Notat

Kommenteret høringsoversigt vedrørende udkast til lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internet-trusler m.v.

12. april 2011

IT- og Telestyrelsen
Holsteinsgade 63
2100 København Ø
Telefon 3545 0000
Telefax 3545 0010
E-post itst@itst.dk
Netsted www.itst.dk
CVR-nr. 26769388

Sagsbehandler
Hans Bøgesvang Riis
Telefon 3545 0248
Telefax 3545 0010
E-post hbr@itst.dk

Sagsnr.
Dok nr.

Videnskabsministeriet har i perioden 11. februar – 4. marts 2011 gennemført en høring over udkast til lovforslag om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler (GovCERT).

Resultatet af høringen
Videnskabsministeriet har i alt modtaget 18 eksterne høringssvar (Banedanmark, Dansk Energi, Danske Regioner, Dansk IT, Datatilsynet, DI – ITEK, DK—CERT, Domstolsstyrelsen, Erhvervs- og Byggestyrelsen, Finansrådet, Forbrugerrådet, IT-Politisk Forening, Kort og Matrikelstyrelsen, Politiets Efterretningstjeneste, PROSA, Rigsrevisionen, Telia og Tor Bloch (tidligere videnskabelig direktør i UNI-C)). 12 af høringssvarene indeholder substansbemærkninger til lovforslaget.

Der redegøres i dette høringsnotat for de væsentligste bemærkninger til lovforslaget.

Høringssvarene har givet anledning til visse tilføjelser, præciseringer og uddybninger af lovforslaget.

1. Generelle bemærkninger
Finansrådet bifalder beslutningen om at etablere en statslig CERT i Danmark og støtter lovforslaget. Rådet er endvidere enig i, at behandling af personoplysninger er påkrævet, for at GovCERT's formål kan opfyldes. Råbet bemærker desuden, at GovCERT allerede nu bør være opmærksom på de fremtidige trusler mod den offentlige infrastruktur, herunder angreb med avanceret kriminelt software, som f.eks. trojanere.

DI – ITEK bakker lovforslaget op og bemærker, at etableringen af GovCERT er et vigtigt skridt i retning af at forbedre Danmarks informationssikkerhed. DI – ITEK er enig i, at der er et stort behov for at sikre beskyttelsen af primært statslige institutioner og derudover regioner, kommuner og sektorer beskæftiget med kritisk infrastruktur. Det er vigtigt, at Danmark får en myndighed, som kan indgå i det internationale samarbejde for at bekæmpe it-kriminalitet.

DI – ITEK finder det dog principielt betænkeligt, at GovCERT får adgang til pakke- og trafikdata, idet dette kan skabe utryghed for danske borgere. Jo flere

som har adgang til denne type data, desto større utryghed for borgerne. Denne utryghed forværres af, at lovforslaget undtager mange af de bestemmelser, som normalt bidrager til borgernes retssikkerhed, herunder grundlovens § 72, den Europæiske Menneskerettighedskonventions artikel 8 og persondataloven. DI – ITEK bemærker hertil, at borgere kan kryptere deres meddelelser, hvis der ønskes særlig sikkerhed, og at lovforslaget lægger op til en god beskyttelse ved en række tiltag, herunder begrænsning af adgangen til data, sletning af data hurtigst muligt, et selvstændigt tilsyn, et præcist og afgrænset formål mv.

DI – ITEK bemærker, at der kan være behov for modernisering af loven, f.eks. vil kommunikationen mellem to betroede parter kunne undtages IDS-overvågningen. DI – ITEK anbefaler derfor, at loven suppleres med en evalueringsforpligtelse, hvor det f.eks. hvert andet år vurderes, hvorvidt GovCERT kan foretage en mindre indgribende teknisk analyse end den nuværende IDS-analyse af al kommunikation.

Dansk IT erkender fuldt ud behovet for, at GovCERT i visse tilfælde undtagelsesvist kan behandle personlige og personfølsomme oplysninger.

Banedanmark ser frem til, at GovCERT kan tilbyde de ydelser, som der lægges op til. Banedanmark har herudover ikke bemærkninger til lovforslaget.

Telia støtter lovforslagets sigte. Telia finder det tilfredsstillende, at tilslutning til GovCERT er frivillig og baserer sig på et påregneligt grundlag.

Danske Regioner støtter hensigten med GovCERT og bakker op om, at GovCERT's behandling af personoplysninger reguleres ved lov. Region Hovedstaden og Region Nordjylland har i Danske Regioners høringssvar afgivet særskilte bemærkninger jf. nedenfor.

Region Nordjylland er enig i, at landets kritiske tekniske infrastruktur skal sikres. Regionen forholder sig dog kritisk til lovforslaget. Regionen bemærker bl.a., at det er problematisk, at IDS-sensoren lagrer data, uden at regionen er vidende om det, hvis regionen tilslutter sig GovCERT. Derudover har regionen en række specifikke bemærkninger jf. nedenfor.

IT-Politisk Forening påskønner, at GovCERT har været meget åbne omkring både tjenestens funktion og lovforslaget.

PROSA støtter oprettelsen af GovCERT og ser dens etablering som et meget positivt bidrag til at øge sikkerheden over for it-kriminelle. PROSA finder det dog bekymrende, at lovforslaget giver GovCERT en bred adgang til at behandle og videregive personoplysninger.

Datatilsynet bemærker, at det må bero på en politisk vurdering, hvorvidt den ønskede lovhjemmel til GovCERT's omfattende overvågning af internettrafik til og fra offentlige myndigheder skal tilvejebringes. Datatilsynet understreger vigtigheden af at anvende privatlivsfremmende teknologier ved GovCERT's behandling af data.

Datatilsynet anfører, at afsnittet om persondataloven under afsnittet om gældende ret i lovforslaget bør gøres mere overordnet.

Videnskabsministeriet (VTU) har med tilfredshed noteret sig de mange positive generelle bemærkninger til lovforslaget. VTU bemærker til DI – ITEK og Datatilsynet, at GovCERT løbende vil vurdere, om det er hensigtsmæssigt at overgå til anden og mindre privatlivsindgribende teknisk behandling af internetkommunikationen, og i øvrigt vurdere om ny og relevant teknologi bør implementeres for at forbedre GovCERT's virke.

VTU er opmærksom på lovforslaget snitflader til anden lovgivning. GovCERT vil således ved enhver behandling af persondata vurdere, hvorvidt behandlingen er relevant i forhold til GovCERT's formål og virke og proportional i forhold til indgrebet i privatlivets fred. De tilsluttede myndigheder/virksomheder vil blive informeret om alle bekræftede sikkerhedshændelser, som IDS-sensoren har registeret.

GovCERT vil løbende kunne se trafikdata fra de tilsluttede myndigheder, hvorimod pakkedata kun vil blive sendt til GovCERT, hvis der er mistanke om en sikkerhedshændelse. GovCERT må under alle omstændigheder kun behandle data, hvis det er nødvendigt som følge af en begrundet mistanke om en sikkerhedshændelse. Data vil endvidere skulle slettes løbende af GovCERT, når data ikke længere er relevant for GovCERT's virke. Dette skulle sikre, at der ikke sker usaglig behandling af (person)data i GovCERT.

VTU har justeret afsnittet om persondataloven under "gældende ret" i overensstemmelse med Datatilsynets bemærkninger.

2. Formål og afgrænsning af loven (§§ 1 og 2)
Telia bemærker, at private virksomheders beslutning om tilslutning, som minimum vil forudsætte, at tilslutningsvilkår er gennemsigtige og prissætning rimelig. Telia opfordrer derfor IT- og Telestyrelsen til at arbejde aktivt for at disse vilkår og priser fastsættes på en sådan måde, at kritiske infrastrukturvirksomheder har klare incitamenter for tilslutning.

Videnskabsministeriet vil ved særskilt regulering fastsætte de præcise vilkår og priser for tilslutning til GovCERT.

3. Definitioner (§ 3)
Region Nordjylland finder, at begrebet "kritisk infrastruktur" bør reserveres til den tekniske infrastruktur. Regionen ønsker desuden en præcisering af definitionen af en sikkerhedshændelse.

IT-Politisk Forening bemærker, at definitionerne af pakke- og trafikdata ikke er tilstrækkeligt præcise. Det bør præciseres i lovforslaget, at en e-mailadresse, hjemmesideadresser og lignende er pakkedata, hvilket er vigtigt, fordi trafikdata kan udleveres til udlandet jf. § 5 i lovforslaget.

Kort- og Matrikelstyrelsen (KMS) bemærker, at der kan udveksles ip-adresser og spørger, om en ip-adresse ikke regnes for en personoplysning. KMS spørger

videre, om en privat ip-adresse vil kunne lukkes af GovCERT, og hvordan der informeres om en sådan lukning, hvis der er hjemmel hertil.

Videnskabsministeriet (VTU) finder, at "kritisk infrastrukter" er det rette begreb at anvende i relation til GovCERT's virke. VTU har på baggrund af bemærkningerne til begrebet "sikkerhedshændelse" indskrevet tre eksempler på sikkerhedshændelser i lovbemærkningerne til § 3 (tidligere § 2). En ip-adresse er at betragte som en personoplysning og bliver behandlet som sådan af GovCERT. VTU vurderer, at begrebet "sikkerhedshændelse" ikke kan indsnævres yderligere henset til den hastige teknologiske udvikling. Det er VTU's vurdering, at en e-mailadresse, hjemmesideadresse og lignende er at betragte som trafikdata. VTU har indskrevet dette i bemærkningerne til bestemmelsen i lovforslaget.

GovCERT kan ikke lukke en privat ip-adresse. I tilfælde af en sikkerhedshændelse, der formodes at komme fra en privat ip-adresse, kan GovCERT rette henvendelse til den internetudbyder, der ejer ip-adressen, og anmode internetudbyderen om at stoppe sikkerhedshændelsen. Det er internetudbyderens eget valg, hvorvidt man vil efterkomme anmodningen.

4. Opbevaring og behandling af data (§ 4)

Dansk IT anfører, at GovCERT's behandling af data skal ske efter en model, hvor det til alle tider kan dokumenteres, hvem der har haft adgang til hvilke data. Logdata må endvidere ikke kunne ændres, uanset rang. Det skal derudover sikres, at adgangen til disse oplysninger kun er mulig for relevante personer.

Telia spørger til det forhold, at den maksimale frist for opbevaring af pakke- og trafikdata er sat til tre år, mens fristen i logningsbekendtgørelsen er ét år. Telia opfordrer til, at både mængden af data og den maksimale opbevaringsperiode genovervejes.

Region Hovedstaden bemærker, at "registrering" bør defineres, idet begrebet ellers vil give anledning til fortolkning.

Tor Bloch, (tidligere direktør for UNI-C) bemærker, at GovCERT bør holde detailleret regnskab med brugen af adgangen til at analysere pakkedata. En flerårig "trendanalyse" kunne i den forbindelse være nyttig.

IT-Politisk Forening bemærker, at GovCERT ikke bør være bemyndiget til at opsamle eller tilgå data, hvis hverken afsender eller modtager frivilligt og eksplicit har tilsluttet sig GovCERT. Foreningen bemærker, at det er vigtigt, at danske internetbrugere ikke kan blive overvåget af en statslig varslingstjeneste, selvom internetudbydere skulle tilslutte sig varslingstjenesten.

Region Nordjylland bemærker, at grundlaget for, hvornår GovCERT kan gemme data ikke er tilstrækkeligt præcist, idet en varslingtjeneste er baseret på, at der altid vil være en begrundet mistanke om en forventet sikkerhedshændelse. Regionen efterspørger en begrundelse for muligheden for at gemme pakkedata i længere tid end 14 dage.

Region Nordjylland bemærker, at IDS-sensoren ofte ikke vil være anvendelig for GovCERT's brugere. Regionen bemærker videre, at det er problematisk, at GovCERT på et tidspunkt vil kunne tilgå selv krypteret information. Desuden bemærkes, at GovCERT bør koncentrere sig om indgående trafikdata.

Region Nordjylland anfører endvidere, at adgangen til personoplysninger bør differentieres og være baseret på en risikovurdering.

Kort- og Matrikelstyrelsen (KMS) bemærker i relation til § 3, at det næppe er muligt at skelne mellem hjemmearbejdspladser og de pc-arbejdspladser, der befinder sig i ministeriets lokaliteter. KMS spørger til forholdet til den Europæiske Menneskerettighedskonvention, hvor det forudsættes, at den ansatte skal give samtykke til GovCERT's behandling af data. Der spørges til, hvordan det hænger det sammen med, at der kun vil blive registreret trafikdata jf. § 3?

Datatilsynet finder det ikke klart, hvorfor det er nødvendigt at opbevare pakkedata i op til 14 dage, hvis der ikke er tegn på en sikkerhedshændelse og anbefaler, at dette præciseres i bemærkningerne til lovforslaget. Det bør endvidere præciseres, hvorfor perioden på 14 dage er valgt, når det samtidig fremgår, at udgangspunktet er, at data kun vil blive opbevaret i seks dage.

PROSA bemærker, at personoplysninger bør slettes eller anonymiseres/krypteres når oplysningerne overføres til nærmere analyse på govCERT's klassificerede net. PROSA anbefaler desuden, at der indføres en anmeldelsesordning, således, at den enkelte medarbejder og GovCERT forpligtes til at anmelde alle tilfælde, hvor der har været tilgang (bortset fra ip-adresser) til personoplysninger til Datatilsynet.

Videnskabsministeriet (VTU) bemærker, at GovCERT løbende vil registrere, hvornår og af hvem data behandles. Logdata opbevares på en særlig logdata-server, som kun kan tilgås af chefen for GovCERT og de to systemadmin-istratorer. Der er ikke rettigheder til at ændre i disse logdata, og det er ikke tilladt at tildele sig selv disse rettigheder. Teoretisk set vil en systemadministrator kunne tildele sig selv disse rettigheder, men GovCERT har to systemadmini-stratorer, hvorfor den anden administrator vil kunne opdage dette og alarmere herom. Af hensyn til intern videndeling og GovCERT's virke vil relevant personale i GovCERT kunne tilgå oplysninger om bekræftede sikkerheds-hændelser og trafikdata – inden for de i § 4 (tidligere § 3) beskrevne tidsfrister. VTU har valgt en maksimal opbevaringsperiode på tre år på baggrund af, at en teknologisk relevant generation typisk har denne længde, hvilket er nærmere beskrevet i lovforslaget. Flerårig viden om tidligere it-angrebs tekniske indretning, vurderes endvidere som værende nødvendig for GovCERT evne til at imødegå kommende it-angreb. I forhold til opbevaringsfristen på et år i logningsbekendtgørelsen bemærker VTU, at opbevaringsfristen i lovforslaget relaterer sig til data knyttet til en bekræftet sikkerhedshændelse i modsætning til logningsbekendtgørelsen, som omhandler bagudrettet logning af hensyn til muligheden for efterforskning af et kriminelt forhold som endnu ikke er kendt. Et års fristen i logningsbekendtgørelsen vil skulle holdes op imod 14 dages fristen i lovforslagets § 4, stk. 2, nr. 2 (tidligere § 3, stk. 2, nr. 2).

GovCERT vil som udgangspunkt slette pakkedata efter seks dage, hvis data ikke er knyttet til en sikkerhedshændelse, men i visse tilfælde kan yderligere undersøgelser være påkrævet for at afgøre, om der er tale om en sikkerhedshændelse. GovCERT vil i disse tilfælde kunne benytte sig af den maksimale frist på 14 dage. VTU vil præcisere dette nærmere i bemærkningerne til lovforslaget. GovCERT vil ikke behandle data i tilfælde, hvor hverken afsender eller modtager af kommunikationen har tilsluttet sig GovCERT. GovCERT vil ikke afkryptere krypteret pakkedata, medmindre det er påkrævet i forbindelse med nærmere analyse af skadelig software – som eksempelvis en virus.

VTU vurderer, at GovCERT IDS har stor værdi for de tilsluttede myndigheder/virksomheder. Både ind- og udgående internetkommunikation er relevant for GovCERT's virke, hvorfor GovCERT ikke vil prioritere i denne information. GovCERT registrerer og behandler både trafik- og pakkedata jf. ordlyden af § 4 (tidligere § 3).

Begrebet "registrering" vil blive præciseret i bemærkningerne til bestemmelsen.

VTU har justeret afsnittet om hjemmearbejdspladser i bemærkningerne til § 4 (tidligere § 3), således at det tydeligt fremgår, at når en hjemmearbejdspladsen er koblet op til myndighedens eller virksomhedens it-systemer vil der ske samme behandling af pakke- og trafikdata, som hvis medarbejderen befinder sig på sit arbejdssted.

GovCERT's klassificerede net er fysisk sikret på en sådan måde, at data ikke kan sendes ud af nettet. Data vil således ikke kunne sendes ud af GovCERT, efter at data er sendt til det klassificerede net. Denne ekstra sikkerhedsforanstaltining sikrer mod, at persondata kommer i hænderne på it-kriminelle. Det skal endvidere bemærkes, at 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.

GovCERT vil orientere Datatilsynet, hvis der skulle forekomme en situation, hvor uvedkommende får adgang til pakkedata indeholdende personoplysninger fra GovCERT's net. Dette gælder ikke den med lovforslaget hjemlede adgang til pakkedata for GovCERT's medarbejdere ved mistanke om sikkerhedshændelser.

5. Videregivelse af data (§ 6)

Kort og Matrikelstyrelsen (KMS) spørger, hvordan de tilsluttede ministerier og politiet skal forholde sig til data knyttet til en sikkerhedshændelse, som videregives til myndigheden fra GovCERT?

Datatilsynet bemærker, at lovforslaget ikke ses at forholde sig til persondatalovens § 27 om overførsel af oplysninger til tredjelande, og det anbefales, at bestemmelsen tydeliggøres i lovforslaget. Det fremgår endvidere ikke at lovforslagets § 5, om bestemmelsen også omfatter udenlandske politimyndigheder. § 27 bør også iagttages i forhold til videregivelse af data til lande uden for EU. Datatilsynet henleder opmærksomheden på § 27, stk. 3, nr. 4, som giver adgang til at overføre oplysninger til tredjelande for at beskytte en vigtig samfundsmæssig interesse.

PROSA bemærker, at det er uklart, hvordan "varslingstjenestens aktiviteter" som nævnt i § 5 afgrænses. PROSA foreslår, at det til § 5 indskærpes, at GovCERT kun må behandle pakkedata, hvis der er begrundet mistanke om en kriminal handling, og at GovCERT kun må udlevere data mod retskendelse.

Videnskabsministeriet (VTU) bemærker, at GovCERT kun i visse tilfælde af en bekræftet sikkerhedshændelse vil videregive information indeholdende persondata til den tilsluttede myndighed. Myndigheden vil i givet fald skulle være opmærksom på øvrig gældende lovgivning, herunder persondataloven. I forbindelse med tilslutning til GovCERT vil dette forhold og øvrige forhold af relevans for tilslutningen blive drøftet og/eller beskrevet i aftalegrundlaget med den tilsluttede myndighed/virksomhed.

VTU finder det relevant at nævne persondatalovens § 27 i lovforslaget og har således indføjet et afsnit om bestemmelsen i bemærkningerne til lovforslaget.

VTU finder, at § 6 (tidligere § 5) har den rette balance mellem hensynet til privatlivets fred og hensynet til formålet med GovCERT, herunder gode samarbejdsrelationer med danske og internationale samarbejdspartnere. VTU finder således ikke grundlag for at justere bestemmelsen.

6. Tilsyn med GovCERT (§ 7)

Dansk IT bemærker, at tilsynet bør være repræsenteret med stærke tekniske kompetencer for at sikre et fyldestgørende tilsyn.

Telia støtter lovforslagets forslag om etablering af et uafhængigt tilsyn. Telia finder dog, at det ikke bør være videnskabsministeren men derimod tilsynet selv, som fastsætter rammerne for tilsynet, ligesom tilsynet selv må kunne afgøre hyppigheden af en afrapportering til ministeren. Det bør derudover være op til tilsynet selv at vurdere om afrapporteringen alene skal ske til videnskabsministeren eller til en bredere kreds.

Region Nordjylland finder, at tilsynet er uden beføjelser og dermed ikke kan betragtes som uafhængigt.

Tor Bloch bemærker, at der bør sikres en lovmæssig og rimelig grad af fornyelse af tilsynets medlemmer, f.eks. ved krav om fornyelse af 1-2 medlemmer for hver ny 4-årig periode og fornyelse af formandskabet efter 2-3 perioder. Årsberetningen om GovCERT skal være et krav og ikke blot en mulighed.

Kort- og Matrikelstyrelsen foreslår, at tilsynet kan foretages af Wamberg udvalget.

Datatilsynet bemærker, at det er uhensigtsmæssigt, at GovCERT er underlagt tilsyn fra to forskellige tilsynsorganer, som begge har en dommer som formand for tilsynet. Det fremgår uklart af lovforslaget, hvilke ophaver, ansvar og kompetencer det særlige tilsyn med GovCERT tilsigtes at skulle have – sammenholdt med de opgaver og kompetencer, som Datatilsynet har efter persondataloven.

Datatilsynet bemærker i den forbindelse, at Datatilsynet ikke har kompetence i forhold til efterretningstjenesternes behandling af personoplysninger. Datatilsynet finder på den baggrund, at den foreslåede tilsynsmodel bør genovervejes. Det bør overvejes at indføre et mere intensivt tilsyn, end det Datatilsynet vil kunne føre, og i den forbindelse i lovforslaget beskrive, at dette tilsyn træder i stedet for Datatilsynet tilsyn på området.

Domstolsstyrelsen henleder opmærksomheden på retsplejelovens § 47a, stk. 3, i forhold til lovforslagets § 6, stk. 2. Styrelsen henviser endvidere til Justitsministeriets skrivelse fra december 2000, hvori justitsministeren i forbindelse med oprettelse af nye nævn, anmoder alle ministerier om at vurdere, om det er tilstrækkeligt velbegrundet, at der indsættes en dommer.

PROSA kan ikke støtte oprettelsen af et tilsyn med GovCERT. PROSA finder ikke, at tilsynet sikrer retssikkerheden. PROSA vurderer, at tilsynet alene bør placeres hos Datatilsynet.

Videnskabsministeriet (VTU) har på baggrund af bemærkningerne til bestemmelsen om tilsynet med GovCERT's virksomhed præciseret bemærkningerne til bestemmelsen, herunder at tilsynet ikke træder i stedet for eller overlapper Datatilsynets tilsyn på området. Af hensyn til kontinuitet og høj faglig kompetence i tilsynet lægger VTU ikke op til at ændre bestemmelsen på en sådan måde, at der tvangsmæssigt skal ske udskiftning af formand eller medlemmer med et fast interval.

VTU vurderer, at det ikke er hensigtsmæssigt, at forsøge at inddrage Wamberg-udvalget i tilsynet med GovCERT.

VTU vurderer på baggrund af Datatilsynets høringssvar, at det er tilstrækkeligt at udpege en jurist i stedet for en dommer som formand for tilsynet. VTU har justeret § 7 (tidligere § 6) og bemærkningerne til bestemmelsen på den baggrund.

7. Delegation af Videnskabsministeriets kompetence (§ 8)

Region Nordjylland finder det problematisk, at bestemmelsen muliggør, at alle dele af den udøvende magt kan inddrages i GovCERT's aktiviteter og dermed blive medansvarlig for tjenestenens behandling af de samme ministeriers personoplysninger.

Videnskabsministeriet bemærker, at § 8 (tidligere § 7) i lovforslaget er en generel bemyndigelsesbestemmelse, som kan være relevant i situationer, hvor det på grund af f.eks. behov for særlig teknisk viden viser sig hensigtsmæssigt for videnskabsministeren at uddelegere sin kompetence til en anden myndighed – det være sig inden for eller uden for Videnskabsministeriets myndighedsområde.