skal virke supplerende frem for konkurrerende i forhold til den indsats, private it-sikkerhedsleverandører udfører. IT-Branchen opfordrer

desuden til, at Center for Cybersikkerhed som udgangspunkt ikke bør udføre opgaver, som private it-sikkerhedsleverandører kunne have løst. IT-Branchen gør herudover opmærksom på, at det i lovforslaget bør tydeliggøres, at midlertidig tilslutning til netsikkerhedstjenesten sker på frivillig basis.

IT-Politisk Forening anfører, at en internetudbyders tilslutning til netsikkerhedstjenesten ikke må medføre, at danske internetbrugere dermed bliver overvåget af netsikkerhedstjenesten. Foreningen finder endvidere ikke, at der er et reelt behov for at udvide kredsen af virksomheder, som kan tilslutte sig netsikkerhedstjenesten. Foreningen henviser i den forbindelse til, at indgrebene i meddelelseshemmeligheden bør begrænses mest muligt, ligesom foreningen finder det uhensigtsmæssigt, at private sikkerhedsfirmaer skal konkurrere med en statslig netsikkerhedstjeneste.

Rådet for Digital Sikkerhed og **Forbrugerrådet Tænk** opfordrer til, at det kun er virksomheder, der er beskæftiget med kritisk infrastruktur, som kan tilsluttes Center for Cybersikkerheds netsikkerhedstjeneste. Rådene finder endvidere, at begrebet kritisk infrastruktur bør defineres i lovforslaget og præciseres ved oplistning af virksomhedstyper i bemærkningerne til lovforslaget. Rådene opfordrer desuden til, at Center for Cybersikkerheds opgaver afgrænses, således at Center for Cybersikkerhed ikke konkurrerer med private sikkerhedsvirksomheder. Rådene opfordrer herudover til, at Center for Cybersikkerheds opgaver ikke udvides som foreslået i lovforslagets §§ 6 og 7, og at disse opgaver i stedet bør overlades til private sikkerhedsvirksomheder.

Lovforslaget indebærer, at kredsen af virksomheder, der kan tilsluttes netsikkerhedstjenesten, udvides, således at virksomheder, der er beskæftiget med samfundsvigtige funktioner, kan tilsluttes. Det vil efter lovforslaget fortsat være frivilligt for statslige myndigheder uden for Forsvarsministeriets område samt regioner, kommuner og virksomheder, om de ønsker at blive tilsluttet netsikkerhedstjenesten.

Den nuværende afgrænsning, hvor kredsen af virksomheder, der kan tilsluttes GovCERT, kun omfatter virksomheder, der er beskæftiget med kritisk infrastruktur, har vist sig at være uhensigtsmæssig. Afgrænsningen indebærer, at det i dag ikke er muligt at tilslutte virksomheder, der f.eks. leverer livsvigtige medicinalprodukter, fremstiller vigtige komponenter til Forsvaret eller varetager drift af offentlige myndigheders administrative it-systemer. Det er ligeledes ikke muligt at tilslutte virksomheder, som på grund af samfundsvigtige forskningsaktiviteter er særligt udsatte for cyberangreb. For at opnå et op-

timalt beskyttelsesniveau er der behov for at sikre, at også disse virksomheder, der mere generelt varetager samfundsvigtige funktioner, kan tilsluttes netsikkerhedstjenesten.

Som det fremgår af lovforslagets bemærkninger, vurderes den foreslåede udvidelse af kredsen af virksomheder, der kan tilsluttes netsikkerhedstjenesten, ikke at ville påvirke det private marked for it-sikkerhedsydelser negativt. Netsikkerhedstjenestens brede dækningsområde samt tjenestens adgang til oplysninger fra andre netsikkerhedstjenester og den øvrige del af Forsvarets Efterretningstjeneste indebærer, at der ikke på det private marked findes sammenlignelige sikkerhedsydelser. En tilslutning til netsikkerhedstjenesten giver den enkelte virksomhed et ekstra lag af sikkerhed mod avancerede cyberangreb, men netsikkerhedstjenestens ydelser vil aldrig kunne træde i stedet for virksomhedernes øvrige it-sikkerhedsforanstaltninger.

Det vurderes tværtimod, at den foreslåede ordning i et vist omfang vil kunne påvirke det private marked for it-sikkerhedsydelser positivt. Således vil de anbefalinger, som netsikkerhedstjenestens monitorering typisk resulterer i, kunne medføre et behov for at styrke informationssikkerhedsniveauet hos de tilsluttede virksomheder – og dermed øge efterspørgslen efter de it-sikkerhedsydelser, der normalt vil blive leveret af private leverandører.

Det fremgår af lovforslagets § 3, stk. 3, at virksomheder, der er beskæftiget med samfundsvigtige funktioner, efter anmodning kan blive tilsluttet netsikkerhedstjenesten. Det fremgår endvidere af lovforslagets § 6, at en midlertidig tilslutning til netsikkerhedstjenesten kun kan ske på baggrund af et skriftligt samtykke fra virksomheden, ligesom det fremgår af § 7, at Center for Cybersikkerheds undersøgelse af et informationssystem forudsætter et skriftligt samtykke fra virksomheden. Virksomheders anvendelse af centerets ydelser er således altid frivillig for den enkelte virksomhed.

På baggrund af høringsudtalelserne er det i lovteksten præciseret yderligere, at virksomheders tilslutning til netsikkerhedstjenesten, herunder også midlertidig tilslutning, kun kan ske på baggrund af en anmodning fra den enkelte virksomhed.

I det omfang, private virksomheder leverer kommunikationsprodukter til kunder, omfatter tilslutningen til netsikkerhedstjenesten ikke disse kunders ind- og udgående internettrafik. Hvis en internetudbyder tilsluttes netsikkerhedstjenesten, vil tilslutningen dermed ikke omfatte den trafik, der genereres af udbyderens kunder. Formålet med tilslutningen

vil alene være at bidrage til at beskytte netværkskommunikation til og fra udbyderen selv. Der henvises herom til bemærkningerne til § 3.

4. Center for Cybersikkerheds behandling af krypterede data

Dansk Industri (DI), **DI ITEK** og **Teleindustrien (TI)** anerkender, at kriminelle ofte anvender kryptering for at skjule deres handlinger. Organisationerne påpeger imidlertid, at borgere og virksomheder ofte bruger kryptering til særligt fortroligt data, og at Center for Cybersikkerhed derfor ved at bryde krypteringen må forventes at få adgang til data, som er endnu mere følsomme end hidtil.

IT-Politisk Forening antager, at den foreslåede adgang for Center for Cybersikkerhed til at behandle krypterede data i praksis vil medføre et krav om, at netsikkerhedstjenesten skal have adgang til de tilsluttede myndigheders og virksomheders krypteringsnøgler. Foreningen anfører endvidere, at der i forbindelse med afkryptering af data er risiko for, at der skabes nye sikkerhedshuller. Foreningen finder, at det bør præciseres i bemærkningerne til lovforslaget, at analyse af krypterede pakkedata ikke under nogen omstændigheder må medføre nye sikkerhedsrisici.

Rådet for Digital Sikkerhed og **Forbrugerrådet Tænk** opfordrer til, at adgangen for Center for Cybersikkerhed til at bryde kryptering gøres betinget af, at der pålægges editionspligt, eller at der stilles krav om en retskendelse. Rådene antager i den forbindelse, at centeret vil forlange, at dekrypteringsnøgler udleveres. Rådene anfører endvidere, at tilsynsmyndigheden bør orienteres om indgrebet.

Det fremgår af bemærkningerne til GovCERT-lovens § 4 (L 197, 1. samling 2010-11), at GovCERT som udgangspunkt ikke vil afkryptere en krypteret e-mail eller andet indhold af en internetkommunikation. Dette har imidlertid i praksis vist sig at indebære en væsentlig og meget uhensigtsmæssig begrænsning for GovCERT's opgaveløsning.

Stadig flere e-mails og anden kommunikation, som indeholder såkaldt malware (f.eks. computervira), sendes i krypteret form for at undgå at blive detekteret af både spamfiltre og andre foranstaltninger, der iværksættes i myndighederne og virksomhederne for at opdage og uskadeliggøre malware. Det vil således i en række tilfælde kun være muligt for Center for Cybersikkerheds netsikkerhedstjeneste at opdage og uskadeliggøre angreb mod myndigheder og virksomheder ved at bryde krypteringen eller på anden måde omgå den.

For den del af netsikkerhedstjenesten, som omfatter GovCERT, er behovet for afkryptering direkte knyttet til netsikkerhedstjenestens opgaver med at analysere ind- og udgående internetkommunikation fra de myndigheder og virksomheder, der er tilsluttet tjenesten. I de situationer, hvor en krypteret e-mail indeholdende malware sendes til en modtager inden for myndigheden eller virksomheden, er det aktuelt for netsikkerhedstjenesten at afkryptere for at få adgang til malwaren. En afkryptering giver efter nærmere analyse netsikkerhedstjenesten mulighed for at identificere tilsvarende malware hos andre myndigheder og virksomheder. Hvis en tilsluttet virksomhed sender krypteret kommunikation til en hjemmeside, som vurderes at være inficeret med malware, vil netsikkerhedstjenesten også have behov for at kunne analysere og afkryptere kommunikationen med henblik på at kunne stoppe angreb hurtigt og effektivt.

For den del af netsikkerhedstjenesten, der er varslingstjeneste for internettrusler på Forsvarsministeriets område, gør der sig de samme overvejelser gældende. Som led i støtten til den militære sikkerhedsmyndighed vil netsikkerhedstjenesten yderligere have til opgave i særlig grad at analysere den trafik, der finder sted på Forsvarets netværk, med henblik på at opdage kompromitteringer. Det er derfor af stor betydning, at der er mulighed for, at netsikkerhedstjenesten løbende kan afkryptere kommunikation på Forsvarets netværk med henblik på at opdage angribere, som forsøger at skjule deres aktiviteter ved at kryptere kommunikationen.

Det foreslås derfor, at den hidtidige begrænsning for så vidt angår afkryptering ikke videreføres. Det skal dog understreges, at lovforslaget ikke indebærer krav om, at tilsluttede myndigheder eller virksomheder skal udlevere den private krypteringsnøgle til Center for Cybersikkerheds netsikkerhedstjeneste. Der henvises herom til bemærkningerne til § 4.

5. Videregivelse af data

Dansk Industri (DI), **DI ITEK** og **Teleindustrien (TI)** noterer med tilfredshed, at pakkedata alene må videregives til politiet.

DKCERT ser positivt på enhver mulighed for at videregive sikkerhedsrelaterede informationer.

IT-Politisk Forening bemærker, at afgræsningen af, om data kan defineres som henholdsvis trafikdata eller pakkedata, har betydning for, hvem oplysningerne kan videregi-

ves til. Foreningen anfører i den forbindelse, at lovforslagets definition af trafikdata er bredere end definitionen i e-privacydirektivet 2002/58/EF. Foreningen mener, at trafikdata bør defineres i overensstemmelsen med e-privacydirektivet.

Retspolitisk Forening finder, at lovforslagets bestemmelser om videregivelse af data forekommer naturlige set i lyset af det nødvendige samarbejde med eksempelvis andre netsikkerhedstjenester. Foreningen anfører endvidere, at det bør overvejes, om videregivelse af følsomme persondata kan ske i anonymiseret form, medmindre formålet med videregivelsen dermed kompromitteres.

Med definitionen af begrebet pakkedata i lovforslaget videreføres GovCERT-lovens definition, dog med en sproglig præcisering af, at pakkedata er indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester – og ikke kun internetbaseret kommunikation. Som hidtil vil det semantiske indhold af kommunikation, der transmitteres gennem digitale netværk eller tjenester, være omfattet af begrebet pakkedata. Det kan f.eks. være indholdet af en e-mailkorrespondance eller indholdet af tilgåede hjemmesider. Derudover er det tekniske indhold af kommunikationen, f.eks. HTML- eller XML-koder, omfattet af begrebet pakkedata.

Også lovforslagets definition af begrebet trafikdata er en videreførelse af GovCERT-lovens definition med enkelte præciseringer. Ved trafikdata forstås data, som behandles med henblik på overførsel af pakkedata. Det vil sige data, som beskriver oprindelse, destination og rutestyringsinformation, herunder oprindelsesdomænet eller den oprindelige elektroniske adresse samt anden tilsvarende information. Trafikdata kan eksempelvis være header-informationen i digitale kommunikationsprotokoller, men vil også omfatte protokoller, der udelukkende anvendes til rute- og kommunikationsstyring, f.eks. DNS og SIP. Konkrete eksempler på trafikdata er oplysninger om ip-adresser, e-mailadresser, hjemmesideadresser, browserversioner, kommunikationens varighed og tidspunktet for kommunikationen.

Populært sagt er trafikdata de oplysninger, der ville stå uden på en kuvert, mens pakkedata er det, der ville stå inde i en kuvert.

Der er med lovforslaget tale om en videreførelse af gældende ret for så vidt angår definitionerne af pakke- og trafikdata.

Efter lovforslagets § 16, nr. 2, kan Center for Cybersikkerhed videregive trafikdata til danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester, andre netsikkerhedstjenester m.v. Sidstnævnte vil omfatte tilsvarende netsikkerhedstjenester i Danmark og udlandet, som Center for Cybersikkerhed har et tæt samarbejde med for at øge centerets muligheder for at forebygge sikkerhedshændelser.

Videregivelse af trafikdata forudsætter i disse tilfælde, at der er begrundet mistanke om en sikkerhedshændelse, og at det konkret vurderes, at videregivelsen er nødvendig. Indeholder videregivelsen personoplysninger, vil de principper om relevans og proportionalitet, som fremgår af lovforslagets § 9, tillige skulle iagttages. Der vil dermed alene kunne videregives personoplysninger i det omfang, dette er relevant og tilstrækkeligt for at opnå formålet med den konkrete videregivelse.

Det skal understreges, at der kun kan ske videregivelse af pakkedata til dansk politi og altså ikke til andre danske eller udenlandske myndigheder.

Det bemærkes i den forbindelse, at Center for Cybersikkerheds videregivelse af personoplysninger vil være underlagt tilsyn af Tilsynet med Efterretningstjenesterne.

5.1. Videregivelse af trafikdata til teleselskaber

Dansk Industri (DI), **DI ITEK**, og **Teleindustrien (TI), Rådet for Digital Sikkerhed** og **Forbrugerrådet Tænk** anerkender, at Center for Cybersikkerhed kan have behov for at videregive trafikdata til udbydere af offentlige elektroniske kommunikationsnet og -tjenester (teleudbyderne). Organisationerne antager imidlertid, at Center for Cybersikkerhed i forbindelse med videregivelsen af trafikdata eksempelvis vil anmode teleudbyderne om at blokere for bestemte ip-adresser. Organisationerne anfører, at det i lovforslaget bør præciseres, at Center for Cybersikkerhed har ansvaret for blokeringer. Organisationerne mener endvidere, at Center for Cybersikkerhed skal forpligtes til at angive, i hvilket tidsrum blokeringen skal opretholdes. Organisationerne finder desuden, at det bør overvejes at kompensere teleselskaberne for udgifterne forbundet med implementeringen af en blokering.

Rådet for Digital Sikkerhed og **Forbrugerrådet Tænk** opfordrer herudover til, at videregivelse af trafikdata til private teleudbydere kun sker efter retskendelse.

Forsvarsministeriet finder, at der bør være restriktive rammer for Center for Cybersikkerheds videregivelse af data, der behandles på baggrund af indgreb i meddelelseshemmeligheden.

For at styrke beskyttelsen af den danske ikt-infrastruktur bør der imidlertid gives mulighed for at videregive trafikdata til udbydere af offentlige elektroniske kommunikationsnet og -tjenester, således at disse aktører – først og fremmest teleselskaber – ved hjælp af de modtagne trafikdata kan styrke deres egen forebyggelse mod cyberangreb på baggrund af oplysninger om f.eks. ip-adresser, der anvendes ved cyberangreb. Dette vil have stor betydning for det samlede informationssikkerhedsniveau i samfundet, da disse udbydere varetager driften af store dele af den ikt-infrastruktur, som samfundsvigtige funktioner er afhængige af.

Center for Cybersikkerheds videregivelse af data til eksempelvis udbydere af offentlige elektroniske kommunikationsnet og -tjenester indebærer imidlertid ikke, at Center for Cybersikkerhed samtidigt vil anmode de pågældende aktører om f.eks. at blokere visse hjemmesider. Oplysningerne stilles alene til rådighed for aktørerne med henblik på, at de – efter deres egen vurdering – vil kunne anvende oplysninger til styrkelse af informationssikkerheden.

Det bemærkes i øvrigt, at Center for Cybersikkerhed – såfremt centeret bliver opmærksom herpå – vil underrette aktørerne, hvis f.eks. ip-adresser, der har været inkluderet i en varsling, ikke længere vurderes at udgøre en fare for informationssikkerheden.

Der henvises herom til afsnit 3.5.2. i de almindelige bemærkninger.

5.2. Videregivelse af trafikdata til udlandet

Dansk Industri (DI), **DI ITEK** og **Teleindustrien (TI)**, **Institut for Menneskerettigheder**, **Rådet for Digital Sikkerhed** og **Forbrugerrådet Tænk** anerkender behovet for at videregive af trafikdata til bl.a. udenlandske netsikkerhedstjenester. Organisationerne anbefaler imidlertid også at begrænse muligheden for videregivelse af trafikdata i lovforslagets § 16, nr. 2, til trafikdata, der vedrører en konkret sikkerhedshændelse.

DKCERT finder, at muligheden for at videregive trafikdata til andre netsikkerhedstjenester er et nødvendigt redskab til at forbedre det internationale samarbejde.

Rådet for Digital Sikkerhed og **Forbrugerrådet Tænk** anbefaler endvidere, at lovforslaget udtrykkeligt nævner, at videregivelse kan ske til udenlandske netsikkerhedstjenester.

Center for Cybersikkerhed har et tæt samarbejde med andre netsikkerhedstjenester i udlandet, f.eks. CERT'er og ikt-sikkerhedsmyndigheder, som bidrager med vigtige informationer, der øger centerets muligheder for at forebygge sikkerhedshændelser i Danmark. Et effektivt internationalt samarbejde på myndighedsniveau forudsætter, at Danmark også kan give disse udenlandske samarbejdspartnere oplysninger, som kan bidrage til at stoppe grænseoverskridende cyberangreb, såvel udgående fra som rettet mod Danmark.

Det følger af lovforslaget, at trafikdata kun kan videregives til andre (herunder udenlandske) netsikkerhedstjenester, hvis det er nødvendigt for udførelsen af netsikkerhedstjenestens opgaver. Det følger endvidere af lovforslaget, at Center for Cybersikkerhed har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser. Videregivelse af trafikdata forudsætter således, at videregivelsen er nødvendig i forhold til at opdage, analysere og bidrage til at imødegå sikkerhedshændelser.

Der er imidlertid på baggrund af høringsudtalelserne sket en tilpasning af lovteksten (§ 16, nr. 2), således at det udtrykkeligt fremgår, at trafikdata alene kan videregives ved begrundet mistanke om en sikkerhedshændelse.

Det bemærkes i øvrigt, at Center for Cybersikkerheds videregivelse af data vil være underlagt tilsyn af Tilsynet med Efterretningstjenesterne.

5.3. Videreformidling af data fra Center for Cybersikkerhed til den øvrige del af Forsvarets Efterretningstjeneste

Dansk Erhverv opfordrer til maksimal åbenhed om de administrative retningslinjer, som Forsvarsministeriet vil udstede med henblik på at sikre, at den interne udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste også fremadrettet sker med respekt for retssikkerheden og den personlige frihed.

Dansk Industri (DI), **DI ITEK** og **Teleindustrien (TI)** anbefaler, at det i de kommende retningslinjer fastslås, at der fra gang til gang skal tages stilling til, om pakkeda-

ta kan videregives fra Center for Cybersikkerhed til Forsvarets Efterretningstjeneste. Organisationerne anbefaler endvidere, at adgang for Forsvarets Efterretningstjeneste kun må gives, når det er nødvendigt i henhold til Center for Cybersikkerheds formål og aktiviteter, eller der foreligger andre nærmere kvalificerede beskyttelsesværdige formål. Organisationerne anbefaler desuden, at det overordnet sikres, at der ikke sker et automatisk og generelt flow af alle trafikdata fra GovCERT til Forsvarets Efterretningstjeneste.

Institut for Menneskerettigheder anbefaler, at der i lovforslaget indføres et krav om, at videregivelse af data fra GovCERT til resten af Forsvarets Efterretningstjeneste forudsætter, at det konkret vurderes nødvendigt for at beskytte den nationale digitale infrastruktur mod sikkerhedsmæssige trusler.

Rådet for Digital Sikkerhed og **Forbrugerrådet Tænk** anfører, at der sker en alvorlig begrænsning af borgernes rettigheder, når kommunikation til den offentlige sektor potentielt kan gøres til genstand for Center for Cybersikkerheds analyser og videregives til Forsvarets Efterretningstjeneste. Rådene opfordrer derfor til en grundlæggende ændring af lovgrundlaget, herunder en adskillelse af Center for Cybersikkerhed fra Forsvarets Efterretningstjeneste. Rådene finder endvidere, at videregivelse af data til Forsvarets Efterretningstjeneste i det mindste bør reguleres således, at der stilles krav om en konkret vurdering af relevans, nødvendighed og proportionalitet i hvert enkelt tilfælde af intern videregivelse.

Den interne udveksling af data i Forsvarets Efterretningstjeneste er – i overensstemmelse med almindelige forvaltningsretlige principper – ikke reguleret i lovforslaget. Med lovforslaget vil det almindelige forvaltningsretlige udgangspunkt således være gældende for Center for Cybersikkerhed. Det indebærer, at der som udgangspunkt er fri adgang til at udveksle data internt i Forsvarets Efterretningstjeneste, herunder mellem Center for Cybersikkerhed og den øvrige del af efterretningstjenesten, hvis dette er nødvendigt for at løse myndighedens opgaver, og der i øvrigt er tale om et sagligt formål. Det sikrer, at alle de relevante ressourcer i Forsvarets Efterretningstjeneste hurtigt og effektivt kan indsættes ved den meget store andel af cyberangreb mod Danmark, som hidrører fra udlandet, og hvor Forsvarets Efterretningstjeneste som udenrigsefterretningstjeneste kan bidrage med væsentlige oplysninger.

Forsvarsministeriet vil imidlertid, som det fremgår af bemærkningerne i lovforslaget (afsnit 3.5.3), i forbindelse med lov om Center for Cybersikkerheds ikrafttræden udstede administrative retningslinjer. Retningslinjerne skal sikre, at den interne udveksling af op-

lysninger mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste også fremadrettet sker med respekt for retssikkerheden og den personlige frihed. Center for Cybersikkerhed behandler data på baggrund af indgreb i meddelelseshemmeligheden, og retningslinjerne vil bl.a. indeholde bestemmelser om, at sådanne data kun kan videreformidles til den øvrige del af Forsvarets Efterretningstjeneste, hvis de pågældende data er knyttet til en cybersikkerhedshændelse. Desuden vil retningslinjerne fastsætte, at medarbejdere, der varetager efterretningsmæssige opgaver i den øvrige del af Forsvarets Efterretningstjeneste, ikke må have adgang til de it-systemer, hvor Center for Cybersikkerhed behandler data på baggrund af indgreb i meddelelseshemmeligheden.

De kommende retningslinjer vil endvidere fastsætte, at data, der er videreformidlet fra Center for Cybersikkerhed til den øvrige del af Forsvarets Efterretningstjeneste, fortsat alene vil kunne videregives efter de regler, der efter lovforslaget gælder for Center for Cybersikkerhed. Det indebærer, at pakkedata udelukkende kan videregives til politiet, og at trafikdata kun kan videregives til den samme kreds af aktører, som Center for Cybersikkerhed efter lovforslagets § 16, nr. 2, kan videregive oplysninger til. Således vil pakkedata aldrig kunne videregives til andre efterretningstjenester.

Retningslinjerne vil blive offentliggjort på Center for Cybersikkerheds hjemmeside, www.cfcs.dk.

Det bemærkes i øvrigt, at den interne udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste også vil være underlagt tilsyn af Tilsynet med Efterretningstjenesterne.

6. Oplysningspligter

Dansk Erhverv opfordrer til, at Center for Cybersikkerhed giver en årlig afrapportering, som skal være med til at skabe gennemsigtighed om centerets arbejde. Dansk Erhverv nævner, at det eksempelvis kunne være relevant at oplyse om baggrunden for og antallet af (midlertidige) tilslutninger, samt statistik på databehandlinger, sikkerhedshændelser, udvekslinger med andre myndigheder og lande m.v.

Dansk Industri (DI), **DI ITEK** og **Teleindustrien (TI)** anfører, at Center for Cybersikkerhed bør forpligtes til at orientere virksomheder og brancheorganisationer, såfremt centeret opdager sikkerhedshændelser, der er målrettet de pågældende virksomheder

eller sektorer. Forpligtelsen skal gælde, uanset om virksomheden eller sektoren er tilsluttet Center for Cybersikkerhed.

IT-Branchen foreslår, at Center for Cybersikkerhed forpligtes til at samarbejde og vidensdele med private it-sikkerhedsleverandører. Branchen foreslår endvidere, at Center for Cybersikkerhed i forhold til de private it-sikkerhedsleverandørers brancheorganisationer løbende skal dele aggregeret og anonymiseret data om konstaterede angreb og trusler hos de tilknyttede myndigheder og virksomheder. Branchen foreslår desuden, at Center for Cybersikkerhed forpligtes til at offentliggøre en årlig gennemsigtighedsrapport, der informerer generelt om, i hvilket omfang centeret foretager indgreb i meddelelseshemmeligheden hos tilsluttede myndigheder og virksomheder.

IT-Politisk Forening mener, at Center for Cybersikkerhed bør forpligtes til løbende at offentliggøre, hvilke myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten, eller som har anmodet centeret om bistand som beskrevet i lovforslagets § 7. Foreningen foreslår endvidere, at tilsynets årlige redegørelse bør indeholde aggregerede oplysninger. Som eksempler på aggregerede oplysninger nævner foreningen skønsmæssige vurderinger af antallet af ip-adresser, der er berørt af indgreb i meddelelseshemmeligheden, og antallet af ip-adresser, der er videregivet til eksterne samarbejdspartnere.

Rådet for Digital Sikkerhed og **Forbrugerrådet Tænk** opfordrer til, at virksomheder – såfremt det er nødvendigt for at sikre samfundsvigtig ikt-infrastruktur – skal forpligtes til at orientere Center for Cybersikkerhed om sikkerhedshændelser og til at stille relevant materiale til rådighed for centerets analyser heraf. Rådene opfordrer endvidere til, at Center for Cybersikkerhed forpligtes til at informere om konstaterede sikkerhedshændelser. Centeret skal i den forbindelse forpligtes til også at informere virksomheder, der har været udsat for en sikkerhedshændelse, samt deres brancheforeninger, også selv om de ikke er tilsluttet netsikkerhedstjenesten.

En vigtig forebyggende aktivitet for Center for Cybersikkerhed er udsendelsen af sikkerhedsvarslinger, hvor myndigheder, virksomheder, andre netsikkerhedstjenester m.v. underrettes om særligt alvorlige sikkerhedshændelser. Sikkerhedsvarslingerne giver modtagerne mulighed for at styrke deres egen forebyggelse mod cyberangreb, hvilket har stor betydning for det samlede informationssikkerhedsniveau i samfundet. Sikkerhedsvarslingerne udsendes efter en konkret vurdering til den modtagerkreds, der vurderes at være relevant.

Center for Cybersikkerhed offentliggør endvidere løbende oplysninger om centerets virke, ligesom centeret offentliggør situationsbilleder og trusselvurderinger på centerets hjemmeside www.cfcs.dk. Center for Cybersikkerhed vil herudover regelmæssigt offentliggøre, hvilke myndigheder og virksomheder der er tilsluttet netsikkerhedstjenesten efter lovforslagets § 3, stk. 2 og 3.

På samme måde, som det er frivilligt for myndigheder og virksomheder at tilslutte sig Center for Cybersikkerheds netsikkerhedstjeneste, er det frivilligt, om en virksomhed ønsker at oplyse Center for Cybersikkerhed om en sikkerhedshændelse hos virksomheden. Center for Cybersikkerhed opfordrer alle virksomheder til at underrette centeret om relevante sikkerhedshændelser, men det foreslås ikke at indføre en egentlig underretningspligt.

Det bemærkes i øvrigt, at netsikkerhedstjenestens indsamling af data sker automatisk og løbende (altså maskinelt) og derfor udgør et kontinuerligt indgreb i meddelelseshemmeligheden. Af tekniske årsager vil der derfor ikke kunne tilvejebringes en opgørelse over antallet af indgreb i meddelelseshemmeligheden. I den forbindelse kan det som nævnt i bemærkningerne til § 24 oplyses, at Tilsynet med Efterretningstjenesternes årlige redegørelse om tilsynet med Center for cybersikkkerhed skal indeholde en fuldt ud anonymiseret beskrivelse af en eller flere konkrete cyberangreb samt en statistik over antallet af tilfælde, hvor en analytiker fra Center for Cybersikkerhed på baggrund af indgreb i meddelelseshemmeligheden har foretaget en analyse af data. Denne statistik vil desuden indeholde en overordnet kategorisering af, hvor alvorlige disse tilfælde har været.

Redegørelsen suppleres af en årlig beretning fra Center for Cybersikkerhed, der også beskriver centerets aktiviteter på det forebyggende område og bringer statistiske oplysninger herom. Desuden skal beretningen indeholde et overblik over de trusselsvurderinger m.v., der er udsendt i årets løb, således at virksomheder og offentligheden kan få et overblik over risikoen for cyberangreb. Herudover udgiver centeret løbende vejledninger, situationsbilleder og lign., ligesom en oversigt over de tilsluttede myndigheder og virksomheder også regelmæssigt bliver offentliggjort. Oversigten vil også omfatte statistiske oplysninger om antallet af myndigheder og virksomheder, der midlertidigt er tilsluttet netsikkerhedstjenesten.

7. Opbevaring og sletning af data

Dansk Industri (DI), **DI ITEK** og **Teleindustrien (TI)** finder det ikke proportionalt, at pakkedata kan opbevares i 13 måneder og foreslår, at fristen sænkes til én måned. Organisationerne anbefaler herudover, at der fastsættes krav om sletning i forbindelse med videregivelse af data.

DKCERT finder, at en udvidelse af slettefristen til maksimalt 13 måneder for både pakke- og trafikdata vil være med til at effektivisere bekæmpelsen af internetrelateret kriminalitet.

Institut for Menneskerettigheder anbefaler, at lovforslagets slettefrist på 13 måneder for pakkedata, som ikke knytter sig til en sikkerhedshændelse, sænkes. Instituttet anbefaler endvidere, at der indføres et krav om sletning af videregivne data. For så vidt angår data, som videregives til politiet, foreslår instituttet, at dataene slettes, når formålet med videregivelsen er ophørt.

IT-Branchen anbefaler, at opbevaringsfristen for data, der ikke er knyttet til en konkret og begrundet mistænkelig sikkerhedstrussel, tilbageføres til det hidtidige niveau, der kendes fra GovCERT-loven.

IT-Politisk Forening mener, at de eksisterende opbevaringsfrister skal bevares, og i særdeleshed, at pakkedata kun skal opbevares kortvarigt.

Retspolitisk Forening tilslutter sig lovforslagets bestemmelser med tilhørende bemærkninger om sletning af data.

Rådet for Digital Sikkerhed og **Forbrugerrådet Tænk** finder det hverken nødvendigt eller proportionalt, at pakkedata, der ikke knyttes til en sikkerhedshændelse, kan gemmes i 13 måneder, og rådene opfordrer til, at fristen ændres til 30 dage. Rådene finder endvidere, at der i forhold til videregivelse af trafikdata til teleudbydere og myndigheder i udlandet bør stilles krav om sletning, når formålet med behandlingen er opfyldt, dog senest efter henholdsvis tre år for data med tilknytning til en sikkerhedshændelse og 30 dage for data uden en sådan tilknytning.

Efter lovforslaget fastsættes der ensartede opbevarings- og sletningsregler for Center for Cybersikkerheds netsikkerhedstjeneste, der fremover vil omfatte både GovCERT's og MILCERT's nuværende aktiviteter.

De fælles regler sikrer, at netsikkerhedstjenestens adgang til at opbevare pakkedata fortsat begrænses mest muligt af hensyn til privatlivets fred. Det fastholdes således som i dag, at netsikkerhedstjenesten højest kan opbevare data, der knytter sig til en sikkerhedshændelse, i tre år.

I forhold til data, der ikke knytter sig til en sikkerhedshændelse, er der imidlertid behov for en forlængelse af den hidtidige opbevaringsperiode. Center for Cybersikkerheds erfaringer med den praktiske anvendelse af de gældende sletningsregler viser, at reglerne i en række tilfælde har medført, at GovCERT ikke har haft tilstrækkelige muligheder for at forhindre cyberangreb. På den baggrund vurderes det, at adgang til yderligere historiske data i tilfælde af en sikkerhedshændelse vil give mulighed for en betydelig styrkelse af Center for Cybersikkerheds forebyggende arbejde.

For det første giver de historiske data mulighed for at tegne et normalbillede af internetaktiviteterne hos den enkelte myndighed eller virksomhed. Ved at analysere data for internetaktiviteten over en længere periode vil Center for Cybersikkerheds netsikkerhedstjeneste f.eks. kunne fastslå, at det hos en konkret myndighed er normal praksis, at der en gang om måneden gennemføres en særlig backup-procedure, hvor store mængder data overføres fra myndigheden til en ekstern modtager, eller at det er en del af normalbilledet, at der også i visse weekender er datatrafik fra en virksomhed – aktiviteter, som ellers ville indikere en mulig sikkerhedshændelse og udløse en alarm hos netsikkerhedstjenesten.

For det andet vil adgang til yderligere historiske data i tilfælde af en sikkerhedshændelse give netsikkerhedstjenesten langt bedre muligheder for at spore cyberangreb, som ikke tidligere er blevet opdaget af de ramte myndigheder eller virksomheder. Her vil Center for Cybersikkerhed på baggrund af en nærmere undersøgelse af en given sikkerhedshændelse typisk kunne fastslå en række karakteristika, f.eks. i form af angrebsmetoder og -værktøjer, og på baggrund af disse karakteristika vil det i historiske data kunne undersøges, om også andre myndigheder og virksomheder har været ramt af tilsvarende – og hidtil uopdagede – angreb. Desuden modtager Center for Cybersikkerhed ofte underretninger fra andre netsikkerhedstjenester, som i konkrete sager har konstateret, at bestemte ip-adresser har været anvendt til alvorlige cyberangreb, og her er det

af stor betydning, at netsikkerhedstjenesten har mulighed for at fastslå, om sådanne ip-adresser også har været i kontakt med netværket hos myndigheder og virksomheder, som er tilsluttet netsikkerhedstjenesten.

Grundet regelmæssige ændringer i normalbilledet, f.eks. i forbindelse med årlig regnskabsaflæggelse og andre årlige aktiviteter, vurderes det endvidere at være af betydning at kunne foretage år-til-år-sammenligning af internetaktiviteten. Ved vurdering af det, der f.eks. umiddelbart vil kunne ligne en afvigelse fra normalbilledet i januar, vil der således kunne foretages en langt mere kvalificeret vurdering, hvis der er mulighed for at sammenligne med aktiviteterne i januar året før.

Lovforslagets opbevarings- og sletningsregler tager endvidere højde for, at der gælder særlige hensyn, når netsikkerhedstjenesten i overensstemmelse med lovforslagets videregivelsesregler har videregivet pakke- og trafikdata til politiet eller trafikdata til andre myndigheder m.v. Videregivelsen vil bl.a. ske i forbindelse med, at Center for Cybersikkerhed udsender sikkerhedsvarslinger, hvor centeret eksempelvis gør myndigheder og virksomheder opmærksomme på, at en bestemt ip-adresse anvendes til cyberangreb. Sådanne varslinger giver myndigheder og virksomheder mulighed for at tage deres forholdsregler, f.eks. ved at blokere den pågældende ip-adresse i en lokal firewall.

Når en sådan videregivelse er sket via en varsling eller tilsvarende, har Center for Cybersikkerhed ikke mulighed for at sikre, at der efterfølgende sker en sletning hos modtageren. Hertil kommer, at Center for Cybersikkerhed som udgangspunkt er forpligtet til at journalisere de afsendte varslinger. Sletning af disse videregivne data vil dermed umiddelbart være i strid med de almindelige principper for journalisering. Tilsvarende må det anses for betænkeligt, hvis data, der er videregivet til politiet til brug ved en eventuel straffesag, risikerer at blive slettet hos Center for Cybersikkerhed, inden en sådan sag er afsluttet, da det vil udelukke muligheden for, at der under sagen kan indhentes supplerende oplysninger hos Center for Cybersikkerhed. Det følger derfor af lovforslaget, at der ikke gælder slettefrister i de tilfælde, hvor der er sket videregivelse af data.

Det skal imidlertid understreges, at danske myndigheder og virksomheder, der modtager sikkerhedsvarslinger fra netsikkerhedstjenesten, efter omstændighederne vil være underlagt persondatalovens behandlingsregler, såfremt en sikkerhedsvarsling indeholder personoplysninger. Det vil bl.a. indebære, at modtagerne skal sikre, at der ikke er mulighed for at identificere fysiske personer i et længere tidsrum end det, der er nødven-

digt af hensyn til de formål, hvortil personoplysningerne behandles. For udenlandske myndigheder og virksomheder, der modtager sikkerhedsvarslinger, som indeholder personoplysninger, vil der gælde nationale regler. Det bemærkes, at sikkerhedsvarslinger alene kan indeholde trafikdata og ikke pakkedata.

Som efter gældende ret fastsætter lovforslaget maksimale opbevaringsperioder for data. Center for Cybersikkerheds netsikkerhedstjeneste vil imidlertid efter lovforslaget fortsat være forpligtet til at slette data, når formålet med behandlingen er opfyldt, hvis dette sker før den maksimale opbevaringsperiodes udløb. Samtidig vil lovforslagets generelle princip om, at indsamlede personoplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den pågældende person i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles, også finde anvendelse på personoplysninger, der behandles af netsikkerhedstjenesten.

Der henvises i øvrigt til § 17, bemærkningerne til § 17 og de almindelige bemærkninger afsnit 3.4.

8. Tilsyn med Center for Cybersikkerheds behandling af personoplysninger

Dansk Industri (DI), **DI ITEK** og **Teleindustrien (TI)** anfører, at det bør sikres, at Tilsynet med Efterretningstjenesterne har adgang til den fornødne it-revisionsmæssige og sikkerhedsmæssige sagkundskab.

DKCERT finder, at den udvidede tilsynsorganisation kan udøve sin funktion på betryggende vis.

Institut for Menneskerettigheder anbefaler, at det sikres, at Tilsynet med Efterretningstjenesterne besidder den fornødne juridiske, it-revisionsmæssige og sikkerhedsmæssige sagkundskab til at foretage et effektivt tilsyn med GovCERT.

IT-Politisk Forening anbefaler, at det nøje overvejes, om Tilsynet med Efterretningstjenesterne har de kompetencer, som er nødvendige for at føre et effektivt tilsyn med Center for Cybersikkerhed.

Retspolitisk Forening finder, at det ikke er logisk, at tilsynsfunktionen placeres hos Tilsynet med Efterretningstjenesterne, set i lyset af den altovervejende civile karakter af centerets opgaver. Foreningen finder, at de beføjelser, der er tillagt Tilsynet med Efter-

retningstjenesterne er så beskedne, at de i praksis næppe har nogen værdi som sikring af enkeltindividers og juridiske personers retssikkerhed. Foreningen finder derfor, at tilsynet med centerets registrering af personoplysninger bør placeres hos Datatilsynet.

Rådet for Digital Sikkerhed og **Forbrugerrådet Tænk** opfordrer til, at det sikres, at den fornødne sagkundskab inden for it-revision og it-sikkerhed er til stede i Tilsynet med Efterretningstjenesterne eller en anden relevant tilsynsmyndighed.

Som led i etableringen af et nyt retsgrundlag for Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste er der fra 1. januar 2014 oprettet et uafhængigt tilsyn med de to efterretningstjenester. Tilsynet med Efterretningstjenesterne har sit eget sekretariat, og både for så vidt angår ressourcer, uafhængighed og beføjelser er der med det nye tilsyn sket en markant styrkelse af kontrollen med efterretningstjenesternes behandling af personoplysninger.

Der er sammenfald mellem de tilsynsopgaver, som Tilsynet med Efterretningstjenesterne udfører i forhold til Forsvarets Efterretningstjeneste, og de tilsynsopgaver, som fremadrettet vil skulle udføres i forhold til Center for Cybersikkerhed. I begge tilfælde er der således tale om varetagelse af en tilsynsopgave i forhold til behandling af personoplysninger, og ved en videreførelse af det nuværende GovCERT-tilsyn ville der reelt være tale om, at to tilsynsorganer udførte en emnemæssigt identisk opgave.

Sammenlignet med det nuværende GovCERT-tilsyn vil der på flere områder være tale om en styrkelse af tilsynsfunktionen. Det nye tilsyns kompetence foreslås udvidet, således at al behandling af personoplysninger i Center for Cybersikkerhed bliver omfattet af Tilsynet med Efterretningstjenesternes kompetence – og dermed ikke kun den del, der vedrører netsikkerhedstjenesten. Tilsynet vil skulle underrette forsvarsministeren om forhold, som ministeren efter tilsynets opfattelse bør have kendskab til, og tilsynet vil kunne afgive udtalelse over for Center for Cybersikkerhed, herunder udtale kritik, afgive henstillinger samt i øvrigt fremsætte tilsynets opfattelse af en sag. Center for Cybersikkerhed skal underrette Tilsynet med Efterretningstjenesterne og forelægge sagen for forsvarsministeren til afgørelse, hvis centeret undtagelsesvist beslutter ikke at følge en henstilling i en udtalelse fra tilsynet. Herved pålægges Center for Cybersikkerhed en oplysningspligt, hvis centeret undtagelsesvist ikke agter at følge en henstilling i en udtalelse fra Tilsynet med Efterretningstjenesterne. Med udtrykket »undtagelsesvist« understreges det, at centeret som nævnt i almindelighed forudsættes at følge henstillinger i tilsynets udtalelser.

Som følge af lovforslagets udvidelse af tilsynets virksomhed til også at omfatte Center for Cybersikkerhed vil tilsynet få tilført yderligere ressourcer, herunder til it-faglig og teknisk sagkundskab.

Tilsynets virksomhed er i øvrigt nærmere beskrevet i afsnit 3.6.3. i de almindelige bemærkninger. Endvidere er i bemærkningerne til § 24 om tilsynets årlige redegørelse om dets tilsynsvirksomhed bl.a. anført følgende: "Redegørelserne skal indeholde statistiske oplysninger om Center for Cybersikkerheds behandling af personoplysninger, herunder oplysninger om antallet af modtagne klagesager i såvel centeret som tilsynet, oplysninger om antallet af aktindsigtssager og afgørelsen af disse samt oplysninger om antallet af sager med relation til sikkerhedshændelser, der er behandlet i centeret. Tilsynet vil også skulle medtage oplysninger om, i hvor mange tilfælde tilsynet har fundet, at Center for Cybersikkerheds behandling af personoplysninger ikke har været i overensstemmelse med reglerne. Redegørelserne vil også blive offentliggjort på Center for Cybersikkerheds hjemmeside, www.cfcs.dk."

9. Samarbejdet med politiet

Rigspolitiet finder det hensigtsmæssigt, såfremt der i bemærkningerne til lovforslaget tilføjes en nærmere beskrivelse af politiets kompetence til at efterforske, herunder at et tæt samarbejde mellem Center for Cybersikkerhed og politiet bl.a. skal sikre understøttelse af politiets efterforskning af mulige strafbare forhold. Rigspolitiet anfører endvidere, at Center for Cybersikkerhed bør forpligtes til uden unødigt ophold at foretage anmeldelse af væsentlige sikkerhedshændelser til politiet. Rigspolitiet anfører desuden, at it-udstyr, der har været ramt af angreb, først bør undersøges af politiet, inden det undersøges nærmere af Center for Cybersikkerhed, ligesom bevismateriale i sager om brud på informationssikkerheden skal sikres i samråd med politiet.

Rigsadvokaten bemærker, at der i lovforslagets bemærkninger bør medtages en beskrivelse af politiets og anklagemyndighedens kompetence til at behandle sager om mulige strafbare forhold, og at det tydeligt bør fremgå, at sager om mulige strafbare forhold skal behandles af politiet og anklagemyndigheden.

Efter drøftelse med Justitsministeriet er indsat følgende 3 afsnit i lovforslaget:

"Der er etableret et tæt samarbejde mellem Center for Cybersikkerhed og politiet, som indebærer, at data om sikkerhedshændelser, hvor der er indikationer på en strafbar

handling, straks videregives til politiet, eller myndigheden eller virksomheden opfordres til at indgive politianmeldelse. Tilsvarende underretter politiet straks Center for Cybersikkerhed, når politiet bliver opmærksom på sager, der har relevans for centerets funktion. Det kan f.eks. være tilfældet, hvis cyberangreb anmeldes til det lokale politi, eller hvis politiet modtager oplysninger om cyberangreb fra udenlandske politimyndigheder." (De almindelige bemærkninger afsnit 3.5.1).

"En sikkerhedshændelse, jf. lovforslagets § 2, nr. 1, vil i nogle tilfælde kunne være et udslag af en strafbar handling. Forebyggelse og efterforskning af strafbare handlinger er opgaver, som hører under politiet, herunder Politiets Efterretningstjeneste, jf. politilovens § 2, nr. 1-3, og § 1, nr. 1 og 2, i lov om Politiets Efterretningstjeneste. I overensstemmelse hermed fremgår det af retsplejelovens § 742, at anmeldelser om mulige strafbare forhold indgives til politiet, og at politiet efter anmeldelse eller af egen drift iværksætter efterforskning, når der er rimelig formodning om, at et strafbart forhold, som forfølges af det offentlige, er begået. Efter retsplejelovens § 96, stk. 1, er det endvidere anklagemyndighedens opgave i forbindelse med politiet at forfølge forbrydelser efter reglerne i retsplejeloven. Center for Cybersikkerhed bør derfor som hidtil kunne videregive oplysninger om mulige strafbare forhold til politiet." (De almindelige bemærkninger afsnit 3.5.2).

"I de tilfælde, hvor politiet efter retsplejelovens § 742 beslutter at iværksætte en efterforskning af mulige strafbare forhold i forbindelse med en sikkerhedshændelse, vil der være en dialog mellem Center for Cybersikkerhed og politiet om politiets eventuelle ønsker til, at Center for Cybersikkerhed tager særlige hensyn for at sikre, at der f.eks. ikke sker en forringelse af spor i sagen. Der kan dog opstå situationer, hvor centeret uanset en igangværende efterforskning må tage nødvendige skridt til at afværge overhængende risiko for skade på nationale cybersikkerhedsinteresser." (Bemærkningerne til § 3).

10. Evaluering af GovCERT-loven

Institut for Menneskerettigheder anfører, at det ikke tydeligt fremgår af hverken evalueringen eller lovforslaget, hvordan evalueringen er foretaget, eller hvem der er blevet hørt.

IT-Branchen anfører, at evalueringen af GovCERT-loven bekræfter, at Center for Cybersikkerhed udøver et vigtigt og nødvendigt arbejde. Indsatsen har gavnet særligt den offentlige sektors it-sikkerhed i Danmark, og bør fortsættes fremover.

IT-Politisk Forening finder det beklageligt, at tilsynet med GovCERT først blev nedsat i september 2013. Foreningen finder ikke, at det ud fra evalueringen kan vurderes, i hvilket omfang GovCERT har bidraget til it-sikkerheden ved at stoppe uautoriseret indtrængen og kompromittering af data. Foreningen vil endvidere opfordre til, at evalueringen udvides med et afsnit om konsekvenserne for borgernes ret til privatliv.

IT- og Telestyrelsen påbegyndte det forberedende arbejde med nedsættelse af et GovCERT-tilsyn efter GovCERT-lovens ikrafttrædelse i juni 2011. IT- og Telestyrelsens nedlæggelse i oktober samme år medførte imidlertid, at nedsættelsen af tilsynet blev udsat til Center for Cybersikkerheds etablering. Center for Cybersikkerhed blev etableret i december 2012, hvorefter det forberedende arbejde med nedsættelsen af tilsynet blev genoptaget.

GovCERT-tilsynets første årsredegørelse er offentliggjort den 24. marts 2014.

Evalueringen af GovCERT-loven indeholder statistiske oplysninger om GovCERT's hidtidige aktiviteter. Det fremgår således af evalueringen, at GovCERT i perioden fra september 2011 til udgangen af marts 2014 har udsendt godt 100 varslinger til GovCERT's kundekreds. Tallet omfatter generelle varslinger til en bredere kreds og specifikke varslinger til enkeltkunder på baggrund af en alarm. Der er siden 2010 registreret godt 1.100 sikkerhedshændelser. Heraf vurderes en fjerdedel at være alvorlige.

11. Andre bemærkninger

Rådet for Digital Sikkerhed og Forbrugerrådet Tænk finder, at definitionen af sikkerhedshændelser i lovforslaget er så bred, at selv mindre hændelser vil være begrundelse nok til at opnå adgang til data uden retskendelse.

Efter lovforslaget vil Center for Cybersikkerheds netsikkerhedstjeneste som hidtil have hjemmel til at foretage indgreb i meddelelseshemmeligheden. Det er en forudsætning, at dette sker med henblik på at understøtte et højt informationssikkerhedsniveau.

Med lovforslaget sikres det, at analyse af pakkedata kun må finde sted ved begrundet mistanke om en sikkerhedshændelse og kun i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen.

Det følger derudover af lovforslaget, at Center for Cybersikkerheds indsamling af personoplysninger skal ske til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål. Personoplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Dansk Industri (DI), **DI ITEK** og **Teleindustrien (TI)** henviser til, at lovforslagets § 17, stk. 3, vedrører registrering af data, som ikke defineres i lovforslaget. Organisationerne anfører i den forbindelse, at der dermed er en risiko for, at Center for Cybersikkerhed kan have data liggende, som ikke er registrerede, og dermed ikke er omfattet af slettefristerne, hvorfor det bør præciseres, at en registrering i overensstemmelse med det persondataretlige begreb er en behandling.

Begrebet registrering i lovforslagets § 17, stk. 3, er omfattet af behandlingsbegrebet, der er defineret i lovforslagets § 2, nr. 5, hvorefter behandling omfatter enhver operation som oplysninger gøres til genstand for.

Det fremgår desuden af bemærkningerne til lovforslagets § 17, at fristerne for sletning regnes fra det tidspunkt, hvor Center for Cybersikkerhed har registreret de pågældende data. Det fremgår udtrykkeligt, at dette svarer til tidspunktet for centerets lagring af data. Der er således ikke korrekt, at centeret "kan have data liggende", som ikke er registrerede.

Dansk Industri (DI), **DI ITEK** og **Teleindustrien (TI)** nævner, at en privat virksomheds udlevering af oplysninger til Center for Cybersikkerhed ikke nødvendigvis er lovlig efter persondataloven eller teleloven. Organisationerne finder derfor, at det bør præciseres, at udleveringen af personoplysninger herunder pakke- og trafikdata til Center for Cybersikkerhed lovligt kan foretages af en tilsluttet virksomhed uden, at der foreligger en konkret anmodning fra Center for Cybersikkerhed.

Det fremgår udtrykkeligt af afsnit 3.3.1 i lovforslagets almindelige bemærkninger, at videregivelse af personoplysninger til Center for Cybersikkerhed er omfattet af persondataloven. Der sker således ikke med lovforslaget en fravigelse af persondataloven for virksomheder. Såfremt en virksomhed tager initiativ til at videregive personoplysninger til Center for Cybersikkerhed, vil virksomheden skulle sikre, at en sådan udlevering er i overensstemmelse med persondataloven.

IT-Branchen foreslår, at det i lovforslaget indskrives, at Center for Cybersikkerheds virke skal evalueres senest efter 4 år med fokus på betydning for sikkerheden, for meddelelseshemmeligheden, for det private marked for it-sikkerhed og centerets evne til at vidensdele løbende med selvsamme.

Det fremgår af bemærkningerne til lovforslagets § 24, at der efter den politiske aftale om lovforslaget skal udarbejdes en rapport om erfaringerne med den nye lovgivning, som oversendes til Folketinget 3 år efter lovens ikrafttræden. Til brug for rapporten vil der blive indhentet bidrag fra Center for Cybersikkerhed, der vil kunne oplyse om centerets almindelige erfaringer med hensyn til den nye lovgivning, og fra Tilsynet med Efterretningstjenesterne, der vil kunne oplyse om tilsynet med Center for Cybersikkerheds overholdelse af den nye lovgivning. Endelig vil Forsvarsministeriet indhente bidrag fra en eller flere uafhængige eksperter på cyberområdet, der kan medvirke til at belyse den nye lovgivnings betydning for kvaliteten og effektiviteten af Center for Cybersikkerheds opgavevaretagelse.

IT-Branchen anbefaler, at lovforslagets frist for den midlertidige tilslutning af virksomheder forlænges fra den foreslåede periode på 2 måneder til en periode på op til 12 måneder. Branchen anfører i den forbindelse, at der i forbindelse med en sikkerhedshændelse typisk kan gå 8-9 måneder, før det fulde omfang af en kompromittering af sikkerheden opdages.

Den midlertidige tilslutning af virksomheder i medfør af lovforslagets § 6 forudsætter, at der er begrundet mistanke om en sikkerhedshændelse. Der vil således skulle foreligge konkrete indikationer, der peger i retning af, at en sikkerhedshændelse har fundet sted eller vil finde sted.

Såfremt der under den midlertidige tilslutning konstateres en konkret sikkerhedshændelse via monitoreringen, forudsættes det (bemærkningerne til § 6), at monitoreringen kan fortsætte, indtil den konkrete sikkerhedshændelse er håndteret, hvorefter den midlertidige tilslutning straks afsluttes.