FOLKETINGSTIDENDE A

FOLKETINGET

Lovforslag nr. **L 197** Folketinget 2010-11

Fremsat den 27. april 2011 af videnskabsministeren (Charlotte Sahl-Madsen)

Forslag

til

Lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v.

§ 1. Loven finder anvendelse på IT- og Telestyrelsens behandling af personoplysninger, som er indeholdt i pakke- og trafikdata, ved driften af den statslige varslingstjeneste for internettrusler.

§ 2. Kommuner og regioner samt private virksomheder, som er beskæftiget med kritisk infrastruktur, kan efter anmodning blive tilsluttet den statslige varslingstjeneste for internettrusler.

Stk. 2. Ministeren for videnskab, teknologi og udvikling kan fastsætte nærmere regler for de i stk. 1 nævnte myndigheders og private virksomheders tilslutning til den statslige varslingstjeneste for internettrusler, herunder regler om betaling af gebyr.

§ 3. I denne lov forstås ved:

1) Pakkedata: Indholdet af internetbaseret kommunikation.
2) Trafikdata: Data, som behandles med henblik på overførsel af pakkedata.
3) Sikkerhedshændelse: Hændelse, der påvirker tilgængelighed, integritet eller fortrolighed af information eller tjenester på internettet.

§ 4. Som led i driften af den statslige varslingstjeneste for internettrusler behandler, herunder indsamler, registrerer, analyserer og opbevarer, IT- og Telestyrelsen uden retskendelse tilsluttede myndigheders og private virksomheders ind- og udgående pakke- og trafikdata. Pakkedata må dog kun analyseres ved begrundet mistanke om en stedfunden eller forventet sikkerhedshændelse og kun i det omfang, det er nødvendigt for at gennemføre den pågældende analyse.

Stk. 2. Registreret pakke- og trafikdata, som nævnt i stk. 1, slettes, når formålet med behandlingen er opfyldt.

Stk. 3. Uanset, at formålet med behandlingen ikke er opfyldt, kan

pakke- og trafikdata, der knytter sig til en sikkerhedshændelse, højst opbevares i tre år,

pakkedata, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 14 dage, og

trafikdata, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 12 måneder.

Stk. 4. Fristerne i nr. 1-3 regnes fra tidspunktet for registreringen af de pågældende data i den statslige varslingstjeneste.

Stk. 5. Ministeren for videnskab, teknologi og udvikling kan fastsætte nærmere regler for den i stk. 1 nævnte behandling af pakke- og trafikdata.

§ 5. § 35 i lov om behandling af personoplysninger finder ikke anvendelse på den statslige varslingstjeneste for internettruslers behandling af personoplysninger.

Stk. 2. Personer, der virker inden for den statslige varslingstjeneste for internettrusler, har tavshedspligt, jf. straffelovens § 152, jf. § 152 a-e, med hensyn til oplysninger, som de gennem deres virksomhed i varslingstjenesten får kendskab til, jf. dog § 6.

§ 6. Data, der behandles som led i den statslige varslingstjenestes aktiviteter, kan kun videregives i følgende tilfælde:

1) Pakke- og trafikdata, der knytter sig til en sikkerhedshændelse, kan videregives til politiet.
2) Pakkedata, der knytter sig til en sikkerhedshændelse, kan videregives til Forsvarets Efterretningstjenestes militære cert, hvor IT- og Telestyrelsen skønner det nødvendigt for at beskytte nationale digitale infrastrukturer mod sikkerhedsmæssige trusler. Forsvarets Efterretningstjeneste behandler, herunder sletter og opbevarer, disse data i overensstemmelse med bestemmelserne i § 4.
3) Trafikdata kan, hvor dette er nødvendigt i henhold til varslingstjenestens formål og aktiviteter, videregives til danske myndigheder, tilsluttede private virksomheder og tilsvarende varslingstjenester i andre lande.

§ 7. Ministeren for videnskab, teknologi og udvikling nedsætter et uafhængigt tilsyn, der følger den statslige varslingstjeneste for internettruslers virksomhed.

BD000642

Videnskabsministeriet,
IT- og Telestyrelsen, j.nr. 11-106193

Stk. 2. Tilsynet består af en jurist som formand og fire sagkyndige medlemmer. Formanden og medlemmerne beskikkes af ministeren for videnskab, teknologi og udvikling. Ministeren for videnskab, teknologi og udvikling skal ved beskikkelsen af medlemmerne lægge vægt på, at tilsynet samlet repræsenterer juridisk, it-revisionsmæssig og sikkerhedsmæssig sagkundskab.

Stk. 3. Formanden og medlemmerne beskikkes for fire år ad gangen og kan genbeskikkes.

Stk. 4. Ministeren for videnskab, teknologi og udvikling fastsætter nærmere regler for tilsynets virksomhed. Ministeren for videnskab, teknologi og udvikling kan herunder beslutte, at tilsynet skal udarbejde en årsberetning om den statslige varslingstjeneste for internettruslers virksomhed.

Stk. 5. IT- og Telestyrelsen stiller sekretariatsbistand til rådighed for tilsynet.

Stk. 6. Staten afholder alle udgifter ved tilsynets virksomhed.

§ 8. Ministeren for videnskab, teknologi og udvikling kan bemyndige en under ministeriet oprettet statslig myndighed eller efter forhandling med vedkommende minister andre statslige myndigheder til at udøve de beføjelser, der i denne lov er tillagt ministeren for videnskab, teknologi og udvikling.

Stk. 2. Ministeren for videnskab, teknologi og udvikling kan fastsætte regler om adgangen til at påklage afgørelser, der er truffet i henhold til bemyndigelse efter stk. 1, herunder om, at afgørelserne ikke skal kunne påklages.

Stk. 3. Ministeren for videnskab, teknologi og udvikling kan fastsætte regler om udøvelsen af de beføjelser, som en anden statslig myndighed efter forhandling med vedkommende minister bliver bemyndiget til at udøve efter stk. 1.

§ 9. Loven træder i kraft den 1. juli 2011.

§ 10. Loven gælder ikke for Færøerne og Grønland.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning
   - 1.1. Lovforslagets formål
   - 1.2. Lovforslagets baggrund
     - 1.2.1. Baggrund for varslingstjenestens etablering
     - 1.2.2. Internationale erfaringer og anbefalinger
     - 1.2.3. Varslingstjenestens opgaver
2. Gældende ret
3. Lovforslagets indhold
   - 3.1. Tilslutning til varslingstjenesten
   - 3.2. Generelt om adgang til data
   - 3.3. Indsamling og opbevaring af data
   - 3.4. Videregivelse af data
     - 3.4.1. Videregivelse af pakkedata
     - 3.4.2. Videregivelse af trafikdata
   - 3.5. Forholdet til persondataloven
     - 3.5.1. Behandling af personoplysninger
     - 3.5.2. Den registreredes rettigheder
   - 3.6. Forholdet til grundlovens § 72
   - 3.7. Forholdet til den europæiske menneskerettighedskonvention
   - 3.8. Uafhængigt tilsyn
4. De økonomiske og administrative konsekvenser for det offentlige
5. De økonomiske og administrative konsekvenser for erhvervslivet
6. De miljømæssige konsekvenser
7. De administrative konsekvenser for borgerne
8. Forholdet til EU-retten
   - 8.1. Generelle overvejelser
   - 8.2. Persondatadirektivet
   - 8.3. E-databeskyttelsesdirektivet
9. De hørte myndigheder og organisationer mv.
10. Sammenfattende skema

1. Indledning

1.1. Lovforslagets formål

Formålet med dette lovforslag er at tilvejebringe en særskilt lovhjemmel for behandlingen af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler (GovCERT) i IT- og Telestyrelsen.

Lovforslaget vedrører blandt andet behandlingen af de personoplysninger indeholdt i pakke- og trafikdata, som GovCERT indsamler fra de tilsluttede myndigheder og private virksomheder via det såkaldte GovCERT IDS. GovCERT IDS gennemgås nærmere nedenfor under punkt 3.3. Lovforslaget vedrører desuden videregivelse af data, der behandles som led i den statslige varslingstjenestes aktiviteter.

Behandlingen af personoplysninger er nødvendig for, at varslingstjenestens formål kan opfyldes. Som beskrevet med dette lovforslag, er det dog kun i visse specifikke og nærmere afgrænsede tilfælde, at GovCERT vil få adgang til personoplysninger.

GovCERT står for Governmental Computer Emergency Response Team og er en tjeneste, som er etableret indenfor IT- og Telestyrelsens ressort under Ministeriet for Videnskab, Teknologi og Udvikling. Det blev aftalt at etablere GovCERT ved en beslutning truffet af regeringens Økonomiudvalg i maj 2009.

GovCERT er placeret i IT- og Telestyrelsen, idet Ministeriet for Videnskab, Teknologi og Udvikling har ressortansvaret for sager vedrørende it-sikkerhed og tillige varetager koordineringen af it- og teleberedskabet.

GovCERT blev ved udgangen af 2010 fuldt funktionsdygtig. GovCERT kan dog først tilbyde alle påtænkte ydelser over for de tilsluttede myndigheder, når der er tilvejebragt den særskilte hjemmel til GovCERT's behandling af personoplysninger indeholdt i pakke- og trafikdata, som foreslås etableret med dette lovforslag.

GovCERT's ydelser stilles som udgangspunkt til rådighed for statens institutioner.

Det er imidlertid endvidere formålet med lovforslaget, at både kommuner og regioner samt private virksomheder, der

beskæftiger sig med kritisk infrastruktur, efter anmodning kan blive tilsluttet tjenesten.

Kommuner og regioner kan tilslutte sig GovCERT i det omfang, varslingstjenesten har kapacitet hertil. Det er en forudsætning for denne tilslutning, at kommuner og regioner, der vælger at tilslutte sig varslingstjenesten, selv betaler fuldt ud for GovCERT's ydelser i det omfang, kommunernes og regionernes tilslutning ikke er finansieret på anden vis, f.eks. via UMTS-midlerne. UMTS-midlerne er de indtægter, som staten fik ved at sælge rettighederne til 3. generations mobiltelefoni.

Dele af den kritiske nationale infrastruktur, som f.eks. elforsyningen, forestås i dag af private virksomheder. Det samfundsmæssige behov for GovCERT's bistand gør sig også gældende for disse virksomheder. Lovforslaget indeholder derfor hjemmel til, at disse virksomheder også kan tilslutte sig varslingstjenesten.

Ansvaret for den enkelte myndighed eller private virksomheds it-sikkerhed ændres ikke som følge af GovCERT's aktiviteter. Det er således fortsat den enkelte myndighed eller virksomheds ansvar at opretholde et passende niveau for it-sikkerhed. GovCERT vil rådgive og bistå de tilsluttede myndigheder i fornødent omfang, uden at der herved ændres ved den eksisterende ansvarsfordeling.

1.2. Lovforslagets baggrund

1.2.1. Baggrund for varslingstjenestens etablering

Internettet og informationssystemer er blevet en afgørende faktor for den økonomiske og samfundsmæssige udvikling. Internettets og informationssystemernes sikkerhed og fleksibilitet får stadig større betydning for samfundet.

Det er regeringens vision, at Danmark skal være blandt verdens førende højteknologiske samfund. Det kræver, at borgere, virksomheder og det offentlige har adgang til avanceret infrastruktur for informations- og kommunikationsteknologi (ikt) og til effektivt at udnytte de muligheder, der følger med digitaliseringen. Det kræver også, at borgere og virksomheder er trygge ved ikt-anvendelsen og har tillid til tjenester på internettet.

Internettet er blevet en del af den kritiske infrastruktur. En række af de funktioner, som udføres af det offentlige, og som er væsentlige for statens virke, afhænger af internettet.

Det er derfor nødvendigt at sikre, at it-systemernes sikkerhedsniveau er tilstrækkeligt til at opretholde en fortsat drift af de offentlige it-systemer.

Den teknologiske udvikling gør det muligt at iværksætte omfattende elektroniske angreb på den internetbaserede infrastruktur, hvilket kan medføre it-sammenbrud. Sådanne sammenbrud kan få alvorlige konsekvenser for vitale samfundsfunktioner, uanset om de er forårsaget af hændelige uheld eller af bevidste handlinger.

Det er en kendsgerning, at angreb på internettet bliver stadig mere sofistikerede, og at hackere stadig bliver hurtigere til at udnytte de sårbarheder, der løbende opstår på internettet.

Som eksempler på angreb mod nationale digitale infrastrukturer kan nævnes angrebene i henholdsvis Estland i april 2007 og Georgien i august 2008. I begge tilfælde bestod angrebene af meget store mængder internetkommunikation (pakke- og trafikdata) mod vigtige offentlige og private hjemmesider og systemer med den følge, at de ikke længere kunne tilgås, ligesom sikkerhedshuller på hjemmesider blev udnyttet til at udskifte indholdet af disse. Angrebene var primært rettet mod tv-stationer, aviser, ministerier og politiske organisationers hjemmesider og medførte i både Estland og Georgien, at regeringerne fik svækket deres interne kommunikationskanaler samt muligheden for at kommunikere med befolkningen. Angrebene var således rettet mod både statens sikkerhed og pressefriheden.

I Estland blev angreb også rettet mod finansinstitutioners hjemmesider med en række alvorlige følger for finanssektoren. En større del af befolkningen kunne således ikke via internettet hæve penge eller udføre finansielle transaktioner i flere dage. Kreditkortterminaler, som kommunikerer med bankerne via internettet, blev også ramt.

Disse eksempler understreger, at et moderne samfund er afhængig af et robust internet.

I erkendelse af internettets vitale betydning besluttede regeringen således i maj 2009 at etablere en statslig varslingstjeneste for internettrusler.

Offentlige myndigheder kommunikerer i dag i høj grad via internettet med borgere og virksomheder. Med oprettelsen af GovCERT ønsker regeringen bl.a. at mindske risikoen for it-angreb, herunder at offentlige myndigheders elektroniske kommunikation med omverdenen bliver afskåret i flere dage, eller at dokumenter uden myndighedens vidende bliver sendt til fremmede stater som følge af et virusangreb. Dette kan udgøre en sikkerhedsrisiko og også have store administrative og økonomiske konsekvenser til følge. Tilsvarende gør sig gældende for private virksomheder beskæftiget med kritisk infrastruktur.

Formålet med GovCERT er således at være en varslingstjeneste for internettrusler, og herved overordnet medvirke til, at der i staten er overblik over trusler og sårbarheder i tjenester, net og systemer relateret til internettet.

GovCERT samarbejder blandt andet med DK-CERT og andre landes nationale CERT'er. DK-CERT (Danish Computer Emergency Response Team) er en tjeneste fra styrelsen UNI-C under Undervisningsministeriet. DK-CERT fungerer som CERT for Forskningsnettet og UNI-C's interne net. GovCERT vil endvidere samarbejde med MILCERT, der er Forsvarsministeriets CERT, som er under opbygning.

GovCERT indgår i IT- og Telestyrelsens sektorberedskab. Beredskabet har til formål at sikre, at samfundsvigtig elektronisk kommunikation kan opretholdes i en beredskabssituation.

1.2.2. Internationale erfaringer og anbefalinger

Internationalt er det erkendt, at det er af stor betydning at reducere de risici, der er forbundet med anvendelsen af internettet. En række europæiske lande har således etableret var-

slingstjenester, som varetager overvågnings- og varslingsopgaver for det statslige område.

Varslingstjenester i de øvrige europæiske lande er typisk karakteriseret ved, at de er statsligt ejet og drevet, og at målgruppen for deres virke er hele staten. Der er dog nationale forskelle på den organisatoriske placering. Hovedparten af varslingstjenesterne er placeret hos civile myndigheder, og der er etableret et tæt samarbejde med sikkerhedsmyndighederne i de pågældende lande. Nedenfor nævnes en række eksempler på udenlandske varslingstjenester.

I Norge blev der i 2000 etableret et Varslingssystem for Digital Infrastruktur (VDI). VDI organiserer og driver et nationalt netværk af indbrudsdetektionssensorer på internettet, som detekterer, om der forsøges udført uønsket aktivitet mod kritisk digital infrastruktur i Norge. VDI omfatter ikke kun de offentlige institutioner, men også en række for samfundet kritiske private virksomheder.

I Sverige er der tilsvarende etableret en national GovCERT, og det er efter norsk forbillede yderligere besluttet at undersøge mulighederne for at udbygge og samordne de eksisterende varslingssystemer.

I Frankrig er GovCERT funktionen varetaget af CERTA, som er en del af det franske militære og civile sikkerhedssystem. CERTA er ansvarlig for at bistå de franske statslige organer med at sikre, at den fornødne informationssikkerhed er til stede, samt hjælpe med at behandle sikkerhedshændelser eller angreb mod statens it-systemer.

Behovet for beskyttelse af it-infrastrukturen berøres i EU-Kommissionens meddelelse *»Beskyttelse mod storstilede cyberangreb og sammenbrud: Øget beredskab, sikkerhed og robusthed«* fra 30. marts 2009. Meddelelsen bygger videre på EU's ambition om at styrke sikkerhed i og tilliden til informationssamfundet. Kommissionen fremhæver i meddelelsen særligt strategien for et sikkert informationssamfund fra 2006.

I meddelelsen lægger Kommissionen vægt på forebyggelse, beredskab og bevidstgørelse og opstiller en plan over øjeblikkelige tiltag, der skal styrke sikkerheden og robustheden i kritisk informationsinfrastruktur. Et af disse tiltag er etablering af velfungerende statslige varslingstjenester i alle medlemslande inden udgangen af 2011.

1.2.3. Varslingstjenestens opgaver

GovCERT vurderer løbende it-sikkerheden for statens anvendelse af internettet og varsler myndigheder om internetbaserede sikkerhedshændelser og trusler. Varslingstjenesten vil også tilbyde bistand med at imødegå konsekvenserne af sikkerhedshændelserne.

I fuld drift vil GovCERT desuden kunne tilbyde en række ydelser, som samlet set sikrer, at der kan reageres hurtigt og effektivt over for trusler mod it-sikkerheden i primært den danske stat. GovCERT vil således i høj grad kunne medvirke til at begrænse, afkorte og i visse tilfælde forhindre nedbrud i it-infrastrukturen.

GovCERT's ydelser kan overordnet opdeles i to hovedgrupper: Ydelser, der tilbydes med henblik på at forebygge alvorlige internetrelaterede sikkerhedshændelser, og ydelser, som tilbydes, efter en hændelse er indtruffet. Ydelserne er aftalt i en fokusgruppe bestående af Statens It, Udenrigsministeriet og SKAT. Ydelseskataloget har endvidere været forelagt Statens It-sikkerhedsforum, Statens It-forum og Statens It-råd.

GovCERT's konkrete opgaver kan opsummeres således:

– Indhentning af information om sikkerhedshændelser og aktiviteter i net og systemer i staten.
– Analyse og vurdering af internetsikkerhedsniveauet i staten samt analyse af enkelthændelser.
– Varsling om internetrelaterede sikkerhedshændelser, rådgivning om modforholdsregler og i særlige tilfælde bistand til myndigheder ved omfattende hændelser.
– Kontaktpunkt for tilsvarende varslingstjenester i andre lande og løbende udveksling af information med disse.

GovCERT's opgaver vedrørende varsling og informationsindsamling forudsætter et opdateret og indgående kendskab til situationen på internettet og især den trafik, som er på den danske del af internettet. Dette kendskab tilegnes gennem analyse af pakke- og trafikdata for virus- og hackerangreb.

Det er derfor nødvendigt at etablere et alarmsystem i form af et såkaldt Intrusion Detection System (GovCERT IDS) på tilsluttede institutioners internetlinjer. IDS-tjenesten er et tilbud til institutionerne, som er tilsluttet GovCERT. GovCERT IDS er yderligere beskrevet i afsnit 3.3.

Da GovCERT vil få kendskab til oplysninger om sårbarheder i it-systemer i staten, er det nødvendigt, at GovCERT klassificerer informationerne i henhold til Statsministeriets sikkerhedscirkulære (cirkulære nr. 204 af 7. december 2001). GovCERT's lokaler og personale er godkendt til at håndtere informationer klassificeret under cirkulæret til niveauet HEMMELIG.

2. Gældende ret

Lov om behandling af personoplysninger (persondataloven) gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling.

Begreberne »personoplysning« og »behandling« er defineret i persondataloven og skal i dette lovforslag forstås i overensstemmelse hermed.

Persondataloven indeholder en række grundlæggende principper for den dataansvarliges behandling af oplysninger, herunder regler om indsamling, ajourføring og opbevaring mv.

Den registreredes rettigheder er tillige reguleret i persondataloven, herunder ret til information om, at der indsamles oplysninger om den pågældende.

Persondataloven vedrører desuden fortrolighed og datasikkerhed. Den dataansvarlige skal bl.a. iværksætte de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Relevante sikkerhedstiltag kan f.eks. være fysisk sikring af datamedier, adgangskontrol og brug af password samt uddannelse og instruktion.

For offentlige myndigheders behandling af personoplysninger gælder både persondatalovens regler om datasikkerhed og den i medfør heraf udstedte sikkerhedsbekendtgørelse, jf. bekendtgørelse nr. 528 af 15. juni 2000 med senere ændringer om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

Der henvises til afsnit 3.5 om forholdet til persondataloven.

3. Lovforslagets indhold

3.1. Tilslutning til varslingstjenesten

GovCERT bygger på, at først og fremmest statslige myndigheder vurderer, om myndigheden ønsker at tilslutte sig GovCERT. Lovforslaget lægger endvidere op til at kommunale og regionale myndigheder samt private virksomheder beskæftiget med kritisk infrastruktur efter anmodning vil kunne tilslutte sig.

3.2. Generelt om adgang til data

Lovforslaget medfører, at GovCERT i et nærmere beskrevet omfang får adgang til både trafikdata og pakkedata. Det er ikke tilstrækkeligt til opfyldelse af GovCERT's formål kun at give GovCERT adgang til trafikdata, men der skal imidlertid være den fornødne proportionalitet mellem adgangen til data, herunder personoplysninger, og hensynet til privatlivets fred. Denne proportionalitetsafvejning er afspejlet i lovforslagets § 4 og uddybes nedenfor.

GovCERT IDS, som etableres som led i GovCERT's virke, holder via en lokal elektronisk alarmenhed opsat hos de tilsluttede offentlige myndigheder øje med internetkommunikationen (pakke- og trafikdata). Alarmenheden registrer al ind- og udgående internetkommunikation. Enheden sender dog kun pakkedata til GovCERT, hvis der er tegn på en sikkerhedshændelse. Trafikdata vil løbende blive overført til GovCERT. GovCERT IDS er yderligere beskrevet under afsnit 3.3.

Hvis GovCERT kun har adgang til at behandle trafikdata, vil blot mulige tegn på it-angreb kunne identificeres. Adgang til pakkedata muliggør derimod en nærmere analyse og beskrivelse af angrebets indhold og karakter, og de relevante modforanstaltninger kan dermed identificeres.

For at GovCERT skal kunne få overblik over sikkerheden på internettet og være i stand til at varsle om it-angreb, er det nødvendigt at have adgang til de pakkedata, som er relateret til den pågældende sikkerhedshændelse. 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 hackeren. Skadens omfang kan herefter fastslås, og de relevante modforanstaltninger kan besluttes.

Som eksempel på en relevant sikkerhedshændelse kan nævnes, 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 PC 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 for den berørte myndighed af et vellykket it-angreb.

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 dermed nødvendigt og proportionalt at give GovCERT adgang til pakkedata. Det skal herefter vurderes, i hvilket omfang GovCERT skal have adgang til pakkedata. Der er med dette lovforslag lagt op til, at pakke- og trafikdata, som knytter sig til en sikkerhedshændelse, kan opbevares i tre år. Pakkedata, der ikke er knyttet til en sikkerhedshændelse, kan højst opbevares i 14 kalenderdage. Som udgangspunkt vil pakkedata dog kun blive opbevaret i seks kalenderdage. Trafikdata, som ikke knytter sig til en sikkerhedshændelse, kan højst opbevares i 12 måneder.

Fristerne i lovforslagets § 4 er fastlagt på baggrund af en it-teknisk vurdering af det nødvendige behov i forhold til GovCERT's formål. I forbindelse med denne vurdering er erfaringer fra andre landes CERT'er inddraget. Fristen på tre år for opbevaring af pakke- og trafikdata knyttet til en sikkerhedshændelse er valgt for at kunne sammenholde angreb med tidligere angreb inden for en teknologisk relevant periode, da der fortsat ses angreb rettet mod sårbarheder eller konfigurationsfejl, der er flere år gamle. Tre år betragtes som den teknologiske levealder for mange it-systemer, hvorefter systemerne må udfases eller gennemgribende opdateres.

Det er væsentligt at være opmærksom på, at fristerne alle er maksimumfrister. GovCERT vil løbende være forpligtet til at slette data, som ikke længere er relevante for GovCERT's virke, uanset at fristerne beskrevet i § 4 ikke er overskredet. Derudover er det i § 4 fastsat, at indsamlede pakkedata kun vil kunne analyseres af GovCERT, hvis der er begrundet mistanke om en sikkerhedshændelse. Det er desuden fastsat i § 4, at det kun er den relevante del af de indsamlede data, som kan analyseres.

Det er i bestemmelsen kvalificeret, at der skal være tale om en begrundet mistanke, for at GovCERT kan få adgang til pakkedata. Formålet hermed er at præcisere, at adgangen til pakkedata er begrænset til de situationer, hvor der ikke blot er tale om en vag og udefineret mistanke om et it-angreb. Det vil kun være i situationer, hvor der er en klar indikation på et it-angreb, at GovCERT vil kunne behandle pakkedata. Denne vurdering vil dog være skønsmæssig fra situation til situation.

Det er med GovCERT IDS pt. ikke muligt at foretage en teknisk graduering af adgangen til pakkedata på en sådan måde, at der f.eks. kun gives adgang til visse dele af indholdet af en e-mail. Der kan kun skelnes mellem adgang til pakkedata eller adgang til trafikdata. GovCERT vil tæt følge mulighederne for at finde en teknisk løsning på denne udfordring.

Længden af fristerne i § 4 er fastsat på baggrund af en proportionalitetsafvejning af hensynet til GovCERT's formål set i forhold til hensynet til privatlivets fred. Det er i visse situationer væsentligt for GovCERT at kunne sammenholde ny-

indsamlede data med ældre data for f.eks. at kunne analysere et it-angreb nærmere. Heroverfor står hensynet til de berørte borgeres privatliv. Denne proportionalitetsafvejning har resulteret i de nævnte frister, som også er fastsat under inddragelse af erfaringer fra andre landes CERT'er.

3.3. Indsamling og opbevaring af data

GovCERT skal for at opfylde sit formål indhente data vedrørende sikkerhedshændelser og aktiviteter i net og systemer hos de tilsluttede myndigheder og private virksomheder, ligesom GovCERT skal varsle ved internetrelaterede sikkerhedshændelser samt generelt vurdere sikkerhedsniveauet på internettet. Der skal endvidere udarbejdes risikoanalyser. GovCERT får herved et løbende og indgående kendskab til sikkerhedssituationen på den danske del af internettet.

Forudsætningen for at kunne tilegne sig dette indgående kendskab er, at internetkommunikationen behandles og analyseres for eventuelle virus- og hackerangreb i de enkeltdele, som internetkommunikationen nedbrydes i ved datatransmissionen. En e-mail kan bestå af alt fra nogle ganske få til flere tusinde enkeltdele afhængig af e-mailens størrelse.

Databehandlingen består eksempelvis af en automatisk scanning af internetkommunikationen efter it-angreb baseret på en angrebssignatur fra kendte it-angreb, og af en manuel vurdering af mulige angrebskarakteristika ved begrundet mistanke om it-angreb.

Det er med henblik på denne behandling af internetkommunikationen, at varslingstjenestens Intrusion Detection System (GovCERT IDS) er etableret. GovCERT IDS behandler myndighedernes ind- og udgående internetkommunikation (pakke- og trafikdata).

GovCERT IDS består bl.a. af decentrale IDS-enheder, som placeres på de tilsluttede myndigheders internetforbindelse(r). Disse enheder analyserer pakke- og trafikdata for angrebsmønstre på internetforbindelsen og lagrer pakke- og trafikdata i en nærmere afgrænset periode, jf. lovforslagets § 4 og nedenfor.

Herudover omfatter GovCERT IDS centrale servere hos GovCERT, som anvendes til at lagring og analyse af pakke- og trafikdata.

Med etableringen af GovCERT IDS vil varslingstjenesten have mulighed for løbende at analysere netværkstrafikken mellem de tilsluttede myndigheder og internettet og herigennem danne sig et normalbillede, hvilket er centralt for GovCERT's virke.

Normalbilledet defineres af GovCERT på grundlag af indsamling af oplysninger i GovCERT IDS og består eksempelvis af en oversigt over, hvilke ip-adresser der typisk kommunikeres med, på hvilket tidspunkt, og i hvilket omfang. Hvis der pludselig sker væsentlige ændringer i normalbilledet, som ikke kan begrundes med særlige aktiviteter hos myndigheden selv, vil der være tale om en formodet sikkerhedshændelse. I det tilfælde vil GovCERT kunne gennemføre tilbundsgående tekniske analyser af pakke- og trafikdata, herunder spore hvorfra eventuel anormal trafik udgår og vurdere, om hensigten med dette må formodes at være fjendtlig. Et eksempel på unormal trafik kan være, at en myndighed uden for normal arbejdstid transmitterer store mængder data til en ip-adresse, hvortil der ikke plejer at være særlig aktivitet.

De oplysninger, som GovCERT behandler, kan betegnes som pakke- og trafikdata. Ved konstatering af bestemte trafikmønstre i pakke- og trafikdata vil GovCERT IDS generere en alarm, som bliver sendt til GovCERT.

Pakkedata vil blive slettet umiddelbart efter GovCERT's analyse, hvis denne ikke viser tegn på en sikkerhedshændelse. Analyseret pakkedata vil således kun blive opbevaret i GovCERT's system til at registrere sikkerhedshændelser, hvis data er knyttet til en sikkerhedshændelse.

De maksimale frister for opbevaring af pakke- og trafikdata og baggrunden for fristernes længde er beskrevet i afsnit 3.2. ovenfor.

Det følger af persondataloven, at de oplysninger, som GovCERT indsamler, ikke må opbevares, på en måde der giver mulighed for at identificere den registrerede, i et længere tidsrum end det, der er nødvendigt af hensyn til formålet med oplysningernes behandling. Persondataloven har således den konsekvens i forhold til de omtalte tidsfrister for sletning af indsamlede oplysninger, at GovCERT er forpligtet til at slette oplysningerne på et tidligere tidspunkt, hvis varslingstjenestens formål ikke længere gør opbevaringen nødvendig. Se yderligere om lovforslagets forhold til persondataloven i afsnit 3.5.

GovCERT IDS indsamler automatisk internetkommunikationen fra de tilsluttede myndigheder og private virksomheder. GovCERT skal således ikke ved denne behandling af data opfylde de af persondatalovens regler, der kun vedrører den form for behandling af personoplysninger, der beskrives som videregivelse. Se i øvrigt om GovCERT's videregivelse af indsamlede data i afsnit 3.4. nedenfor.

GovCERT bygger på en forudsætning om, at der ikke kan eller vil blive indhentet samtykke til GovCERT's behandling af personoplysninger, idet GovCERT's indsamling af bl.a. personoplysninger som nævnt sker automatisk, og det vil dermed i praksis være umuligt at indhente samtykke til behandlingen.

3.4. Videregivelse af data

3.4.1. Videregivelse af pakkedata

Det følger af den foreslåede bestemmelse i § 6, at den statslige varslingstjeneste kan videregive pakkedata og trafikdata, der knytter sig til en sikkerhedshændelse, til dansk politi. Formålet hermed er at sikre, at dansk politi kan modtage oplysninger til brug for efterforskning og forfølgelse af strafbare forhold, der kan være begået i forbindelse med en sikkerhedshændelse, som f.eks. et virusangreb. Ligeledes kan GovCERT videregive pakkedata til den særlige MILCERT, som er under etablering i regi af Forsvarets Efterretningstjeneste, og som er en varslingstjeneste svarende til GovCERT på Forsvarsministeriets område.

Adgangen til at videregive pakkedata er begrænset mest muligt på baggrund af hensynet til privatlivets fred. GovCERT

vil således ikke kunne videregive pakkedata i andre tilfælde end de i § 6 nævnte, jf. herved nærmere de specielle bemærkninger vedrørende lovforslagets § 6.

3.4.2. Videregivelse af trafikdata

GovCERT har behov for en bredere adgang til at udveksle, herunder videregive, trafikdata, som f.eks. ip-adresser, til andre myndigheder og tilsluttede private virksomheder ved varsling eller i tilfælde af sikkerhedshændelser. Videregivelsen skal sikre, at myndighederne og de pågældende virksomheder kan iværksætte lokale modforanstaltninger over for sikkerhedshændelsen. Det kan f.eks. være blokering af kommunikation med en specifik ip-adresse.

GovCERT vil endvidere have behov for at videregive ip-adresser og anden trafikdata til tilsvarende varslingstjenester i andre lande i forbindelse med sikkerhedshændelser på internettet. Derved kan en CERT i et andet land f.eks. anmode den lokale internetudbyder om nedtagning af den angribende ip-adresse. Tilsvarende er det vigtigt, at GovCERT modtager trafikdata fra udenlandske CERT'er til forebyggelse af et it-angreb.

International koordination af forsvar mod elektroniske angreb i form af udveksling af ip-adresser og anden trafikdata er således væsentligt for GovCERT's aktiviteter.

3.5. Forholdet til persondataloven

3.5.1. Behandling af personoplysninger

Formålet med GovCERT er ikke at behandle personoplysninger, men GovCERT vil uundgåeligt skulle behandle personoplysninger indeholdt i pakke- og trafikdata i forbindelse med sine aktiviteter.

I relation til dette lovforslag er det særligt relevant at bemærke, at ip-adresser betragtes som personoplysninger, hvorfor persondataloven finder anvendelse på behandling af trafikdata, idet trafikdata omfatter ip-adresser, jf. bemærkningerne til lovforslagets § 3, nr. 2.

Det er nødvendigt, for at GovCERT kan danne det for varslingsopgaven centrale normalbillede for internetkommunikationen (pakke- og trafikdata), at al ind- og udgående internetkommunikation fra en tilsluttet myndighed indsamles.

Visse af de personoplysninger, som GovCERT behandler, vil uundgåeligt indeholde både almindelige, ikke-følsomme oplysninger (persondatalovens § 6), og følsomme personoplysninger (§§ 7 og 8). Disse oplysninger kan forekomme f.eks. i ukrypterede e-mails fra borgere til ansatte i de tilsluttede myndigheder.

GovCERT's behandling af personoplysningerne skal opfylde persondatalovens § 5, der indeholder en række grundlæggende principper for den behandling af personoplysninger, som den dataansvarlige – her GovCERT – foretager.

Kravet om god databehandlingsskik i persondatalovens § 5, stk. 1, indebærer, at medarbejderne hos de myndigheder, som bliver omfattet af GovCERT's behandlinger, skal have klar og tydelig forudgående information om, at al brug af internettet, herunder e-mails, vil blive behandlet, herunder eventuelt gennemset og opbevaret med de formål, som varetages af GovCERT.

I forhold til saglighedskravet i persondatalovens § 5, stk. 2, vil det eksempelvis være i strid med bestemmelsen, hvis GovCERT's personale i forbindelse med den beskrevne analyse af internetkommunikationen behandler personoplysninger, uden at det sker i forbindelse med forfølgelsen af det saglige formål med bl.a. at begrænse og varsle om hacker- og virusangreb. GovCERT skal således sikre, at behandlingen af personoplysninger ikke sker i videre omfang end dette formål tilsiger.

Vedrørende kravet i persondatalovens § 5, stk. 2, om formålsbestemthed bemærkes, at den foreslåede ordning netop går ud på (alene) at give GovCERT adgang til at udføre varslingsopgaven bl.a. med henblik på at begrænse hacker- og virusangreb.

GovCERT skal i forhold til persondatalovens § 5 dermed nøje overveje, hvorvidt en senere brug af de behandlede oplysninger er uforenelig med det oprindelige formål med indsamlingen af oplysningerne.

Disse overvejelser har resulteret i lovforslagets § 6, hvorefter der kun kan ske videregivelse af data, der er indsamlet som led i GovCERT's aktiviteter og kun i henhold til GovCERT's formål. Pakkedata vil kunne videregives til dansk politi og kun, hvis data knytter sig til en sikkerhedshændelse. Pakkedata vil yderligere kunne videregives til Forsvarets Efterretningstjeneste til brug for aktiviteter i forbindelse med den særlige MILCERT, som har tilsvarende funktion og formål, som GovCERT, på Forsvarsministeriets område. På samme måde, som GovCERT sikrer statslige institutioners internetkommunikation, sikrer MILCERT Forsvarsministeriets internetkommunikation.

Både GovCERT og MILCERT indgår i det samlede danske beredskab og i tilfælde af et alvorligt it-angreb, skal MILCERT og GovCERT kunne dele ressourcer for at sikre en hurtig imødegåelse af angrebet. DK-CERT er ikke en del af det danske beredskab og har derfor ikke samme behov for at kunne udveksle pakkedata.

Pakkedata vil ikke kunne videregives i andre tilfælde end de ovenfor nævnte.

Derudover indebærer lovforslagets § 6, nr. 3, at GovCERT som led i aktiviteterne skal have mulighed for at overføre trafikdata til danske myndigheder, tilsluttede private virksomheder og tilsvarende varslingstjenester i andre lande i henhold til varslingstjenestens formål og aktiviteter. Her er overførselsmuligheden således begrænset til trafikdata, hvorfor f.eks. indholdet af e-mails ikke vil kunne overføres.

Persondatalovens § 27 regulerer overførsel af oplysninger til tredjelande. Med lovforslaget sikres det, at der i alle nødvendige tilfælde kan videregives oplysninger om trafikdata til tredjelandene. GovCERT kan ikke videregive indholdet af en internetkommunikation (pakkedata), herunder indholdet af en e-mail til tredjelande.

Der henvises i øvrigt til de specielle bemærkninger nedenfor vedrørende lovforslagets § 6.

I forhold til persondatalovens § 5, stk. 3, og spørgsmålet om proportionalitet, indebærer bestemmelsen, at GovCERT's aktiviteter skal gennemføres på en sådan måde, at de virker mindst muligt integritetskrænkende for den almindelige borger, således at det i videst muligt omfang undgås, at personoplysninger behandles, herunder ikke mindst, at indholdet af e-mails ikke behandles.

Ud over de generelle betingelser i persondatalovens § 5 skal betingelserne i persondatalovens §§ 6-8 være opfyldt.

Det er et krav i disse bestemmelser, at behandling (uden samtykke) skal være nødvendig. Der er i den forbindelse overladt den dataansvarlige et vist skøn. Denne vurdering skal i første omgang foretages af IT- og Telestyrelsen som dataansvarlig myndighed.

Selve den beskrevne indsamling af al ind- og udgående internetkommunikation og de deri indeholdte personoplysninger vil have den fornødne hjemmel i persondatalovens §§ 6-8. Der findes således i persondatalovens § 6, stk. 1, § 7, stk. 2, og § 8, stk. 1 og 6, mulighed for, at en offentlig myndighed som IT- og Telestyrelsen (GovCERT) kan behandle personoplysninger uden samtykke fra de registrerede.

Jo mere indgribende den efterfølgende behandling af personoplysningerne kan siges at være, desto strengere krav stilles der til opfyldelsen af det nødvendighedskrav, der ligger i persondatalovens §§ 6-8 og til opfyldelsen af de beskrevne principper i § 5.

GovCERT vil skulle vurdere opfyldelsen af disse regler løbende i det daglige arbejde. GovCERT vil således kun kunne behandle og eventuelt nærmere analysere en e-mailkorrespondance, når det er nødvendigt af hensyn til opfyldelsen af varslingsopgaven, herunder håndteringen af hackerangreb.

Til gengæld vurderes det, at der i disse undtagelsesvise situationer, hvor f.eks. et hackerangreb skal håndteres, vil være hjemmel til den behandling af personoplysninger, som opgaven nødvendigvis medfører, inden for rammerne af persondatalovens behandlingsregler.

Der er i øvrigt ingen grund til at antage, at vurderingen af nødvendigheden og proportionaliteten i forbindelse med GovCERT's behandling af personoplysninger efter persondatalovens §§ 5-8 vil falde anderledes ud efter persondataloven end den tilsvarende vurdering, som foretages nedenfor i afsnit 3.7 vedrørende forholdet til Den Europæiske Menneskerettighedskonventions artikel 8.

Disse regler i persondataloven er i forhold til GovCERT's aktiviteter afspejlet i lovforslagets § 4, stk. 1.

Sammenfattende er det således muligt for IT- og Telestyrelsen (GovCERT) som dataansvarlig i forbindelse med udøvelsen af aktiviteterne at sikre, at beskyttelsen i persondatalovens § 5-8 også respekteres.

3.5.2. Den registreredes rettigheder

I forhold til persondatalovens kapitel 8 om den dataansvarliges oplysningspligt over for den registrerede bemærkes, at GovCERT's indsamling af oplysninger – i lighed med det for tv-overvågning gældende – skal anses for at være foretaget hos andre end den registrerede, jf. persondatalovens § 29, stk. 1.

Der påhviler derfor som udgangspunkt IT- og Telestyrelsen som dataansvarlig en oplysningspligt over for de registrerede efter persondatalovens § 29, stk. 1, men der kan – af relevans for GovCERT's aktiviteter - gøres undtagelse herfra, hvis opfyldelse af oplysningspligten er umulig eller uforholdsmæssig vanskelig jf. persondatalovens § 29, stk. 3.

For så vidt angår indsigtsretten efter persondatalovens § 31 bemærkes, at der kan gøres undtagelse herfra i samme omfang som efter reglerne i bl.a. offentlighedslovens § 14, jf. persondatalovens § 32, stk. 2. Det fremgår af offentlighedslovens § 14, at pligten til at meddele oplysninger er begrænset af særlige bestemmelser om tavshedspligt fastsat ved lov eller med hjemmel i lov for personer, der virker i offentlig tjeneste eller hverv.

Som følge af den særlige bestemmelse om tavshedspligt, som pålægges GovCERT's personale ved lovforslagets § 5, stk. 2, i overensstemmelse med offentlighedslovens § 14, er de personoplysninger, som GovCERT behandler i forbindelse med sit virke, undtaget fra indsigtsretten jf. persondatalovens § 32, stk. 2.

I forhold til retten til at gøre indsigelse, jf. persondatalovens § 35, åbner persondatadirektivets artikel 14, stk. 1, litra a, mulighed for, at det kan bestemmes ved lov, at indsigelsesretten afskæres. På den baggrund er der indsat en undtagelsesbestemmelse i lovforslaget, som lægger op til, at persondatalovens § 35 ikke skal finde anvendelse på GovCERT's aktiviteter. Dette medfører, at registrerede ikke vil kunne gøre indsigelse over for GovCERT's behandling af personoplysninger.

En registreret kan dog fortsat klage til Datatilsynet over GovCERT's behandling af personoplysninger vedrørende den pågældende, jf. persondatalovens § 40 og kapitel 16.

3.6. Forholdet til grundlovens § 72

Grundlovens § 72 har følgende ordlyd: "Boligen er ukrænkelig. Husundersøgelse, beslaglæggelse og undersøgelse af breve og andre papirer samt brud på post-, telegraf- og telefonhemmeligheden må, hvor ingen lov hjemler en særegen undtagelse, alene ske efter en retskendelse. "

Det antages i den juridiske litteratur, at indholdet af e-mails også er omfattet af grundlovens beskyttelse af meddelelseshemmeligheden (brud på post-, telegraf- og telefonhemmeligheden). En myndigheds brud på meddelelseshemmeligheden forudsætter uden for strafferetsplejens område som udgangspunkt dels en udtrykkelig lovhjemmel og dels en forudgående retskendelse i det konkrete tilfælde, med mindre der også foreligger en udtrykkelig lovhjemmel til at undtage kravet om retskendelse. Retskendelse behøves heller ikke i situationer, hvor den, som foranstaltningen vedrører, giver samtykke til, at undersøgelsen bliver foretaget.

Den foreslåede ordning går ud på, at GovCERT skal behandle, herunder efter omstændighederne analysere, tilsluttede myndigheders og private virksomheders ind- og udgående trafik- og pakkedata. GovCERT skal i den forbindelse i et vist

omfang have ret til at skaffe sig adgang til pakkedata, eksempelvis indholdet af e-mails.

Ordningen efter lovforslaget vil uundgåeligt i visse tilfælde indebære et indgreb i meddelelseshemmeligheden i grundlovens forstand. Der vil dog i vidt omfang foreligge et samtykke, som indebærer, at det ikke vil være nødvendigt at indhente retskendelse efter grundlovens § 72. Der vil imidlertid også forekomme tilfælde, hvor et sådant samtykke ikke foreligger, og eftersom det i praksis ikke vil være muligt at indhente en retskendelse, indeholder lovforslaget på den baggrund en undtagelse fra grundlovens § 72's krav herom.

Videnskabsministeriet har bl.a. af hensyn til grundlovens § 72 overvejet nødvendigheden og proportionaliteten af den foreslåede ordning. Der henvises i den forbindelse til bemærkningerne ovenfor under afsnit 3.2, hvoraf det fremgår, at der med lovforslaget er fundet den påkrævede proportionalitet mellem hensynet til GovCERT's formål og hensynet til privatlivets fred for de berørte borgere.

3.7. Forholdet til Den Europæiske Menneskeretskonvention

Ifølge artikel 8, stk. 1, i Den Europæiske Menneskerettighedskonvention (EMRK) har enhver ret til respekt for sit privatliv og familieliv.

Beskyttelsen efter artikel 8 omfatter både indgreb i meddelelseshemmeligheden, f.eks. overvågning af e-mailkorrespondance og internetkommunikation, og offentlige myndigheders indsamling, opbevaring og anvendelse mv. af personoplysninger generelt.

Indgreb i kommunikation via bl.a. e-mails vil som udgangspunkt udgøre et indgreb efter EMRK artikel 8. Hvis en offentlig arbejdsgiver overvåger en ansats brug af e-mail og internet, vil det således udgøre et indgreb i den ansattes ret til privatliv og korrespondance, når den ansatte med rimelighed kunne forvente ikke at blive overvåget (se Copland mod Storbritannien, dom af 3. april 2007, præmis 41-42).

Det samme vil være tilfældet, hvor en arbejdsgiver tillader en (anden) myndighed at overvåge den ansattes brug af e-mail og internet.

Det forudsættes imidlertid, at den ansatte i forbindelse med afsendelse af privat e-mail giver samtykke til GovCERT-behandlingen. Når det er op til myndighedens personalepolitik, om medarbejderne må sende eller modtage privat e-mail, må myndigheden således også kunne fastsætte, at medarbejderne kun må sende privat e-mail mod at samtykke til GovCERT-behandlingen. Det antages på den baggrund, at iværksættelsen af overvågningen af udgående e-mails med privat indhold ikke i sig selv vil udgøre et indgreb i rettighederne efter EMRK artikel 8.

For så vidt angår indgående private e-mails samt offentlige myndigheders indsamling, opbevaring og anvendelse mv. af personoplysninger vil der derimod være tale om et indgreb i borgernes ret til privatliv.

Da det som følge af den ovenfor beskrevne tekniske opbygning af GovCERT ikke kan udelukkes, at GovCERT vil behandle personoplysninger om en persons privatliv, må aktiviteterne anses for et indgreb i retten til respekt for privatlivet, jf. konventionens artikel 8, stk. 1.

Det følger herefter af konventionens artikel 8, stk. 2, at et sådant indgreb kun kan foretages, hvis det er foreskrevet ved lov og er nødvendigt i et demokratisk samfund til varetagelse af nærmere bestemte anerkendelsesværdige formål.

Med den foreslåede lov vil der blive klar lovhjemmel for GovCERT's aktiviteter, som bygger på en legitim og helt åbenlys samfundsmæssig interesse i at håndtere sikkerhedshændelser af it-mæssig karakter for offentlige myndigheder i Danmark.

Indgrebet i privatlivet skal herudover efter artikel 8, stk. 2, have et sagligt formål og være proportionalt.

GovCERT har til formål at mindske konsekvenserne af sikkerhedshændelser på internettet gennem analyse, information, varsling og koordination. GovCERT's aktiviteter tilsigter således at beskytte den nationale sikkerhed, den offentlige tryghed og landets økonomiske velfærd samt andres rettigheder og friheder. Formålet må således anses for sagligt.

IT- og Telestyrelsens rapport om varsling af internettrusler fra 2007 konkluderede, at der i Danmark er behov for en særskilt tjeneste til at håndtere sådanne sikkerhedshændelser for det danske samfund som et led i den nationale it-sikkerhedsstrategi. Den varslingsopgave mv., som er tiltænkt GovCERT, må således siges at være både egnet til og nødvendig for at nå det beskrevne saglige mål om at forhindre hacker- og virusangreb mv.

Der kan i den forbindelse også henvises til den nedenfor i afsnit 8.1 beskrevne meddelelse fra EU-Kommissionen og resolution fra Europarådet om, at oprettelsen af statslige it-beredskabsenheder (»GovCERT'er«) er en måde, hvorpå medlemsstaterne kan løse de notoriske trusler mod staternes it-sikkerhed.

Den samfundsmæssige interesse i at forhindre og håndtere sikkerhedshændelser af it-mæssig karakter for offentlige myndigheder i Danmark må således anses at overstige hensynet til privatlivet for de personer, om hvilke GovCERT behandler personoplysninger. Aktiviteterne er endvidere begrænset til de tilsluttede myndigheder og virksomheders ind- og udgående data.

GovCERT's formål er som nævnt ikke i sig selv at indsamle personoplysninger. Indsamlingen er i stedet en uundgåelig konsekvens af varslingsopgaven. GovCERT vil i øvrigt kun opbevare oplysningerne, så længe opbevaringen er nødvendig i forhold til varslingsopgaven.

Personoplysningerne vil derudover heller ikke blive offentliggjort; tværtimod er opbevaringen af oplysningerne underlagt strenge sikkerhedsforanstaltninger, så bl.a. offentliggørelse undgås.

Hertil kommer, at GovCERT efter lovforslagets § 7 i supplement til Datatilsynets kontrol vil blive underlagt kontrol af et uafhængigt tilsyn.

Sammenfattende er det opfattelsen, at den behandling af personoplysninger, som er en nødvendig del af GovCERT's

aktiviteter, vil opfylde betingelserne i artikel 8, stk. 2, i Den Europæiske Menneskerettighedskonvention.

3.8. Uafhængigt tilsyn

Lovforslaget indeholder en bestemmelse om, at ministeren for videnskab, teknologi og udvikling nedsætter et uafhængigt tilsyn, som skal følge nærmere angivne dele af GovCERT's virksomhed. Tilsynet vil blandt andet kunne bestå i en årlig afrapportering til ministeren for videnskab, teknologi og udvikling om GovCERT's virksomhed.

Lovforslaget ændrer ikke på Datatilsynets tilsynskompetence i henhold til persondataloven.

Der henvises i øvrigt til de specielle bemærkninger vedrørende lovforslagets § 7

4. De økonomiske og administrative konsekvenser for det offentlige

Regeringen besluttede i forbindelse med oprettelsen af den danske GovCERT, at opgaverne skal finansieres inden for Ministeriet for Videnskab, Teknologi og Udviklings eksisterende ramme. I efteråret 2009 blev det i forbindelse med udmøntningen af UMTS-midlerne besluttet at give yderligere midler til udvidelse af GovCERT's dækningsområde for perioden 2010 til 2012. UMTS-midlerne er de indtægter, som staten fik ved at sælge rettighederne til 3. generations mobiltelefoni

I denne UMTS-finansierede periode vil ministeriet udvide dækningen i et nærmere bestemt omfang og indenfor de UMTS-finansierede rammer til også at omfatte kommuner og regioner samt private virksomheder beskæftiget med kritisk infrastruktur (f.eks. finans-, energi-, samt it- og telesektoren). Ministeriet vil endvidere i perioden iværksætte en informationsindsats rettet mod borgere, små og mellemstore virksomheder. GovCERT vil i det udvidede dækningsområde køre et testforløb med fem kommuner eller regioner, som vil blive finansieret via UMTS-midlerne. Alle øvrige varslings- og overvågningsaktiviteter i det udvidede dækningsområde vil blive gebyrfinansieret.

Tilsluttede statslige institutioner vil blive tilbudt en alarmenhed. Ønskes yderligere alarmenheder opstillet vil der skulle betales gebyr herfor.

De tilsluttede myndigheder kan få forøgede administrative byrder i mindre omfang.

Tilslutning til GovCERT er frivillig for det offentlige.

5. De økonomiske og administrative konsekvenser for erhvervslivet

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet, idet tilslutning til GovCERT er frivillig. Tilsluttede private virksomheder beskæftiget med kritisk infrastruktur vil dog kunne have begrænsede økonomiske omkostninger, der dækker GovCERT's udgifter til levering af varslingsydelsen, herunder etablering og løbende servicering af GovCERT IDS hos den tilsluttede virksomhed.

6. De miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

7. De administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

8. Forholdet til EU-retten

Lovforslaget implementerer ikke EU-regulering. Lovforslaget indeholder dog regler af relevans for to EU-direktiver.

8.1. Generelle overvejelser

Der er på EU-niveau foretaget en række overvejelser, der i høj grad svarer til overvejelserne bag iværksættelsen af GovCERT, vedrørende behovet for, at medlemsstaterne iværksætter en eller anden form for statslig overvågningstjeneste for internettrusler.

EU-Kommissionen vedtog således den 30. marts 2009 en meddelelse om beskyttelse af kritisk informationsinfrastruktur med undertitlen *»Beskyttelse mod storstilede cyber-angreb og sammenbrud: Øget beredskab, sikkerhed og robusthed«.*

I denne handlingsplan opfordrer Kommissionen således medlemsstaterne til bl.a. at oprette »landsdækkende statslige CERT-enheder« og sikre, at disse GovCERT'er *»fungerer som nøglekomponent i det nationale beredskab og i informationsudveksling, koordinering og reaktion på sikkerhedshændelser«.*

Der kan i den forbindelse bl.a. også henvises til Rådets resolution af 18. december 2009 om en samordnet europæisk strategi for net- og informationssikkerhed (EUT 2009/C 321/01).

EU har ikke ønsket at fastlægge det nærmere indhold af de statslige varslingstjenester.

8.2. Persondatadirektivet

Persondatadirektivet (direktiv 95/46/EF med senere ændringer) er gennemført i dansk ret med persondataloven.

Persondatadirektivet må anses for at omfatte GovCERT's aktiviteter, i det omfang disse inkluderer behandling af personoplysninger.

Da lovforslaget i videst muligt omfang er indrettet i overensstemmelse med persondataloven, vil Danmarks forpligtelser efter persondatadirektivet ikke blive beskrevet detaljeret i det følgende.

I det tilfælde, hvor lovforslaget er udtryk for en undtagelsesvis fravigelse af persondataloven, er der ovenfor i afsnit 3.5.2 nærmere redegjort for, hvorfor lovforslaget er i overensstemmelse med persondatadirektivet.

Det vurderes således, at lovforslaget ligger inden for rammerne af persondatadirektivet.

8.3. E-databeskyttelsesdirektivet

Det generelle persondatadirektiv er suppleret af det specifikke direktiv om elektronisk kommunikation, herefter e-

databeskyttelsesdirektivet (direktiv 2002/58/EF med senere ændringer). E-databeskyttelsesdirektivet blev således vedtaget for at supplere persondatadirektivet med en række særlige bestemmelser inden for den elektroniske kommunikation.

E-databeskyttelsesdirektivet finder anvendelse på behandling af personoplysninger i forbindelse med brug af internettet (elektronisk kommunikation, herunder internet og e-mails).

I forhold til GovCERT's aktiviteter er det relevant at bemærke, at det følger af direktivets artikel 5, stk. 1, at medlemsstaterne skal sikre kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, dvs. f.eks. ved brug af internettet og e-mails.

Kommunikationshemmeligheden skal både sikres for så vidt angår selve indholdet af kommunikationen og de dermed forbundne trafikdata om brugen af internettet. Det vil f.eks. sige, at afsenderen af en e-mail skal sikres imod, at e-mailen opsnappes, åbnes og læses af andre end adressaten.

Som beskrevet ovenfor i afsnit 3.3 ligger det i GovCERT IDS, at oplysninger af privat karakter i en e-mail undtagelsesvist kan blive afsløret over for GovCERT's personale og således andre end adressaten, hvilket vil være i konflikt med artikel 5, stk. 1, i e-databeskyttelsesdirektivet, selvom det måtte ske sjældent. Der henvises i den forbindelse også til afsnit 3.6 ovenfor vedrørende den tilsvarende problemstilling i forhold til grundlovens § 72.

Efter artikel 15, stk. 1, i e-databeskyttelsesdirektivet er der dog adgang til at indskrænke rækkevidden af direktivet med hensyn til bl.a. kommunikationshemmeligheden, hvis en sådan indskrænkning er nødvendig, passende og forholdsmæssig i et demokratisk samfund af hensyn til statens sikkerhed, forsvaret, den offentlige sikkerhed, forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem.

Direktivets artikel 15 tillader således, at der i national lovgivning fastsættes regler, der indskrænker beskyttelsen af kommunikationshemmeligheden. Betingelsen er imidlertid, at det sker for at varetage et eller flere af de hensyn, der er nævnt i artikel 15, stk. 1, herunder især – i forhold til GovCERT's aktiviteter – hensynet vedrørende uautoriseret brug af det elektroniske kommunikationssystem og den offentlige sikkerhed.

Det vurderes på den baggrund, at den indskrænkning i kommunikationshemmeligheden, som GovCERT's beskrevne aktiviteter måtte medføre, er proportional og i overensstemmelse med e-databeskyttelsesdirektivet, da indskrænkningen indføres for, i direktivets forstand, at undgå uautoriseret brug af det elektroniske kommunikationssystem og beskytte den offentlige sikkerhed.

Det vurderes således, at lovforslaget ligger inden for rammerne af e-databeskyttelsesdirektivet.

9. De hørte myndigheder og organisationer mv.

Et udkast til lovforslag har været sendt i høring hos:

AC, BaneDanmark, Beredskabsstyrelsen, Brancheforum Digitale Medier, Dansk Energi, Dansk Erhverv, Danske Regioner, Dansk Industri, Dansk IT, Datatilsynet, Domstolsstyrelsen, Energinet.dk, Energistyrelsen, Finansrådet, Foreningen Danske Olieberedskabslagre, Forbrugerombudsmanden, Forbrugerrådet, Foreningen Danske Internet Medier, Foreningen for Open Source Leverandører i Danmark, Forsvarets Efterretningstjeneste, FTF, ISP-sikkerhedsforum, IT-Brancheforeningen, ITEK, It-politisk forening, It-sikkerhedskomiteen, Kommunernes Landsforening, Konkurrence- og Forbrugerstyrelsen, LO, Politiets Efterretningstjeneste, PROSA, Rigspolitiet, Rigsrevisionen, Rådet for persondata og informationssikkerhed, Rådet for større IT-sikkerhed, Statens It-forum, Statens It-råd, Telekommunikationsindustrien i Danmark, UNI C (DK-CERT).

10. Sammenfattende skema

	Positive konsekvenser /mindre udgifter	Negative konsekvenser/ merudgifter
Økonomiske konsekvenser for det offentlige	Ingen	Tilslutningen til den statslige varslingstjeneste er frivillig. De tilsluttede statslige myndigheder kan få øgede udgifter til it-udstyr i mindre omfang. Fem kommuner eller regioner vil af UMTS-midlerne få finansieret et testforløb indtil 2012. Øvrige regionale og kommunale myndigheder kan tilslutte sig mod betaling af gebyr.
Administrative konsekvenser for det offentlige	Ingen	Tilslutningen til den statslige varslingstjeneste er frivillig. De tilsluttede myndigheder kan i mindre omfang få forøgede administrative byrder.
Økonomiske konsekvenser for erhvervslivet	Ingen	Tilslutningen til den statslige varslingstjeneste er frivillig. Tilsluttede

		private virksomheder kan få begrænsede økonomiske omkostninger.
Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Administrative konsekvenser for borgere	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget implementerer ikke EU-regulering. Det vurderes, at lovforslaget ligger inden for rammerne af e-databeskyttelsesdirektivet og persondatadirektivet.	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Den foreslåede bestemmelse angiver, at formålet med lovforslaget er at skabe klare rammer for GovCERT's behandling af personoplysninger indeholdt i de indsamlede pakke- og trafikdata.

Til § 2

Med stk. 1 ønskes indført mulighed for, at også kommuner og regioner samt private virksomheder, der beskæftiger sig med kritisk infrastruktur, skal kunne vælge at tilslutte sig varslingstjenesten.

Det er hensigten, at kommuner og regioner kun skal kunne tilslutte sig GovCERT, i det omfang varslingstjenesten har kapacitet hertil. Det forudsættes i den forbindelse, at de kommuner og regioner, der vælger at tilslutte sig varslingstjenesten, selv betaler fuldt ud for GovCERT's ydelser i det omfang kommunernes og regionernes tilslutning ikke er finansieret på anden vis, som f.eks. via UMTS-midlerne.

Dele af den kritiske infrastruktur i Danmark er ejet af private virksomheder. Det gælder f.eks. elforsyningen. Dette afføder et samfundsmæssigt behov for, at også sådanne sektorer kan omfattes af GovCERT's dækningsområde for at sikre samfundets samlede sikkerhed og robusthed på internettet. Private virksomheder beskæftiget med kritisk infrastruktur har dermed også mulighed for at anmode om tilslutning til den statslige varslingstjeneste for internettrusler.

Begrebet »kritisk infrastruktur« omfatter her, i overensstemmelse med begrebets fortolkning på det beredskabsmæssige område, de sektorer, der forestår vitale samfundsmæssige interesser, f.eks. finans-, energi samt it- og telesektoren. Begrebet skal fortolkes dynamisk og vil således udvikle sig over tid i takt med samfundsudviklingen, som kan gøre det relevant at inddrage nye sektorer under begrebet kritisk infrastruktur.

For så vidt angår tilslutningen til GovCERT, kan ministeren for Videnskab, teknologi og udvikling ifølge stk. 2 fastsætte nærmere regler herom, herunder om vilkår og betaling for tilslutning til GovCERT. De anførte myndigheder og virksomheder kan herefter vælge at tilslutte sig GovCERT på baggrund af disse regler. De anførte myndigheder og private virksomheder, der måtte tilslutte sig varslingstjenesten, vil ved pålæggelse af et gebyr selv skulle finansiere tjenestens ydelser.

Til § 3

Den foreslåede bestemmelse definerer tre centrale begreber i loven.

Pakkedata er i denne lov afgrænset til kun at omfatte indholdet af internetbaseret kommunikation. Begrebet omfatter det semantiske indhold af en internetbaseret kommunikation, herunder indholdet af en e-mailkorrespondance eller indholdet af tilgåede websider, og derudover det tekniske indhold af kommunikationen, som f.eks. HTML- eller XML-koder.

I forbindelse med GovCERT's analyse af sikkerhedshændelser er det primært det tekniske indhold af kommunikationen og ikke det semantiske indhold af kommunikationen, som er interessant for analysen.

Ved trafikdata forstås i dette lovforslag data, som beskriver overførsel af pakkedata i en internetkommunikation, herunder ip-adresser, internetkommunikationens varighed og tidspunkt, e-mailadresser, hjemmesideadresser mv.

Trafikdata er tillige defineret i bekendtgørelse nr. 714 af 26. juni 2008 om udbud af elektroniske kommunikationsnet og -tjenester (udbudsbekendtgørelsen) og identisk i e-databeskyttelsesdirektivet (direktiv 2002/58/EF med senere ændringer). Definitionen af trafikdata i dette lovforslag er justeret i forhold til denne definition. Sidste led i definitionen vedrørende debitering er således udeladt, idet data vedrørende debitering ikke har relevans for dette lovforslag. Derudover er det præciseret, at det kun er internetbaseret kommunikation, som er omfattet af begrebet trafikdata. Der er herudover ikke med dette lovforslag tiltænkt nogen fravigelse af definitionen af trafikdata i e-databeskyttelsesdirektivet og udbudsbekendtgørelsen.

Ved en sikkerhedshændelse forstås, at der enten sker en påvirkning af tilgængelighed, integritet eller fortrolighed af information eller tjenester på internettet. Et eksempel på en sikkerhedshændelse, der påvirker tilgængelighed, kan være et såkaldt denial-of-service angreb, hvor en internettjeneste, f.eks. en hjemmeside, rammes af et stort antal forespørgsler, således at andre brugere ikke kan få adgang til hjemmesiden. En sikkerhedshændelse, der påvirker integritet, kan eksempelvis være et indbrud i en database, hvor tal ændres uden myndighedens vidende. En sikkerhedshændelse, der påvirker fortrolighed, kan være en såkaldt »trojansk hest«, der stjæler data fra en myndighed.

Begrebet er defineret i loven med henblik på at præcisere afgrænsningen af de tilfælde, hvor GovCERT har mulighed for at opbevare pakke- og trafikdata i op til tre år.

Til § 4

Det er formålet med den foreslåede bestemmelse, at der tilvejebringes klar lovhjemmel til GovCERT's behandling af personoplysninger i forbindelse med analyse- og varslingsopgaverne, herunder til indsamling, registrering og opbevaring af oplysninger om de tilsluttede myndigheders og virksomheders ind- og udgående internetkommunikation, dvs. pakke- og trafikdata, med henblik på varetagelsen af varslingsopgaven.

For så vidt angår hjemmearbejdspladser, som medarbejdere i de tilsluttede myndigheder og virksomheder måtte have behandler GovCERT pakke- og trafikdata, når hjemmearbejdspladsen er koblet op til myndighedens eller virksomhedens it-systemer. Der sker således samme behandling af pakke- og trafikdata, som hvis medarbejderen befinder sig på sit arbejdssted. Internetkommunikation til og fra hjemmearbejdspladsen vil ikke blive registreret af GovCERT IDS-enheden opsat hos arbejdsgiveren, når medarbejderen ikke er koblet op til arbejdsgiverens it-systemer. GovCERT IDS er nærmere beskrevet i afsnit 3.3. i de almindelige bemærkninger. I de tilfælde, hvor der kommunikeres fra en hjemmearbejdsplads til et arbejdssted, som er tilknyttet GovCERT, vil denne trafik i sagens natur blive registreret i samme omfang, som al anden kommunikation til og fra arbejdsstedet.

GovCERT's aktiviteter vil omfatte behandling af bl.a. personoplysninger, således som dette defineres i § 3, nr. 1, i persondataloven. IT- og Telestyrelsen (GovCERT) betragtes i den forbindelse som dataansvarlig, jf. persondatalovens § 3, nr. 4.

I tilfælde af begrundet mistanke om en stedfunden eller forventet sikkerhedshændelse vil indholdet af f.eks. borgeres private e-mails til tilsluttede myndigheder eller virksomheder uundgåeligt kunne blive afsløret over for GovCERT's personale og således andre end adressaten. Der vil f.eks. være tale om en begrundet mistanke om en sikkerhedshændelse, hvis der er klare tegn på, at en afsendt e-mail har været anvendt til at aflevere et it-angreb, f.eks. en virus, mod en myndighed.

GovCERT's personale vil i forbindelse med alarmer og øvrige sikkerhedshændelser nærmere analysere pakkedata for den pågældende periode, hændelsen vedrører. Meddelelseshemmeligheden efter grundlovens § 72 kan dermed i disse tilfælde blive brudt. Ved en alarm forstås, at der fra GovCERT IDS bliver sendt data, som er indsamlet hos den tilsluttede myndighed, til GovCERT, fordi der er konstateret en afvigelse fra »normalbilledet« af internetkommunikationen til og fra myndigheden. "Normalbilledet" er beskrevet i afsnit 3.3. i de almindelige bemærkninger. En alarm indikerer, at en sikkerhedshændelse har fundet sted.

Når det således af stk. 1 følger, at GovCERT's aktiviteter foretages »uden retskendelse« skyldes det, at der med bestemmelsen, udover at skabe en klar hjemmel for de undtagelsesvise brud på meddelelseshemmeligheden, sigtes til at skabe klar hjemmel for at fravige udgangspunktet i grundlovens § 72 om retskendelse.

Det er i den forbindelse væsentligt at være opmærksom på, at GovCERT med den foreslåede lov kun får hjemmel til at analysere pakkedata ved begrundet mistanke om en stedfunden eller forventet sikkerhedshændelse. Adgangen til pakkedata er yderligere begrænset af, at kun den del af de indsamlede pakkedata, som er relevant for den pågældende analyse af sikkerhedshændelsen, vil kunne analyseres. Adgangen for GovCERT til pakkedata er herved begrænset mest muligt for at imødekomme hensynet til privatlivets fred.

GovCERT vil som udgangspunkt ikke afkryptere en krypteret e-mail eller andet indhold af en internetkommunikation. Den eneste undtagelse hertil er, hvis ikke-krypteret kommunikation, som GovCERT har modtaget fra GovCERT IDS, indeholder en skadelig fil, f.eks. en virus, med et krypteret indhold. I dette tilfælde vil GovCERT kunne afkryptere indholdet af denne fil for nærmere at analysere virussen. GovCERT vil ikke kunne foretage denne delvise afkryptering, hvis hele kommunikationen er krypteret.

Opbevaringsperioden for indsamlede oplysninger om de tilsluttede myndigheders ind- og udgående internetkommunikation vil højst være tre år for så vidt angår pakke- og trafikdata, der knytter sig til en sikkerhedshændelse på internettet. Opbevaringsperioden påregnes dog i de mange tilfælde at være væsentligt kortere, idet GovCERT er forpligtet til at slette data, så snart data ikke længere er relevant i forhold til GovCERT's formål og aktiviteter.

Såfremt der ikke foreligger en sikkerhedshændelse, er de maksimale opbevaringstider væsentligt kortere, henholdsvis 14 kalenderdage for pakkedata og 12 måneder for trafikdata. Pakkedata vil som udgangspunkt blive slettet efter seks kalenderdage, men hvis yderligere undersøgelser er påkrævet for at afgøre, om der er tale om en sikkerhedshændelse, vil GovCERT kunne anvende op til i alt 14 kalenderdage, inden pakkedata skal slettes.

Det vurderes, at de foreslåede maksimale opbevaringsperioder er de kortest mulige i forhold til formålet med GovCERT. Fristerne regnes fra tidspunktet for registreringen af data i GovCERT, hvilket skal forstås som tidspunktet for lagringen af data i IDS-enheden. Baggrund for fristernes længde er nærmere beskrevet i afsnit 3.2.

Den behandling af personoplysninger, som GovCERTs adgang til de tilsluttede myndigheders ind- og udgående internetkommunikation (pakke- og trafikdata) uundgåeligt vil afstedkomme, vil til enhver tid skulle overholde reglerne i persondatalovens §§ 5-8 om behandling af personoplysninger.

I bestemmelsens stk. 3 foreslås det, at den nærmere tekniske udmøntning kan ske ved, at ministeren for videnskab, teknologi og udvikling fastsætter nærmere regler herom. Disse regler kan blandt andet omfatte specifikke beskrivelser af, hvordan den tekniske behandling af data skal ske fra data bliver indsamlet af GovCERT IDS, og indtil data bliver lagret på centrale servere hos GovCERT.

Til § 5

I bestemmelsens stk. 1 foreslås det, at persondatalovens § 35 om retten til at gøre indsigelse ikke skal finde anvendelse i forbindelse med GovCERT's aktiviteter. Bestemmelsen vil

medføre, at registrerede ikke vil kunne gøre indsigelse mod GovCERT's behandling af personoplysninger.

Det vurderes således, at behovet for at gøre indsigelse i denne situation, hvor indsamlingen af personoplysninger er en nødvendig konsekvens af GovCERT's virke, er mindre fremtrædende end de administrative byrder, det vil kunne pålægge GovCERT, hvis registrerede kunne gøre indsigelse.

Der henvises i den forbindelse til afsnit 3.5.2 i de almindelige bemærkninger, og det dér anførte om persondatalovens § 35.

Bestemmelsen i stk. 2 indebærer, at GovCERT's personale er underlagt en særlig tavshedspligt i forhold til de oplysninger, som personalet bliver bekendt med i kraft af deres stilling. De oplysninger, som GovCERT behandler, kan derfor ikke videregives til uvedkommende. Baggrunden for denne særlige tavshedspligt for GovCERT's personale er den særligt fortrolige karakter og omfanget af de oplysninger, som personalet potentielt har adgang til.

De personer, som GovCERT indsamler oplysninger om, har som følge af bestemmelsen ikke ret til indsigt i oplysningerne efter persondatalovens § 31, jf. persondatalovens § 32, stk. 2. Der henvises til det i afsnit 3.5.2 i de almindelige bemærkninger anførte om de to bestemmelsers forhold til lovforslaget.

Bestemmelsen udelukker ikke en berettiget videregivelse af oplysninger efter lovforslagets § 6.

Til § 6

Det følger af den foreslåede bestemmelse i nr. 1, at den statslige varslingstjeneste (GovCERT) kan videregive pakke- og trafikdata, der knytter sig til en sikkerhedshændelse, til dansk politi. Formålet hermed er at sikre, at politiet kan modtage oplysninger til brug for efterforskning og forfølgelse af strafbare forhold, der kan være begået i forbindelse med en sikkerhedshændelse, som f.eks. et virusangreb.

GovCERT indgår i det statslige teleberedskab, der skal sikre, at internetkommunikation kan opretholdes i en beredskabssituation. GovCERT's aktiviteter dækker statslige myndigheders internetkommunikation bortset fra internetkommunikationen på Forsvarsministeriets område. Under Forsvarsministeriet er der indledt en opbygning af en militær CERT (MILCERT), der, ligesom GovCERT sikrer øvrige statslige myndigheders internetkommunikation, sikrer Forsvarsministeriets klassificerede og ikke klassificerede kommunikation og indgår i forsvarets beredskab. GovCERT og MILCERT er blandt de centrale aktører i statens samlede beredskab over for trusler og angreb rettet mod nationale digitale infrastrukturer. MILCERT er som del af den militære sikkerhedstjeneste organisatorisk forankret i Forsvarets Efterretningstjeneste. I tilfælde af en sikkerhedshændelse vil det i visse tilfælde være nødvendigt meget hurtigt at iværksætte en koordineret indsats mellem GovCERT og MILCERT for at sikre et sammenhængende beredskab og en effektiv anvendelse af samfundets samlede ressourcer i forsvaret mod trusler rettet mod de statslige myndigheders kritiske digitale infrastrukturer. Denne indsats forudsætter, at GovCERT og MILCERT meget hurtigt kan udveksle relevant information, herunder pakkedata relateret til sikkerhedshændelsen. Med forslaget til nr. 2, skabes således hjemmel til, at GovCERT i visse tilfælde kan videregive pakkedata til Forsvarets Efterretningstjeneste. Denne videregivelse af data er betinget af, at data er knyttet til en sikkerhedshændelse, og af, at videregivelsen er nødvendig for det it-sikkerhedsmæssige samarbejde mellem de to CERTer. Forsvarets Efterretningstjeneste skal behandle, herunder slette og opbevare, de videregivne pakkedata i overensstemmelse med de regler i dette lovforslags § 4, som tilsvarende gælder for GovCERT's virke. Videregivelse af trafikdata til Forsvarets Efterretningstjeneste vil skulle reguleres i henhold til reglen i den foreslåede bestemmelses nr. 3.

Med forslaget i nr. 3 sikres det, at den statslige varslingstjeneste kan videregive trafikdata til danske myndigheder – det kan f.eks. være DK-CERT, som overvåger forskningsnettet – og tilsluttede private virksomheder beskæftiget med kritisk infrastruktur, hvor dette er nødvendigt som led i varslingstjenestens aktiviteter og i henhold til varslingstjenestens formål. Det kan f.eks. være information om en konkret ip-adresse, som har angrebet en myndighed til forebyggelse af yderligere angreb.

Nr. 3 sikrer herudover, at GovCERT kan udveksle trafikdata, herunder ip-adresser, med tilsvarende varslingstjenester i andre lande, også uden for EU, i forbindelse med sikkerhedshændelser på internettet.

Der vil ikke efter bestemmelsen i nr. 3, kunne videregives pakkedata, herunder eksempelvis indholdet af en e-mailkorrespondance.

Det følger af den foreslåede bestemmelse, at andre regler i lovgivningen om indsamling og videregivelse af oplysninger mellem forvaltningsmyndigheder ikke vil kunne anvendes i forhold til data, der er indsamlet af den statslige varslingstjeneste som led i varslingstjenestens aktiviteter.

Heri ligger bl.a., at hvis politiet til brug for f.eks. efterforskning af et strafbart forhold, der ikke er begået i forbindelse med en sikkerhedshændelse (jf. nr. 1), ønsker pakkedata eller trafikdata fra den statslige varslingstjeneste, må politiet gå frem efter de almindelige straffeprocessuelle regler i retsplejelovens fjerde bog og i den forbindelse efter omstændighederne indhente retskendelse.

Til § 7

Formålet med § 7 er at pålægge ministeren for videnskab, teknologi og udvikling at nedsætte et uafhængigt tilsyn, der skal følge nærmere angivne dele af GovCERT's virksomhed. Ministeren for videnskab, teknologi og udvikling fastsætter nærmere regler for tilsynets virksomhed.

Tilsynet vil f.eks. skulle føre tilsyn med informationer om it-angreb på offentlige myndigheder eller private virksomheder, herunder angrebsmetoden og effekten af angrebet. Tilsynet vil desuden skulle føre tilsyn med informationer, der kan anvendes til berigelseskriminalitet eller til at gøre skade på it-systemer, it-net, produktionssystemer eller lignende (tekniske oplysninger om sikkerhedshændelser).

Det foreslås, at tilsynet skal forestås af en jurist som formand og fire sagkyndige medlemmer, der må betragtes som

upolitiske, og som beskikkes som følge af den almindelige tillid og agtelse, der er knyttet til deres person. Det er en endvidere en forudsætning, at tilsynets medlemmer kan sikkerhedsgodkendes.

Lovforslaget ændrer ikke på Datatilsynets kompetence i henhold til persondataloven.

Tilsynet ifølge dette lovforslags § 7 vil således ikke behandle forhold, som hører under andre myndigheders kompetence.

Til § 8

En beslutning om, at en kompetence overlades generelt, f.eks. af en minister til en styrelse, bør af hensyn til borgernes mulighed for at kunne vide, hvem der er rette myndighed, altid angives i en bekendtgørelse, jf. afsnit 4 i Justitsministeriets vejledning nr. 153 af 22. september 1987 om udarbejdelse af administrative forskrifter. Det foreslås derfor, at der i loven indsættes en hjemmel for ministeren for videnskab, teknologi og udvikling til at bemyndige en under Ministeriet for Videnskab, Teknologi og Udvikling oprettet styrelse eller tilsvarende institution til at udøve de beføjelser, der i loven er tillagt ministeren.

Ministeren kan herefter i en bekendtgørelse udnytte adgangen til at delegere opgaver og beføjelser til en statslig myndighed under ministeriet. Bemyndigelseshjemlen er formuleret, så den med sikkerhed kan rumme statslige myndigheder under Ministeriet for Videnskab, Teknologi og Udvikling, som organisatorisk er underordnet styrelserne. Ministeren kan således efter den foreslåede bestemmelse delegere sine beføjelser efter loven til enhver myndighed inden for ministeriets administrative hierarki uanset myndighedens placering i det administrative hierarki, herunder myndigheder, som er underordnet styrelser.

Endvidere foreslås det, at ministeren for videnskab, teknologi og udvikling efter forhandling med vedkommende minister kan bemyndige andre statslige myndigheder til at udøve de beføjelser, som i loven er tillagt ministeren for videnskab, teknologi og udvikling. Der er kun tale om statslige myndigheder. Der kan således ikke i medfør af denne bestemmelse ske delegation til private virksomheder eller organisationer. Omfanget af delegationen til den pågældende statslige myndighed skal ske efter forhandling med vedkommende minister.

Forslaget i stk. 2 er en konsekvens af det foreslåede stk. 1. Det foreslås derfor, at ministeren for videnskab, teknologi og udvikling får hjemmel til at fastsætte regler om adgangen til at påklage afgørelser vedrørende GovCERT's virksomhed, der er truffet i henhold til bemyndigelse efter stk. 1, herunder at afgørelserne ikke skal kunne påklages. Ministeren vil herved kunne afskære klageadgangen fra organisatorisk underordnede statslige myndigheder til styrelserne eller for andre statslige myndigheder. Ministeren kan f.eks. således ikke blot afskære klageadgang til ministeren, men også klageadgang til styrelserne. Adgangen til at afskære klage knytter sig kun til afgørelser på områder, som er delegeret fra ministeren i henhold til loven. Lovforslaget berører ikke øvrige klagemuligheder.

Det foreslås i stk. 3, at ministeren for videnskab, teknologi og udvikling får hjemmel til at fastsætte regler om udøvelsen af de beføjelser, som en anden statslig myndighed efter forhandling med vedkommende minister bliver bemyndiget til at udøve efter stk. 1. Bestemmelsen omhandler de tilfælde, hvor ministeren udnytter sin adgang til at delegere beføjelser til andre statslige myndigheder uden for Ministeriet for Videnskab, Teknologi og Udvikling.

Til § 9

Det foreslås, at loven træder i kraft den 1. juli 2011.

Til § 10

Den foreslåede bestemmelse angår lovens territoriale gyldighed. Det er hensigten med bestemmelsen at fastlægge, at GovCERT's aktiviteter ikke vedrører de grønlandske og færøske dele af riget.