U D K A S T

Forslag

til

Lov om Center for Cybersikkerhed

Kapitel 1

Opgaver og organisation

§ 1. Center for Cybersikkerhed har til opgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

Stk. 2. Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste.

Kapitel 2

Definitioner

§ 2. I denne lov forstås ved:

1) *Sikkerhedshændelse*: En hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.
2) *Pakkedata*: Indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester.
3) *Trafikdata*: Data, som behandles med henblik på at transmittere pakkedata.
4) *Personoplysninger*: Enhver form for information om en identificeret eller identificerbar fysisk person.
5) *Behandling*: Enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for.

Kapitel 3

Center for Cybersikkerheds netsikkerhedstjeneste

§ 3. Center for Cybersikkerheds netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder på Forsvarsministeriets område samt hos øvrige tilsluttede myndigheder og virksomheder, jf. stk. 2 og 3.

Stk. 2. De øverste statsorganer samt statslige myndigheder kan efter anmodning blive tilsluttet netsikkerhedstjenesten.

Stk. 3. Regioner og kommuner samt virksomheder, der er beskæftiget med samfundsvigtige funktioner, kan efter anmodning blive tilsluttet netsikkerhedstjenesten, såfremt Center for Cybersikkerhed konkret vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

Stk. 4. Center for Cybersikkerhed kan fastsætte nærmere regler om vilkårene for tilslutning efter stk. 3, herunder regler om betaling for tilslutning.

Kapitel 4

Indgreb i meddelelseshemmeligheden

§ 4. Center for Cybersikkerheds netsikkerhedstjeneste kan uden retskendelse behandle pakke- og trafikdata hidrørende fra netværk hos tilsluttede myndigheder og virksomheder, jf. § 3, stk. 2 og 3, med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet.

§ 5. Center for Cybersikkerheds netsikkerhedstjeneste kan uden retskendelse behandle pakke- og trafikdata hidrørende fra netværk hos myndigheder på Forsvarsministeriets område, jf. § 3, stk. 1, med henblik på at understøtte et højt informationssikkerhedsniveau på området.

§ 6. Ved begrundet mistanke om en sikkerhedshændelse kan en myndighed eller virksomhed, som ikke er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste efter § 3, midlertidigt tilsluttes netsikkerhedstjenesten, som herefter uden retskendelse kan behandle pakke- og trafikdata hidrørende fra netværk hos myndigheden eller virksomheden, når

1) myndigheden eller virksomheden har givet skriftligt samtykke til behandlingen,
2) behandlingen vurderes at kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner er afhængige af, og
3) den midlertidige tilslutning har en varighed på højst to måneder.

§ 7. Ved begrundet mistanke om en sikkerhedshændelse kan Center for Cybersikkerheds netsikkerhedstjeneste uden retskendelse behandle data, som er indeholdt i eller hidrører fra et informationssystem, der anvendes af en myndighed eller virksomhed, når

1) myndigheden eller virksomheden har stillet informationssystemet eller dataene herfra til rådighed for netsikkerhedstjenesten og givet skriftligt samtykke til, at netsikkerhedstjenesten behandler dataene, og
2) behandlingen vurderes at kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner er afhængige af.

Kapitel 5

Forholdet til anden lovgivning, behandling af personoplysninger m.v.

§ 8. Center for Cybersikkerheds virksomhed er undtaget fra lov om offentlighed i forvaltningen bortset fra lovens § 13. Center for Cybersikkerheds virksomhed er endvidere undtaget fra forvaltningslovens kapitel 4-6 og fra lov om behandling af personoplysninger, jf. § 2, stk. 11, i lov om behandling af personoplysninger.

Stk. 2. Forsvarsministeren kan bestemme, at kapitel 8-10 i lov om behandling af personoplysninger, lov om offentlighed i forvaltningen samt forvaltningslovens kapitel 4-6 helt eller delvis finder anvendelse for Center for Cybersikkerhed vedrørende

1) centerets behandling af anmodninger om tilslutning til netsikkerhedstjenesten, jf. § 3, stk. 3,
2) centerets virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet og
3) centerets personalesager.

Stk. 3. Enhver form for behandling af personoplysninger i Center for Cybersikkerhed er omfattet af kapitel 6. Ved behandling af data, herunder personoplysninger, i medfør af kapitel 4 finder de særlige behandlingsregler i kapitel 7 endvidere anvendelse.

Kapitel 6

Behandling af personoplysninger i Center for Cybersikkerhed

§ 9. Center for Cybersikkerheds indsamling af personoplysninger skal ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål. Senere behandling af personoplysninger, der alene sker i historisk, statistisk eller videnskabeligt øjemed, anses ikke for uforenelig med de formål, hvortil oplysningerne er indsamlet.

Stk. 2. 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.

§ 10. Behandling af personoplysninger må kun finde sted, hvis

1) den pågældende person har givet sit udtrykkelige samtykke hertil,
2) behandlingen er nødvendig af hensyn til opfyldelsen af en aftale, som den pågældende person er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den pågældende persons anmodning forud for indgåelsen af en sådan aftale,
3) behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse,
4) behandlingen er nødvendig til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar,
5) behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som Center for Cybersikkerhed eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt,
6) behandlingen er nødvendig for, at Center for Cybersikkerhed eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den pågældende person ikke overstiger denne interesse, eller
7) behandlingen vedrører personoplysninger, der er omfattet af kapitel 4.

§ 11. Der må ikke behandles personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og personoplysninger om helbredsmæssige og seksuelle forhold.

Stk. 2. Bestemmelsen i stk. 1 finder ikke anvendelse, hvis

1) den pågældende person har givet sit udtrykkelige samtykke til en sådan behandling,
2) behandlingen vedrører personoplysninger, som er blevet offentliggjort af den pågældende person,
3) behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares,

4) behandlingen er nødvendig til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar, eller
5) behandlingen vedrører personoplysninger, der er omfattet af kapitel 4.

§ 12. Der må ikke behandles personoplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 11, stk. 1, nævnte, medmindre det er nødvendigt for varetagelsen af Center for Cybersikkerheds opgaver.

Stk. 2. De i stk. 1 nævnte personoplysninger må ikke videregives. Videregivelse kan dog ske, hvis

1) den pågældende person har givet sit udtrykkelige samtykke til videregivelsen,
2) videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår,
3) videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe,
4) videregivelsen er nødvendig for udførelsen af en persons eller virksomheds opgaver for det offentlige, eller
5) videregivelsen omfatter personoplysninger, der er omfattet af kapitel 4.

§ 13. Behandling af personoplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne. Der skal endvidere foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende personoplysninger. Personoplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

§ 14. Indsamlede personoplysninger må ikke 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.

Kapitel 7

Analyse, videregivelse og sletning af data

§ 15. Analyse af pakkedata, der er omfattet af §§ 4, 6 og 7, må kun finde sted ved begrundet mistanke om en sikkerhedshændelse og kun i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen.

§ 16. Data, der er omfattet af §§ 4, 6 og 7, kan kun videregives i følgende tilfælde:

1) Ved begrundet mistanke om en sikkerhedshændelse kan data videregives til politiet.
2) Hvis det er nødvendigt for udførelsen af netsikkerhedstjenestens opgaver, kan trafikdata videregives til danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester, andre netsikkerhedstjenester, virksomheder, der er omfattet af §§ 4, 6 og 7, samt til myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger.

§ 17. Data, der er omfattet af kapitel 4, slettes, når formålet med behandlingen er opfyldt.

Stk. 2. Uanset at formålet med behandlingen ikke er opfyldt, jf. stk. 1, må

1) data, der knytter sig til en sikkerhedshændelse, højst opbevares i tre år, og
2) data, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 13 måneder.

Stk. 3. Fristerne i stk. 2 regnes fra tidspunktet for Center for Cybersikkerheds registrering af de pågældende data.

Stk. 4. Hvis data er videregivet i medfør af § 16, finder stk. 1 og 2 ikke anvendelse på disse data.

Kapitel 8

Sikkerhedsforanstaltninger

§ 18. Center for Cybersikkerhed træffer passende tekniske og organisatoriske foranstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Kapitel 9

Tilsyn med behandling af personoplysninger

§ 19. Tilsynet med Efterretningstjenesterne, jf. § 16 i lov om Politiets Efterretningstjeneste (PET), fører efter reglerne i dette kapitel tilsyn med Center for Cybersikkerheds behandling af personoplysninger.

Stk. 2. Tilsynet udøver sine funktioner i fuld uafhængighed.

§ 20. Tilsynet påser efter klage eller af egen drift, at Center for Cybersikkerhed overholder reglerne i kapitel 4, 6 og 7 vedrørende behandling af personoplysninger.

§ 21. Tilsynet kan som led i sin virksomhed efter § 20 afgive udtalelse over for Center for Cybersikkerhed.

Stk. 2. Tilsynet underretter forsvarsministeren om forhold, som ministeren efter tilsynets opfattelse bør have kendskab til.

Stk. 3. Hvis Center for Cybersikkerhed undtagelsesvis beslutter ikke at følge en henstilling i en udtalelse fra tilsynet, jf. stk. 1, skal centeret underrette tilsynet herom og uden unødigt ophold forelægge sagen for forsvarsministeren til afgørelse.

§ 22. Tilsynet kan hos Center for Cybersikkerhed kræve enhver oplysning og alt materiale, der er af betydning for dets virksomhed.

Stk. 2. Tilsynets medlemmer og sekretariat har til enhver tid mod behørig legitimation uden retskendelse adgang til alle lokaler, hvorfra en behandling, som foretages for Center for Cybersikkerhed, administreres, hvorfra der er adgang til de oplysninger, som behandles, eller hvor tekniske hjælpemidler opbevares eller anvendes.

Stk. 3. Tilsynet kan afkræve Center for Cybersikkerhed skriftlige udtalelser om faktiske og retlige forhold.

Stk. 4. Tilsynet kan anmode om, at en repræsentant for Center for Cybersikkerhed er til stede med henblik på at redegøre for de behandlede sager.

§ 23. Tilsynets virksomhed er undtaget fra lov om offentlighed i forvaltningen bortset fra lovens § 13.

Stk. 2. Tilsynets virksomhed er undtaget fra forvaltningslovens kapitel 4-6 og fra lov om behandling af personoplysninger.

§ 24. Tilsynet afgiver en årlig redegørelse om sin virksomhed til forsvarsministeren. Redegørelsen offentliggøres.

Kapitel 10

Ikrafttrædelses- og overgangsbestemmelser m.v.

§ 25. Loven træder i kraft den 1. juli 2014.

Stk. 2. Lov nr. 596 af 14. juni 2011 om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v. ophæves samtidigt.

Stk. 3. Aftaler, der er indgået efter den i stk. 2 nævnte lov, opretholdes, indtil de bortfalder efter deres indhold eller opsiges.

Stk. 4. Pakke- og trafikdata, der er indsamlet efter den i stk. 2 nævnte lov, behandles og opbevares efter de hidtil gældende regler.

Stk. 5. Begæringer om aktindsigt, som er indgivet før lovens ikrafttræden, afgøres efter de hidtil gældende regler.

§ 26. Loven gælder ikke for Færøerne og Grønland, men kan ved kongelig anordning sættes helt eller delvis i kraft for Færøerne og Grønland med de ændringer, som de færøske og grønlandske forhold tilsiger.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

Danske myndigheder og virksomheder er i stigende grad udsat for cyberangreb, hvor stater, grupper og enkeltpersoner forsøger at trænge ind i den danske it- og teleinfrastruktur. Det kan således konstateres, at både statslige aktører, aktivister og kriminelle organisationer bruger internettet til at spionere mod Danmark eller til at anrette skade på eksempelvis danske hjemmesider og servere. Truslen om sådanne angreb medfører en betydelig og stigende sikkerhedsrisiko for et højt digitaliseret samfund som det danske.

For at øge beskyttelsen mod cyberangreb oprettede regeringen i 2012 Center for Cybersikkerhed som en del af Forsvarets Efterretningstjeneste. Center for Cybersikkerhed varetager funktionen som Danmarks nationale it-sikkerhedsmyndighed, og centerets hovedopgave er at styrke sikkerheden i den informations- og kommunikationsteknologiske infrastruktur (ikt-infrastruktur), som samfundsvigtige funktioner er afhængige af.

Formålet med dette lovforslag er 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.

2. Baggrunden for lovforslaget

2.1. Oprettelsen af Center for Cybersikkerhed

Ved kongelig resolution af 3. oktober 2011 blev ressortansvaret for sager vedrørende beskyttelse af kritisk it-infrastruktur samt statens varslingstjeneste for internettrusler, GovCERT, overført til Forsvarsministeriet.

Af regeringsgrundlaget af samme dato, "Et Danmark, der står sammen", fremgår det endvidere, at "[r]egeringen vil med respekt for retssikkerheden og den personlige frihed styrke beskyttelsen mod cyberangreb. En robust infrastruktur for informations- og kommunikationsteknologi er vigtig for landets økonomi og sikkerhed. For at styrke beskyttelsen mod cyberangreb mv. samles de forskellige myndigheders indsats i et IT sikkerhedscenter (under Forsvarsministeriet), der skal varetage opgaven som den nationale IT-sikkerhedsmyndighed og Governmental Computer Emergency Response Team (GovCERT)."

På den baggrund blev Center for Cybersikkerhed den 18. december 2012 oprettet som en del af Forsvarets Efterretningstjeneste. Baggrunden for placeringen af Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste var særligt at opnå synergieffekter i form af eksempelvis udnyttelse af Forsvarets Efterretningstjenestes erfaringer inden for it-sikkerhedsområdet, viden om det internationale trusselsbillede på cyberområdet og særlige adgang til oplysninger fra udlandet om cybertrusler.

Center for Cybersikkerhed varetager bl.a. følgende opgaver:

- GovCERT (Governmental Computer Emergency Response Team), der er den statslige varslingstjeneste for internettrusler. GovCERT blev oprettet i 2009 og var tidligere en del af IT- og Telestyrelsen.

- MILCERT (Military Computer Emergency Response Team), der er varslingstjeneste for internettrusler på Forsvarsministeriets område og siden oprettelsen i 2010 har været en del af Forsvarets Efterretningstjeneste.
- National it-sikkerhedsmyndighed. Politiets Efterretningstjeneste varetager dog funktionen som it-sikkerhedsmyndighed på Justitsministeriets område.
- Informationssikkerhed og beredskab på teleområdet. Opgaven blev tidligere varetaget af IT- og Telestyrelsen.

Center for Cybersikkerheds opgaver er nærmere beskrevet i bemærkningerne til den foreslåede § 1.

I forbindelse med oprettelsen af Center for Cybersikkerhed besluttede regeringen, at forsvarsministeren skulle fremsætte et lovforslag, der regulerer Center for Cybersikkerheds virksomhed. Dette forslag til lov om Center for Cybersikkerhed udmønter regeringsbeslutningen.

2.2. Reguleringen af Center for Cybersikkerheds virksomhed

Forsvarets Efterretningstjenestes virksomhed er reguleret ved lov nr. 602 af 12. juni 2013 om Forsvarets Efterretningstjeneste (FE-loven), der trådte i kraft den 1. januar 2014. Lovens § 1, stk. 3, har følgende ordlyd: "Forsvarets Efterretningstjeneste er national it-sikkerhedsmyndighed, militær varslingstjeneste for internettrusler m.v. (MILCERT) og statslig varslingstjeneste for internettrusler (GovCERT). Opgaver i medfør heraf er ikke omfattet af kapitel 2-7, men reguleres særskilt". Bestemmelsen indebærer, at Center for Cybersikkerhed er omfattet af FE-lovens § 2, som fastslår, at Forsvarets Efterretningstjeneste er underlagt og virker under ansvar over for forsvarsministeren, samt at Forsvarets Efterretningstjeneste inden for sit ansvarsområde holder Forsvarsministeriet underrettet om forhold af betydning for Danmark og danske interesser, om forhold af væsentlig betydning for tjenestens virksomhed og om vigtigere enkeltsager.

GovCERT's virksomhed er i øvrigt reguleret ved lov nr. 596 af 14. juni 2011 om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v. (GovCERT-loven). Forslaget til GovCERT-loven blev ved Folketingets 3. behandling den 1. juni 2011 vedtaget med 111 stemmer for og ingen stemmer imod forslaget.

Endvidere er Center for Cybersikkerhed som helhed omfattet af Forsvarsministeriets retningslinjer af 13. maj 2013 for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste. Med retningslinjerne er der fastsat en række bestemmelser om behandlingsgrundlag og behandlingssikkerhed ved behandling af personoplysninger i Center for Cybersikkerhed. Bestemmelserne bygger på principperne i persondataloven. Retningslinjerne fastsætter derudover en række bestemmelser om den interne udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste.

Retningslinjerne kan ses på Center for Cybersikkerheds hjemmeside, www.cfcs.dk.

2.3. Udviklingen i trusselsbilledet

Det danske samfund er i stigende grad afhængigt af at kunne anvende mulighederne på internettet. Internettet er i dag af central betydning for befolkningens økonomiske velfærd og sociale relationer og for centrale, vigtige samfundsfunktioner samt erhvervslivets forretnings- og konkurrencevilkår.

Informations- og kommunikationsteknologi (ikt) og digitalisering får stadig større betydning for den danske økonomi, og betydningen forventes fortsat at stige i årene fremover. Digitalisering er en af de vigtigste faktorer, der kan bidrage til at øge produktiviteten i virksomhederne samt skabe nye produkter, tjenester og forretningsmodeller.

I december 2012 fremlagde Europa-Kommissionen således en opdateret version af sin ikt-strategi fra 2010 (Europas Digitale Dagsorden). Heri fremhæves det, at Europas fremtidige vækst og konkurrenceevne afhænger af evnen til at udnytte alle de digitale muligheder. På trods af fremskridt på den digitale dagsorden er der ifølge Kommissionen behov for at gøre mere, hvis Europa skal opnå den vækst og konkurrenceevne, som ikt kan bibringe. Kommissionen vurderer, at fuld implementering af den opdaterede ikt-strategi vil øge EU's bruttonationalprodukt med 5 pct. frem mod 2020 (svarende til 1.500 euro pr. borger).

Cyberangrebet på Georgien under den kortvarige væbnede konflikt med Rusland i 2008 samt de omfattende og koordinerede cyberangreb mod Estland i 2007, der satte en række vigtige samfundsfunktioner ud af drift, er eksempler på cyberangreb, der har været med til at sætte cybersikkerhed på den internationale dagsorden. Det er endvidere konstateret, at it-baseret spionage og tyveri af intellektuel ejendom i de senere år har medført et betragteligt værditab i flere lande.

Forsvarets Efterretningstjeneste vurderer, at de alvorligste cybertrusler mod Danmark i øjeblikket kommer fra statslige aktører, der udnytter internettet til at spionere og stjæle dansk intellektuel ejendom, f.eks. patenteret viden, forskningsresultater og forretningshemmeligheder. Truslen kommer navnlig fra stater, som bruger informationerne til at understøtte deres egen økonomiske, militære og samfundsmæssige udvikling. Der er tegn på, at nogle stater bruger private hackere til at udføre cyberangreb på statens vegne. En stat kan på denne måde unddrage sig et juridisk og politisk ansvar, da det ofte er vanskeligt at påvise, at den pågældende stat står bag.

Truslen på cyberområdet kommer også fra såkaldte hacktivister, dvs. hackere, hvis aktivitet ofte er politisk motiveret. Derudover kan hackere have økonomiske motiver. Hackerne kan besidde store tekniske færdigheder og er i stand til at forstyrre eller anrette skade på eksempelvis danske hjemmesider og servere.

Imidlertid er også militante islamister i stigende grad begyndt at vise interesse for at anvende internettet til at udføre cyberangreb, og al-Qaida har i en video opfordret til såkaldt elektronisk jihad mod vestlige lande. De militante islamister anser dog fortsat cyberangreb og hacking for sekundære angrebsmåder i forhold til traditionelle terrorangreb.

Et særligt fokusområde er den såkaldte insider-trussel, som kommer fra ansatte, der ubevidst eller bevidst bryder sikkerheden på deres arbejdsplads og derved medvirker til tyveri af data eller overfører skadelig software. Dette kan ske ved manglende kendskab til eller forståelse for opstillede sikkerhedsbestemmelser eller bevidst for at røbe udvalgte informationer.

Teknologien vil i fremtiden blive endnu mere kompleks. Antallet af maskiner og udstyr, der bliver opkoblet til internettet, stiger kraftigt hvert år, og ansatte i offentlige myndigheder, virksomheder og organisationer vil i stigende omfang kunne få adgang til informationer i myndighedernes, virksomhedernes eller organisationernes netværk fra mobile enheder, ligesom flere informationer vil blive lagret på internettet (cloud storage) og ikke på lokale servere eller computere. Det medfører et ændret risikobillede og vil kræve nye sikkerhedsforanstaltninger.

Danmark er et af de lande i verden, hvor den offentlige sektor er kommet længst med at bruge it og ny teknologi til at forny og udvikle velfærdssamfundet. Imidlertid ønsker regeringen, regioner og kommuner at sætte endnu mere fart på anvendelsen af digitale løsninger til at forny den offentlige sektor og gøre den mere effektiv. Den fællesoffentlige digitaliseringsstrategi skal således bidrage væsentligt til at realisere potentialet og dermed til at sikre en holdbar samfundsøkonomi. Danmarks digitale førerposition skal således danne afsæt for de næste store skridt på den digitale vej til fremtidens velfærd, og i det fortsatte arbejde med at etablere en tidssvarende og robust offentlig digital infrastruktur, der kan håndtere, at stadig flere af velfærdssamfundets kritiske processer foregår digitalt, vil sikkerhed være et af de væsentligste indsatsområder.

På den baggrund ønsker regeringen med dette lovforslag at styrke Center for Cybersikkerheds muligheder for at beskytte Danmark mod fremtidige cyberangreb, der er rettet mod den danske it- og teleinfrastruktur og øvrig ikt-infrastruktur, som samfundsvigtige funktioner er afhængige af, f.eks. inden for energi- og vandforsyning eller kontrolsystemer i industrien.

2.4. Lovforslagets formål

Formålet med dette lovforslag er først og fremmest at etablere et samlet lovgrundlag for Center for Cybersikkerhed.

Som led heri foreslås den regulering af den statslige varslingstjeneste for internettrusler, som i dag sker i GovCERT-loven, videreført og opdateret på en række områder på baggrund af de erfaringer, der er gjort med GovCERT-loven siden lovens ikrafttræden i 2011. Dette sker bl.a. på baggrund af en evaluering af GovCERT-loven, som er gennemført i henhold til GovCERT-lovens § 9. En redegørelse, som er udarbejdet på baggrund af evalueringen, er optrykt som bilag til dette lovforslag.

Særligt på baggrund af den alvorlige udvikling i trusselsbilledet foreslås det med lovforslaget, at Center for Cybersikkerhed får styrket mulighederne for at beskytte Danmark mod cyberangreb. Det vil især ske ved en udvidelse af centerets muligheder for at undersøge sikkerhedshændelser, herunder cyberangreb, i samarbejde med myndigheder og virksomheder, således at der i større omfang end i dag kan indhentes de informationer, som er nødvendige for at afklare, hvilke angrebsværktøjer og -metoder som er anvendt ved sikkerhedshændelser. Dette vil styrke muligheden for at forebygge nye og tilsvarende hændelser. Styrkelsen vil ske med respekt for retssikkerheden og den personlige frihed.

Det følger af § 2, stk. 11, i lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven), at loven ikke gælder for behandlinger, der udføres for politiets og forsvarets efterretningstjenester. Da Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, finder persondataloven således ikke anvendelse på centerets virksomhed. Med lovforslaget foreslås det imidlertid, at en række af de centrale principper i persondataloven også skal finde anvendelse på Center for Cybersikkerheds virksomhed. Datatilsynet vil dog ikke skulle føre tilsyn med Center for Cybersikkerheds overholdelse af lovforslagets bestemmelser om behandling af personoplysninger. Denne tilsynsopgave vil blive varetaget af Tilsynet med Efterretningstjenesterne.

3. Lovforslagets hovedindhold

3.1. Center for Cybersikkerheds netsikkerhedstjeneste

3.1.1. Gældende ret

I dag omfatter Center for Cybersikkerhed to separate CERT'er (Computer Emergency Response Team): GovCERT er den statslige varslingstjeneste for internettrusler, og tjenesten dækker statslige, regionale og kommunale myndigheder samt visse virksomheder, mens MILCERT er varslingstjeneste for internettrusler m.v. på Forsvarsministeriets område.

Begge CERT'er monitorerer løbende aktiviteterne på de tilsluttede myndigheder og virksomheders forbindelser til eksterne netværk, herunder internettet. Indsamlingen af data sker primært ved hjælp af elektroniske alarmenheder, som er opsat hos de enkelte myndigheder og virksomheder, hvor de monitorerer ind- og udgående netværkskommunikation, herunder internetkommunikation.

Denne monitorering giver CERT'erne et normalbillede af netværkskommunikationen og dermed også det overblik, der er nødvendigt for at opdage afvigelser. Cyberangreb og andre sikkerhedshændelser kan således optræde som afvigelser fra normalbilledet og udløse en alarm hos CERT'en, hvorefter alarmen vil blive behandlet. Behandlingen kan omfatte en analyse, hvis resultat danner baggrund for udsendelse af en sikkerhedsvarsling fra Center for Cybersikkerhed, rådgivning om modforholdsregler samt bistand til myndighederne ved omfattende sikkerhedshændelser. På MILCERT's område kan behandlingen tillige resultere i påbud til Forsvarets myndigheder om iværksættelse af særlige forholdsregler m.v.

I andre tilfælde opdages cyberangreb ad anden vej, f.eks. ved at der konstateres uregelmæssigheder hos en angrebet myndighed eller virksomhed. Såfremt analysen heraf kan afgøre, hvordan angrebet eller angrebsforsøget har fundet sted, vil CERT'erne sikre, at alarmenhederne hos de tilsluttede myndigheder og virksomheder opdateres, således at lignende angrebsforsøg straks kan opdages. CERT'ernes monitorering af netværkskommunikation sikrer således, at der løbende sker en styrkelse af cybersikkerheden i Danmark.

Det er først og fremmest statslige myndigheder, som kan tilsluttes GovCERT. Tilslutningen er frivillig. Kommunale og regionale myndigheder samt private virksomheder, som er beskæftiget med kritisk infrastruktur, kan blive tilsluttet GovCERT i det omfang, GovCERT har kapacitet hertil, jf. GovCERT-lovens § 2.

På nuværende tidspunkt er langt de fleste ministerområder tilsluttet GovCERT, hvortil kommer enkelte kommuner, regioner og virksomheder. En række myndigheder på Forsvarsministeriets område er tilsluttet MILCERT.

3.1.2. Forsvarsministeriets overvejelser

Med etableringen af GovCERT og MILCERT er der taget et vigtigt skridt for at øge beskyttelsen mod cyberangreb. De to CERT'er udfører således en vigtig opgave, hvor en række sikkerhedshændelser løbende bliver opdaget, ligesom CERT'erne ved større cyberangreb mod myndigheder og virksomheder har ydet en effektiv assistance til de ramte institutioner.

Det er imidlertid Forsvarsministeriets opfattelse, at såvel den teknologiske udvikling som udviklingen i trusselsbilledet giver behov for en styrkelse af statens CERT-funktion.

Først og fremmest vil der, i overensstemmelse med hensigten bag samlingen af myndighedernes indsats i Center for Cybersikkerhed, 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 en række synergieffekter, ligesom den samlede kapacitet, som kan indsættes ved større cyberangreb, vil blive væsentligt større.

Samtidig er der behov for, at netsikkerhedstjenesten også i højere grad kan inddrage Center for Cybersikkerheds øvrige sikkerhedstekniske eksperter, som f.eks. kan undersøge it-udstyr, der har været ramt af angreb, med henblik på at klarlægge angrebsmetoder og -værktøjer. Center for Cybersikkerheds samlede aktiviteter inden for både opdagelse af sikkerhedshændelser og efterfølgende sikkerhedsteknisk analyse af disse bør derfor samles i én funktion og underlægges samme regulering, således at der som udgangspunkt heller ikke skelnes mellem, om opgaverne er forebyggende eller afhjælpende, eller mellem, om opgaverne udføres på det civile eller militære område.

Den nuværende afgrænsning, hvor kredsen af virksomheder, der kan tilsluttes GovCERT, kun omfatter virksomheder, som er beskæftiget med kritisk infrastruktur, har endvidere vist sig at være uhensigtsmæssig. Afgrænsningen indebærer, at det i dag i vidt omfang 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, eller som på grund af samfundsvigtige forskningsaktiviteter er særligt udsatte for cyberangreb. Det skyldes, at disse funktioner ikke umiddelbart efter GovCERT-loven anses for at være en del af samfundets kritiske infrastruktur. For at opnå et optimalt beskyttelsesniveau er der behov for at sikre, at også virksomheder, der mere generelt varetager samfundsvigtige funktioner, kan tilsluttes en CERT.

I dag sker tilslutning til GovCERT alene på grundlag af faste tilslutningsaftaler. Det er imidlertid Forsvarsministeriets opfattelse, at der er behov for, at myndigheder og virksomheder også på midlertidig basis kan tilsluttes en CERT.

En midlertidig tilslutning kan for det første være hensigtsmæssig i forhold til myndigheder og virksomheder, som ikke normalt er udsat for et sådant trusselsbillede, at en fast tilslutning til en CERT er hensigtsmæssig, men som på grund af aktuelle begivenheder i en kortere periode er udsat for et så konkret trusselsbillede, at der er behov for den ekstra sikkerhed, som en tilslutning indebærer.

En midlertidig tilslutning bør for det andet kunne ske, hvis en virksomhed, der ikke er beskæftiget med samfundsvigtige funktioner, udsættes for et særligt alvorligt cyberangreb, der kan påvirke samfundsvigtige funktioner. Der vil f.eks. kunne være tale om, at det konstateres, at en virksomheds it-system uden virksomhedens vidende indgår i et skadeligt netværk beregnet til cyberangreb, hvorfra der rettes angreb mod offentlige myndigheder, eller hvortil hackere henter følsomme oplysninger fra myndigheder eller virksomheder.

Den midlertidige tilslutning bør dog forudsætte, at der er begrundet mistanke om en sikkerhedshændelse.

I forhold til både tilsluttede og ikke-tilsluttede myndigheder og virksomheder kan Forsvarsministeriet endvidere konstatere et stort behov for, at Center for Cybersikkerhed efter et cyberangreb kan analysere data fra en kompromitteret computer, server eller andet informationssystem, dels for at kunne bistå den ramte myndighed eller virksomhed med at afhjælpe følger af angrebet, dels for at kunne styrke de forebyggende foranstaltninger ved at opdatere CERT'ernes alarmenheder på baggrund af resultatet af en analyse af den konkrete sikkerhedshændelse. Der er derfor behov for, at Center for Cybersikkerhed får hjemmel til at foretage denne type analyse, som bør kunne ske i de tilfælde, hvor myndigheden eller virksomheden giver skriftligt samtykke hertil.

De to CERT'ers nuværende virksomhed er primært baseret på de alarmenheder, der er beskrevet i afsnit 3.1.1, og som ligeledes er detaljeret beskrevet i bemærkningerne til forslaget til GovCERT-loven (lovforslag L 197, 1. samling 2010-11, afsnit 3.3). Den teknologiske udvikling på cybersikkerhedsområdet betyder imidlertid, at der løbende udvikles nye tekniske hjælpemidler, som giver mulighed for en mere effektiv sikring mod cyberangreb, og Forsvarsministeriet finder derfor, at det bør sikres, at Center for Cybersikkerhed ikke er bundet til at anvende en bestemt teknologi, men at de rammer, der fastsættes for CERT-aktiviteterne, er teknologineutrale og således gælder uanset valg af teknologi.

3.1.3. Den foreslåede ordning

Forsvarsministeriet foreslår, at GovCERT's og MILCERT's aktiviteter samt Center for Cybersikkerheds øvrige aktiviteter i tilknytning til CERT-aktiviteterne fremover betegnes "Center for Cybersikkerheds netsikkerhedstjeneste", og at disse aktiviteter som udgangspunkt underlægges samme regulering. Betegnelsen "netsikkerhedstjeneste" er ny og vil erstatte betegnelsen "varslingstjeneste", som anvendes i GovCERT-loven.

Center for Cybersikkerheds netsikkerhedstjeneste vil være betegnelsen for centerets funktion som netsikkerhedstjeneste og dækker altså ikke over en afgrænset organisatorisk enhed i centeret. Funktionen som netsikkerhedstjeneste vil omfatte den samlede kapacitet i forbindelse med monitorering af netværkskommunikation, hvilket primært vil sige den nuværende GovCERT, MILCERT og centerets sikkerhedstekniske kapacitet, samt støttefunktioner, f.eks. af juridisk karakter.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 3.

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

For så vidt angår regioner og kommuner samt virksomheder, der beskæftiger sig med samfundsvigtige funktioner, vil det være Center for Cybersikkerhed, som træffer afgørelse om, hvorvidt en anmodning om tilslutning kan imødekommes. Det vil ske ud fra en vurdering af, om tilslutningen konkret kan bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet. Ved denne vurdering vil der – ud over et hensyn til netsikkerhedstjenestens aktuelle kapacitet – blive lagt vægt på, om den pågældende myndighed eller virksomhed har en it-organisation og it-infrastruktur, der kan sikre en optimal monitorering af netværkskommunikation og indgå i en løbende dialog med netsikkerhedstjenesten, samt på at sikre, at de myndigheder og virksomheder, som er tilsluttet net-

sikkerhedstjenesten, er repræsentative, således at der kan opnås et samlet billede af informationssikkerhedsniveauet i Danmark. Kriterierne er nærmere uddybet i bemærkningerne til den foreslåede § 3.

Den foreslåede udvidelse af kredsen af virksomheder, der kan tilsluttes netsikkerhedstjenesten, vurderes 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, som virksomhederne kan benytte. Samtidig kan netsikkerhedstjenestens ydelser ikke træde i stedet for virksomhedernes øvrige it-sikkerhedsforanstaltninger, men skal alene betragtes som et ekstra lag af sikkerhed.

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

Videre foreslås det, at Center for Cybersikkerhed får udvidet mulighederne for at indsamle erfaringer om sikkerhedshændelser hos myndigheder og virksomheder, når der derved kan opnås en yderligere sikring af den danske ikt-infrastruktur, som samfundsvigtige funktioner er afhængige af. Det foreslås, at netsikkerhedstjenesten for en midlertidig periode på højst to måneder får mulighed for at gennemføre monitorering af netværkskommunikationen hos en myndighed eller virksomhed, der ikke fast er tilsluttet netsikkerhedstjenesten, men som giver skriftligt samtykke til monitoreringen. Det foreslås desuden, at netsikkerhedstjenesten kan behandle data fra informationssystemer såsom computere, servere m.v., der ejes af myndigheder eller virksomheder, når disse aktører giver skriftligt samtykke hertil.

Der henvises til bemærkningerne til de foreslåede §§ 6 og 7 samt afsnit 3.2.

For at sikre, at netsikkerhedstjenesten kan tilpasse sig til den teknologiske udvikling og til enhver tid kan anvende de teknologier, som giver optimale muligheder for at opnå et højt informationssikkerhedsniveau, sikres det endeligt, at reguleringen af netsikkerhedstjenesten ikke baseres på en bestemt teknologisk monitoreringsløsning.

3.2. Indgreb i meddelelseshemmeligheden

3.2.1. Gældende ret

Efter GovCERT-loven skal GovCERT behandle – og herunder efter omstændighederne analysere – tilsluttede myndigheders og private virksomheders ind- og udgående pakke- og trafikdata. Ved trafikdata forstås data, som behandles som led i overførslen af internetbaseret kommunikation, f.eks. e-mail-adresser eller hjemmesideadresser. Ved pakkedata forstås selve indholdet af den internetbaserede kommunikation, f.eks. indholdet af en e-mail eller indholdet af den hjemmeside, som tilgås.

Denne behandling indebærer i begrænset omfang indgreb i meddelelseshemmeligheden i grundlovens forstand, primært ved adgang til indholdet af kommunikation i form af pakkedata. En sådan adgang har alene til formål at klarlægge konkrete sikkerhedshændelsers karakter, og GovCERT's

interesse er rettet mod tekniske oplysninger om sikkerhedshændelserne, f.eks. analyse af en virus i en fil, der er vedhæftet en e-mail. Der vil i vidt omfang foreligge et samtykke, som indebærer, at det ikke er nødvendigt at indhente retskendelse efter grundlovens § 72. Der forekommer imidlertid også tilfælde, hvor et sådant samtykke ikke foreligger, og eftersom de pågældende pakkedatas nærmere karakter normalt først kan fastslås ved en analyse, vil det i praksis ikke være muligt at indhente en retskendelse. Derfor indeholder GovCERT-loven en undtagelse fra grundlovens krav herom.

Denne undtagelse er indført på baggrund af en overvejelse af nødvendigheden og proportionaliteten af ordningen, hvor der blev lagt vægt på, at et overblik over sikkerheden på internettet og muligheden for at varsle om it-angreb nødvendigvis forudsætter, at der er adgang til de pakkedata, som er relaterede til de konkrete sikkerhedshændelser. Kun med adgang til pakkedata kan konsekvenserne af sikkerhedshændelsen klarlægges, herunder hvilke dokumenter, e-mails m.v. der f.eks. er blevet kopieret og videresendt fra den tilsluttede myndighed til en hacker. Skadens omfang kan herefter fastslås, og de relevante modforholdsregler kan besluttes.

Som eksempel på en relevant sikkerhedshændelse nævnes i bemærkningerne til GovCERT-loven (lovforslag L 197, 1. samling 2010-11, afsnit 3.2), at en e-mail med et virusinficeret PDF-dokument omgår både antivirusprogrammer og firewall hos en myndighed og herefter kopierer og sender dokumenter fra den inficerede computer tilbage til hackeren uden myndighedens vidende. Hvis GovCERT ikke har adgang til pakkedata, vil GovCERT ikke kunne analysere og reagere over for denne virus sammen med den berørte myndighed. Uden adgang til pakkedata vil det endvidere ikke være muligt for GovCERT at fastslå konsekvenserne af et vellykket it-angreb for den berørte myndighed. De nødvendige oplysninger til brug for effektiv analyse og håndtering af angreb ligger således i pakkedata, og GovCERT vil ikke kunne håndtere kritiske it-angreb på betryggende vis uden adgang til pakkedata. Det er derfor både nødvendigt og proportionalt, at GovCERT har adgang til pakkedata.

Ordningen blev endvidere vurderet i forholdet til artikel 8 i Den Europæiske Menneskerettighedskonvention, hvorefter enhver har ret til respekt for sit privatliv og familieliv. Beskyttelsen efter artikel 8 omfatter både indgreb i meddelelseshemmeligheden, f.eks. monitorering af e-mailkorrespondance og internetkommunikation, og offentlige myndigheders indsamling, opbevaring og anvendelse m.v. af personoplysninger generelt.

Der blev ved vurderingen lagt vægt på, at den samfundsmæssige interesse i at forhindre og håndtere sikkerhedshændelser af it-mæssig karakter for offentlige myndigheder må anses for at overstige hensynet til privatlivet for de personer, om hvilke GovCERT behandler personoplysninger. Ligeledes blev der lagt vægt på, at aktiviteterne er begrænsede til de tilsluttede myndigheder og virksomheders ind- og udgående data, samt at GovCERT's formål ikke i sig selv er at indsamle personoplysninger. Indsamlingen er i stedet en uundgåelig konsekvens af varslingsopgaven. Personoplysningerne vil derudover heller ikke blive offentliggjort. Tværtimod er opbevaringen af oplysningerne underlagt strenge sikkerhedsforanstaltninger, så bl.a. offentliggørelse undgås.

Konklusionen var på den baggrund, at behandlingen ville opfylde betingelserne i artikel 8, stk. 2, i Den Europæiske Menneskerettighedskonvention.

3.2.2. Forsvarsministeriets overvejelser

Erfaringerne med GovCERT's behandling – herunder indsamling, registrering, analyse og opbevaring – af ind- og udgående pakkedata viser, at ordningen har fungeret efter hensigten på det noget begrænsede anvendelsesområde. Som forventet har det således i en lang række tilfælde vist sig, at netop adgangen til indholdet af internetkommunikation – pakkedata – har været et uundværligt redskab i GovCERT's arbejde med at vurdere it-sikkerheden for statslige myndigheders anvendelse af internettet og varsle myndigheder om internetbaserede sikkerhedshændelser og trusler.

Med den gældende ordning, hvor GovCERT's adgang til pakkedata er begrænset til de situationer, hvor der ikke blot er tale om en vag og udefineret mistanke om en sikkerhedshændelse, men hvor der kræves en klar indikation på en sikkerhedshændelse, er der efter Forsvarsministeriets opfattelse på GovCERT's dækningsområde opnået en hensigtsmæssig balance mellem på den ene side hensynet til at understøtte et højt informationssikkerhedsniveau og på den anden side respekten for retssikkerheden og den personlige frihed.

På den baggrund anser Forsvarsministeriet det for velbegrundet at udbrede den velfungerende GovCERT-ordning til også at omfatte dækningsområdet for MILCERT, der grundlæggende udfører samme opgaver som GovCERT, blot på Forsvarsministeriets område. Dermed vil det kunne sikres, at der også på dette område skabes de bedst mulige forudsætninger for at understøtte et højt informationssikkerhedsniveau. Afvejningerne i forhold til såvel grundlovens § 72 som artikel 8 i Den Europæiske Menneskerettighedskonvention, jf. afsnit 3.2.1, er identiske i forhold til MILCERT og fører til samme konklusion.

Som anført i afsnit 3.1 foreslås det med dette lovforslag, at Center for Cybersikkerheds netsikkerhedstjeneste, der fremover vil omfatte både GovCERT og MILCERT, får mulighed for at udføre monitorering af netværkskommunikation hos myndigheder eller virksomheder, som i en midlertidig periode på højst to måneder tilsluttes netsikkerhedstjenesten. Denne ordning er baseret på samme hensyn, som gør sig gældende i forhold til GovCERT's nuværende opgave som varslingstjeneste, og Forsvarsministeriet anser det for naturligt, at der også ved midlertidige tilslutninger gives mulighed for indgreb i meddelelseshemmeligheden ud fra samme overvejelser om nødvendighed og proportionalitet, som er anført i afsnit 3.2.1.

Endelig er der, som ligeledes beskrevet i afsnit 3.1, konstateret et behov for, at Center for Cybersikkerhed efter et cyberangreb kan analysere data fra en kompromitteret computer, server eller andet informationssystem, dels for at kunne bistå den ramte myndighed eller virksomhed med at afhjælpe følgerne af angrebet, dels for at kunne styrke de forebyggende foranstaltninger ved at opdatere netsikkerhedstjenestens alarmenheder på baggrund af resultatet af en analyse af den konkrete sikkerhedshændelse. En sådan analyse vil – på samme vis som den løbende monitorering – kunne indebære et behov for analyse af data i form af f.eks. vedhæftede filer med virus. Bortset fra, at analysen her vil tage udgangspunkt i data fra eksempelvis en computer i stedet for data fra en internetkommunikation, er der grundlæggende tale om en ordning, der er identisk med GovCERT's nuværende aktiviteter. Forsvarsministeriet anser det derfor for både naturligt og hensigtsmæssigt at udvide adgangen til indgreb i meddelelseshemmeligheden til også at omfatte disse situationer.

3.2.3. Den foreslåede ordning

Forsvarsministeriet foreslår, at den nuværende ordning, hvorefter GovCERT som led i monitoreringen af de tilsluttede myndigheder og virksomheders netværkskommunikation har mulighed for at foretage indgreb i meddelelseshemmeligheden, videreføres samt udvides til at omfatte indgreb i meddelelseshemmeligheden i forbindelse med monitoreringen af myndigheder på Forsvarsministeriets område, midlertidigt tilsluttede myndigheder og virksomheder samt ved undersøgelser af informationsudstyr, som er eller mistænkes for at være ramt af en sikkerhedshændelse.

Med den foreslåede § 4 vil Center for Cybersikkerheds netsikkerhedstjeneste således fortsat have mulighed for uden retskendelse at behandle pakke- og trafikdata fra tilsluttede myndigheder og virksomheder med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet, og med § 5 foreslås en identisk ordning for myndigheder på Forsvarsministeriets område.

Med den foreslåede § 6 vil adgangen til indgreb i meddelelseshemmeligheden blive udvidet til at omfatte myndigheder og virksomheder, der midlertidigt tilsluttes netsikkerhedstjenesten, mens der med § 7 sker en udvidelse til at omfatte situationer, hvor myndigheder eller virksomheder stiller et informationssystem – f.eks. en inficeret computer eller server – til rådighed for netsikkerhedstjenesten med henblik på en analyse af infektionen. Både efter § 6 og § 7 vil en forudsætning for, at der kan ske indgreb i meddelelseshemmeligheden, være, at der er en begrundet mistanke om en sikkerhedshændelse, ligesom det konkret skal vurderes, at behandlingen af data vil kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at sikre den danske ikt-infrastruktur, som samfundsvigtige funktioner er afhængige af.

Det foreslåede kapitel 4 vil alene finde anvendelse, hvis der i forbindelse med monitoreringen af netværkskommunikation er behov for, at netsikkerhedstjenesten tilgår indhold af en kommunikation eller oplysninger om, at en sådan kommunikation har fundet sted. Center for Cybersikkerheds netsikkerhedstjeneste vil altid ud fra et proportionalitetshensyn i videst muligt omfang søge at løse opgaverne ved hjælp af data, som ikke vil kræve et indgreb i meddelelseshemmeligheden, og i disse tilfælde vil behandlingen af personoplysninger ske efter de generelle behandlingsbestemmelser i det foreslåede kapitel 6, jf. afsnit 3.3.

3.3. Forholdet til anden lovgivning samt behandling af personoplysninger i Center for Cybersikkerhed

3.3.1. Gældende ret

Det følger af persondatalovens § 2, stk. 11, at loven ikke gælder for behandlinger, der udføres for politiets og forsvarets efterretningstjenester. Det er dog i FE-loven bestemt, at visse dele af persondataloven finder anvendelse på Forsvarets Efterretningstjenestes behandling af personoplysninger vedrørende i Danmark hjemmehørende fysiske og juridiske personer. Bestemmelserne gælder dog ikke for Center for Cybersikkerhed, jf. FE-lovens § 1, stk. 3, 2. pkt.

Da Center for Cybersikkerhed er oprettet som en del af Forsvarets Efterretningstjeneste, indebærer persondatalovens § 2, stk. 11, dermed, at persondataloven ikke gælder for centeret. I det omfang GovCERT-loven – der blev vedtaget, da GovCERT var en del af IT- og Telestyrelsen – indeholder bestemmelser, der fraviger persondataloven, har disse bestemmelser dermed heller ikke betydning for Center for Cybersikkerhed.

Videregivelse af personoplysninger til Center for Cybersikkerhed er dog omfattet af persondataloven, uanset der i sådanne tilfælde tillige er tale om en behandling (indsamling), som foretages for en efterretningstjeneste. Endvidere vil Datatilsynet også for så vidt angår Center for Cybersikkerhed kunne indhente de fornødne oplysninger til afgørelse af, om et forhold falder ind under persondataloven, jf. lovens § 62, stk. 1. Dette vil i praksis ske gennem Forsvarsministeriet.

Forsvarets Efterretningstjenestes virksomhed, herunder bl.a. Forsvarets Efterretningstjenestes behandling af personoplysninger vedrørende i Danmark hjemmehørende fysiske personer, er reguleret i FE-loven. Center for Cybersikkerheds virksomhed er imidlertid som nævnt ikke omfattet af FE-lovens materielle bestemmelser, herunder lovens bestemmelser om behandling af personoplysninger, jf. lovens § 1, stk. 3, 2. pkt.

Som en konsekvens af, at persondataloven ikke gælder for Center for Cybersikkerhed, har Forsvarsministeriet den 13. maj 2013 udstedt retningslinjer for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste. I retningslinjerne konstateres det, at uanset at formålet med Center for Cybersikkerheds virksomhed ikke er behandling af personoplysninger, kan det ikke undgås, at personoplysninger bliver behandlet i et vist – om end begrænset – omfang i forbindelse med udførelsen af Center for Cybersikkerheds opgaver. I lyset heraf skal chefen for Forsvarets Efterretningstjeneste sikre, at medarbejderne, der virker inden for Center for Cybersikkerhed, følger de udstedte retningslinjer for behandling af personoplysninger m.v. og de dertilhørende bestemmelser om kontrol.

Med retningslinjerne er der fastsat en række bestemmelser om behandlingsgrundlag og behandlingssikkerhed ved behandling af personoplysninger i Center for Cybersikkerhed. Bestemmelserne bygger på principperne i persondataloven.

Efter § 11 i FE-loven er Forsvarets Efterretningstjenestes virksomhed undtaget fra lov om offentlighed i forvaltningen (offentlighedsloven) bortset fra lovens § 13 om notatpligt. Forsvarets Efterretningstjenestes virksomhed er endvidere undtaget fra forvaltningslovens kapitel 4-6 om partens aktindsigt, partshøring og begrundelse m.v. Imidlertid kan forsvarsministeren bestemme, at persondatalovens kapitel 8-10 og forvaltningslovens kapitel 4-6 helt eller delvis finder anvendelse for behandling af personoplysninger for Forsvarets Efterretningstjeneste vedrørende tjenestens sikkerhedsgodkendelsessager og egne personalesager. Center for Cybersikkerhed er som tidligere nævnt ikke omfattet af disse bestemmelser i FE-loven.

3.3.2. Forsvarsministeriets overvejelser

Forsvarsministeriet finder, at de centrale principper i persondataloven så vidt muligt bør gælde for Center for Cybersikkerhed. De særlige forhold, som gør sig gældende for centerets aktiviteter, tilsiger imidlertid, at centeret ikke i samme omfang som andre offentlige myndigheder bør være omfattet af den almindelige persondataretlige lovgivning. Center for Cybersikkerhed har som nævnt heller ikke hidtil været omfattet af den almindelige persondataretlige lovgivning.

Med lovforslaget lægges der op til, at bestemmelserne om behandlingsgrundlag og behandlingssikkerhed ved behandling af personoplysninger i Forsvarsministeriets retningslinjer af 13. maj 2013 videreføres ved lov, således at principperne i persondatalovens regler om behandling af personoplysninger i vidt omfang finder anvendelse på Center for Cybersikkerhed.

Som hidtil vil principperne i reglerne om oplysningspligt over for den registrerede og om den registreredes indsigts- og indsigelsesret ikke finde anvendelse på centerets virksomhed. Formålet med Center for Cybersikkerheds netsikkerhedstjeneste er ikke at behandle personoplysninger, men netsikkerhedstjenesten vil uundgåeligt skulle behandle personoplysninger indeholdt i pakke- og trafikdata i forbindelse med sine aktiviteter. Indsamlingen af personoplysninger er således en nødvendig del af netsikkerhedstjenestens virke, og det er Forsvarsministeriets vurdering, at opfyldelse af en oplysningspligt over for den registrerede vil være uforholdsmæssig vanskelig, ligesom behovet for at kunne begære indsigt eller gøre indsigelse er mindre fremtrædende end de administrative byrder, det vil påføre netsikkerhedstjenesten.

Forsvarsministeriet har overvejet, om der i forhold til øvrige dele af Center for Cybersikkerheds virksomhed – som national it-sikkerhedsmyndighed og som myndighed for informationssikkerhed og beredskab på teleområdet – er behov for at fravige gældende ret ved at indføre oplysningspligt over for den registrerede samt give den registrerede indsigts- og indsigelsesret. Det karakteristiske for disse myndighedsområder er, at Center for Cybersikkerheds myndighedsudøvelse som altovervejende hovedregel er rettet mod andre myndigheder og virksomheder. Det er derfor Forsvarsministeriets opfattelse, at der ikke på nuværende tidspunkt er behov for at indføre en oplysningspligt i forhold til fysiske personer. Samtidig finder Forsvarsministeriet dog, at der bør være mulighed for at lade persondatalovens kapitel 8-10 (om oplysningspligt over for den registrerede, den registreredes indsigtsret og øvrige rettigheder, bl.a. indsigelsesret) finde anvendelse på de pågældende myndighedsområder samt på Center for Cybersikkerheds behandling af egne personalesager, såfremt der på et senere tidspunkt måtte vise sig et behov herfor.

Som følge af Center for Cybersikkerheds særlige adgang til at behandle data, herunder personoplysninger, på baggrund af indgreb i meddelelseshemmeligheden finder Forsvarsministeriet, at der fortsat bør gælde skærpede regler for analyse, videregivelse og sletning af disse data samt for sikkerhedsforanstaltninger i forbindelse med opbevaringen af og adgangen til data. På disse særlige områder bør der efter Forsvarsministeriets opfattelse fortsat gælde regler, der fastsætter mere vidtgående krav end efter persondataloven, f.eks. med hensyn til sletningsfrister.

Forsvarsministeriet lægger vægt på, at de forskellige dele af Forsvarets Efterretningstjeneste så vidt muligt er underlagt samme regulering på centrale forvaltningsretlige områder. I forhold til offentlighedsloven og forvaltningsloven finder Forsvarsministeriet derfor, at der som udgangspunkt bør gælde samme regler for Center for Cybersikkerhed som for den øvrige del af Forsvarets Efterretningstjeneste, hvilket vil indebære, at offentlighedsloven ikke finder anvendelse på Center for Cybersikkerhed.

Dette skal endvidere ses i lyset af, at netsikkerhedstjenesten i overensstemmelse med sit formål behandler store mængder data, hvor behandlingens fokus som altovervejende hovedregel er på oplysninger af rent teknisk karakter. Kun i sjældne tilfælde vil netsikkerhedstjenesten således have behov for at anvende oplysninger om fysiske og juridiske personer m.v., som er indeholdt i de behandlede data, og sagsbehandling af anmodninger om aktindsigt i sådanne oplysninger vil være særdeles ressourcekrævende, da det vil forudsætte en gennemgang af store mængder data.

Tilsvarende hensyn gør sig gældende i forhold til forvaltningslovens kapitler om partens aktindsigt, partshøring og begrundelse m.v. Hertil kommer, at Center for Cybersikkerhed kun i meget begrænset omfang træffer afgørelse i sager, der involverer fysiske eller juridiske personer, hvorved der ikke

er væsentlige hensyn, som taler imod, at Center for Cybersikkerhed på samme vis som den øvrige del af Forsvarets Efterretningstjeneste undtages fra forvaltningslovens kapitel 4-6.

Imidlertid finder Forsvarsministeriet, at særlige forhold gør sig gældende for Center for Cybersikkerheds virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet og ved centerets behandling af anmodninger om tilslutning til netsikkerhedstjenesten, jf. den foreslåede § 3, stk. 3. Det samme er tilfældet i forhold til centerets behandling af egne personalesager. På disse områder er der hensyn, der taler for, at der bør være mulighed for at anvende offentlighedsloven og forvaltningsloven.

3.3.3. Den foreslåede ordning

Forsvarsministeriet foreslår, at en række centrale principper i persondataloven skal gælde for behandling af personoplysninger i Center for Cybersikkerhed.

I lovforslaget bliver det således slået fast, 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.

Der henvises til bemærkningerne til de foreslåede §§ 9, 13 og 14.

Herudover foreslår Forsvarsministeriet, at persondatalovens principper for, hvornår der må ske behandling af personoplysninger, i vidt omfang skal gælde for Center for Cybersikkerhed.

I lighed med persondataloven inddeler lovforslaget personoplysningerne i tre niveauer eller typer: For det første følsomme oplysninger om menneskers rent private forhold, der kan dreje sig om oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold. For det andet andre typer af oplysninger om rent private forhold, der også anses for at være følsomme, hvilket drejer sig om oplysninger om strafbare forhold, væsentlige sociale problemer og lignende følsomme privatlivsoplysninger, f.eks. om interne familieforhold. Og for det tredje de oplysningstyper, der ikke vedrører rent private forhold - de såkaldte almindelige personoplysninger. Almindelige personoplysninger kan f.eks. være identifikationsoplysninger, oplysninger om økonomiske forhold, kundeforhold eller andre lignende ikke følsomme oplysninger. For hvert af de tre niveauer fastsættes i lovforslaget regler for, hvornår der kan ske behandling af personoplysninger.

Der henvises til bemærkningerne til de foreslåede §§ 10-12.

Herudover foreslås det, at der fastsættes særlige regler om analyse, videregivelse og sletning af data, der behandles på baggrund af indgreb i meddelelseshemmeligheden. Disse regler er nærmere beskrevet i afsnit 3.4 og 3.5 samt i bemærkningerne til de foreslåede §§ 8 og 15-17.

Center for Cybersikkerheds behandling af personoplysninger foreslås at være underlagt tilsyn af Tilsynet med Efterretningstjenesterne. Tilsynets virksomhed er nærmere beskrevet i afsnit 3.6 og i bemærkningerne til de foreslåede §§ 19-24.

Endelig foreslår Forsvarsministeriet, at Center for Cybersikkerhed – som det er tilfældet for den øvrige del af Forsvarets Efterretningstjeneste – undtages fra offentlighedsloven, dog ikke lovens § 13 om notatpligt, samt undtages fra forvaltningslovens kapitel 4-6.

Særlige forhold gør sig gældende for Center for Cybersikkerhed virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet, ved centerets behandling af anmodninger om tilslutning til netsikkerhedstjenesten, jf. den foreslåede § 3, stk. 3, samt ved centerets behandling af egne personalesager. Forsvarsministeriet foreslår på den baggrund, at forsvarsministeren bemyndiges til at bestemme, at offentlighedsloven, forvaltningslovens kapitel 4-6 og persondatalovens kapitel 8-10 helt eller delvis finder anvendelse for disse områder.

Endvidere forudsættes det, at Center for Cybersikkerhed i størst muligt omfang efterlever 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 størst muligt omfang behandles efter principperne i offentlighedsloven. Ved modtagelse af anmodninger om aktindsigt – herunder egenacces efter offentlighedslovens § 8 – 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 ikke foretage en søgning i de store mængder data, som centerets netsikkerhedstjeneste til enhver tid opbevarer, eller i dokumenter, der vedrører øvrige dele af Forsvarets Efterretningstjeneste.

Der henvises til bemærkningerne til den foreslåede § 8.

3.4. Opbevaring og sletning af data

3.4.1. Gældende ret

Der er i GovCERT-lovens § 4, stk. 2-4, fastsat detaljerede regler om, hvor længe GovCERT må opbevare de pakke- og trafikdata, der behandles på grundlag af indgreb i meddelelseshemmeligheden.

Udgangspunktet efter § 4, stk. 2, er, at pakke- og trafikdata skal slettes, når formålet med behandlingen er opfyldt. I § 4, stk. 3, er der imidlertid fastsat maksimale opbevaringsperioder, som finder anvendelse, uanset om GovCERT's formål med behandlingen endnu ikke er opfyldt. Hvis der er tale om en sikkerhedshændelse, kan pakke- og trafikdata, der knytter sig til denne sikkerhedshændelse, højst opbevares i tre år. For øvrige pakkedata, der ikke er knyttet til en sikkerhedshændelse, er den maksimale opbevaringsperiode 14 dage, hvorefter data skal slettes. Trafikdata, der ikke er knyttet til en sikkerhedshændelse, kan højst opbevares i 12 måneder.

Der er ikke ved lov fastsat regler for MILCERT's opbevaring og sletning af pakke- og trafikdata.

3.4.2. Forsvarsministeriets overvejelser

Forsvarsministeriet finder, at der bør fastsættes ensartede opbevarings- og sletningsregler for Center for Cybersikkerheds netsikkerhedstjeneste, der fremover vil omfatte både GovCERT's og MIL-CERT's nuværende aktiviteter. De fælles regler bør sikre, at netsikkerhedstjenestens adgang til at opbevare pakkedata fortsat begrænses mest muligt af hensyn til privatlivets fred.

På den baggrund bør det fastholdes, at data, der knytter sig til en sikkerhedshændelse, højst kan opbevares i tre år.

I forhold til data, der ikke knytter sig til en sikkerhedshændelse, har Forsvarsministeriet imidlertid konstateret et behov for en forlængelse af den hidtidige opbevaringsperiode. Center for Cybersikkerheds erfaringer med den praktiske anvendelse af de gældende sletningsregler viser således, at reglerne i en række tilfælde har medført, at netsikkerhedstjenesten ikke har haft optimale muligheder for at forhindre cyberangreb. På den baggrund vurderes det, at adgang til yderligere historiske data 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 back-up-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 give netsikkerhedstjenesten langt bedre muligheder for at spore cyberangreb, som ikke tidligere er blevet opdaget af de ramte myndigheder eller virksomheder. Det vil især være tilfældet, når det konstateres, at en konkret myndighed eller virksomhed er blevet ramt af et cyberangreb. Her vil Center for Cybersikkerhed på baggrund af en nærmere undersøgelse af angrebet 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.

Jo længere perioden, hvor der er adgang til at søge efter karakteristika, er, jo større er muligheden for at opdage hidtil uopdagede cyberangreb.

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.

Forsvarsministeriet finder desuden, at opbevarings- og sletningsreglerne bør tage højde for, at der gælder særlige hensyn, når netsikkerhedstjenesten i overensstemmelse med lovforslagets videregivelsesregler har videregivet data til politiet, andre myndigheder, samarbejdspartnere 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 i sagens natur 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. Forsvarsministeriet finder derfor, at der ikke bør gælde slettefrister i de tilfælde, hvor der er sket videregivelse af data.

Det bemærkes, 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 nødvendigt af hensyn til de formål, hvortil personoplysningerne behandles. For europæiske myndigheder og virksomheder, der modtager sikkerhedsvarslinger, som indeholder personoplysninger, vil der gælde tilsvarende nationale regler.

3.4.3. Den foreslåede ordning

Forsvarsministeriet foreslår, at data, der er knyttet til en sikkerhedshændelse, fortsat højst må opbevares i tre år, hvorefter de skal slettes. Det er samme tidsmæssige grænse, som er fastsat i GovCERT-lovens § 4, stk. 3.

For så vidt angår øvrige data, der ikke er knyttet til en sikkerhedshændelse, foreslås det, at der fastsættes en fælles opbevaringsperiode på højst 13 måneder, som giver mulighed for at undersøge, om myndigheder og virksomheder har været udsat for hidtil uopdagede cyberangreb samt foretage år-til-år-sammenligninger af normalbilledet hos de tilsluttede myndigheder og virksomheder.

Som efter gældende ret vil der være tale om maksimale opbevaringsperioder. Center for Cybersikkerheds netsikkerhedstjeneste vil således fortsat være forpligtet til at slette data, når formålet med behandlingen er opfyldt, hvis dette sker før den maksimale opbevaringsperiodes udløb. Samtidig vil det generelle princip i den foreslåede § 14 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.

Endvidere foreslår Forsvarsministeriet, at reglerne om sletning ikke skal gælde i forhold til de helt særlige situationer, hvor data er videregivet, jf. afsnit 3.5 og den foreslåede § 16.

Der henvises til bemærkningerne til den foreslåede § 17.

3.5. Videregivelse af data

3.5.1. Gældende ret

GovCERT's muligheder for at videregive pakke- og trafikdata er reguleret i GovCERT-lovens § 6. Efter bestemmelsens nr. 1 kan både pakke- og trafikdata, der knytter sig til en sikkerhedshændelse, videregives til politiet. Efter § 6, nr. 3, kan trafikdata videregives til danske myndigheder, tilsluttede private virksomheder og tilsvarende varslingstjenester i andre lande, hvis en sådan videregivelse er nødvendig i henhold til varslingstjenestens formål og aktiviteter.

Efter GovCERT-lovens § 6, nr. 2, er der en særlig udvidet adgang til at videregive pakkedata til MILCERT, som på tidspunktet for GovCERT-lovens vedtagelse var en del af Forsvarets Efterretningstjeneste, mens GovCERT var en del af IT- og Telestyrelsen.

3.5.2. Forsvarsministeriets overvejelser

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

Center for Cybersikkerheds netsikkerhedstjeneste bør fortsat have adgang til at videregive trafikdata til den kreds af aktører, som er angivet i GovCERT-lovens § 6, nr. 3: Danske myndigheder, tilsluttede private virksomheder og tilsvarende varslingstjenester i andre lande.

For at styrke beskyttelsen af den danske ikt-infrastruktur finder Forsvarsministeriet imidlertid, at der også bør 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 forbedre deres sikkerhedssystemer 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 Cybersikkerhed har endvidere 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.

En af Center for Cybersikkerheds vigtigste forebyggende aktiviteter er udsendelse af sikkerhedsvarslinger, hvor myndigheder, virksomheder, andre netsikkerhedstjenester m.v. underrettes om særligt alvorlige sikkerhedshændelser. Sikkerhedsvarslingerne udsendes til en afgrænset kreds af aktører og bliver ikke i øvrigt offentliggjort. Sikkerhedsvarslingerne giver modtagerne mulighed for at styrke deres egen forebyggelse mod cyberangreb (f.eks. ved at blokere for trafik fra IP-adresser, der

indgår i hackeres angrebsinfrastruktur) og undersøge, om de selv har været udsat for cyberangreb (f.eks. ved at gennemgå logfiler for e-mails fra afsendere, der har angrebet andre myndigheder eller virksomheder). Center for Cybersikkerhed bør derfor have mulighed for at udsende sikkerhedsvarslinger, der indeholder de trafikdata, som kan styrke modtagernes informationssikkerhedsniveau, f.eks. de nævnte IP-adresser. Sikkerhedsvarslingerne bør fortsat aldrig kunne indeholde pakkedata.

3.5.3. Den foreslåede ordning

Forsvarsministeriet foreslår, at politiet ved begrundet mistanke om en sikkerhedshændelse fortsat vil kunne modtage data fra Center for Cybersikkerhed. Der vil som efter den gældende ordning være tale om både pakke- og trafikdata, hvortil kommer data, der er indeholdt i eller hidrører fra et informationssystem, jf. den foreslåede § 7.

Kredsen af aktører, hvortil der kan videregives trafikdata, foreslås udvidet til også at omfatte udbydere af offentlige elektroniske kommunikationsnet og -tjenester (teleselskaber) samt andre netsikkerhedstjenester. Desuden foreslås det, at Center for Cybersikkerhed får hjemmel til at udsende sikkerhedsvarslinger, der indeholder trafikdata.

Der henvises til bemærkningerne til den foreslåede § 16.

For så vidt angår den interne udveksling af data i Forsvarets Efterretningstjeneste bemærkes det, at GovCERT-lovens bestemmelser om videregivelse af data i dag også regulerer forhold, der som følge af oprettelsen af Center for Cybersikkerhed (og placeringen af centeret ved Forsvarets Efterretningstjeneste) har intern karakter. Det gælder f.eks. spørgsmålet om videregivelse af data fra GovCERT til MILCERT, der nu begge er en del af Center for Cybersikkerhed. En sådan intern udveksling af data har efter oprettelsen af Center for Cybersikkerhed ikke længere karakter af videregivelse, og 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 cyberangrebene mod Danmark, som hidrører fra udlandet, og hvor Forsvarets Efterretningstjeneste som udenrigsefterretningstjeneste kan bidrage med en række værdifulde oplysninger.

Forsvarsministeriet vil imidlertid i forbindelse med lov om Center for Cybersikkerheds ikrafttræden udstede administrative retningslinjer, der sikrer, 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. Center for Cybersikkerhed behandler data på baggrund af indgreb i meddelelseshemmeligheden, og retningslinjerne vil blandt andet 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.

Såvel Center for Cybersikkerheds videregivelse af personoplysninger som den interne udveksling af oplysninger vil være underlagt tilsyn af Tilsynet med Efterretningstjenesterne, jf. afsnit 3.6 nedenfor.

3.6. Tilsyn med behandling af personoplysninger

3.6.1. Gældende ret

Det følger af GovCERT-lovens § 7, at der skal nedsættes et uafhængigt tilsyn, der følger GovCERT's virksomhed.

Tilsynet, der nedsættes af forsvarsministeren, skal bestå af en formand, der er jurist, og fire sagkyndige medlemmer. Det er en forudsætning, at tilsynets medlemmer kan sikkerhedsgodkendes. Medlemmerne beskikkes som følge af den almindelige tillid og agtelse, der er knyttet til deres person, og der lægges vægt på, at tilsynet repræsenterer juridisk, it-revisionsmæssig og sikkerhedsmæssig sagkundskab. GovCERT-tilsynets virke er nærmere beskrevet i Forsvarsministeriets forretningsorden af 13. maj 2013 for Tilsynet med den statslige varslingstjeneste for internettrusler mv. (GovCERT).

GovCERT-tilsynet fører alene tilsyn med GovCERT's virksomhed og ikke med Center for Cybersikkerheds virksomhed generelt.

3.6.2. Forsvarsministeriets overvejelser

Der er mellem Center for Cybersikkerhed og det nuværende GovCERT-tilsyn etableret et velfungerende og konstruktivt samarbejde.

Som led i etableringen af et nyt retsgrundlag for Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste er der imidlertid fra 1. januar 2014 oprettet et uafhængigt tilsyn med de to efterretningstjenester. Tilsynet, der benævnes Tilsynet med Efterretningstjenesterne, har i forhold til Forsvarets Efterretningstjeneste til opgave at føre tilsyn med tjenestens overholdelse af FE-lovens regler vedrørende behandling af personoplysninger om i Danmark hjemmehørende fysiske og juridiske personer. Tilsynet 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 Forsvarets Efterretningstjenestes behandling af personoplysninger.

Der er betydelige 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 vil der reelt være tale om, at to tilsynsorganer udfører en emnemæssigt identisk opgave.

Det er på den baggrund Forsvarsministeriets opfattelse, at Center for Cybersikkerheds placering som en del af Forsvarets Efterretningstjeneste klart taler for, at Tilsynet med Efterretningstjenesterne også bør varetage tilsynsopgaven i forhold til Center for Cybersikkerhed.

3.6.3. Den foreslåede ordning

Forsvarsministeriet foreslår, at Tilsynet med Efterretningstjenesterne varetager opgaven med at føre tilsyn med Center for Cybersikkerheds overholdelse af lovforslagets regler om behandling af personoplysninger.

Tilsynsfunktionen foreslås tilrettelagt efter samme model, som gælder i forhold til Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste, herunder at tilsynet også i forhold til Center for Cybersikkerhed vil være fuldt uafhængigt og agere efter klage eller af egen drift. Ligeledes vil tilsynet kunne afgive udtalelse over for Center for Cybersikkerhed, og tilsynet vil skulle underrette forsvarsministeren om forhold, som ministeren efter tilsynets opfattelse bør have kendskab til.

På visse områder vil Tilsynet med Efterretningstjenesternes tilsynsvirksomhed i forhold til Center for Cybersikkerhed dog adskille sig fra tilsynsvirksomheden i forhold til Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste.

En vigtig opgave for Tilsynet med Efterretningstjenesterne i forhold til de to efterretningstjenester er således at varetage en særlig indsigtsordning, hvor fysiske eller juridiske personer kan anmode tilsynet om at undersøge, hvorvidt en efterretningstjeneste uberettiget behandler oplysninger om den pågældende. Tilsynet sikrer i så fald, at dette ikke er tilfældet, og giver herefter den pågældende meddelelse herom. Hvis særlige forhold taler herfor, kan Tilsynet med Efterretningstjenesterne endvidere pålægge en efterretningstjeneste at give hel eller delvis indsigt i oplysninger.

I modsætning til efterretningstjenesterne har Center for Cybersikkerhed ikke til formål at behandle personoplysninger, og personoplysninger vil som den altovervejende hovedregel være uden interesse for centeret, der via netsikkerhedstjenesten primært søger at indsamle tekniske oplysninger, som gør det muligt at undersøge og forebygge cyberangreb. Som led i denne indsamling vil Center for Cybersikkerhed dog uundgåeligt behandle personoplysninger, fordi personoplysningerne er indeholdt i de data, som indsamles med henblik på at lokalisere de relevante tekniske oplysninger om sikkerhedshændelser. Center for Cybersikkerhed foretager imidlertid ikke en egentlig registrering af disse personoplysninger, ligesom der ikke opereres med sager om enkeltpersoner.

Den tilsynsvirksomhed, som Tilsynet med Efterretningstjenesterne vil skulle udøve i forhold til Center for Cybersikkerhed, vil derfor have en karakter, der på visse områder kan sammenlignes med det tilsyn, som Datatilsynet udøver i forhold til andre offentlige myndigheder, idet tilsynet vil skulle påse, at Center for Cybersikkerhed efterlever bestemmelserne i det foreslåede kapitel 4 (om indgreb i meddelelseshemmeligheden), kapitel 6 (om behandling af personoplysninger) og kapitel 7 (om analyse, videregivelse og sletning af data). Endvidere vil tilsynet skulle påse, at Center for Cybersikkerhed i forbindelse med centerets behandling af personoplysninger overholder de krav til sikkerhedsforanstaltninger, der følger af kapitel 8. Endelig vil tilsynet have til opgave at påse, at yderligere regler om behandling af personoplysninger, der fastsættes i administrative retningslinjer, overholdes.

Tilsynet vil f.eks. kunne udøves gennem kontrol af centerets interne procedurer i forbindelse med videregivelse og sletning af oplysninger samt stikprøvekontrol af, om sletning sker rettidigt. Hertil kommer, at tilsynet på baggrund af klager fra fysiske personer vil kunne undersøge, om Center for

Cybersikkerhed i konkrete sager har handlet i overensstemmelse med bestemmelserne om videregivelse og sletning af oplysninger.

I forhold til Forsvarets Efterretningstjeneste indebærer FE-lovens særlige indsigtsordning, at tilsynet i konkrete sager efter anmodning skal sikre, at efterretningstjenesten ikke uberettiget behandler oplysninger om en i Danmark hjemmehørende fysisk eller juridisk person. Derefter skal tilsynet give den pågældende meddelelse herom. Af meddelelsen skal det imidlertid alene kunne udledes, at der ikke uberettiget behandles oplysninger om den pågældende. Det skal ikke fremgå eller kunne udledes, om der ikke behandles eller har været behandlet oplysninger, om der tidligere uberettiget har været behandlet oplysninger, eller om der berettiget behandles oplysninger. Et tilsvarende hensyn gør sig ikke gældende i forhold til tilsynets behandling af klagesager vedrørende Center for Cybersikkerhed, hvor der således i tilsynets afgørelser efter omstændighederne f.eks. vil kunne gives oplysninger om, at centeret har behandlet oplysninger om klageren.

Der henvises til bemærkningerne til de foreslåede §§ 19-24.

Forsvarsministeriet vil drøfte med det nuværende GovCERT tilsyn, under hvilken form det eventuelt vil kunne videreføres som et rådgivende organ, der ikke varetager tilsynsopgaver, men sikrer en velfungerende dialog og erfaringsudveksling mellem centeret og forsknings- og erhvervslivet.

4. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget indebærer en styrkelse af Center for Cybersikkerheds netsikkerhedstjeneste. Endvidere vil Tilsynet med Efterretningstjenesternes virksomhed skulle udvides til også at omfatte Center for Cybersikkerhed.

Hvert ministerområde vil som hidtil blive tilbudt vederlagsfri monitorering af én forbindelse til internettet. Såfremt der på et ministerområde er ønske om monitorering af yderligere forbindelser til internettet, vil myndigheden efter anmodning kunne få monitoreret mere end én forbindelse, hvis der sker dækning af Center for Cybersikkerheds udgifter til indkøb og/eller udvikling af evt. monitoreringsudstyr og udgifter til driften heraf. Fællesstatslige internetforbindelser, der leveres gennem Statens It eller tilsvarende fælles driftsselskaber, monitoreres som hidtil vederlagsfrit af Center for Cybersikkerhed som følge af de særlige sikkerhedsmæssige hensyn, der knytter sig til en centraliseret tjeneste. På Forsvarsministeriets område vil der ske vederlagsfri monitorering af de myndigheder, som af den militære it-sikkerhedsmyndighed pålægges at blive tilsluttet netsikkerhedstjenesten.

Regionale og kommunale myndigheder samt offentligt ejede virksomheder, der ønsker at blive tilsluttet netsikkerhedstjenesten, vil som hidtil skulle dække de udgifter, der er forbundet med indkøb og/eller udvikling af evt. monitoreringsudstyr, samt dække Center for Cybersikkerheds udgifter til driften heraf.

Myndigheder og offentligt ejede virksomheder, der er tilsluttet netsikkerhedstjenesten, vil løbende modtage varslinger og alarmer fra netsikkerhedstjenesten. Det forudsættes i den forbindelse, at de tilsluttede myndigheder efter behov indgår i en nærmere dialog om varslinger og alarmer, herunder stiller relevante logoplysninger til rådighed for netsikkerhedstjenesten samt foretager den relevante interne opfølgning. Tilslutning til netsikkerhedstjenesten kan dermed i mindre omfang have administrative konsekvenser for tilsluttede myndigheder og offentligt ejede virksomheder.

5. Økonomiske og administrative konsekvenser for erhvervslivet m.v.

Virksomheder, der er beskæftiget med samfundsvigtige funktioner, vil efter en konkret vurdering kunne blive tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste, jf. afsnit 3.1. Der vil ved tilslutning blive opkrævet en betaling, der dækker de udgifter, som er forbundet med indkøb og/eller udvikling af evt. monitoreringsudstyr, samt Center for Cybersikkerheds udgifter ved monitoreringen. De første to måneders tilslutning betragtes dog som en indkøringsperiode, hvor der ikke sker opkrævning.

Virksomheder, der er tilsluttet netsikkerhedstjenesten, vil løbende modtage varslinger og alarmer fra netsikkerhedstjenesten. Det forudsættes i den forbindelse, at de tilsluttede virksomheder efter behov indgår i en nærmere dialog om varslinger og alarmer, herunder stiller relevante logoplysninger til rådighed for netsikkerhedstjenesten samt foretager den relevante interne opfølgning. Tilslutning til netsikkerhedstjenesten kan dermed i mindre omfang have administrative konsekvenser for tilsluttede virksomheder.

6. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

8. Forholdet til EU-retten

Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, og de opgaver, som centeret i medfør af dette lovforslag skal udføre, vedrører den offentlige sikkerhed, forsvaret og statens sikkerhed.

Den samlede karakter af de opgaver, som Center for Cybersikkerhed i dag løser, medfører således, at centeret ikke er omfattet af Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesdirektivet), jf. direktivets artikel 3, stk. 2, hvorefter direktivet bl.a. ikke gælder for behandling af oplysninger vedrørende den offentlige sikkerhed, forsvar og statens sikkerhed.

9. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslaget har været sendt i høring hos:

Advokatrådet, Amnesty International, Brancheorganisation for Den Danske Vejgodstransport (ITD), Danmarks Rederiforening, Dansk Energi, Dansk Erhverv, Dansk Internet Forum (DIFO), DANSK IT, Danske Advokater, Danske Regioner, Datatilsynet, Dansk Industri (DI), Den Danske Dommerforening, DI ITEK, DKCERT, Domstolsstyrelsen, Finansrådet, Foreningen Danske Oliberedskabslagre, Foreningen af Open Source Leverandører, Foreningen af Vandværker i Danmark, Færøernes Landsstyre, Grønlands Selvstyre, Institut for Menneskerettigheder, ISP Sikkerhedsfo-

rum, 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, Rigspolitichefen, Rigsadvokaten, Rigsrevisionen, Rådet for Digital Sikkerhed, Statens IT-projektråd, Telekommunikationsindustrien (TI) og The Open Web Application Security Project (OWASP Danmark).

10. Sammenfattende skema

	Positive konsekvenser/ mindreudgifter	Negative konsekvenser/ merudgifter
Økonomiske konsekvenser for stat, regioner og kommuner	Ingen.	Udgifter til omkostningsdækning ved den frivillige tilslutning til netsikkerhedstjenesten for regioner, kommuner og statslige virksomheder samt for ministerområder, der ønsker monitorering af flere internetforbindelser.
Administrative konsekvenser for stat, regioner og kommuner	Ingen.	Behandling af de varslinger og alarmer, som tilsluttede myndigheder modtager fra netsikkerhedstjenesten, vil i et mindre omfang medføre administrativt ressourceforbrug hos myndighederne.
Økonomiske konsekvenser for erhvervslivet m.v.	Ingen.	Udgifter til omkostningsdækning ved frivillig tilslutning til netsikkerhedstjenesten.
Administrative konsekvenser for erhvervslivet m.v.	Ingen.	Behandling af de varslinger og alarmer, som tilsluttede virksomheder modtager fra netsikkerhedstjenesten, vil i et mindre omfang medføre administrativt ressourceforbrug hos virksomhederne.
Administrative konsekvenser for borgerne	Ingen.	Ingen.
Miljømæssige konsekvenser	Ingen.	Ingen.
Forholdet til EU-retten	Lovforslaget indeholder ikke EU-retlige aspekter af betydning.	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Bestemmelsens *stk. 1* giver en beskrivelse af Center for Cybersikkerheds hovedopgave, som er at bidrage til et højt sikkerhedsniveau i informations- og kommunikationsteknologisk infrastruktur (ikt-infrastruktur) og dermed understøtte et højt informationssikkerhedsniveau i Danmark. En robust ikt-infrastruktur er vigtig for Danmarks sikkerhed og økonomi, og en lang række af de vigtigste samfundsfunktioner er afhængige af, at ikt-infrastrukturen er velfungerende.

Center for Cybersikkerhed er tillagt en række konkrete opgaver, som hver især bidrager til løsningen af centerets hovedopgave.

Center for Cybersikkerheds netsikkerhedstjeneste, jf. den foreslåede § 3, har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser på såvel det civile som det militære område. Som national it-sikkerhedsmyndighed varetager centeret desuden en række opgaver af forebyggende og afhjælpende karakter, herunder rådgivning af statslige myndigheder om informationssikkerhed samt tekniske analyser og assistance til myndigheder ved cyberangreb.

På Forsvarsministeriets område leder og kontrollerer Center for Cybersikkerhed den militære it-sikkerhedstjeneste. Som led heri bidrager centeret til udvikling af Forsvarets ikt-systemer med sikkerhedsdesign, udgiver militære ikt-sikkerhedsbestemmelser, kvalitetssikrer informationssikkerheden og yder sikkerhedsteknisk støtte samt sikkerhedsgodkender ikt-systemer og -installationer, bl.a. på baggrund af TEMPEST-målinger (måling af uønsket elektromagnetisk udstråling). Herudover sikrer centeret bevismateriale i sager om brud på informationssikkerheden, udfører tekniske sikkerhedseftersyn og monitering af kontorer og mødelokaler, hvor der skal gennemføres klassificerede samtaler, med henblik på opdagelse og fjernelse af lytteudstyr m.v. Center for Cybersikkerhed løser endvidere de militære opgaver inden for informationssikkerhed, som Danmark gennem sit medlemskab af NATO er forpligtet til, herunder varetagelse af funktionerne som National Security Authority (NSA), National Accreditation Authority (NAA), National Communication Security Authority (NCSA) og National TEMPEST Authority.

Hertil kommer, at Center for Cybersikkerhed har myndighedsansvaret for informationssikkerhed og beredskab i relation til samfundets teleforsyning, herunder ved krisestyring med henblik på i videst muligt omfang at tilgodese samfundsvigtige myndigheder og virksomheders adgang til telefoni og internetkommunikation ved større kriser.

Den hastige udvikling på informationssikkerhedsområdet medfører, at Center for Cybersikkerheds opgaver udvikler sig dynamisk. Det er således forudsat, at der løbende vil ske en udvikling af de konkrete opgaver, som centeret løser med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet.

Bestemmelsens *stk. 2* fastslår Center for Cybersikkerheds organisatoriske tilhørsforhold. Regeringen besluttede i 2011, at myndighedernes indsats på it-sikkerhedsområdet skulle samles i et it-sikkerhedscenter, og at dette center – Center for Cybersikkerhed – skulle være en del af Forsvarets Efterretningstjeneste under Forsvarsministeriet.

Forsvarets Efterretningstjenestes opgaver er reguleret ved lov nr. 602 af 12. juni 2013 om Forsvarets Efterretningstjeneste (FE-loven), der trådte i kraft den 1. januar 2014. Det fremgår af FE-lovens § 1, stk. 3, 2. pkt, at Forsvarets Efterretningstjenestes opgaver som national it-sikkerhedsmyndighed, militær varslingstjeneste for internettrusler m.v. (MILCERT) og statslig varslingstjeneste for internettrusler (GovCERT) ikke reguleres af FE-lovens materielle bestemmelser, men vil blive reguleret særskilt.

Der henvises i øvrigt til afsnit 2.1 og 2.2 i de almindelige bemærkninger.

Til § 2

Den foreslåede § 2 definerer fem centrale begreber i loven, hvoraf begreberne sikkerhedshændelse, pakkedata og trafikdata med enkelte sproglige tilpasninger og præciseringer videreføres fra GovCERT-lovens § 3, mens begreberne personoplysninger og behandling defineres i overensstemmelse med persondatalovens § 3, nr. 1 og 2.

Nr. 1 viderefører definitionen af sikkerhedshændelse fra GovCERT-lovens § 3, nr. 3, med en sproglig præcisering af, at sikkerhedshændelser er hændelser med en negativ påvirkning af tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester. Det præciseres endvidere, at begrebet sikkerhedshændelse omfatter hændelser, der vurderes at ville kunne have den beskrevne påvirkning.

Definitionen indebærer, at enhver unormal situation, der potentielt kan kompromittere informationssystemer, digitale netværk, digitale tjenester eller andre elektroniske systemer eller data, der lagres, processeres eller transmitteres af disse systemer, vil være at betragte som en sikkerhedshændelse. Desuden præciseres det, at begrebet omfatter data, informationssystemer, digitale netværk og digitale tjenester, således at det udtrykkeligt fremgår, at også hændelser, som rammer lukkede netværk (netværk, der ikke er forbundet til internettet), kan have karakter af sikkerhedshændelser.

Et eksempel på en sikkerhedshændelse, der negativt påvirker tilgængeligheden af en digital tjeneste, er et overbelastningsangreb (denial-of-service angreb), hvor f.eks. en hjemmeside rammes af et stort antal forespørgsler, så brugere ikke kan få adgang til hjemmesiden. En sikkerhedshændelse, der negativt påvirker integriteten af såvel data som et informationssystem, kan eksempelvis være indtrængen i en database, hvor oplysninger ændres uden databaseejerens vidende. En sikkerhedshændelse, der negativt påvirker fortroligheden af et informationssystem, kan være en såkaldt "trojansk hest", hvor der installeres et program på en myndigheds informationssystem, som muliggør uautoriseret kopiering af data fra myndigheden.

Med definitionen af begrebet pakkedata i *nr. 2* videreføres GovCERT-lovens § 3, nr. 1, 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.

Bestanddelene af en internetkommunikation betegnes teknisk som "pakker". Denne tekniske betegnelse er ikke identisk med betegnelsen pakkedata efter den foreslåede § 2, nr. 2. En "pakke" i teknisk forstand vil således bestå af såvel pakke- som trafikdata i lovforslagets forstand.

Det foreslåede *nr. 3* definerer begrebet trafikdata. Der er tale om en videreførelse af GovCERT-lovens § 3, nr. 2, 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.

Definitionen af begrebet personoplysninger i *nr. 4* er identisk med den tilsvarende definition i persondatalovens § 3, nr. 1, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Definitionen af begrebet behandling i *nr. 5* er identisk med den tilsvarende definition i persondatalovens § 3, nr. 2, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Til § 3

Den foreslåede § 3 fastsætter de overordnede rammer for Center for Cybersikkerheds netsikkerhedstjeneste. Der er for så vidt angår netsikkerhedstjenestens aktiviteter på det civile område tale om en delvis videreførelse af GovCERT-lovens § 2, mens netsikkerhedstjenestens aktiviteter på Forsvarsministeriets område (MILCERT) ikke tidligere har været reguleret ved lov.

Det foreslås med *stk. 1*, at betegnelsen "netsikkerhedstjeneste" erstatter GovCERT-lovens "varslingstjeneste". Netsikkerhedstjeneste vil være den fremtidige betegnelse for Center for Cybersikkerheds samlede aktiviteter i forbindelse med at opdage, analysere og bidrage til at imødegå sikkerhedshændelser. Netsikkerhedstjenesten vil således omfatte alle de kapaciteter ved Center for Cybersikkerhed, der på forskellig vis bidrager til monitoreringens gennemførelse, herunder CERT-aktiviteterne på det civile område (GovCERT) og det militære område (MILCERT), sikkerhedstekniske aktiviteter (f.eks. analyse af malware samt forensic-undersøgelser i forbindelse med sikring af bevismateriale i sager om informationssikkerhed på Forsvarsministeriets område) samt støttefunktioner.

Netsikkerhedstjenestens opgave er som nævnt at opdage, analysere og bidrage til at imødegå sikkerhedshændelser. Der er ikke med denne formulering tilsigtet en ændring i forhold til de opgaver, som GovCERT hidtil har løst med hjemmel i GovCERT-loven, men opgaverne vil blive udført på både det civile og det militære område. Myndigheder og institutioner på Forsvarsministeriets myndighedsområde har ikke været omfattet af GovCERT-loven, da MILCERT har varetaget funktionen for de militære myndigheder.

Ved tilslutning til netsikkerhedstjenesten vil der som hidtil blive indgået en tilslutningsaftale, der nærmere regulerer specifikke forhold i relationen mellem netsikkerhedstjenesten og den enkelte

tilsluttede myndighed eller virksomhed. Tilslutningen anses for at være sket, når denne aftale er indgået. På Forsvarsministeriets område er det den militære it-sikkerhedsmyndighed, som pålægger myndigheder at blive tilsluttet netsikkerhedstjenesten, og på dette område indgås ikke tilslutningsaftaler.

En myndighed eller virksomhed, der tilsluttes netsikkerhedstjenesten, vil modtage en sikkerhedsydelse, der er tilpasset den enkelte myndigheds eller virksomheds behov. Der vil eksempelvis kunne ske en monitorering af myndighedens eller virksomhedens forbindelse til internettet, således at netsikkerhedstjenesten ved hjælp af f.eks. en lokalt placeret alarmenhed kan opdage og analysere sikkerhedshændelser. På den baggrund – og på baggrund af tilsvarende analyser hos de øvrige tilsluttede myndigheder og virksomheder – kan netsikkerhedstjenesten dels alarmere myndigheden eller virksomheden, når der konstateres konkrete sikkerhedshændelser, dels udsende mere generelle varslinger. Desuden vil tilsluttede myndigheder og virksomheder kunne modtage varslinger på baggrund af oplysninger, som Center for Cybersikkerhed modtager fra Forsvarets Efterretningstjenestes udenrigsefterretningstjeneste, andre netsikkerhedstjenester samt andre udenlandske samarbejdspartnere.

Netsikkerhedstjenesten vil desuden yde rådgivning om informationssikkerhed til de tilsluttede myndigheder og kunne yde bistand, hvis en myndighed eller virksomhed rammes af en alvorlig sikkerhedshændelse.

Stk. 2 beskriver de statslige aktører m.v., som efter anmodning kan tilsluttes netsikkerhedstjenesten. Der er tale om en videreførelse af gældende ret efter GovCERT-loven, hvorefter netsikkerhedstjenestens ydelser som udgangspunkt stilles til rådighed for statens institutioner. Som hidtil vil alle de øverste statsorganer – det vil sige Folketinget med tilhørende institutioner, regenten og domstolene – kunne tilsluttes netsikkerhedstjenesten.

Den foreslåede *stk. 3* er en delvis videreførelse af GovCERT-lovens § 2, stk. 1. Regioner og kommuner og visse virksomheder kan således fortsat efter anmodning blive tilsluttet netsikkerhedstjenesten. Kredsen af virksomheder, der kan tilsluttes, udvides imidlertid fra virksomheder, der er beskæftiget med kritisk infrastruktur, til virksomheder, der er beskæftiget med samfundsvigtige funktioner.

Ved samfundsvigtige funktioner forstås i denne sammenhæng funktioner, som er særligt vigtige for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed, herunder funktioner inden for sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet. Som eksempler på nye typer af virksomheder, der vil få mulighed for at blive tilsluttet netsikkerhedstjenesten, kan nævnes medicinalvirksomheder, fødevarevirksomheder, virksomheder, der leverer vigtige komponenter til Forsvaret, og virksomheder, der varetager driften af administrative it-systemer for det offentlige. Bestemmelsen er ikke begrænset til virksomheder, men omfatter alle juridiske personer, der er beskæftiget med samfundsvigtige funktioner.

Da netsikkerhedstjenestens kapacitet er begrænset, foreslås det, at Center for Cybersikkerhed får hjemmel til at foretage en konkret vurdering af, om en anmodning fra en region, kommune eller virksomhed, der ønsker at blive tilsluttet netsikkerhedstjenesten, kan imødekommes.

Centerets afgørelse vil blive truffet ud fra en overordnet vurdering af, om den pågældende myndigheds eller virksomheds tilslutning vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet. Ved denne vurdering vil der som i dag blive lagt vægt på netsikkerhedstjenestens aktuelle kapacitet, men der vil endvidere blive lagt vægt på, om den pågældende myndighed eller virksomhed har en it-infrastruktur, der kan udnytte fordelene ved den monitoreringsydelse, som leveres. Det forudsætter, at it-infrastrukturen er hensigtsmæssigt indrettet, at den pågældende myndighed eller virksomhed har et tilfredsstillende informationssikkerhedsniveau, og at it-driftsorganisationen har et beredskab, der kan håndtere alarmer fra netsikkerhedstjenesten. Der vil endvidere blive lagt vægt på, at netsikkerhedstjenesten samlet set opnår en samfundsmæssigt repræsentativ dækning, således at netsikkerhedstjenesten dækker så mange forskellige sektorer, brancher, virksomhedstyper og it-teknologier som muligt, hvorved netsikkerhedstjenesten får optimale muligheder for at forebygge cyberangreb. Centerets afgørelse vil kunne påklages til Forsvarsministeriet.

Det foreslås med *stk. 4*, at den hidtidige ordning fra GovCERT-lovens § 2, stk. 2, videreføres, således at Center for Cybersikkerhed ved bekendtgørelse kan fastsætte nærmere regler for regioners, kommuners og virksomheders tilslutning til netsikkerhedstjenesten, herunder regler om betaling af gebyr.

Med hjemmel i GovCERT-lovens § 2, stk. 2, er bekendtgørelse nr. 1304 af 17. december 2012 om vilkår for tilslutning til den statslige varslingstjeneste for internettrusler udstedt. Bekendtgørelsen regulerer bl.a. ejerskab og håndtering af monitoreringsudstyr samt ansvar for sikkerhedsforanstaltninger. Desuden følger det af bekendtgørelsen, at tilsluttede myndigheder og virksomheder betaler et årligt beløb til dækning af driftsudgifter og herudover betaler de udgifter, der er forbundet med GovCERT's indkøb og/eller udvikling af alarmenhed og service af denne.

Det forudsættes, at regioner, kommuner og virksomheder, der ønsker at blive tilsluttet netsikkerhedstjenesten, som hidtil dækker de udgifter, der er forbundet med indkøb og/eller udvikling af evt. monitoreringsudstyr, samt Center for Cybersikkerheds udgifter til monitoreringen. De første to måneders tilslutning betragtes dog som en indkøringsperiode, hvor der ikke sker opkrævning.

De myndigheder, der tilsluttes efter stk. 2, modtager som hidtil netsikkerhedstjenestens ydelser vederlagsfrit. Ønsker en myndighed særlige ydelser, f.eks. monitorering af flere forskellige forbindelser til internettet, vil myndigheden blive opkrævet betaling, som dækker udgifterne til indkøb og/eller udvikling af evt. monitoreringsudstyr og udgifter til driften heraf.

Til § 4

Den foreslåede § 4 giver Center for Cybersikkerheds netsikkerhedstjeneste hjemmel til at foretage indgreb i meddelelseshemmeligheden i forbindelse med behandling af pakke- og trafikdata hidrørende fra netværk hos tilsluttede myndigheder og virksomheder.

Netsikkerhedstjenesten har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder, jf. den foreslåede § 3. Netsikkerhedstjenesten varetager opgaver i forhold til tilsluttede myndigheder og virksomheder på det civile område (§ 4), myndigheder og institutioner på Forsvarsministeriets myndighedsområde (§ 5), midlertidigt tilsluttede myndigheder og virksomheder (§ 6) og ved undersøgelse af informationssystemer (§ 7).

Bestemmelsen er en indholdsmæssigt uændret videreførelse af GovCERT-lovens § 4, stk. 1, der giver GovCERT hjemmel til uden retskendelse at behandle, herunder indsamle, registrere, analysere og opbevare, tilsluttede myndigheders og private virksomheders ind- og udgående pakke- og trafikdata. Der er med den ændrede formulering af bestemmelsen – som alene angiver samlebetegnelsen "behandler" og undlader eksemplificering heraf – ikke tilsigtet en ændring af anvendelsesområdet.

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. Konsekvensen er, at GovCERT ikke kan tilgå en krypteret e-mail, uanset at denne indeholder skadelige filer, f.eks. virus, ligesom GovCERT's muligheder for at opdage og imødegå angreb mod hjemmesider, der af sikkerhedsmæssige årsager anvender krypterede forbindelser, begrænses markant. Desuden er det konstateret, at angribere ofte anvender krypteret kommunikation for at søge at skjule cyberangreb. Begrænsningen for så vidt angår afkryptering foreslås på den baggrund ikke videreført.

Til § 5

Den foreslåede § 5 giver Center for Cybersikkerheds netsikkerhedstjeneste hjemmel til at foretage indgreb i meddelelseshemmeligheden i forbindelse med behandling af pakke- og trafikdata hidrørende fra netværk hos myndigheder på Forsvarsministeriets område.

Den it-sikkerhedsmæssige monitorering af netværkskommunikation hos myndigheder og institutioner på Forsvarsministeriets myndighedsområde er hidtil blevet varetaget af MILCERT, der ikke har været reguleret ved lov. Med § 5 foreslås den hjemmel, der siden 2011 har været gældende for GovCERT's monitoreringsaktiviteter på det civile område, udvidet til også at gælde for det militære område. Monitoreringen vil fremover ske i regi af Center for Cybersikkerheds netsikkerhedstjeneste, der vil omfatte både GovCERT's og MILCERT's nuværende aktiviteter.

Den foreslåede § 5, der giver hjemmel til indgreb i meddelelseshemmeligheden i forhold til myndigheder på Forsvarsministeriets område, er indholdsmæssigt identisk med den foreslåede § 4, der giver hjemmel til indgreb i meddelelseshemmeligheden i forhold til tilsluttede myndigheder og virksomheder på det civile område.

Reguleringen af netsikkerhedstjenestens adgang til at foretage indgreb i meddelelseshemmeligheden på henholdsvis det civile og det militære område er opdelt i to bestemmelser, da der på enkelte områder foreslås at gælde særlige regler for det militære område. Det sker for at sikre, at der ikke med den foreslåede ordning sker en indskrænkning i forhold til de muligheder for monitorering, som MILCERT hidtil har haft. På Forsvarsministeriets område, hvor der i betydeligt omfang håndteres klassificerede oplysninger, vil der således fortsat være behov for en videre adgang til at analysere monitorerede data og til at videregive data til relevante samarbejdspartnere.

Der henvises til afsnit 3.2 i de almindelige bemærkninger.

Til § 6

Den foreslåede § 6 giver Center for Cybersikkerheds netsikkerhedstjeneste hjemmel til at foretage indgreb i meddelelseshemmeligheden i forbindelse med behandling af pakke- og trafikdata hidrø-

rende fra netværk hos en myndighed eller virksomhed, der ikke fast er tilsluttet netsikkerhedstjenesten efter den foreslåede § 3, men som tilsluttes i en tidsbegrænset periode.

Den foreslåede ordning er baseret på GovCERT-lovens § 4, stk. 1, der giver GovCERT hjemmel til uden retskendelse at indsamle, registrere, analysere og opbevare tilsluttede myndigheders og private virksomheders ind- og udgående pakke- og trafikdata. Med § 6 sikres det, at en myndighed eller virksomhed, som ikke er beskæftiget med samfundsvigtige funktioner efter § 3, stk. 3, kan tilsluttes i en kortere periode, såfremt der er begrundet mistanke om, at den udsættes for et alvorligt cyberangreb eller er angrebet på en måde, som kan påvirke samfundsvigtige funktioner negativt.

En midlertidig tilslutning kan ske i forhold til myndigheder og virksomheder, som ikke normalt er udsat for et sådant trusselsbillede, at en fast tilslutning til netsikkerhedstjenesten er hensigtsmæssig, men som på grund af aktuelle begivenheder i en kortere periode er udsat for et så konkret trusselsbillede, at der er behov for den ekstra sikkerhed, som en tilslutning indebærer. Det kan f.eks. være tilfældet, hvis en myndighed træffer afgørelse i en enkeltstående sag, der giver international opmærksomhed, eller hvis en virksomhed står over for at skulle byde på en højteknologisk opgave, og der på den baggrund opstår en begrundet mistanke om, at de vil blive udsat for et cyberangreb. En midlertidig tilslutning kan også ske, hvis virksomheder, der ikke er beskæftiget med samfundsvigtige funktioner, rammes af særligt alvorlige cyberangreb. Der vil f.eks. kunne være tale om, at en virksomheds it-system uden virksomhedens vidende indgår i et skadeligt netværk beregnet til cyberangreb, hvorfra der rettes angreb mod offentlige myndigheder, eller hvortil hackere henter følsomme oplysninger fra myndigheder eller virksomheder.

Det foreslås, at en midlertidig tilslutning til netsikkerhedstjenesten 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 eller vil finde sted. En begrundet mistanke vil efter omstændighederne f.eks. kunne foreligge, hvis en myndighed eller virksomhed udsættes for trusler af mere generel karakter fra aktører eller grupper af aktører, der vil kunne tænkes at benytte sig af cyberangreb, eller hvis en virksomhed befinder sig i en situation – f.eks. ved offentliggørelse af en ny opfindelse – hvor der har været eksempler på, at der i tilsvarende situationer er sket cyberangreb.

Der skal efter bestemmelsens *nr. 1* foreligge et skriftligt samtykke fra myndigheden eller virksomheden til behandlingen af pakke- og trafikdata. Uanset at der er tale om en midlertidig tilslutning til netsikkerhedstjenesten, vil der således skulle indgås en tilslutningsaftale, og denne aftale skal foreligge skriftligt, inden netsikkerhedstjenesten kan behandle pakke- og trafikdata.

Efter det foreslåede *nr. 2* er det et krav, at Center for Cybersikkerheds netsikkerhedstjeneste forud for en midlertidig tilslutning konkret skal have vurderet, at adgangen til i en kortere periode at behandle pakke- og trafikdata hidrørende fra netværk hos den pågældende myndighed eller virksomhed vil styrke centerets muligheder for at sikre den ikt-infrastruktur, som samfundsvigtige funktioner er afhængige af. Ved midlertidig tilslutning af virksomheder er det således – i modsætning til ved fast tilslutning efter den foreslåede § 3, stk. 3 – ikke et krav, at den pågældende virksomhed selv beskæftiger sig med samfundsvigtige funktioner. Der vil dermed f.eks. kunne ske midlertidig tilslutning af en virksomhed, hvor en eller flere servere er blevet inficeret med malware og er blevet del af et netværk af inficerede maskiner (et såkaldt botnet), hvorfra der rettes angreb mod offentlige myndigheder, uanset virksomhedens størrelse eller branche.

Endelig er det efter den foreslåede *nr. 3* som nævnt et krav, at der er tale om en midlertidig tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste. Den midlertidige periode kan højst udgøre to måneder regnet fra det tidspunkt, hvor der er indgået en tilslutningsaftale. Hvis formålet med monitoreringen er opfyldt, inden der er forløbet to måneder, eller hvis en eller flere af betingelserne i nr. 1 og 2 ikke længere er opfyldt, vil monitoreringen straks blive indstillet.

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

Såfremt der efter den midlertidige tilslutnings afslutning på ny opstår en begrundet mistanke om en sikkerhedshændelse, vil der kunne indgås en ny, midlertidig tilslutningsaftale.

Der henvises i øvrigt til afsnit 3.1 og 3.2 i de almindelige bemærkninger.

Til § 7

Den foreslåede § 7 giver Center for Cybersikkerheds netsikkerhedstjeneste hjemmel til at foretage indgreb i meddelelseshemmeligheden i forbindelse med behandling af data, som er indeholdt i eller hidrører fra et informationssystem, der anvendes af en myndighed eller virksomhed.

Den foreslåede ordning er baseret på GovCERT-lovens § 4, stk. 1, der giver GovCERT hjemmel til uden retskendelse at indsamle, registrere, analysere og opbevare tilsluttede myndigheders og private virksomheders ind- og udgående pakke- og trafikdata. Med § 7 foreslås denne hjemmel imidlertid udvidet til også at gælde for behandling af data, som er indeholdt i eller hidrører fra et informationssystem, hvor der er en begrundet mistanke om en sikkerhedshændelse. Bestemmelsen vil således eksempelvis give Center for Cybersikkerhed mulighed for at klarlægge et cyberangrebs årsag, omfang og konsekvenser gennem undersøgelser af det ramte informationssystem.

Begrebet informationssystem skal forstås i overensstemmelse med definitionen i Rådets rammeafgørelse 2005/222/RIA af 24. februar 2005 om angreb på informationssystemer. Efter denne definition, der endvidere er anvendt i lov nr. 352 af 19. maj 2004 om ændring af bl.a. straffeloven, forstås ved et informationssystem "enhver enhed eller gruppe af indbyrdes forbundne eller beslægtede enheder, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af edb-data samt edb-data, som lagres, behandles, fremfindes eller overføres i forbindelse med systemernes drift, brug, beskyttelse og vedligeholdelse".

Ved edb-data forstås tilsvarende her "enhver form for gengivelse af fakta, informationer eller begreber i et format, der egner sig til behandling i et informationssystem, herunder et program, som kan anvendes til at få et informationssystem til at udføre en funktion".

Anvendelse af bestemmelsen 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 eller vil finde sted.

Det er efter *nr. 1* et krav, at informationssystemet eller dataene herfra skal stilles til rådighed for Center for Cybersikkerheds netsikkerhedstjeneste, og at der skal foreligge et samtykke til, at Center

for Cybersikkerhed behandler disse data. Samtykket skal foreligge skriftligt, inden netsikkerhedstjenesten kan behandle data.

Efter *nr. 2* er det et krav, at netsikkerhedstjenesten forud for behandlingen af data konkret skal have vurderet, at behandlingen vil styrke centerets muligheder for at sikre ikt-infrastruktur, som samfundsvigtige funktioner er afhængige af. I forhold til virksomheder er det således ikke et krav, at en virksomhed selv beskæftiger sig med samfundsvigtige funktioner.

Hvis Center for Cybersikkerhed behandler data fra et informationssystem, hvor der ikke ved behandlingen sker indgreb i meddelelseshemmeligheden, vil en sådan behandling ikke være omfattet af den foreslåede § 7, men alene af de generelle bestemmelser om behandling af personoplysninger i det foreslåede kapitel 6. Det vil f.eks. kunne være tilfældet, hvis Center for Cybersikkerhed får stillet en server, der ikke indeholder e-mail-korrespondance, til rådighed med henblik på at undersøge et cyberangreb.

Der henvises i øvrigt til afsnit 3.1 og 3.2 i de almindelige bemærkninger.

Til § 8

Den foreslåede § 8 vedrører Center for Cybersikkerheds forhold til offentlighedsloven, forvaltningsloven og persondataloven. Den behandling af personoplysninger, som finder sted i Center for Cybersikkerhed, er i dag reguleret i Forsvarsministeriets retningslinjer af 13. maj 2013 for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste.

Det foreslås med *stk. 1*, at Center for Cybersikkerhed – som det er tilfældet for den øvrige del af Forsvarets Efterretningstjeneste – undtages fra offentlighedsloven, dog ikke lovens § 13 om notatpligt, samt undtages fra forvaltningslovens kapitel 4-6.

Det forudsættes imidlertid, at Center for Cybersikkerhed i størst muligt omfang efterlever 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 relevant omfang vurderer, om det i afgørelsessager konkret er muligt at anvende forvaltningslovens principper om partens aktindsigt, partshøring og begrundelse m.v. Tilsvarende forudsættes det, at anmodninger om aktindsigt i størst muligt omfang behandles efter principperne i offentlighedsloven, jf. afsnit 3.3.3 i de almindelige bemærkninger.

Det følger af § 2, stk. 11, i lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven), at loven ikke gælder for behandlinger, der udføres for politiets og forsvarets efterretningstjenester. Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, og persondataloven finder dermed ikke anvendelse på centerets virksomhed.

I forhold til Center for Cybersikkerheds behandling af anmodninger om tilslutning til netsikkerhedstjenesten, jf. det foreslåede § 3, stk. 3, centerets virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet, og centerets personalesager foreslås det med *stk. 2*, at forsvarsministeren bemyndiges til at bestemme, at offentlighedsloven, forvaltningslovens kapitel 4-6 og persondatalovens kapitel 8-10 helt eller delvis finder anvendelse for disse områder.

Det foreslåede *stk. 3* fastsætter de overordnede rammer for reguleringen af Center for Cybersikkerheds behandling af personoplysninger. Lov om Center for Cybersikkerhed vil erstatte bestemmelserne om behandlingsgrundlag og behandlingssikkerhed ved behandling af personoplysninger i Forsvarsministeriets retningslinjer af 13. maj 2013, og det foreslåede kapitel 6 regulerer centerets behandling af personoplysninger. Der er – som med retningslinjerne – tale om, at en række af persondatalovens centrale principper vil finde anvendelse på Center for Cybersikkerhed. Det understreges således, at kapitel 6 finder anvendelse på alle former for behandling af personoplysninger i centeret – såvel i netsikkerhedstjenesten som i forbindelse med øvrige myndighedsopgaver.

De generelle bestemmelser i kapitel 6 suppleres imidlertid af kapitel 7, som kun finder anvendelse på netsikkerhedstjenestens behandling af data, herunder personoplysninger, efter kapitel 4 (indgreb i meddelelseshemmeligheden). Baggrunden for de særlige regler, som gælder for data, der indsamles ved monitorering af netværkskommunikation eller i øvrigt tilvejebringes ved indgreb i meddelelseshemmeligheden, er, at behandlingen af disse oplysninger søges begrænset i størst muligt omfang, bl.a. af hensyn til privatlivets fred.

Der henvises i øvrigt til afsnit 3.3 i de almindelige bemærkninger.

Til § 9

Den foreslåede § 9 viderefører med enkelte sproglige tilpasninger den gældende § 10, stk. 2 og 3, i Forsvarsministeriets retningslinjer af 13. maj 2013 for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste.

Den foreslåede *stk. 1*, hvorefter Center for Cybersikkerhed bl.a. skal sikre, at behandling af personoplysninger ikke sker i videre omfang end formålet tilsiger, er identisk med persondatalovens § 5, stk. 2, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Den foreslåede *stk. 2*, som fastsætter principper om relevans og proportionalitet, er identisk med persondatalovens § 5, stk. 3, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Til § 10

Den foreslåede § 10, der fastsætter de overordnede rammer for, hvornår behandling af personoplysninger må finde sted, er en delvis videreførelse af § 11 i Forsvarsministeriets retningslinjer af 13. maj 2013 for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste.

I forhold til retningslinjernes § 11 foreslås bestemmelsen udvidet med yderligere en behandlingshjemmel, således at behandling af personoplysninger efter den foreslåede § 10, nr. 7, også kan finde sted, hvis der er tale om personoplysninger, der er omfattet af det foreslåede kapitel 4.

De foreslåede *§ 10, nr. 1, 2, 3, 5* og *6*, er med sproglige tilpasninger identiske med de tilsvarende bestemmelser i persondatalovens § 6 og skal fortolkes i overensstemmelse med disse bestemmelsers forarbejder og relevante praksis.

Behandlingshjemlen i *§ 10, nr. 4*, som er en videreførelse af § 11, nr. 6, i retningslinjerne, foreslås som konsekvens af de særlige opgaver, som Center for Cybersikkerhed udfører som netsikkerhedstjeneste og national it-sikkerhedsmyndighed. Efter bestemmelsen vil behandling af personoplysninger kunne finde sted, hvis behandlingen er nødvendig til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar. Anvendelse af bestemmelsen forudsætter således, at der er fare for, at statens sikkerhed eller rigets forsvar vil lide skade. Det kan f.eks. være tilfældet i forbindelse med cyberangreb mod danske myndigheders informationssystemer. Hensynet til statens sikkerhed eller rigets forsvar skal fortolkes i overensstemmelse med det tilsvarende udtryk i offentlighedslovens § 31.

Med den foreslåede *§ 10, nr. 7*, fastsættes en generel hjemmel til at behandle personoplysninger, hvis de er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden). Det bemærkes i den forbindelse, at der med den foreslåede § 15 er fastsat nærmere rammer for analyse af pakkedata, der er omfattet af §§ 4, 6 og 7, mens der i den foreslåede § 17 er fastsat regler for sletning af de pågældende data.

Til § 11

Den foreslåede § 11 fastsætter rammerne for Center for Cybersikkerheds behandling af personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og personoplysninger om helbredsmæssige og seksuelle forhold.

Bestemmelsen er en delvis videreførelse af § 12 i Forsvarsministeriets retningslinjer af 13. maj 2013 for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste.

De foreslåede *§ 11, stk. 1,* og *stk. 2, nr. 1-3*, er med sproglige tilpasninger identiske med de tilsvarende bestemmelser i persondatalovens § 7 og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

For så vidt angår *§ 11, stk. 2, nr. 4*, henvises til bemærkningerne til den foreslåede § 10, nr. 4.

For så vidt angår *§ 11, stk. 2, nr. 5,* der foreslår en ny behandlingshjemmel ved behandling af personoplysninger, som er omfattet af det foreslåede kapitel 4, henvises til bemærkningerne til den foreslåede § 10, nr. 7.

Til § 12

Den foreslåede § 12 fastsætter rammerne for Center for Cybersikkerheds behandling af personoplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i den foreslåede § 11, stk. 1, nævnte.

Bestemmelsen er en delvis videreførelse af § 13 i Forsvarsministeriets retningslinjer af 13. maj 2013 for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste.

De foreslåede *§ 12, stk. 1,* og *stk. 2, nr. 1-4*, er med sproglige tilpasninger identiske med de tilsvarende bestemmelser i persondatalovens § 8 og skal fortolkes i overensstemmelse med disse bestemmelsers forarbejder og relevante praksis.

For så vidt angår *§ 12, stk. 2, nr. 5*, der foreslår en ny behandlingshjemmel ved behandling af personoplysninger, som er omfattet af det foreslåede kapitel 4, henvises til bemærkningerne til den foreslåede § 10, nr. 7.

Til § 13

Den foreslåede § 13, der fastsætter krav til datakvalitet, er en indholdsmæssigt uændret videreførelse af § 10, stk. 4, i Forsvarsministeriets retningslinjer af 13. maj 2013 for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste.

Bestemmelsen er identisk med den tilsvarende bestemmelse i persondatalovens § 5, stk. 4, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Til § 14

Den foreslåede § 14, der fastsætter tidsmæssige begrænsninger for opbevaring af indsamlede personoplysninger, er en uændret videreførelse af § 10, stk. 5, i Forsvarsministeriets retningslinjer af 13. maj 2013 for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste.

Bestemmelsen er identisk med den tilsvarende bestemmelse i persondatalovens § 5, stk. 5, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 17, som fastsætter særlige bestemmelser om sletning af data, der er omfattet af det foreslåede kapitel 4. Denne bestemmelse erstatter GovCERT-lovens § 4, stk. 2-4.

Til § 15

Den foreslåede § 15 fastsætter rammerne for Center for Cybersikkerheds netsikkerhedstjenestes adgang til at analysere pakkedata, der er omfattet af de foreslåede §§ 4, 6 og 7 (indgreb i meddelelseshemmeligheden). Som led i netsikkerhedstjenestens drift sker der løbende en fuldautomatisk behandling af data fra de tilsluttede myndigheder og virksomheders netværkskommunikation med henblik på at identificere mulige sikkerhedshændelser. Bestemmelsen indebærer, at netsikkerhedstjenestens sikkerhedsanalytikere kun må foretage en analyse af pakkedata, hvis der er en begrundet mistanke om en sikkerhedshændelse – og da kun i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen.

Der er tale om en videreførelse af GovCERT-lovens § 4, stk. 1, 2. pkt., med enkelte sproglige tilpasninger.

Med §§ 6 og 7 foreslås netsikkerhedstjenestens adgang til indgreb i meddelelseshemmeligheden udvidet til også at omfatte situationer, hvor en myndighed eller virksomhed midlertidigt er tilsluttet netsikkerhedstjenesten, samt situationer, hvor myndigheder eller virksomheder stiller et informati-

onssystem til rådighed for netsikkerhedstjenesten. Den foreslåede § 15 vil som konsekvens heraf også omfatte analyse af pakkedata, som stammer fra disse kilder.

Til § 16

Den foreslåede § 16 regulerer Center for Cybersikkerheds muligheder for at videregive data, der er omfattet af §§ 4, 6 og 7 og dermed behandles på baggrund af indgreb i meddelelseshemmeligheden.

Bestemmelsen er en delvis videreførelse af GovCERT-lovens § 6.

Med §§ 6 og 7 foreslås netsikkerhedstjenestens adgang til indgreb i meddelelseshemmeligheden udvidet til også at omfatte situationer, hvor en myndighed eller virksomhed midlertidigt er tilsluttet netsikkerhedstjenesten, samt situationer, hvor myndigheder eller virksomheder stiller et informationssystem til rådighed for netsikkerhedstjenesten. Den foreslåede § 16 vil som konsekvens heraf også omfatte videregivelse af data, der stammer fra disse kilder.

Det følger af den foreslåede *nr. 1*, at Center for Cybersikkerhed ved begrundet mistanke om en sikkerhedshændelse kan videregive data, der stammer fra indgreb i meddelelseshemmeligheden, til dansk politi (og anklagemyndigheden). Dermed sikres, at centeret kan videregive alle relevante oplysninger til politiet i de tilfælde, hvor det kan være relevant for politiet at indlede en strafferetlig efterforskning.

Kravet om, at der skal være tale om en begrundet mistanke om en sikkerhedshændelse, indebærer, at Center for Cybersikkerhed alene kan videregive de pågældende data, hvis der foreligger konkrete indikationer, der peger i retning af, at en sikkerhedshændelse har fundet eller vil finde sted.

Med *nr. 2* foreslås, at Center for Cybersikkerhed kan videregive trafikdata til den samme kreds af aktører, som er angivet i GovCERT-lovens § 6, nr. 3: Danske myndigheder, tilsluttede private virksomheder og tilsvarende varslingstjenester i andre lande. Betegnelsen "tilsvarende varslingstjenester i andre lande" foreslås dog erstattet med "andre netsikkerhedstjenester", som vil omfatte tilsvarende netsikkerhedstjenester i Danmark og udlandet, f.eks. CERT'er, CSIRT'er (Computer Security Incident Response Teams), ikt-sikkerhedsmyndigheder og efterretningstjenester, som Center for Cybersikkerhed har et tæt samarbejde med for at øge centerets muligheder for at forebygge sikkerhedshændelser.

Kredsen af aktører foreslås endvidere udvidet til også at omfatte udbydere af offentlige elektroniske kommunikationsnet og -tjenester (teleselskaber) samt myndigheder og virksomheder, der er omfattet af lovforslagets §§ 6 og 7.

For så vidt angår udbydere af offentlige elektroniske kommunikationsnet og -tjenester vil muligheden for at videregive trafikdata indebære, at især teleselskaber kan forbedre deres sikkerhedssystemer, således at den ikt-infrastruktur, som samfundsvigtige funktioner i overvejende grad er afhængige af, kan sikres yderligere, f.eks. ved at teleselskaberne informeres om IP-adresser, der anvendes ved cyberangreb.

Den foreslåede mulighed for at videregive trafikdata til virksomheder, der er omfattet af de foreslåede §§ 6 og 7, er en konsekvens af lovforslagets bemyndigelse til, at der kan behandles data i henhold til de to nævnte bestemmelser. Videregivelse af trafikdata til disse virksomheder vil være af

afgørende betydning for deres muligheder for at træffe passende modforholdsregler til håndtering af de sikkerhedshændelser, der konstateres som led i monitoreringen af netværkskommunikation eller ved undersøgelse af deres informationssystemer.

En af Center for Cybersikkerheds vigtigste forebyggende aktiviteter er udsendelse af sikkerhedsvarslinger, hvor myndigheder, virksomheder, andre netsikkerhedstjenester m.v. underrettes om særligt alvorlige sikkerhedshændelser. Begrebet virksomhed omfatter i denne sammenhæng alle juridiske personer. Sikkerhedsvarslingerne giver modtagerne mulighed for at styrke deres egen forebyggelse mod angreb (f.eks. ved at blokere for trafik fra IP-adresser, der indgår i hackeres angrebsinfrastruktur) og undersøge, om de har været udsat for angreb (f.eks. ved at gennemsøge logfiler for e-mails fra afsendere, der har angrebet andre myndigheder eller virksomheder). Det foreslås derfor, at Center for Cybersikkerhed kan udsende sikkerhedsvarslinger, som indeholder trafikdata, der kan styrke modtagernes informationssikkerhedsniveau.

Videregivelse af trafikdata efter nr. 2 forudsætter, at det konkret vurderes, at videregivelsen er nødvendig. Indeholder videregivelsen personoplysninger, vil principperne om relevans og proportionalitet, jf. den foreslåede § 9, stk. 2, tillige skulle iagttages. Der vil dermed alene kunne videregives personoplysninger, som er relevante og tilstrækkelige for at opnå formålet med den konkrete videregivelse.

Den foreslåede § 16 skal ses i sammenhæng med den foreslåede § 12, som generelt regulerer Center for Cybersikkerheds adgang til at videregive personoplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i den foreslåede § 11, stk. 1, nævnte. Erfaringsmæssigt vil Center for Cybersikkerhed kun i meget sjældne tilfælde have behov at videregive personoplysninger af de nævnte typer, men i forbindelse med alvorlige cyberangreb kan der være behov for at videregive personoplysninger om strafbare forhold til politiet. Den foreslåede § 12, stk. 2, nr. 5, giver hjemmel til videregivelse af de nævnte typer af personoplysninger, hvis oplysningerne er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden). Spørgsmålet om videregivelse vil derefter skulle vurderes efter den foreslåede § 16.

Det bemærkes, at Center for Cybersikkerheds videregivelse af personoplysninger vil være underlagt tilsyn af Tilsynet med Efterretningstjenesterne, jf. de foreslåede §§ 19-24.

Til § 17

Den foreslåede § 17 fastsætter de tidsmæssige rammer for Center for Cybersikkerheds opbevaring af de data, der behandles i medfør af det foreslåede kapitel 4 og dermed behandles på baggrund af indgreb i meddelelseshemmeligheden.

Bestemmelsen skal ses i sammenhæng med den foreslåede § 14, hvorefter indsamlede personoplysninger generelt 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. Mens § 14 finder anvendelse på al behandling af personoplysninger i Center for Cybersikkerhed, finder de særlige regler i § 17 som nævnt alene anvendelse på de data, der behandles på baggrund af indgreb i meddelelseshemmeligheden.

Bestemmelsen er en delvis videreførelse af GovCERT-lovens § 4, stk. 2-4.

Efter det foreslåede *stk. 1* vil data skulle slettes, når formålet med behandlingen er opfyldt, hvilket er en videreførelse af GovCERT-lovens § 4, stk. 2, idet bestemmelsen dog foreslås udvidet til at omfatte alle former for data, der behandles på baggrund af indgreb i meddelelseshemmeligheden. Der vil på den baggrund ske en løbende vurdering af de behandlede data med henblik på at sikre, at data, der ikke længere er relevante i forhold til netsikkerhedstjenestens formål og aktiviteter, straks slettes.

Det foreslåede *stk. 2* fastsætter øvre grænser for, hvor længe data, der ikke er slettet efter stk. 1, kan opbevares. Bestemmelsen finder dermed anvendelse på data, hvor det er blevet vurderet, at der fortsat er behov for behandling i netsikkerhedstjenesten. Uanset at formålet med behandlingen således i disse tilfælde endnu ikke er opfyldt, vil data skulle slettes inden for de absolutte frister, som er fastsat i bestemmelsen.

Stk. 2, nr. 1, vedrører data, der er knyttet til en sikkerhedshændelse. Det kan f.eks. være en IP-adresse, som har været anvendt ved et cyberangreb mod en dansk myndighed, eller en e-mail-adresse, som har været anvendt til at sende malware (computerprogram, der installeres uden at brugeren ønsker det, f.eks. virus, trojansk hest eller spyware) til danske myndigheder. Sådanne data vil især blive anvendt i netsikkerhedstjenestens monitoreringsudstyr for at give mulighed for, at nye angreb, som kommer fra samme kilde, eller som anvender samme angrebsmetode og -værktøjer, straks kan opdages.

Efter bestemmelsen må data, der knytter sig til en sikkerhedshændelse, højst opbevares i tre år, hvorefter de skal slettes. Det er samme tidsmæssige grænse, som er fastsat i GovCERT-lovens § 4, stk. 3. Såfremt data inden for den tre-årige periode igen konstateres anvendt i forbindelse med en sikkerhedshændelse, vil en ny tre-årig periode starte. Hvis en IP-adresse eksempelvis i september 2014 anvendes til et cyberangreb mod en dansk myndighed, vil netsikkerhedstjenesten således kunne anvende oplysninger om IP-adressen til at forebygge nye angreb frem til september 2017, hvor oplysningerne skal slettes. Hvis samme IP-adresse i august 2017 anvendes til et nyt angrebsforsøg, og dermed atter får tilknytning til en sikkerhedshændelse, vil netsikkerhedstjenesten imidlertid kunne anvende oplysninger om IP-adressen i monitoreringsudstyr m.v. frem til august 2020, hvor oplysningerne skal slettes, hvis IP-adressen ikke på det tidspunkt atter har været anvendt i forbindelse med en sikkerhedshændelse.

Stk. 2, nr. 2, vedrører øvrige data, der ikke er knyttet til en sikkerhedshændelse. Det foreslås, at sådanne data højst må opbevares i 13 måneder, hvilket er en udvidelse i forhold til GovCERT-lovens § 4, stk. 3, hvorefter trafikdata, der ikke knytter sig til en sikkerhedshændelse, højst må opbevares i 12 måneder, mens de tilsvarende pakkedata højst må opbevares i 14 dage.

Med *stk. 3* foreslås det, at de frister for sletning, som følger af stk. 2, regnes fra det tidspunkt, hvor Center for Cybersikkerhed har registreret de pågældende data, hvilket svarer til tidspunktet for centerets lagring af data. Dette svarer til gældende ret efter GovCERT-lovens § 4, stk. 4.

Ved behandling af data, der er indeholdt i eller hidrører fra et informationssystem, som stilles til rådighed af en myndighed eller en virksomhed, jf. den foreslåede § 7, regnes fristen fra det tidspunkt, hvor der er indhentet et skriftligt samtykke fra myndigheden eller virksomheden og det pågældende informationssystem er modtaget hos eller stillet til rådighed for Center for Cybersikkerhed.

Med *stk. 4* foreslås det, at slettefristerne i stk. 1 og 2 ikke finder anvendelse på helt særlige situationer, hvor data er videregivet.

Efter den foreslåede § 16, nr. 1, kan data videregives til politiet ved begrundet mistanke om en sikkerhedshændelse, ligesom det følger af den foreslåede § 16, nr. 2, at trafikdata bl.a. kan videregives til danske myndigheder og til de virksomheder, der er tilsluttet netsikkerhedstjenesten.

Videregivelse af trafikdata vil primært ske i forbindelse med udsendelse af varslinger, hvor Center for Cybersikkerhed gør myndigheder og virksomheder opmærksomme på, at f.eks. 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 videregivelse er sket via en varsling eller tilsvarende, har Center for Cybersikkerhed i sagens natur ikke mulighed for at sikre, at der efterfølgende sker en sletning hos modtageren, ligesom centeret selv vil være forpligtet til at journalisere de udsendte varslinger m.v. Det foreslås derfor, at trafikdata, der er indeholdt i sådanne varslinger m.v. – f.eks. IP-adresser – hverken hos Center for Cybersikkerhed eller hos modtagerne af varslingerne vil skulle slettes efter § 17, stk. 1 og 2.

Data, der er videregivet til politiet i sager, hvor der er begrundet mistanke om en sikkerhedshændelse, vil typisk vedrøre mulige straffelovsovertrædelser, og det vil i sådanne sager være betænkeligt, hvis Center for Cybersikkerhed efter tre år ikke længere må opbevare de videregivne oplysninger. Det foreslås på den baggrund, at data, der videregives efter § 16, nr. 1, ikke vil skulle slettes efter § 17, stk. 1 og 2.

Uanset at sletningsreglerne i § 17, stk. 1 og 2, ikke finder anvendelse, vil personoplysninger indeholdt i data fortsat skulle behandles i overensstemmelse med den foreslåede § 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.

Der henvises til afsnit 3.4 i de almindelige bemærkninger.

Til § 18

Den foreslåede § 18 opstiller overordnede krav til Center for Cybersikkerheds interne informationssikkerhed i forhold til alle typer af oplysninger, der behandles i centeret. Bestemmelsen er en videreførelse af § 14, stk. 2, i Forsvarsministeriets retningslinjer af 13. maj 2013 for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste.

Bestemmelsen er indholdsmæssigt identisk med den tilsvarende bestemmelse i persondatalovens § 41, stk. 3, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Til § 19

Med bestemmelsen foreslås det, at det fremover skal være Tilsynet med Efterretningstjenesterne, som fører tilsyn med Center for Cybersikkerheds behandling af personoplysninger. Tilsynet med Efterretningstjenesternes virksomhed er nærmere reguleret i lov nr. 604 af 12. juni 2013 om Politiets Efterretningstjeneste (PET).

Tilsynet med Efterretningstjenesterne fører i forvejen tilsyn med Forsvarets Efterretningstjeneste, jf. FE-lovens § 13. Det følger imidlertid af FE-lovens § 1, stk. 3, 2. pkt., at Center for Cybersikkerhed ikke reguleres af FE-lovens materielle bestemmelser, herunder lovens bestemmelser om tilsyn.

Tilsynet med Efterretningstjenesterne afløser det hidtidige tilsyn, der i medfør af GovCERT-lovens § 7 er nedsat for at følge GovCERT's virksomhed. Samtidig foreslås det, at tilsynets kompetence udvides, således at al behandling af personoplysninger i Center for Cybersikkerhed bliver omfattet af Tilsynet med Efterretningstjenesternes kompetence.

Rammerne for Tilsynet med Efterretningstjenesternes virksomhed i forhold til Center for Cybersikkerhed svarer til rammerne for tilsynets virksomhed i forhold til Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste.

Til § 20

Med bestemmelsen foreslås det, at Tilsynet med Efterretningstjenesterne efter klage eller af egen drift kan påse Center for Cybersikkerheds overholdelse af de foreslåede regler i kapitel 4, 6 og 7 vedrørende behandling af personoplysninger. Det vil indebære, at tilsynet som udgangspunkt får samme tilsynsrolle i forhold til centeret, som Datatilsynet i medfør af persondataloven har i forhold til andre offentlige myndigheder.

Bestemmelsen svarer til ordningen efter FE-lovens § 15 og PET-lovens § 18.

Tilsynet med Efterretningstjenesterne vil ikke få til opgave at udtale sig om, hvorvidt Center for Cybersikkerhed udfører sine opgaver på en hensigtsmæssig måde. Det vil fortsat være op til centeret selv (under ansvar for Forsvarsministeriet) inden for de retlige rammer for centerets virksomhed at tilrettelægge sin sagsbehandling. Tilsynet med Efterretningstjenesterne har ligeledes ikke til opgave at overveje eller tage stilling til, om der af enkelte medarbejdere i Center for Cybersikkerhed måtte være begået fejl eller forsømmelser, der kan give anledning til, at der søges et retligt ansvar gennemført eller i øvrigt rettes kritik mod den enkelte, idet dets opgave er at vurdere centerets virksomhed. Opstår der tilfælde, hvor spørgsmål om ansvar for enkeltpersoner kan rejses, skal dette behandles efter almindelige personaleretlige regler m.v.

Tilsynet med Efterretningstjenesterne vil primært have til opgave at føre tilsyn med Center for Cybersikkerheds behandling af personoplysninger, der efter det foreslåede kapitel 4 behandles på baggrund af indgreb i meddelelseshemmeligheden. På dette område vil tilsynet således både efter klage og af egen drift påse Center for Cybersikkerheds overholdelse af kapitel 6 og 7. Det forudsættes, at tilsynet i forhold til Center for Cybersikkerheds øvrige behandling af personoplysninger primært vil agere efter klage og således kun i særlige tilfælde af egen drift vil iværksætte undersøgelser.

Endvidere vil tilsynet skulle påse, at Center for Cybersikkerhed i forbindelse med centerets behandling af personoplysninger overholder de krav til sikkerhedsforanstaltninger, der følger af kapitel 8. Endelig vil tilsynet have til opgave at påse, at yderligere regler om behandling af personoplysninger, der fastsættes i administrative retningslinjer, overholdes.

Til § 21

Den foreslåede § 21 regulerer Tilsynet for Efterretningstjenesternes reaktionsmuligheder. Bestemmelsen svarer til ordningen efter FE-lovens § 16 og PET-lovens § 19.

Tilsynet med Efterretningstjenesterne vil efter *stk. 1* – ligesom Folketingets Ombudsmand – kunne afgive udtalelser over for Center for Cybersikkerhed, herunder udtale kritik, afgive henstillinger samt i øvrigt fremsætte tilsynets opfattelse af en sag. En sådan udtalelse vil ikke være retligt bindende for Center for Cybersikkerhed, men det forudsættes, at centeret i almindelighed vil følge tilsynets udtalelser, jf. det foreslåede stk. 3.

Efter *stk. 2* skal Tilsynet med Efterretningstjenesterne som led i sin virksomhed orientere forsvarsministeren om vigtige afgørelser og udtalelser.

I *stk. 3* fastslås det, at 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. Samtidig sikres det, at forsvarsministeren konkret involveres i den pågældende sag. Det sikres derved, at det er forsvarsministeren og ikke tilsynet, der har det endelige ansvar i sådanne tilfælde. Med udtrykket "undtagelsesvist" understreges det, at centeret som nævnt i almindelighed forudsættes at følge henstillinger i tilsynets udtalelser.

Til § 22

Tilsynet med Efterretningstjenesterne sikres med den foreslåede § 22 adgang til de oplysninger, der er nødvendige til gennemførelse af dets virksomhed. Bestemmelsen svarer til ordningen efter FE-lovens § 17 og PET-lovens § 20.

Efter *stk. 1* kan Tilsynet med Efterretningstjenesterne hos Center for Cybersikkerhed kræve enhver oplysning og alt materiale af betydning for tilsynets virksomhed. Udtrykket "materiale" skal forstås i vid forstand og omfatter bl.a. dokumenter i traditionel forstand, elektroniske oplysninger, båndoptagelser, film m.v.

Efter *stk. 2* skal Tilsynet med Efterretningstjenesterne endvidere til enhver tid mod behørig legitimation uden retskendelse have adgang til alle lokaler, hvorfra en behandling, som foretages for Center for Cybersikkerhed, administreres, eller hvorfra der er adgang til de oplysninger, som behandles, eller hvor tekniske hjælpemidler opbevares eller anvendes. Det forudsættes med den foreslåede bestemmelse, at tilsynet har mulighed for selv at gøre sig bekendt med oplysninger og materiale på opbevaringsstedet, herunder oplysninger og materiale i arkiver, registre, installationer og anlæg af enhver art. Hermed opnår tilsynet f.eks. adgang til i forbindelse med inspektioner at foretage opslag i centerets registre m.v. på stedet og sikre sig, at tilsynet gøres bekendt med alle akter og sager.

Efter bestemmelsens *stk. 3* kan Tilsynet med Efterretningstjenesterne afkræve Center for Cybersikkerhed skriftlige udtalelser om faktiske og retlige forhold af betydning for tilsynets kontrolvirksomhed efter § 20. Tilsynet vil efter bestemmelsen kunne udbede sig centerets stillingtagen til bestemte juridiske temaer og/eller anmode om en redegørelse for centerets praksis og den bagvedliggende retsopfattelse. Bestemmelsen svarer til ombudsmandslovens § 19, stk. 2.

Endvidere kan Tilsynet med Efterretningstjenesterne efter den foreslåede bestemmelse i *stk. 4* anmode om, at en repræsentant fra Center for Cybersikkerhed deltager, når tilsynet foretager inspektioner hos centeret eller behandler sager, med henblik på, at den pågældende repræsentant kan redegøre for de behandlede sager i det omfang, tilsynet har behov for det.

Det forudsættes, at Tilsynet med Efterretningstjenesterne i forbindelse med adgangen til oplysninger, materiale og lokaliteter i videst muligt omfang tager hensyn til Center for Cybersikkerheds samarbejdspartnere m.v. og tilrettelægger sit arbejde således, at tilsynet alene skaffer sig kendskab til oplysninger, der er af betydning for kontrollens gennemførelse.

Til § 23

Med bestemmelsen, der svarer til ordningen efter FE-lovens § 18 og PET-lovens § 21, foreslås det, at Tilsynet med Efterretningstjenesternes virksomhed undtages fra reglerne i offentlighedsloven (dog med undtagelse af lovens § 13 om notatpligt), forvaltningslovens kapitel 4-6 (om aktindsigt, partshøring og begrundelse m.v.) samt persondataloven.

Der er efter lovforslaget ikke en almindelig ret til direkte indsigt i personoplysninger, der behandles af Center for Cybersikkerhed, jf. afsnit 3.3 i de almindelige bemærkninger. Bestemmelsen sikrer bl.a., at en klager ikke kan få indsigt i de oplysninger, som Center for Cybersikkerhed eventuelt måtte have behandlet om vedkommende, ved at begære indsigt efter persondataloven i de oplysninger, som tilsynet måtte behandle i anledning af klagerens anmodning til tilsynet.

Til § 24

Tilsynet med Efterretningstjenesterne skal efter den foreslåede § 24 afgive en årlig redegørelse om dets tilsynsvirksomhed til forsvarsministeren, som offentliggør redegørelsen. Bestemmelsen svarer til ordningen efter FE-lovens § 19 og PET-lovens § 22.

Redegørelsen må – netop fordi den vil være beregnet til offentliggørelse – ikke indeholde oplysninger, hvis offentliggørelse kan skade statens sikkerhed, forholdet til udenlandske samarbejdspartnere, Center for Cybersikkerheds kilder, kapaciteter og metoder m.v. I det omfang, der i redegørelsen er en omtale af klagesager, skal de enkelte klagere være anonymiserede.

Inden for disse rammer skal sigtet med Tilsynet med Efterretningstjenesterne redegørelser være at give en generel information om karakteren af det tilsyn, der udøves med Center for Cybersikkerhed. Bl.a. vil det være muligt uden tilsidesættelse af tavshedspligten i mere generelle vendinger at redegøre for tilsynets virksomhed – herunder også i form af en generel beskrivelse af, hvilke forhold tilsynet måtte have valgt særligt at interessere sig for som led i sit tilsyn.

Tilsynet vil også kunne medtage oplysninger om, i hvor mange tilfælde tilsynet har fundet, at Center for Cybersikkerheds behandling af personoplysninger ikke har været i overensstemmelse med reglerne.

Til § 25

Den foreslåede § 25 fastsætter ikrafttrædelses- og overgangsbestemmelserne for lov om Center for Cybersikkerhed.

Det foreslås med *stk. 1*, at loven træder i kraft den 1. juli 2014, hvorefter lov nr. 596 af 14. juni 2011 om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v. (GovCERT-loven) ophæves, jf. *stk. 2*. Forsvarsministeriets retningslinjer af 13. maj 2013 for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste vil endvidere blive ophævet ved lovens ikrafttræden.

Efter *stk. 3* vil aftaler, der er indgået efter GovCERT-loven, fortsat have gyldighed efter GovCERT-lovens ophævelse. Tilslutningsaftaler indgået mellem GovCERT og myndigheder og virksomheder vil dermed være gældende, indtil de måtte bortfalde eller blive opsagt.

Lovforslaget indebærer, at der på flere områder sker en ændring af reglerne for indsamling og videregivelse af pakke- og trafikdata. Da visse af ændringerne indebærer, at pakke- og trafikdata vil kunne behandles i større omfang end hidtil, foreslås det med *stk. 4*, at pakke- og trafikdata, der er indsamlet efter de mere restriktive regler i GovCERT-loven, fortsat skal behandles i overensstemmelse med GovCERT-loven. På Forsvarsministeriets område, hvor MILCERT's aktiviteter ikke hidtil har været lovregulerede, finder loven anvendelse på data, der indsamles efter lovens ikrafttræden.

Det foreslås endvidere med *stk. 5*, at begæringer om aktindsigt, som er indgivet før lovens ikrafttræden, afgøres efter de hidtil gældende regler, hvilket indebærer, at begæringerne vil skulle behandles efter offentlighedsloven, som efter de foreslåede regler fremover ikke vil finde anvendelse for Center for Cybersikkerhed.

Til § 26

Med § 26 fastlægges lovens territoriale gyldighed. Det foreslås, at loven ikke skal gælde for Færøerne og Grønland, men at den ved kongelig anordning kan sættes helt eller delvis i kraft for Færøerne og Grønland med de ændringer, som de færøske og grønlandske forhold tilsiger.