FORSVARSMINISTERIET

KOMMENTERET HØRINGSOVERSIGT

vedrørende

forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden)

Dato: 27. marts 2019

Enhed: JSN
Sagsnr.: 2019/000950
Dok.nr.: 890135
Bilag: Ingen

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Tlf.: 728 10000
Fax: 728 10300
E-mail: fmn@fmn.dk
www.fmn.dk
EAN: 5798000201200
CVR: 25 77 56 35

Et udkast til lovforslaget har i perioden fra den 7. januar 2019 til den 4. februar 2019 været sendt i høring hos følgende myndigheder og organisationer m.v.:

Advokatrådet, Akademikernes Centralorganisation (AC), Amnesty International, Dansk Arbejdsgiverforening (DA), Dansk Energi, Dansk Erhverv, Dansk Industri (DI), Dansk Internet Forum (DIFO), DANSK IT, Danske Advokater, Danske Rederier, Danske Regioner, Datatilsynet, Den Danske Dommerforening, DKCERT, Finans Danmark, Finanssektorens Arbejdsgiverforening, Foreningen af Vandværker i Danmark, Foreningen Danske Olieberedskabslagre, Funktionærernes og Tjenestemændenes Fællesråd (FTF), Institut for Menneskerettigheder, ISP Sikkerhedsforum, IT-Branchen, IT-Politisk Forening, ITD, Justitia, KL, Landbrug & Fødevarer, Landsorganisationen i Danmark (LO), Ledernes Hovedorganisation, Lægemiddelindustriforeningen (LIF), Procesindustriens Brancheforening, PROSA, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Rigsombudsmanden i Grønland, Rigsombudsmanden på Færøerne, Rådet for Digital Sikkerhed, samtlige byretspræsidenter, Statens IT-projektråd, Teleindustrien (TI) og Tilsynet med Efterretningstjenesterne.

Forsvarsministeriet har modtaget høringssvar fra:

Advokatrådet, Akademikerne, Amnesty International, Dansk Arbejdsgiverforening (DA), Dansk Energi, Dansk Erhverv, DANSK IT, Dansk Journalistforbund, Dansk Magisterforening, Danske Medier, Danske Rederier, Danske Regioner, Danske Vandværker, DANVA, Datatilsynet, Den Danske Dommerforening, DI, DIFO, DR, Energinet, Fagbevægelsens Hovedorganisation, Finans Danmark, Finanssektorens Arbejdsgiverforening, Forsikring og Pension, Færøernes Landsstyre, Ingeniørforeningen (IDA), Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, ITD, KL, Københavns Byret, Lederne, Lægeforeningen, PROSA, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Rådet for Digital Sikker-

hed, Teleindustrien, Tilsynet med Efterretningstjenesterne og Tradeshift ApS.

Nedenfor er gengivet de væsentligste punkter i de modtagne høringssvar. Forsvarsministeriets kommentarer til høringssvarene er angivet i kursiv.

1. Generelt

Færøernes Landsstyre har ikke bemærkninger til lovforslaget. Præsidenten for Vestre Landsret har ikke ønsket at udtale sig om lovforslaget.

Dansk Energi, Dansk Erhverv, DANSK IT, Dansk Journalistforbund, Dansk Magisterforening, Danske Medier, Danske Regioner, Danske Vandværker, DANVA, DI, DIFO, DR, Finans Danmark, Finanssektorens Arbejdsgiverforening, Forsikring og Pension, Ingeniørforeningen (IDA), Institut for Menneskerettigheder, IT-Branchen, ITD, KL, Lederne, Lægeforeningen, Rådet for Digital Sikkerhed, Teleindustrien og Tradeshift anerkender lovforslagets overordnede målsætning om styrkelse af cybersikkerheden.

2. Definitioner og terminologi

Datatilsynet henstiller til, at de definitioner i lovforslaget, som tager udgangspunkt i databeskyttelsesreguleringen – såsom "behandling" – ændres, således at de svarer til de definitioner, der følger af databeskyttelsesforordningen. Datatilsynet bemærker endvidere, at pakkedata, trafikdata, stationære data og malware også kan indeholde personoplysninger, som defineret i databeskyttelsesforordningen og i den foreslåede § 2, stk. 1, nr. 6, i lovforslaget. Tilsynet bemærker desuden, at der i lovforslaget sondres skarpt mellem, om oplysningerne hører under enten et af begreberne "pakkedata, trafikdata, stationære data og malware" eller begrebet "personoplysninger", selv om der meget ofte vil være et betydeligt sammenfald. Det er efter Datatilsynets opfattelse vigtigt, at dette præciseres og direkte fremgår af bemærkningerne til lovforslaget. Datatilsynet finder endvidere, at det bør præciseres, at begrebet sikkerhedshændelse også omfatter brud på persondatasikkerheden.

Efter den gældende § 8, stk. 3, i lov om Center for Cybersikkerhed, der ikke foreslås ændret, er enhver form for behandling af personoplysninger i Center for Cybersikkerhed omfattet af lovens kapitel 6. Ved behandling af data, herunder personoplysninger, hvor der i medfør af kapitel 4 er sket indgreb omfattet af grundlovens § 72, finder de særlige behandlingsregler i kapitel 7 endvidere anvendelse.

Lovens struktur er således, at reglerne i kapitel 6 gælder for enhver behandling af personoplysninger, således som disse defineres i lovens

§ 2, nr. 4, der foreslås videreført uændret som § 2, nr. 6. Hvis der er tale om data, herunder personoplysninger, som er tilvejebragt ved indgreb, der er omfattet af grundlovens § 72, finder de særligt restriktive behandlingsregler i kapitel 7 endvidere anvendelse. Det gælder, uanset om data indeholder personoplysninger eller ej.

Forsvarsministeriet vil for god ordens skyld tilføje i bemærkningerne, at pakkedata, trafikdata, stationære data og malware kan indeholde personoplysninger. Forsvarsministeriet vil endvidere præcisere i bemærkningerne, at en sikkerhedshændelse også vil kunne omfatte brud på persondatasikkerheden.

Teleindustrien anfører, at en definition af begrebet "malware" udelukkende bør indeholde en objektiv, teknisk beskrivelse af, hvad der betragtes som malware, og ikke en kvalificering af, at en "særligt bestyrket mistanke" kan medføre subsumption af data under begrebet. Teleindustrien mener, at sidstnævnte vil medføre uforudsigelighed, da begrebets definition hermed vil afhænge af Center for Cybersikkerheds subjektive vurdering af de pågældende data.

En objektiv og teknisk beskrivelse af malware ville skulle omfatte en lang række forskelligartede typer data i form af typeeksempler på kendte angrebsmetoder. Henset til den hastige teknologiske udvikling er det Forsvarsministeriets opfattelse, at en sådan beskrivelse af, hvad der aktuelt betragtes som malware, vil være stærkt uhensigtsmæssig, da der så vil være behov for en lovændring, hver gang angrebsaktører tager nye typer angrebsværktøjer i brug.

I lovforslaget er malware derfor defineret som data, hvor der er særligt bestyrket mistanke om, at data er anvendt af en angrebsaktør med det formål at forårsage et brud på informationssikkerheden.

Det bemærkes i den forbindelse, at særligt bestyrket mistanke er det kriterium, der bl.a. anvendes i retsplejeloven i forbindelse med varetægtsfængsling efter lovens § 762, stk. 2. Der er således tale om et meget højt mistankekrav.

DANSK IT anbefaler, at begrebet "offentligt tilgængelig" i § 6 c vedrørende sinkholes ændres til "forudsat de er ledige", da dette efter DANSK IT's opfattelse er en mere retvisende betegnelse for, at et domæne, ip-adresse eller e-mail ikke er ejet af nogen, men kan erhverves og anvendes af Center for Cybersikkerhed.

Forsvarsministeriet vil ændre den foreslåede § 6 c i overensstemmelse med det af DANSK IT anbefalede.

3. Center for Cybersikkerheds generelle adgang til data

En række høringsparter kritiserer, at Center for Cybersikkerhed med lovforslaget vil få adgang til meget store mængder data på baggrund af et bredt kriterium om, at adgangen til data kan ske med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet.

Danske Regioner, IDA og Lægeforeningen udtrykker bekymring over Center for Cybersikkerheds adgang til personfølsomme oplysninger. Lægeforeningen mener, at lovforslaget i højere grad skal sikre, at personfølsomme helbredsoplysninger ikke deles blandt personer, der ikke har patienterne i aktuel behandling.

Dansk Journalistforbund anfører endvidere, at der gives mulighed for, at en efterretningstjeneste kan overvåge al kommunikation til, fra og i en medievirksomhed, hvilket Dansk Journalistforbund anser for problematisk i forhold til mediernes uafhængighed i almindelighed og i særdeleshed muligheden for, at medierne og den enkelte journalist kan beskytte sine kilder.

Lovforslaget lægger op til, at Center for Cybersikkerhed som led i centerets opgave med at opdage, analysere og bidrage til at imødegå it-sikkerhedshændelser kan behandle data fra myndigheder og virksomheder, såfremt behandlingen kan bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

Centerets behandling omfatter imidlertid både en maskinel og en manuel behandling af data.

Der er en forholdsvis bred adgang til at foretage maskinel behandling, hvilket skyldes, at den maskinelle (og helt automatiserede) scanning af data, der foretages af centerets alarmenheder, nødvendigvis må omfatte al ind- og udgående trafik hos en myndighed eller virksomhed for at kunne opdage cyberangreb. Kun ved at gennemføre denne maskinelle scanning kan det fastslås, om der potentielt er sket en it-sikkerhedshændelse.

Centerets brede adgang til maskinel behandling af data skal ses i sammenhæng med de restriktive analyseregler i den foreslåede § 15, hvorefter Center for Cybersikkerhed kun i nærmere opregnede tilfælde må tilgå data manuelt. Det følger således af den foreslåede § 15, stk. 1, nr. 2, at manuelle analyser af indholdet af data (pakkedata og stationære data) i forbindelse med monitorering alene må ske, såfremt der er begrundet mistanke om en (it-)sikkerhedshændelse og kun i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen.

Bestemmelsen indebærer, at Center for Cybersikkerheds analytikere kun kan tilgå indhold af kommunikation (pakkedata) og øvrige ind-

holdsdata (stationære data), hvis det sker som led i centerets arbejde med it-sikkerhedshændelser. Det indebærer, at analytikerne som det klare udgangspunkt ikke vil kunne tilgå korrespondance. Kun hvis der opstår en begrundet mistanke om, at der er sket en it-sikkerheds-hændelse – typisk i form af et cyberangreb – kan analytikerne tilgå disse data, og i så fald kun de data, som det er nødvendigt at tilgå for at analysere selve it-sikkerhedshændelsen. Analytikernes tilgang til data logges i Center for Cybersikkerheds systemer, og al tilgang til personoplysninger er underlagt både egenkontrol og Tilsynet med Efterretningstjenesternes løbende, uafhængige kontrol.

Dansk Energi henleder opmærksomheden på, at installation af sikkerhedssoftware på interne systemer er en særlig udfordring, når virksomheder har kontorer i flere lande, der er fuldt integreret i de administrative it- og teleløsninger. Finans Danmark efterlyser også, at lovforslaget forholder sig til problemstillingen, hvor en række finansielle institutter og virksomheder behandler data for ikke-danske kunder og i den forbindelse skal overholde udenlandske regler og er underlagt et udenlandsk tilsyn. Forsikring og Pension finder det også problematisk, at der ikke er taget stilling til situationen, hvor centeret vil få adgang til udenlandske data.

Center for Cybersikkerhed kan i relation til virksomheder alene foretage monitorering af data i Danmark. Det afgørende vil således være, om virksomhedens behandling af data finder sted i Danmark eller i udlandet – ikke om der er tale om oplysninger, der stammer fra Danmark eller fra udlandet.

4. Påbud om tilslutning til netsikkerhedstjenesten

En lang række høringsparter er generelt kritiske overfor lovforslagets nye initiativ vedrørende påbud om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste, herunder især muligheden for at give påbud om installation af sikkerhedssoftware på lokale netværk og enheder.

Som det er anført i lovforslaget, forudsættes det, at påbud kun anvendes meget sjældent og kun i yderste konsekvens. Vurderingen er, at der maksimalt vil blive givet et lavt et-cifret antal påbud om året.

Formålet med påbudsordningen er at give Center for Cybersikkerhed et værktøj, som kan anvendes i de sjældne situationer, hvor f.eks. en virksomhed er af afgørende vigtighed for Danmarks infrastruktur, men hvor virksomheden ikke selv ønsker at samarbejde med Center for Cybersikkerhed. Uden muligheden for påbud vil det være overladt til denne virksomhed selv at træffe beslutninger, som kan gøre virksomheden til det svage led i den danske infrastruktur. Men rammes en sådan virksomhed af et alvorligt cyberangreb, vil

konsekvenserne af dette angreb ikke blot ramme virksomheden selv, men potentielt hele samfundet.

Forsvarsministeriet har noteret sig, at en lang række høringsparter giver udtryk for en særlig bekymring over, at påbudsordningen også omfatter monitorering via sikkerhedssoftware på lokale netværk og enheder. Høringsparterne henviser især til, at centeret dermed vil få adgang til virksomhedernes forretningshemmeligheder, ligesom høringsparterne henviser til risikoen for, at installation af sikkerheds-software kan gå ud over it-systemernes stabilitet. Forsvarsministeriet vil på den baggrund tilpasse lovforslaget, således at påbuds-muligheden alene omfatter ekstern monitorering ved hjælp af alarm-enheder.

En lang række høringsparter påpeger endvidere, at det ikke ud fra lovforslaget er muligt entydigt at fastslå, om en konkret virksomhed vil få et påbud eller ej. Dermed er det svært for virksomhederne at vurdere, om de risikerer at få et påbud. En række høringsparter finder således, at begrebet "særligt samfundsvigtig karakter" bør præciseres i lovforslaget.

Der er ikke i lovforslaget fastsat objektive kriterier, der gør det muligt for en konkret virksomhed entydigt at vurdere, om den vil få et påbud. Objektive kritierier kan vanskeligt opstilles, da det ikke f.eks. er antal ansatte, antal kunder, omsætningens størrelse og tilsvarende kriterier, der i sig selv viser, om en virksomhed er så samfundsvigtig, at et påbud kan være aktuelt.

Et påbud må derfor nødvendigvis baseres på et skøn, men dette skøn vil skulle udøves indenfor de rammer, der er fastsat i lovforslaget. Lovforslaget beskriver således, at kravet er, at en virksomhed eller myndighed skal være særligt samfundsvigtig (og kriterierne herfor beskrives), samt at den skal have væsentlig betydning for Danmarks kritiske infrastruktur. Det indebærer, at langt de færreste virksom-heder vil blive omfattet.

Center for Cybersikkerhed skal desuden i videst muligt omfang efter-leve principperne i forvaltningslovens kapitel 4-6. Det indebærer bl.a., at Center for Cybersikkerhed forud for, at centeret træffer afgø-relse om at meddele et påbud, efter principperne i forvaltningslovens § 19 i en række tilfælde vil skulle høre den relevante part i sagen over de faktiske oplysninger, som centeret forventer at lægge vægt på i afgørelsen. Center for Cybersikkerheds afgørelse vil endvidere skulle indeholde en begrundelse med henvisning til de retsregler, i henhold til hvilke afgørelsen er truffet. Da afgørelsen til en vis grad vil bero på et administrativt skøn, vil begrundelsen tillige skulle angive de hovedhensyn, der har været bestemmende for skønsudøvelsen. Afgørelsen vil herudover skulle indeholde en redegørelse for de op-

lysninger vedrørende sagens faktiske omstændigheder, som er tillagt betydning for afgørelsen, jf. principperne i forvaltningslovens § 24.

Flere høringsparter anfører, at lovforslagets initiativ om fjernelse af gebyret for tilslutning i sig selv vil være tilstrækkeligt til at sikre tilslutning til netsikkerhedstjenesten, og at det derfor ikke er nødvendigt med en påbudsordning.

Forsvarsministeriet er enig i vurderingen af, at en fjernelse af gebyret for tilslutning vil medføre, at flere virksomheder vil ønske at blive tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste. Dette er også baggrunden for, at det – som anført ovenfor – forventes, at påbudsordningen kun vil skulle anvendes et lavt et-cifret antal gange om året.

DANSK IT og IT-Branchen påpeger, at der alene er almindelig rekursadgang i forhold til påbud, og at der som minimum bør være rekurs til en uafhængig myndighed. Retspolitisk Forening anbefaler, at der indføres et krav om indhentning af retskendelse om tilslutning efter påbud, idet det efter foreningens opfattelse er retssikkerhedsmæssigt utilstrækkeligt at pege på administrativ rekurs med efterfølgende mulighed for domstolsprøvelse, bl.a. set i lyset af, at centerets virksomhed ikke er omfattet af forvaltningslovens begrundelseskrav.

DANSK IT og DANVA opfordrer endvidere til, at der bør være en tidsmæssig grænse for påbuddet, således at meddelte påbud genovervejes efter en periode.

Som nævnt ovenfor vil Center for Cybersikkerheds afgørelse om at meddele påbud om tilslutning skulle begrundes. Afgørelsen vil som led i den almindelige rekursadgang kunne påklages til Forsvarsministeriet. Det skal endvidere understreges, at afgørelsen vil kunne indbringes for domstolene.

Forsvarsministeriet vil tilpasse lovforslaget, således at det fremgår, at påbud om tilslutning skal revurderes mindst hvert halve år.

Dansk Erhverv bemærker, at påbudsordningen vil betyde, at Center for Cybersikkerhed vil kunne installere aktivt udstyr og software på en virksomheds infrastruktur samt kunne pålægge virksomheden at indrette sin virksomhed efter det. En sådan bestemmelse vil efter Dansk Erhvervs opfattelse kunne ramme danske virksomheder negativt, f.eks. hvad angår eksport, internationalt samarbejde og teknologiudvikling. Dansk Energi og IDA henviser ligeledes til, at der ved påbud kan installeres aktiv software i en virksomhed, og at dette ikke bør kunne pålægges en virksomhed.

Som nævnt ovenfor vil Forsvarsministeriet tilpasse lovforslaget, således at påbudsmuligheden alene omfatter ekstern monitorering ved hjælp af alarmenheder.

Det skal understreges, at muligheden for at meddele påbud om tilslutning alene vil omfatte monitorering via alarmenheder med passiv funktionalitet. Den aktive funktionalitet, hvor der bl.a. kan ske sletning, blokering og omdannelse af data, vil alene kunne anvendes efter aftale med den pågældende virksomhed eller myndighed.

DANSK IT anfører desuden, at lovforslaget bør forholde sig til, hvordan en virksomhed skal opfylde et påbud uden at bryde aftalte hemmeligholdelsesforpligtelser, eller udlevere oplysninger om konfiguration og drift, som virksomheden ikke råder over, da de tilhører en leverandør.

Det skal understreges, at Center for Cybersikkerhed alene behandler tilvejebragte data ud fra et formål om at opdage, analysere og bidrage til at imødegå it-sikkerhedshændelser.

Derudover bemærkes det, at danske myndigheder på en række områder har mulighed for at få adgang til virksomheders data, enten på baggrund af et lovkrav eller efter forudgående kendelse. Principielt er Center for Cybersikkerheds adgang til data ikke anderledes end disse andre ordninger, dog således at rammerne for, hvilke data, som Center for Cybersikkerhed kan tilgå, hvordan de skal behandles samt hvornår og til hvem, oplysninger om sikkerhedshændelser efterfølgende kan videregives, er detaljeret reguleret og – for så vidt angår personoplysninger – undergivet tilsyn fra et særligt kontrolorgan.

Dansk Journalistforbund, Danske Medier og DR betoner vigtigheden af, at medievirksomheder i Danmark ikke under nogen omstændigheder kan tvinges til at underlægge sig et system, hvorved man uden retskendelse kan behandle virksomhedernes data, herunder indholdet af den kommunikation, der transmitteres.

Medier vil ikke kunne meddeles påbud om tilslutning til netsikkerhedstjenesten, da de ikke er omfattet at den foreslåede § 3, stk. 4.

5. Indgreb omfattet af grundlovens § 72

Flere organisationer, herunder DI, Forsikring og Pension, IDA og KL, giver udtryk for bekymring over, at Center for Cybersikkerhed kan behandle data uden retskendelse. Amnesty International finder ikke, at Forsvarsministeriet leverer en holdbar argumentation for, hvorfor der ikke kan ske domstolskontrol af centerets indgreb omfattet af grundlovens § 72. Dansk Energi og DANVA mener, at Center for Cybersikkerheds adgang til data uden retskendelse bør fordre, at centret kan godtgøre begrundet mistanke, og at indgrebet var nødven-

digt. Institut for Menneskerettigheder anbefaler, at der redegøres for, hvordan usikkerheden ved en sikkerhedshændelse adskiller sig fra usikkerheder, når der i øvrigt foretages indgreb i meddelelseshemmeligheden, og henstiller til, at der efterfølgende indhentes en retskendelse.

Efter grundlovens § 72 må indgreb i meddelelseshemmeligheden alene ske efter en retskendelse, med mindre der ved lov er fastsat en særegen undtagelse.

En sådan særegen undtagelse har været gældende siden 2011, hvor GovCERT, der senere blev en del af Center for Cybersikkerhed, ved lov fik hjemmel til at foretage indgreb i meddelelseshemmeligheden uden retskendelse. Denne hjemmel blev videreført med lov om Center for Cybersikkerhed i 2014, og det er samme type hjemmel, som lovforslaget bygger på.

Der er to særlige karakteristika for Center for Cybersikkerheds monitoreringsaktiviteter:

For det første har aktiviteterne primært en forebyggende karakter. Det indebærer, at centeret monitorerer internettrafik og – efter lovforslaget – aktivitet på lokale enheder. Det sker for at opdage eventuelle it-sikkerhedshændelser, men monitoreringen sker ikke på baggrund af en konkret mistanke om, at den enkelte myndighed eller virksomhed er ramt af en it-sikkerhedshændelse. Formålet er netop at være på forkant, således at en it-sikkerhedshændelse opdages (og gerne stoppes), hvis den indtræffer. Dermed eksisterer der ikke på forhånd et mistankegrundlag, som vil kunne afprøves af en domstol.

For det andet sker der som led i monitoreringen en fuldautomatisk analyse af store mængder datatrafik. Også af denne årsag vil det ikke være muligt at etablere en ordning, hvor hvert indgreb i meddelelseshemmeligheden kræver en kendelse, da det ville forudsætte, at der blev meddelt flere tusinde kendelser i timen.

Advokatrådet anfører, at det er retssikkerhedsmæssigt betænkeligt, at det udelukkende overlades til Center for Cybersikkerhed at vurdere, hvornår centeret kan indsamle oplysninger, uden nogen form for domstolskontrol. Advokatrådet foreslår, at der som minimum bør ske en efterfølgende domstolskontrol.

Som altovervejende hovedregel sker Center for Cybersikkerheds monitorering på baggrund af en aftale mellem centeret og den enkelte myndighed eller virksomhed. I denne aftale fastsættes omfanget af monitoreringen nærmere, f.eks. hvilke af myndighedens eller virksomhedens netværksforbindelser, som monitoreringen skal omfatte. Kun i helt særlige tilfælde vil monitoreringen fremover kunne ske på baggrund af et påbud.

Center for Cybersikkerheds mulighed for at tilgå data er detaljeret reguleret i lovforslaget. Den foreslåede § 15 fastsætter således rammerne for, hvornår centeret må fortage automatiserede, maskinelle analyser af data, og hvornår centerets analytikere må foretage manuelle analyser af data. Tilsynet med Efterretningstjenesterne kontrollerer, at centerets behandling af personoplysninger sker i overensstemmelse med disse regler.

Dommerforeningen udtaler, at foreningen forudsætter, at måtte man via de af lovforslaget omfattede indgreb, som uden retskendelse giver adgang til trafikdata, pakkedata og nu tillige stationære data hidrørende fra pc'ere, smartphones, tablets og servere hos myndigheder og virksomheder, der er tilsluttet (herunder påtvunget tilsluttede), jf. lovudkastets forslag til § 4, komme i besiddelse af oplysninger, som rejser mistanke om et strafbart forhold, vil sådanne oplysninger ikke kunne anvendes, medmindre der forholdes i overensstemmelse med retsplejelovens straffeprocessuelle regler.

Det skal understreges, at Center for Cybersikkerheds formål med at foretage indgreb, der er omfattet af grundlovens § 72, udelukkende er at opdage, analysere og bidrage til at imødegå it-sikkerhedshændelser. Center for Cybersikkerhed behandler alene de tilvejebragte data med dette formål.

En it-sikkerhedshændelse vil kunne udgøre et strafbart forhold. Efterforskningen og strafforfølgningen af strafbare forhold henhører imidlertid under politiets og anklagemyndighedens kompetence – og vil skulle ske i overensstemmelse med den regulering, der gælder for politiet og anklagemyndigheden, ikke med hjemmel i lov om Center for Cybersikkerhed.

6. Aktivt cyberforsvar

Dansk Energi udtrykker bekymring over aktivt cyberforsvar og anfører, at det ikke kan afvises, at tredjemand eller tilsluttede virksomheder og myndigheder lider økonomisk tab, såfremt det aktive cyberforsvar f.eks. ødelægger systemer eller blokerer mails. DANVA mener, at erstatningsansvar ved sikkerhedsbrud forårsaget af Center for Cybersikkerheds udstyr bør beskrives nærmere. Dansk Energi oplyser, at man forventer, at der gives en kompensation, hvis en virksomhed lider tab som følge af Center for Cybersikkerheds installerede udstyr. KL og DI giver udtryk for tilsvarende overvejelser om erstatningsansvar.

Advokatrådet opfodrer til en undersøgelse af, hvordan det kan afhjælpes at have konsekvenser for borgerne, såfremt aktiv sikkerhedssoftware ved en fejl blokerer en borgers mail til en myndighed.

DANSK IT anfører, at sletning som led i det aktive cyberforsvar bør ske efter aftale med myndigheden eller virksomheden, og at det endvidere bør anføres i lovforslaget, at sletningen af personoplysninger kun bør ske, hvis det er strengt nødvendigt for at opretholde et højt sikkerhedsniveau. Teleindustrien anfører, at påbud om tilslutning alene bør omfatte "passive" elementer.

Lægeforeningen giver udtryk for, at sletning af journaldata vil være meget ødelæggende for patientbehandling.

Efter lovforslaget vil aktivt cyberforsvar udelukkende blive anvendt efter aftale med den pågældende myndighed eller virksomhed. Aktivt cyberforsvar indgår således ikke i den foreslåede påbudsordning.

Der vil dermed altid være en dialog mellem myndigheden eller virksomheden og Center for Cybersikkerhed, hvor de nærmere rammer for anvendelse af det aktive cyberforsvar kan aftales, herunder hvilke it-systemer, der skal omfattes af aktivt cyberforsvar, samt hvordan risikoen for utilsigtede driftsproblemer reduceres til et niveau, der for begge parter er acceptabelt. Det vil ligeledes være den enkelte myndighed eller virksomhed, der kan tage stilling til, om aktivt cyberforsvar skal anvendes på it-systemer, hvor der er risiko for, at kommunikation med kunder og borgere påvirkes, og tage stilling til, hvordan kunder og borgere i givet fald skal orienteres.

Såfremt en handling eller undladelse fra Center for Cybersikkerheds side resulterer i en skade, der medfører et tab for en person eller en virksomhed, vil et eventuelt erstatningsansvar skulle vurderes efter de almindelige regler for offentlige myndigheders erstatningsansvar.

7. Sikkerhedstekniske undersøgelser

Akademikerne finder det meget bekymrende, at en statslig myndighed skal have mulighed for bl.a. at målrette sikkerhedstekniske undersøgelser mod medarbejdere. Akademikerne finder bl.a., at den foreslåede ordning som udgangspunkt vil være i strid med grundlovsfæstede rettigheder og Den Europæiske Menneskerettighedskonvention.

Fagbevægelsens Hovedorganisation konstaterer, at f.eks. spearphishing er reguleret i aftaler om kontrolforanstaltninger på det statslige, regionale og kommunale område (og ligeledes det private), hvorefter medarbejdere skal varsles om foranstaltninger, medmindre formålet med foranstaltningen herved forspildes. Såfremt dette er tilfældet, skal medarbejderne orienteres snarest efter iværksættelse af foranstaltninger, og der skal redegøres for, hvorfor der ikke kunne orienteres på forhånd. DA bemærker, at det må antages, at de forebyggende sikkerhedstekniske undersøgelser er omfattet af de gældende arbejds- og ansættelsesretlige principper. DA henviser i den

forbindelse til, at DA og LO f.eks. har indgået en aftale om kontrolforanstaltninger.

Dansk Magisterforening finder det endvidere dybt problematisk, at der efter organisationens opfattelse kan lægges fælder ud for udvalgte medarbejdere, og at det kan få ansættelsesretlige konsekvenser for medarbejdere, hvilket anses som uproportionalt i forhold til lovforslagets formål. Lederne udtrykker bekymring for, at ledere skal medvirke til en situation, hvorefter deres medarbejdere kan miste deres arbejde. PROSA udtrykker også bekymring og anfører samtidig, at eventuelle sanktioner, hvis der er brud på it-sikkerheden, bør være overfor lederne og ikke medarbejderne, medmindre medarbejderne handler i ond tro.

Dansk Magisterforening mener endvidere, at det skal præciseres og afgrænses, hvornår og med hvilke midler Center for Cybersikkerhed har adgang til at iværksætte forebyggelsesaktiviteter rettet mod medarbejderne, og at virksomheder og myndigheder som udgangspunkt bør pålægges en orienteringspligt overfor medarbejderne om, at der iværksættes kontrolforanstaltninger.

Advokatrådet finder det betænkeligt, at en offentlig myndighed kan gøre brug af metoder, hvorefter en medarbejder lokkes til at bryde en myndigheds eller virksomheds sikkerhedsregler.

Formålet med Center for Cybersikkerheds sikkerhedstekniske undersøgelser vil ikke være at bidrage til, at der kan indledes personalesager mod medarbejdere, der har udvist mangel på sikkerhedsbevidsthed. Formålet med undersøgelserne er derimod at højne det generelle sikkerhedsniveau i myndigheden eller virksomheden.

Sikkerhedstekniske undersøgelser vil endvidere kun blive gennemført efter anmodning fra en myndighed eller virksomhed, ligesom undersøgelserne tilpasses den enkelte myndigheds eller virksomheds behov og ønsker. Det vil være op til den pågældende myndighed eller virksomhed at sikre, at den sikkerhedstekniske undersøgelse, der konkret aftales med Center for Cybersikkerhed, lever op til eventuelle forpligtelser, som gælder for myndigheden eller virksomheden, herunder aftaler om kontrolforanstaltninger, lokalaftaler, lokale it-politikker osv.

Forsvarsministeriet vil på baggrund af bemærkningerne fra høringsparterne tilpasse lovforslaget, således at Center for Cybersikkerheds afrapportering efter sikkerhedstekniske undersøgelser for så vidt angår myndighedens eller virksomhedens medarbejdere vil være anonymiseret. Oplysninger om identiteten på medarbejdere, der f.eks. har begået et sikkerhedsbrud, vil dermed ikke blive udleveret til den myndighed eller virksomhed, som er genstand for undersøgelsen.

Centerets afrapportering til myndigheder og virksomheder efter en sikkerhedsteknisk undersøgelse vil dermed for så vidt angår myndighedens eller virksomhedens medarbejdere være en anonymiseret gennemgang af centerets observationer. Hvis der konstateres manglende sikkerhedsbevidsthed blandt medarbejderne, vil Center for Cybersikkerhed f.eks. anbefale myndigheden eller virksomheden at gennemføre yderligere uddannelse af medarbejderne generelt.

8. Edition

Danske Regioner anser det for retssikkerhedsmæssigt betænkeligt, at der i forbindelse med sager om udlevering af oplysninger på baggrund af forudgående kendelse alene er krav om, at oplysningerne skal kunne medvirke til at afdække sikkerhedshændelser og ikke en konkret mistanke om en strafbar lovovertrædelse.

Teleindustrien anfører, at udbyderne bør kompenseres for omkostningerne ved at yde Center for Cybersikkerhed bistand i forbindelse med edition svarende til den omkostningsdækning, udbyderne ifølge Teleindustrien har ret til ved politiets indgreb i meddelelseshemmeligheden.

Editionsordningen har til formål at give Center for Cybersikkerhed de nødvendige oplysninger til, at centeret kan imødegå eller begrænse effekten af en it-sikkerhedshændelse, f.eks. ved at underrette offeret for et cyberangreb om en kompromittering af vedkommendes it-system. Center for Cybersikkerhed undersøger it-sikkerhedshændelser, uanset om der er konkret mistanke om en strafbar lovovertrædelse eller ej, og uanset om hændelsen er genstand for efterforskning hos politiet eller ej. Det vurderes på den baggrund ikke at være hensigtsmæssigt at indføre et krav om mistanke om en strafbar lovovertrædelse, idet det vil hindre centeret i på et tidligt tidspunkt at underrette offeret for en it-sikkerhedshændelse.

Editionsordningen indebærer udelukkende, at der skal udleveres oplysninger fra udbydernes kundedatabase i form af kontaktoplysninger på den kunde, som er bruger af et bestemt domænenavn mv. Der er således ikke tale om, at der skal udleveres loggede oplysninger eller foretages tekniske foranstaltninger. På den baggrund er det Forsvarsministeriets vurdering, at udbydernes omkostninger vil være meget begrænsede.

Teleindustrien bemærker, at organisationen kan støtte det hensyn, der med den foreslåede § 7 b m.fl. er taget til den, som indgreb vedrører. Organisationen understreger væsentligheden af domstolsprøvelse af indgreb i meddelelseshemmeligheden og privatlivets fred, herunder at sikre varetagelsen af hensynet til den, udleveringen af oplysninger vedrører. Derfor er forslaget om beskikkelse af advokat efter Teleindustriens vurdering et særdeles hensigtsmæssigt tiltag,

som værner positivt om et indgrebssubjekts retssikkerhed. DANSK IT anbefaler, at advokaten møder sammen med en it-kyndig.

Præsidenten for Københavns Byret bemærker på byretspræsidenternes vegne, at anklagemyndigheden efter retsplejelovens editionsregler kan indhente samme type – men også en lang række andre – oplysninger, og at behandlingen af editionsbegæringer efter retsplejeloven foregår uden medvirken af indgrebsadvokat. Henset til den meget nøje afgrænsning af karakteren af oplysninger, som editionsordningen i lovforslaget omfatter, sammenholdt med, at oplysningerne skal tjene til at afdække en sikkerhedshændelse, ses der efter byretspræsidenternes opfattelse ikke at være grundlag for at fravige det udgangspunkt, som er fastlagt i retsplejeloven, hvorefter der ved behandlingen af sådanne pålæg ikke medvirker indgrebsadvokat. Dommerforeningen bemærker, at foreningen tilslutter sig bemærkningen om, at bistand af en indgrebsadvokat er ufornøden. Præsidenten for Østre Landsret henholder sig i det hele til Dommerforeningens høringssvar.

Forsvarsministeriet vil på baggrund af de samstemmende bemærkninger fra byretspræsidenterne, Dommerforeningen og Præsidenten for Østre Landsret tilpasse lovforslaget, således at der ikke vil skulle medvirke indgrebsadvokater ved behandling af editionssager.

Præsidenten for Københavns Byret bemærker i øvrigt på byretspræsidenternes vegne, at editionspålægget hviler på en forudsætning om, at man ikke har kendskab til, hvem der er bruger af den pågældende e-mailkonto, ip-adresse eller domænenavn, hvorfor bestemmelsen i lovforslagets § 7, stk. 2, ikke forekommer relevant.

Forsvarsministeriet vil på baggrund af bemærkningen fra byretspræsidenterne tilpasse lovforslaget.

9. Slettefrister

Amnesty International finder ikke, at der er en klar begrundelse for, hvorfor data, der ikke hidrører fra en sikkerhedshændelse, skal kunne gemmes i tre år, eller hvorfor videregivet data ikke skal slettes. Amnesty International finder desuden, at en generel slettefrist på fem år forekommer at være unødig og uønskeligt lang.

Institut for Menneskerettigheder anbefaler, at der i lovbemærkningerne nøje redegøres for, hvorledes det sikres, at en udvidelse af slettefristen ikke vil føre til uproportionale indgreb i retten til respekt for privatliv.

IDA anerkender, at Center for Cybersikkerhed har identificeret et behov for at arkivere data i forbindelse med sikkerhedshændelser i en længere periode end hidtil antaget, men bemærker, at de ikke kan

bakke op om en udvidelse af slettefristen, når centret er underlagt Forsvarets Efterretningstjeneste, og at det i øvrigt er problematisk, at slettefristen ikke gælder for andre, når data er delt. Rådet for Digital Sikkerhed mener ikke, at videregivelse af data bør fravige slettekrav for data, hvis formål er opfyldt. Rådet anbefaler endvidere, at der stilles krav om underretning ved sletning, således at de aktører, til hvem data er videregivet, underrettes om, at centeret har foretaget sletning. Teleindustrien finder heller ikke, at der skal gælde udvidede slettefrister for videregivet data

Retspolitisk Forening anbefaler, at personoplysninger indeholdt i data anonymiseres efter et år, og at fristen for at slette data tilknyttet en sikkerhedshændelse nedsættes til tre år.

Som det fremgår af afsnit 3.8.2 i de almindelige bemærkninger til det fremsatte lovforslag er baggrunden for udvidelsen af opbevaringsfristerne, at de restriktive regler for opbevaring af data knyttet til en it-sikkerhedshændelse i en række konkrete tilfælde har vist sig at udgøre en betydelig hindring for centerets beskyttelse af samfundsvigtig infrastruktur. Det foreslås på den baggrund, at slettefristen for data tilknyttet en sikkerhedshændelse udvides fra tre til fem år.

På tilsvarende vis er den nuværende pligt til inden 13 måneder at slette data, der ikke er knyttet til en it-sikkerhedshændelse, uhensigtsmæssig i de tilfælde, hvor eksempelvis danske myndigheder er genstand for længerevarende angrebskampagner. For så vidt angår data, der ikke er tilknyttet en it-sikkerhedshændelse, foreslås opbevaringsfristen udvidet fra 13 måneder til tre år, men kun for data, der stammer fra myndigheder, som i særlig grad beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold, samt virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold.

Udvidelsen af slettefristerne er således resultatet af nøje overvejelser, og udvidelsen er begrænset til det, som er nødvendigt, for at centeret kan udføre sine opgaver.

Derudover bemærkes det, at Center for Cybersikkerhed fortsat i medfør af det foreslåede § 17, stk. 1, er forpligtet til at slette data, når formålet med behandlingen efter en konkret vurdering er udtømt.

Det følger af § 17, stk. 5, at slettefristerne i § 17, stk. 1 og 2, ikke finder anvendelse på data, der er videregivet til andre end den myndighed eller virksomhed, hvorfra data hidrører. Bestemmelsen er en videreførelse af gældende ret, idet undtagelsen fra sletteregelerne dog ikke vil omfatte situationer, hvor videregivelsen alene er sket til den myndighed eller virksomhed, som data hidrører fra. I de tilfælde vil Center for Cybersikkerhed fortsat skulle slette data efter stk. 1 og 2.

Uanset at sletteregelerne i stk. 1 og 2 ikke finder anvendelse, vil personoplysninger indeholdt i data fortsat skulle behandles i overensstemmelse med den gældende § 14, hvorefter 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.

10. Forholdet til den Europæiske Menneskerettighedskonvention og proportionalitetsprincippet

IT-Politisk Forening anfører, at der er foretaget en helt utilstrækkelig og mangelfuld vurdering af, om lovforslaget er foreneligt med Den Europæiske Menneskerettighedskonvention.

Institut for Menneskerettigheder anbefaler på grund af Center for Cybersikkerheds organisatoriske placering under Forsvarets Efterretningstjeneste, at der i bemærkningerne redegøres for centerets adgang til personoplysninger i lyset af den relevante praksis fra Den Europæiske Menneskerettighedsdomstol.

Forholdet til Den Europæiske Menneskerettighedskonvention (EMRK) er indgående beskrevet i afsnit 5 i de almindelige bemærkninger til det fremsatte lovforslag. I den forbindelse er der foretaget en nærmere vurdering af den foreslåede ordning i relation til kravene i EMRK art. 8, stk. 2. På baggrund heraf er det Forsvarsministeriets vurdering, at den foreslåede ordning samlet set er i overensstemmelse med EMRK art. 8.

En række høringsparter har anført, at de ikke anser de foreslåede udvidelser af Center for Cybersikkerheds beføjelser for at være i overensstemmelse med proportionalitetsprincippet. I den forbindelse efterlyses en præcisering af, hvordan proportionaliteten konkret sikres.

De foreslåede udvidelser af Center for Cybersikkerheds beføjelser er nøje overvejet, herunder i forhold til proportionalitetsprincippet.

Derudover bemærkes det, at Center for Cybersikkerhed er underlagt det almindelige forvaltningsretlige proportionalitetsprincip. Det indebærer f.eks., at centeret altid skal benytte den løsning, der vil virke mindst indgribende for at opnå det ønskede mål. Center for Cybersikkerhed vil derfor altid indgå i en dialog med den pågældende myndighed eller virksomhed med henblik på at finde den mest hensigtsmæssige og mindst indgribende løsning.

11. Behandlingen af personoplysninger og forholdet til databeskyttelsesforordningen

11.1. Undtagelse fra databeskyttelsesforordningen

Datatilsynet bemærker, at databeskyttelsesforordningen og databeskyttelsesloven ikke finder anvendelse på den behandling af personoplysninger, som udføres for eller af politiets eller forsvarets efterretningstjenester. Datatilsynet henstiller dog til, at lovforslagets henvisninger til persondataloven ændres, så der i stedet henvises til de gældende databeskyttelsesretlige regler.

IDA henviser til, at Center for Cybersikkerhed i forbindelse med lovforslaget ikke har revideret kapitel 6 vedrørende håndtering af personoplysninger, som nu følger den tidligere persondatalov. Dette lægger efter IDA's vurdering op til, at centret undtager sig selv fra GDPR. IDA's it-panel vurderer, at centret bør leve op til GDPR, og en justering anbefales.

Center for Cybersikkerhed er ikke omfattet af databeskyttelsesforordningen og databeskyttelsesloven, da centeret er en del af Forsvarets Efterretningstjeneste. Lov om Center for Cybersikkerhed indeholder imidlertid en detaljeret regulering af centerets behandling af personoplysninger, som er baseret på den tidligere gældende persondatalov. Uanset at disse bestemmelser indgår i lov om Center for Cybersikkerhed, vil fortolkningen af bestemmelserne naturligt skulle ske i overensstemmelse med den mangeårige praksis, som er udviklet for de tilsvarende bestemmelser i persondataloven.

Folketinget vedtog den 3. maj 2018 lovforslag L 155 om konsekvensændringer af lov om Center for Cybersikkerhed som følge af databeskyttelsesforordningen og databeskyttelsesloven. Med denne lovændring besluttede Folketinget, at gældende ret i videst muligt omfang skulle videreføres, således at lovens bestemmelser om behandling af personoplysninger fortsat skulle baseres på principperne fra persondataloven og ikke tilpasses til databeskyttelsesforordningen og databeskyttelsesloven.

Forsvarsministeriet finder ikke anledning til at fravige denne ordning, men det bemærkes dog, at lov om Center for Cybersikkerhed giver forsvarsministeren hjemmel til at sætte databeskyttelsesforordningen og databeskyttelsesloven i kraft for udvalgte dele af Center for Cybersikkerheds aktiviteter. Denne mulighed ændrer lovforslaget ikke på.

11.2. Præcisering af dataansvar

Danske Regioner savner præcisering af, hvad den brede adgang for Center for Cybersikkerhed til data betyder i forhold til anden lovgiv-

ning, f.eks. i forhold til GDPR, herunder den ansvarskonstruktion, der med lovforslaget er tiltænkt. Danske Regioner spørger, om Center for Cybersikkerhed kan betragtes som databehandler, selvstændig dataansvarlig eller fælles dataansvarlig.

Datatilsynet henstiller til, at det overvejes og præciseres, hvem der er dataansvarlig for de behandlinger af personoplysninger, der sker som følge af det aktive og passive cyberforsvar og i forbindelse med forebyggende sikkerhedstekniske undersøgelser. Datatilsynet understreger i forlængelse heraf vigtigheden af, at det er klart, hvem der er dataansvarlig for de enkelte behandlinger af personoplysninger, særligt for de registrerede, som efter de databeskyttelsesretlige regler har en række rettigheder over for de dataansvarlige, men også for de tilsluttede myndigheder og virksomheder i forhold til deres forpligtelser efter de databeskyttelsesretlige regler, herunder overholdelse af de registreredes rettigheder.

Dansk Energi, DANSK IT, DI, Finanssektorens Arbejdsgiverforening og KL finder, at forholdet til databeskyttelsesforordningen bør uddybes. DANVA finder det afgørende, at Center for Cybersikkerheds arbejde tager højde for databeskyttelsesloven.

Danske Erhverv finder, at tilsluttede myndigheder og virksomheder – for at leve op til databeskyttelsesforordningens oplysningspligter overfor de registrerede – skal kunne oplyse, at de indgår i Center for Cybersikkerheds monitorering. Dansk Erhverv opfordrer derfor Forsvarsministeriet til at udarbejde en standard-informationstekst i forhold til databeskyttelsesforordningen, som en tilsluttet virksomhed kan indeholde i sin personalepolitik i forhold til behandling af persondata.

Der vil i lovforslaget blive tilføjet en nærmere beskrivelse af dataansvaret for de behandlinger af personoplysninger, som sker i forbindelse med Center for Cybersikkerheds aktiviteter.

Center for Cybersikkerhed vil endvidere til brug for de tilsluttede virksomheder og myndigheder udarbejde en standardbeskrivelse af centerets behandling af personoplysninger.

11.3. Myndigheders og virksomheders ansvar efter databeskyttelsesforordningen i relation til tilslutning og videregivelse af data til Center for Cybersikkerhed

Datatilsynet finder, at det skal overvejes nærmere, om de tilsluttede myndigheder eller virksomheders behandling i forbindelse med videregivelse af personoplysninger i overensstemmelse med lovforslaget kan ske inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

Forsvarsministeriet vil præcisere lovforslagets bemærkninger om videregivelse af data med henblik på at tydeliggøre de databeskyttelsesretlige hjemler til videregivelse af persondata i forbindelse med, at myndigheder og virksomheder tilsluttes Center for Cybersikkerheds netsikkerhedstjeneste eller anmoder om bistand fra centeret.

11.4. Brud på persondatasikkerheden

Datatilsynet anfører, at Center for Cybersikkerhed vil kunne få kendskab til brud på persondatasikkerheden, som den tilsluttede myndighed eller virksomhed ikke nødvendigvis selv er bekendt med. Datatilsynet henleder i den forbindelse opmærksomheden på de forpligtelser, den tilsluttede myndighed eller virksomhed har efter databeskyttelsesforordningens artikel 33 til at anmelde et brud på persondatasikkerheden uden unødig forsinkelse og om muligt senest 72 timer efter, at denne er blevet bekendt med bruddet. Datatilsynet henviser endvidere til artikel 32 om den dataansvarliges forpligtelse til at sikre persondatasikkerheden. På den baggrund forekommer det efter Datatilsynets opfattelse uhensigtsmæssigt, at Center for Cybersikkerhed kan blive bekendt med et brud på persondatasikkerheden hos en tilsluttet myndighed eller virksomhed, uden at centeret er forpligtet til at oplyse den tilsluttede myndighed eller virksomhed herom.

DANSK IT anfører, at sletning af personoplysninger som led i det aktive cyberforsvar kan udgøre et persondatasikkerhedsbrud. DANSK IT anbefaler, at lovgiver forholder sig til databeskyttelsesreguleringen, herunder i forhold til bl.a. anmeldelsespligt og underretning af de registrerede ved et brud på persondatasikkerheden.

Center for Cybersikkerheds netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå it-sikkerhedshændelser. Som led i en it-sikkerhedshændelse vil der ofte være sket et brud på persondatasikkerheden.

Når Center for Cybersikkerhed konstaterer en væsentlig it-sikkerhedshændelse, vil den videre håndtering at hændelsen ske i tæt samarbejde med den ramte myndighed eller virksomhed. Som det klare udgangspunkt vil det således ikke kunne forekomme, at Center for Cybersikkerhed er bekendt med en væsentlig it-sikkerhedshændelse, der også indebærer et brud på persondatasikkerheden, uden at den tilsluttede myndighed eller virksomhed også er bekendt hermed – og kan foretage det fornødne.

Eneste undtagelse hertil er situationer, hvor Center for Cybersikkerhed ikke kan identificere den myndighed eller virksomhed, der er ramt af en væsentlig it-sikkerhedshændelse, samt den typisk korte periode, hvor centeret samler de nødvendige oplysninger om en væsentlig it-sikkerhedshændelse inden den første kontakt til den ramte myndighed eller virksomhed.

Det vil dog forekomme, at centeret konstaterer en it-sikkerhedshændelse, som også er et brud på persondatasikkerheden, men hvor it-sikkerhedshændelsens karakter gør, at centeret ikke foretager sig yderligere – f.eks. fordi der ud fra en it-sikkerhedsmæssig synsvinkel er tale om en uvæsentlig it-sikkerhedshændelse. Forsvarsministeriet skal i den forbindelse bemærke, at det ikke ligger inden for Center for Cybersikkerheds opgaver at foretage monitorering med det formål at opdage eventuelle brud på persondatasikkerheden.

Sker der mod forventning et brud på persondatasikkerheden som følge af en fejl begået af Center for Cybersikkerhed, underretter centeret den tilsluttede myndighed eller virksomhed, som derefter kan foretage sig det fornødne.

12. Datasikkerhed

Danske Regioner udtrykker bekymring for sikkerheden omkring den øgede datamængde hos Center for Cybersikkerhed. Advokatrådet er bekymret for den store mængde data, som Center for Cybersikkerhed vil indsamle med de nye værktøjer og opfordrer til, at det overvejes, om det er nødvendigt at indsamle så store mængder af data, da det giver mulighed for misbrug. Rådet finder det endvidere bemærkelsesværdigt, at der ikke er større fokus på sikkerhed omkring de indsamlede data. PROSA udtrykker en tilsvarende bekymring for, at én myndighed opbevarer så mange data og anfører, at det bør overvejes, hvad der skal gøres, hvis Center for Cybersikkerhed bliver kompromitteret.

DANVA henviser til, at kunde- og selskabsdata er meget vigtige, og at sikkerheden omkring disse bør prioriteres højt. ITD understreger behovet for fortrolighed omkring forretningstekniske data og betegner det som helt afgørende, at oplysninger om virksomheders konkurrencemæssige forhold beskyttes.

Center for Cybersikkerhed er national it-sikkerhedsmyndighed og Danmarks kompetencecenter for cybersikkerhed. Centeret er desuden en del af en efterretningstjeneste og er i sit virke særdeles fokuseret på sikkerhed.

Centerets medarbejdere er desuden sikkerhedsgodkendt på meget højt niveau og vant til at håndtere sensitive og klassificerede oplysninger i overensstemmelse med sikkerhedsbestemmelser mv. Endvidere er centerets it-systemer underlagt særligt restriktive sikkerhedskrav, og hertil kommer, at Tilsynet med Efterretningstjenesterne som uafhængigt kontrolorgan fører tilsyn med, at Center for Cybersikkerheds behandling af personoplysninger sker i overensstemmelse med lovgivningen.

Finans Danmark bemærker, at lovforslaget ikke forholder sig til den situation, hvor Center for Cybersikkerheds systemer påvirker den tilsluttede virksomheds driftsstabilitet. Finanssektorens Arbejdsgiverforening finder, at det er vigtigt at sikre, at de tiltag, centeret gennemfører, ikke skader virksomhedernes egne foranstaltninger til sikring af datasikkerheden. Forsikring og Pension udtrykker bekymring om, hvorvidt centerets anvendte tekniske løsninger vil kunne ændre en virksomheds sikkerhedsniveau og eventuelt påvirke systemernes og infrastrukturens ydeevne. IT-Branchen anbefaler, at virksomhederne ved et påbud om tilslutning får mulighed for selv at vælge teknologi og udstyr, der benyttes til centerets monitorering. Danske Regioner, DIFO og Forsikring og Pension finder det ikke klart, hvilke konsekvenser installation af software fra Center for Cybersikkerhed vil have på allerede eksisterende it-systemer, og hvad centrets ansvar er, hvis systemer hos tilsluttede myndigheder påvirkes af den installerede software. Den tekniske løsning vurderes ikke tilstrækkeligt beskrevet, og Danske Regioner opfordrer til, at beskrivelsen uddybes i bemærkningerne. Dansk Erhverv og Energinet savner ligeledes beskrivelse af det tekniske udstyr, der kan installeres, og Energinet finder, at Center for Cybersikkerheds udstyr potentielt kan påvirke industrielt udstyr på en negativ måde. Energinet nævner i den forbindelse, at der vil være en særlig risiko ved at anvende sikkerhedssoftware i lukkede industrielle systemer, da der ved tilslutning skabes en adgang til internettet med deraf følgende sikkerhedsrisiko.

DANSK IT finder, at det bør tydeliggøres, hvordan anvendelse af eksempelvis privatejet sikkerhedssoftware håndteres med henblik på at sikre, at anvendelsen ikke påvirker virksomhedens drift negativt.

Center for Cybersikkerheds monitoreringsudstyr er gennemtestet for at sikre, at udstyret ikke i sig selv vil indebære en øget sikkerhedsrisiko. Center for Cybersikkerhed vil derudover altid i samarbejde med den enkelte myndighed eller virksomhed forsøge at identificere, hvordan udstyret kan installeres på den mest hensigtsmæssige måde.

I relation til monitorering via sikkerhedssoftware vil Forsvarsministeriet som nævnt ovenfor tilpasse lovforslaget, således at sikkerhedssoftware ikke vil være omfattet af påbudsmuligheden. Installation af sikkerhedssoftware vil dermed altid ske efter aftale med den pågældende myndighed eller virksomhed, som vil kunne afveje risiciene ved monitorering med sikkerhedssoftware inden en eventuel tilslutning.

Det bemærkes i øvrigt, at den softwareløsning, som vil blive anvendt, vil variere fra system til system, ligesom den vil være under løbende udvikling. Forsvarsministeriet finder det på den baggrund ikke hensigtsmæssigt, at der på et område med så hastig teknisk udvikling fastsættes tekniske rammer for softwaren i lovforslaget.

13. Vidensdeling og åbenhed

Danske Regioner savner en angivelse af centerets muligheder for at vidensdele i forhold til indsamlede data. Dansk Energi ønsker uddybet, hvordan virksomheder får besked om mindre alvorlige sårbarheder eller trusler, som centeret måtte få kendskab til. Finans Danmark finder også, at berørte virksomheder har et krav på at modtage rettidig information om alvorligheden og det potentielle omfang af en vurderet sikkerhedshændelse. DANVA og Finans Danmark opfordrer til vidensdeling og åbenhed. DIFO mener, at Center for Cybersikkerhed skal forpligtes til at dele data med virksomheder og myndigheder og bistå de tilsluttede myndigheder med den viden, der kommer ud af overvågning. DANSK IT og IT-Branchen opfordrer til vidensdeling med private sikkerhedsfirmaer, hvis Center for Cybersikkerhed ligger inde med relevant viden. Dansk Energi opfordrer til et tæt og tillidsfuldt samarbejde. DI ser også behov for øget vidensdeling.

Dansk Erhverv opfordrer til at fokusere på offentlige-private samarbejder og nævner, at der er behov for et ligebyrdigt samspil mellem offentlige og private spillere i et samarbejde, hvor viden går begge veje. Dansk Erhverv finder på den baggrund, at der er andre måder at dele viden med centeret på end at give centeret beføjelser til bl.a. påbud.

PROSA mener, at der er mangel på transparens, fordi Center for Cybersikkerhed ligger under en efterretningstjeneste, og PROSA foreslår, at rollen som Danmarks nationale it-sikkerhedsmyndighed og nationale kompetencecenter bør ligge under f.eks. Indenrigsministeriet, samtidig med, at et center, der beskæftiger sig med hemmelige, klassificerede oplysninger, skal blive under Forsvarets Efterretningstjeneste.

Institut for Menneskerettigheder anbefaler, at der i lovforslaget indføres en bestemmelse om betingelserne for videregivelse af data fra centeret til resten af Forsvarets Efterretningstjeneste, således at forholdet reguleres på lovniveau.

Center for Cybersikkerhed har til opgave at understøtte et højt sikkerhedsniveau i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af. I den forbindelse er en af centerets primære opgaver at opdage, analysere og bidrage til at imødegå it-sikkerhedshændelser hos myndigheder og virksomheder, der er beskæftiget med samfundsvigtige funktioner. En stor del af denne forebyggende indsats kan kun ske i tæt samarbejde og dialog med de relevante myndigheder og virksomheder. Center for Cybersikkerhed har derfor allerede i dag stor fokus på vidensdeling.

Centeret indgår således løbende i dialog med de enkelte virksomheder og myndigheder om konkrete it-sikkerhedshændelser. Derudover

vidensdeler centeret også mere bredt i forbindelse med centerets udsendelse af bl.a. varslinger, vejledninger og trusselsvurderinger. Centeret har endvidere oprettet en række interessentfora, herunder et vidensdelingsnetværk for decentrale cyber- og informationssikkerhedsenheder i de samfundskritiske sektorer, samt et strategisk samarbejdsforum for virksomheder og brancheorganisationer.

Center for Cybersikkerhed arbejder løbende på at udvikle og forbedre sin rådgivnings- og vidensdelingsindsats, og Forsvarsministeriet finder det naturligt, at dette udviklingsarbejde sker i tæt dialog med relevante interessenter.

Forsvarsministeriet vil desuden tage initiativ til, at der bliver oprettet et offentligt-privat cybersikkerhedsråd. Formålet med rådet er at kvalificere myndighedernes arbejde og styrke det digitale demokrati, herunder udbredelse af viden om – og forståelse for – de trusler og muligheder, som digitaliseringen og den nye teknologi medfører. Rådet vil have deltagelse af Digitaliseringsstyrelsen, Center for Cybersikkerhed og repræsentanter med særlig it-sikkerhedsmæssig kompetence fra den private sektor, brancheorganisationer, forskningsverdenen og forbrugersiden.

IT-Politisk Forening bemærker, at der mangler transparens, idet der med lovforslaget fjernes mulighed for offentliggørelse af tilsluttede organisationer.

Det fremgår af bemærkningerne til den foreslåede § 3, stk. 3, at Center for Cybersikkerhed regelmæssigt vil offentliggøre, hvor mange myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten efter bestemmelsens stk. 2 og 3, samt fordelingen på sektorer.

I dag offentliggøres der jævnligt en liste over de myndigheder og virksomheder, der er tilsluttet, men der har blandt virksomhederne været en bekymring over, at der dermed offentliggøres oplysninger om, hvordan den enkelte virksomheds cyberforsvar er indrettet (eller ikke er indrettet).

14. Konkurrence med private it-sikkerhedsfirmaer

Flere høringsparter udtrykker bekymring for, at Center for Cybersikkerhed vil komme til at konkurrere med private it-sikkerhedsfirmaer, hvis gebyret for tilslutning til netsikkerhedstjenesten bortfalder og centerets værktøjer udvides med sikkerhedssoftware og forebyggende sikkerhedstekniske undersøgelser.

DANSK IT og IT-Branchen mener, at lovforslaget, såfremt det vedtages, får betydning for det private marked, idet det vil gøre Center for Cybersikkerhed i stand til at tilbyde og påbyde ydelser, som i dag tilbydes af kommercielle aktører, og at det vil skabe ulige konkurren-

ce. Rådet for Digital Sikkerhed er af den opfattelse, at lovforslaget vil have en meget betydelig konkurrenceforvridende effekt.

Teleindustrien opfordrer til, at Center for Cybersikkerhed i videst muligt omfang skal udbyde opgaverne til private sikkerhedsfirmaer, således at de kan forestå de forebyggende sikkerhedsforanstaltninger for centeret. Teleindustrien ser også gerne, at Center for Cybersikkerhed vælger flere alternative udbydere, således at de tilsluttede virksomheder kan vælge blandt disse udbydere, da der kan være udbydere, som af forretningsmæssige grunde ikke kan arbejde internt hos den tilsluttede virksomhed.

DI stiller sig endvidere uforstående overfor, at der skal anvendes offentlige ressourcer på gratis at tilbyde ydelser, som i forvejen tilbydes på det private marked, og organisationen mener, at ydelserne er konkurrenceforvridende.

Som det er understreget i lovforslaget, er det Forsvarsministeriets vurdering, at lovforslagets nye initiativer ikke vil påvirke det private marked for it-sikkerhedsløsninger negativt.

Center for Cybersikkerhed har fokus på de avancerede cybertrusler, der typisk kommer fra statslige eller statssponsorerede angrebsaktører. At en myndighed eller virksomhed bliver tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste vil aldrig indebære, at virksomheden så kan undlade at anvende en "almindelig" it-sikkerhedsløsning til håndtering af de langt hyppigere forekommende "almindelige" cybertrusler. Center for Cybersikkerheds løsning kan alene supplere myndighedens eller virksomhedens it-sikkerhedsløsning, aldrig erstatte den.

I forhold til forebyggende sikkerhedstekniske undersøgelser, så forudsættes det, at de gennemføres hos myndigheder og virksomheder, hvor der gør sig særlige sikkerhedshensyn gældende, hvorefter de ikke ønsker at anvende private it-sikkerhedsfirmaer, eller hvor sikkerhedsundersøgelser hos et mindre antal repræsentative virksomheder kan give et billede af den generelle sikkerhedstilstand i en samfundsvigtig sektor.

15. Økonomiske konsekvenser

Danske Regioner er positive over for gebyrfrihed, men betegner det som uklart, hvor mange ekstra ressourcer der kræves for at installere og drifte Center for Cybersikkerheds hardware og software. DANVA, Dansk Energi og DI stiller ligeledes spørgsmålstegn ved, hvilke omkostninger virksomhederne forventes at afholde. Danske Rederier er positive overfor afskaffelsen af gebyr, men bemærker, at der fortsat kan være væsentlige omkostninger forbundet med at være tilsluttet netsikkerhedstjenesten. Finans Danmark bemærker, at lovforslaget

ikke forholder sig til, at tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste kan medføre omkostninger i forbindelse med eksempelvis dekryptering af data eller kompleks systemarkitektur. Teleindustrien anfører, at selv om gebyret bortfalder, vil der fortsat påhvile en virksomhed en potentielt betragtelig omkostning i forhold til implementering, udrulning og sikring af udstyrets kompatibilitet med virksomhedens eksisterende udstyr.

Lægeforeningen udtrykker bekymring for meromkostninger for læger i almen praksis og speciallægepraksis og i de virksomheder, der leverer lægesystemer, hvis de bliver anmodet om eller pålagt at tilslutte sig netsikkerhedstjenesten.

Rådet for Digital Sikkerhed anfører, at der bør afsættes en statslig pulje til finansiering af de nødvendige tiltag og værktøjer hos de enkelte organisationer.

Virksomheder og myndigheder, der allerede er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste, vil opnå en besparelse på grund af forslaget om, at det løbende gebyr for tilslutning bortfalder. For virksomheder eller myndigheder, der efterfølgende tilsluttes centerets netsikkerhedstjeneste, vil der være begrænsede merudgifter i forhold til udgifter til samarbejde med centeret i forbindelse med centerets installation af hardware og software samt drift og gennemførelse, herunder samarbejde med centeret i forbindelse med håndtering af konkrete sikkerhedshændelser.

Der henvises i øvrigt til beskrivelsen i afsnit 6 og 7 i de almindelige bemærkninger til det fremsatte lovforslag vedrørende henholdsvis de økonomiske konsekvenser og implementeringskonsekvenser for det offentlige og de økonomiske og administrative konsekvenser for erhvervslivet mv.

16. Sammenhæng med sektorstrategier samt anden regulering

Danske Regioner bemærker, at regionerne har et sektoransvar, der indebærer et ansvar for at opretholde sikkerheden omkring borgernes behandling og sundhedsdata. Dansk Energi ønsker endvidere at få klarlagt rollefordelingen mellem Center for Cybersikkerhed, sektoransvarlige myndigheder, sektor-CERT'er og virksomheder. DI finder også, at der er behov for en klar ansvarsfordeling mellem Center for Cybersikkerhed, virksomhederne og eventuelle tilsynsmyndigheder.

Danske Rederier påpeger herudover, at det er væsentligt, at der er overensstemmelse mellem de virksomheder, som en sektoransvarlig myndighed har udpeget som følge af NIS-direktivet, og dem, som Center for Cybersikkerhed ønsker at påbyde tilslutning til netsikkerhedstjenesten. Også Forsikring og Pension henviser til sektorstrategi-

erne og mener, at ny lovgivning bør afvente effekten af de tiltag, der er iværksat.

Lovforslaget er et led i udmøntningen af den nationale strategi for cyber- og informationssikkerhed, der blev lanceret i maj 2018. Det fremgår således af strategien, at Forsvarsministeriet vil fremsætte et forslag til ændret lovgivning på cyberområdet, som vil medføre en styrkelse af Center for Cybersikkerheds muligheder for at opdage og stoppe cyberangreb samt styrke centerets analytiske arbejde.

Det indgår ikke i strategien, at der skal foretages ændringer i sektoransvaret, og det ændrer lovforslaget heller ikke på.

Det følger af strategien, at der skal ske en fælles indsats på cyber- og informationssikkerhedsområdet, herunder en styrkelse af indsatsen i seks samfundskritiske sektorer: Energi, sundhed, tele, finans, søfart og transport. Udmøntningen af denne indsats medfører, at hver sektor skal udarbejde en sektorstrategi og opstille en decentral cyber- og informationssikkerhedsenhed (DCIS). Rolle og ansvarsfordelingen mellem de decentrale cyber- og informationssikkerhedsenheder og Center for Cybersikkerhed bliver for hver sektor beskrevet i en samarbejdsaftale.

Dansk Energi finder det essentielt, at danske initiativer på cyber- og informationssikkerhedsområdet harmoniseres og spiller samen med relevante internationale krav og initiativer både på EU-niveau og regionalt. Dansk Energi bemærker i den forbindelse, at det vil være spild af ressourcer, hvis den danske regulering efterfølgende vil skulle vige for EU-praksis eller -regulering. DI understreger vigtigheden af, at nationale initiativer som dette lovforslag (og tilhørende initiativer, som udmøntes i forlængelse heraf) harmoniseres og spiller sammen med internationale initiativer i regi af EU og i globale sammenhænge. DI påpeger, at selv mindre divergenser i forhold til internationale regler vil være byrdefulde for mange virksomheder.

Forsvarsministeriet følger løbende udviklingen på cyberområdet, herunder i relation til EU-regulering, og ministeriet tager i den forbindelse stilling til, om udviklingen medfører et behov for ændring i den nationale regulering.

Finans Danmark efterspørger bl.a. en beskrivelse af, hvordan reglerne i lovforslaget spiller sammen med reglerne om finansiel virksomhed. Finanssektorens Arbejdsgiverforening og Forsikring og Pension foreslår, at Finanstilsynet høres om, hvorvidt videregivelse af oplysninger fra finansielle virksomheder er berettiget efter den finansielle lovgivning.

Med henblik på at tydeliggøre forholdet mellem reglerne i lovforslaget og regler om tavshedspligt i anden lovgivning vil Forsvarsministeriet

indsætte en bestemmelse i lovforslaget om, at myndigheders og virksomheders samarbejde med Center for Cybersikkerhed ikke er begrænset af bestemmelser om tavshedspligt fastsat ved lov eller med hjemmel i lov.

Danske Regioner bemærker til den foreslåede § 8 a, stk. 1, at det bør tydeliggøres i bemærkningerne, hvilke oplysninger, som er arkiveringspligtige. Ydermere bør det begrundes, hvorfor arkiveringen skal omfatte alle oplysninger og ikke kun personoplysninger.

Det fremgår af bemærkningerne til den foreslåede § 8 a, stk. 1, at bestemmelsen indebærer, at Center for Cybersikkerhed vil kunne overføre oplysninger til opbevaring i arkiv i det omfang Rigsarkivaren har fastsat bevarings- og kassationsbestemmelser for de pågældende bestemmelser.

Det er således Rigsarkivaren, der træffer beslutning om, hvilke oplysninger, der skal overføres til arkiv.

Det fremgår endvidere af bemærkningerne, at den foreslåede ændring skyldes, at det ikke kan udelukkes, at der af Rigsarkivaren udstedes bevarings- og kassationsbestemmelser vedrørende oplysninger, som ikke er personoplysninger.

17. Øvrige bemærkninger

Datatilsynet bemærker, at det fremgår af de almindelige bemærkninger til lovforslaget, at der vil blive udarbejdet en rapport om erfaringerne med den nye lovgivning, som oversendes til Folketinget tre år efter lovens ikrafttræden. Datatilsynet finder, at rapporten om erfaringerne med den nye lovgivning bør oversendes til Folketinget allerede ét år efter lovens ikrafttræden. Forsikring og Pension anbefaler også, at rapporten oversendes allerede efter ét år og følges op med rapportering efter andet og tredje år.

Forsvarsministeriet vurderer, at der vil være behov for en vis periode med den nye lovgivning, før der kan gøres status over erfaringerne. Forsvarsministeriet finder derfor, at en rapport om erfaringerne med loven først bør oversendes efter tre år.

DI finder det særligt bekymrende, at Tilsynet med Efterretningstjenesterne svækkes ved, at der i lovforslaget indføres en mulighed for, at centeret kan vælge ikke at følge en henstilling i en udtalelse fra tilsynet.

Det anførte må bygge på en misforståelse, idet lovforslaget ikke indeholder en sådan ændring – ej heller andre ændringer, der vedrører Tilsynet med Efterretningstjenesternes kompetence. Efter gældende ret er der for Center for Cybersikkerhed, FE og PET etableret identi-

ske ordninger, som indebærer, at hvis tjenesterne undtagelsesvist beslutter ikke at følge en henstilling i en udtalelse fra tilsynet, så skal den pågældende tjeneste underrette tilsynet herom og uden unødigt ophold forelægge sagen for ressortministeren til afgørelse. Hvis ministeren vælger ikke at følge henstillingen, skal regeringen underrette Folketingets Udvalg vedrørende Efterretningstjenesterne herom.