# Oversigt over høringssvar til udkast til lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v.

1. BaneDanmark
2. Dansk Energi
3. Danske Regioner, herunder Region Nordjylland
4. Dansk IT
5. Datatilsynet
6. DI-ITEK
7. DK-CERT (UNI-C)
8. Domstolsstyrelsen
9. Erhvervs- og Byggestyrelsen
10. Finansrådet
11. Forbrugerrådet
12. IT-Politisk Forening
13. Kort og Matrikelstyrelsen
14. Politiets Efterretningstjeneste
15. PROSA
16. Rigsrevisionen
17. Telia
18. Tor Bloch

banedanmark

It & Telestyrelsen
Holsteinsgade 63, 4.sal
2100 København Ø

02.03.11

## Høring: Udkast til lovforslag om den statslige varslingstjeneste for internettruslers behandling af personoplysninger

Banedanmark har læst lovforslaget, som skal danne grundlag for etablering af den statslige varslingstjeneste GovCERT.

Lovforslaget er en forudsætning for at GovCERT kan indsamle oplysninger fra de tilsluttede myndigheder, for at kunne analysere sig frem til en given sikkerhedshændelse som rammer eller kan ramme virksomhedens it-infrastruktur via internettet.

Angreb via nettet er udbredte og der er eksempler på at cyberterrorister decideret går efter kritisk it-infrastruktur, og etablering af en GOVCERT skulle kunne give en større robusthed i tilfælde af et større cyberangreb.

Overvågning af internettrafik kan være med til at forebygge et sammenbrud, da der kan sættes ind med hurtige afværge foranstaltninger, således at vital it-infrastruktur ikke ødelægges eller afbrydes.

Lovforslaget beskriver rammerne for GovCERT og giver den nødvendige lovhjemmel til at behandle og indsamle personoplysninger som er indeholdt i de pakke og trafikdata som transmitteres til de tilsluttede myndigheder.

Banedanmark har ingen kommentarer til lovforslaget, og ser frem til at den statslige varslingstjeneste kan tilbyde de ydelser, som der lægges op til.

Venlig hilsen

Kenneth Lau Rentius
It-chef


| It | Telefon | Telefax | Journalnr. |
|---|---|---|---|
| Informationssikkerhed | 8234 0000 | | 051-0004 |
| Amerika Plads 15 | Direkte | maa@bane.dk | CVR 18632276 |
| 2100 København Ø | 82345803 | www.bane.dk | Side 1(1) |

**Høringssvar – Dansk Energi**

Til IT- og Telestyrelsen

Dansk Energi takker for modtagelsen af høring vedrørende udkast til lovforslag om den statslige varslingstjeneste for internettruslers (GovCERT) behandling af personoplysninger.

Dansk Energi har ingen bemærkninger til det fremsendte, men takker for muligheden for at komme med kommentarer.

**Med venlig hilsen**

Mie Yung Glockmann
Konsulent, cand.jur.
+45 35 300 477 +45 22 750 477
-
Dansk Energi
Rosenørns Alle 9
1970 Frederiksberg C
+45 35 300 400

N O T A T

DANSKE REGIONER

IT og Telestyrelsen, GovCERT

Sendt til: info@govcert.itst.dk

04-03-2011

Sag nr. 11/463

Dokumentnr. 12300/11

**Regionernes bemærkninger til udkast til lovforslag om den statslige varslingstjeneste for internettruslers behandling af personoplysninger**

Danske Regioner har indhentet bemærkninger til lovforslaget fra de enkelte regioner.

I bemærkningerne fra Region Hovedstaden, Region Sjælland og Region Nordjylland støttes hensigten med GovCERT, herunder at GovCERT medvirker til, at der i staten er overblik over trusler og sårbarheder i tjenester, net og systemer på internettet.

Der er ligeledes opbakning til, at GovCERTs behandling af personoplysninger reguleres ved lov.

Det er en bemærkning fra Region Hovedstaden, til teksten i § 3, hvor der står, at ”Fristerne i nr. 1-3 beregnes fra tidspunktet for registreringen af de pågældende data i den statslige varslingstjeneste”. Her bør ”registrering” defineres, idet det ellers vil give anledning til fortolkning.

Samtidig er der fra Region Nordjyllands side udtrykt bekymring for om alarmsystemet i form af et såkaldt Intrusion Detection System (GovCERT IDS) vil have den ønskede effekt, herunder om triggermekanismen til langtidslagring og analyse af personoplysninger teknisk set er tilstrækkelig. Der henvises til vedlagte bemærkninger til lovforslaget fra Region Nordjylland.

Bilag: Høringssvar fra Region Nordjylland

REGION NORDJYLLAND

Til
Danske Regioner

**Høringssvar:**

**Udkast til lovforslag om den statslige varslingstjeneste for internettruslers behandling af personoplysninger**

**Regionssekretariatet**
Informationssikkerhed

Niels Bohrs Vej 30
Postboks 8300
9220 Aalborg Øst
Tlf.: 9635 1000
Fax. 9815 2009
www.rn.dk

Direkte:

Ref.:Steen Ledet

Journalnummer: 1-10-82-0002-11

Dato: 1. marts 2011

Region Nordjylland støtter bestræbelser, der kan sikre at kanaler, der benyttes til digital kommunikation mellem borgere og myndigheder samt kommunikationen mellem myndighederne, er minimalt sårbare over for trusler, som kan afbryde kommunikationen.

For internettet og andre åbne kanaler krypterer regionen personhenførbar information. Regionens ansatte har mulighed for at benytte internettet til privat brug i beskedent omfang. Privat brug skal naturligvis beskyttes på lige fod med regionens kommunikation. Endelig driver regionen sygehuse og tilbud til borgerne 24/7. Vi kan ikke i fuld udstrækning forudse produktionen, så en typisk kommunikationsprofil hen over døgnet er vanskelig at etablere.

Driftsmæssigt benytter regionen forskellige netværk både til andre virksomheder i sundhedsvæsenet og til vore leverandører af drift og serviceydelser.

Lovforslaget har i § 3 en meget svævende beskrivelse af en sikkerhedshændelse og hvornår man må gemme pakke- og trafikdata i forhold til den. Varslingstjenesten er jo baseret på, at man altid har en begrundet mistanke om en forventet sikkerhedshændelse. Så det er ikke begrundelse nok for at gemme pakkedata i lang tid. I § 3, stk. 2 har man efter reglen maksimalt 14 dage til at afgøre om der er tale om en konkret sikkerhedshændelse, som kan begrunde lagring af pakkedata i længere tid.

Problemet med en IDS placeret uden for de IPS-tiltag der er internt i en virksomheds tekniske infrastruktur, er at den til de fleste af varslingstjenestens brugere er ubrugelig og vil generere så mange falske positiver, at den udvidede lagringsperiode bliver ulovlig.

Vi og vore samarbejdspartnere og de kriminelle samt andre, der vil os det ondt krypterer pakkedata. Vi gør det for at beskytte personoplysninger. Da man ikke i varslingstjenesten kan skelne mellem lovligt og ulovligt indhold vil man med tid og datakraft nok kunne tilgå selv krypteret information. Vi er forpligtet til at meddele en sådan tiltvunget adgang til de berørte personer. Derfor er vi ikke interesserede i, at pakkedata gemmes længere end nødvendigt. Vi kan ikke se meningen i at gemme pakkedata ud over de 14 dage.

Varslingstjenesten skal jo nødvendigvis følges op ved en konkret sikkerhedshændelse af tiltag, der ud fra analyser af trafikdata får nogle filtre aktiveret. Derfor er det er væsentligt at koncentrere sig om trafikdata på indgående trafik. Udgående trafik vil give for mange falske positiver.

Det beskrevne tilsyn i § 6 er åbenbart uden beføjelser mht. behandlingen af personoplysninger og kan ikke betegnes som uafhængigt.

§ 7 er interessant, da den muliggør, at alle dele af den udøvende magt kan inddrages i den statslige varslingstjenestes aktiviteter og dermed blive medansvarlig for tjenestens behandling af de samme ministeriers personoplysninger på internettet.

Begrebet "Kritisk infrastruktur" bør reserveres til den tekniske infrastruktur. Virksomhederne nævnt i § 1, stk. 2 er betydende for Danmarks almindelige drift.

Generelt om lovforslaget mener vi, at det ikke har en brugbar kvalitet, som regionen kan drage nytte af i vore bestræbelser på at håndtere og forklare borgerne om vor behandling af persondata. Vi er til stadighed fuldstændig bundne af Persondatalovens § 41, stk. 3. Internettet er i kommunikationssammenhæng ikke at betragte som tilhørende nogle andre rent juridisk. Varslingstjenesten er juridisk at betragte som en databehandler, da vi har dataansvaret for personoplysninger indtil de når den oprindelige destination. Vi skal have en databehandleraftale med denne tjeneste. Det vil blive temmelig uoverskueligt at varetage dette ansvar hvis der hos regionen og en anden modtagende myndighed er IDS-bokse, som har forskellige opfattelser af en situation og derfor lagrer vore pakkedata uden at vi er orienteret om det.

Vi er enige i, at landets kritiske tekniske infrastruktur skal sikres. Det findes der mange grundlæggende tekniske metoder til at opnå, men trafikovervågning er blot en enkelt af disse. Reglen er, at man implementerer sikkerhedsforanstaltninger ud fra en risikovurdering. I denne risikovurdering, skal man naturligvis inddrage de relevante scenarier baseret på en BIA. Lovforslaget antager, at der ikke differentieres, så personoplysninger må være til rådighed for tjenesten altid. Det ville efter vor mening give et mere brugbart resultat hvis staten kortlægger og udbygger en teknisk infrastruktur. Skal vi have individuel støtte, så skal det være til opbygning og vedligeholdelse af en lokal IPS-funktionalitet.

4. marts 2011

IT- & Telestyrelsen
Att. Hans Bøgesvang Riis

**Høring vedrørende udkast til lovforslag om den statslige varslingstjeneste for internettruslers (GovCERT) behandling af personoplysninger.**

DANSK IT er inviteret til at afgive høringssvar vedr. udkast til lovforslag om den statslige varslingstjeneste for internettruslers (GovCERT) behandling af personoplysninger.

DANSK IT deler fuldt Videnskabsministeriets og IT- & Telestyrelsens erkendelse af internettets vigtighed for samfundet. Endvidere erkender DANSK IT fuldt ud behovet for at GovCERT i visse tilfælde og i forbindelse med beskyttelsen af den offentlige digitale infrastruktur og væsentlige private aktører, undtagelsesvist kan behandle personlige og personfølsomme oplysninger.

Foreningen mener dog at det bør sikres at dette sker efter en model hvor det til alle tider er muligt at dokumentere, hvem der har haft adgang til hvilke data. Og at det samtidig organisatorisk sikres at adgangen til personlige eller personfølsomme oplysninger kun sker af personer, for hvem det tekniske og sikkerhedsmæssige aspekt af denne adgang er relevant. Det må endvidere ikke være muligt for enkeltpersoner (uanset deres rang, arbejdsfunktion eller andet) at kunne ændre i de logdata der skabes i forbindelse med adgangen til personlige eller personfølsomme oplysninger.

DANSK IT hilsner tilsynet med den statslige varslingstjeneste velkomment. Men mener, at tilsynet skal være tilstrækkeligt repræsenteret med relevante stærke tekniske kompetencer for at sikre et fyldestgørende tilsyn med den statslige varslingstjeneste.

DANSK IT står naturligvis til rådighed for uddybning af de fremførte spørgsmål og anbefalinger.

Med venlig hilsen
DANSK IT

Benjamin Willum Funder
politisk konsulent

DATATILSYNET

IT- og Telestyrelsen
Holsteinsgade 63
2100 København Ø

Sendt til: info@govcert.itst.dk

7. marts 2011

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2011-112-0406
Sagsbehandler
Vita Horneman
Direkte 3319 3232

**Vedrørende høring over udkast til lovforslag om den statslige varslingstjeneste for internettruslers (GovCERT) behandling af personoplysninger**

Datatilsynet har ved e-post af 11. februar 2011 modtaget ovenstående udkast til lovforslag i høring.

Datatilsynet skal i den anledning bemærke følgende:

**1.** Udkastets § 3, stk. 1, har følgende ordlyd:

> "§ 3 Den statslige varslingstjeneste for internettrusler behandler, herunder registrerer, analyserer og opbevarer, uden retskendelse tilsluttede myndigheders og private virksomheders ind- og udgående pakke- og trafikdata. Den statslige varslingstjeneste for internettrusler må alene analysere indsamlede pakkedata i tilfælde af begrundet mistanke om en stedfunden eller forventet sikkerhedshændelse og kun i det omfang, det er nødvendigt for den pågældende analyse."

Den 18. februar 2010 afgav Datatilsynet – efter behandling i Datarådet – en udtalelse om de påtænkte databehandlinger hos GovCERT. Tilsynet tilkendegav bl.a. følgende:

"**2.1.** Som udgangspunkt kan offentlige myndigheder efter persondataloven[1] indsamle og registrere personoplysninger, når det er nødvendigt for varetagelsen af myndighedens opgaver.

Vurderingen af, i hvilket omfang det i forbindelse med analyse- og varslingstjenesten er nødvendigt for GovCERT at behandle personoplysninger, der indgår i nettrafikken, må i første omgang foretages af IT- og Telestyrelsen som dataansvarlig myndighed.

De påtænkte databehandlinger indebærer imidlertid en omfattende overvågning af internettrafik til og fra offentlige myndigheder, som omfatter både trafikinformation og trafikindhold. Datatilsynet skal endvidere pege på, at indsamling og registrering at oplysninger om internettrafik på andre områder sker i henhold til lovhjemmel[2].

Datatilsynet finder derfor, at IT- og Telestyrelsen og Videnskabsministeriet nøje må overveje, om GovCERTs aktiviteter herunder behandlingen af personoplysninger i forbindelse med

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.
[2] Det gælder f.eks. reglerne i bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen, bek. nr. 988 af 28/09/2006) og reglerne om hastesikring i retsplejeloven.

analyse og varslingsopgaverne er af en sådan karakter, at der bør søges tilvejebragt særskilt lovhjemmel."

Datatilsynet noterer sig, at der med det foreliggende lovforslag er lagt op til etablering af en sådan særskilt lovhjemmel.

Efter Datatilsynets opfattelse må det herefter bero på en politisk vurdering, hvorvidt den ønskede lovhjemmel, der fortsat indebærer en omfattende overvågning af internettrafik til og fra offentlige myndigheder – omfattende både trafikdata og trafikindhold, skal tilvejebringes.

**2.1.** Adgangen til trafik- og pakkedata beskrives i lovforslagets almindelige bemærkninger, pkt. 3.3.

Det fremgår bl.a., at det med GovCERTs alarmsystem ikke p.t. er 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 ifølge udkastet kun skelnes mellem adgang til pakkedata eller adgang til trafikdata. Det fremgår endvidere, at GovCERT vil følge mulighederne tæt for at finde en teknisk løsning herpå.

Datatilsynet skal i tilknytning hertil på ny[3] understrege vigtigheden af, at GovCERT holder sig ajour med mulighederne for anvendelse af privatlivsfremmende teknologier, f.eks. således, at e-mails, som ikke viser tegn på virus eller spam, automatisk slettes straks ved indsamlingen i IDS'en forud for overførsel af data til videre behandling i GovCERT. Som alternativ til helt at slette e-mails kan man f.eks. slette eller overskrive indholdet i e-mails straks ved indsamlingen i IDS'en forud for en overførsel af data til videre behandling i GovCERT.

**2.2.** § 3, stk. 2 har følgende indhold:

> "Stk. 2. Den statslige varslingstjeneste for internet trusler sletter de i stk. 1 nævnte pakke- og trafikdata, når formålet med behandlingen er opfyldt. Uanset, at formålet med behandlingen ikke er opfyldt, kan
>
> 1) pakke- og trafikdata, der knytter sig til en konkret sikkerhedshændelse, maksimalt opbevares i tre år.
> 2) pakkedata, der ikke knytter sig til en konkret sikkerhedshændelse, maksimalt opbevares i 14 dage.
> 3) trafikdata, der ikke knytter sig til en konkret sikkerhedshændelse, maksimalt opbevares i 12 måneder.
>
> Fristerne i nr. 1-3 beregnes fra tidspunktet for registreringen af de pågældende data i den statslige varslingstjeneste."

Følgende fremgår af udkastets pkt. 3.3.:

> "Der er lagt op til, at pakke- og trafikdata, som knytter sig til en konkret sikkerhedshændelse, kan opbevares i tre år. Pakkedata, der ikke er knyttet til en konkret sikkerhedshændelse, kan maksimalt lagres i 14 kalenderdage. Som udgangspunkt vil pakkedata dog kun blive opbevaret i seks kalenderdage. Trafikdata, som ikke knytter sig til en konkret sikkerhedshændelse, kan maksimalt opbevares i 12 måneder. Det er vigtigt at være opmærksom på, at fristerne alle er maksimumfrister. GovCERT vil lø-

[3] Datatilsynet har i sin udtalelse af 18. februar 2010 ligeledes henvist til anvendelse af privatlivsfremmende teknologier

> bende være forpligtet til at slette data, som ikke længere er relevante for GovCERT's virke, uanset at fristerne beskrevet i § 3 ikke er overskredet. Derudover er det i § 3 fastsat, at indsamlede pakkedata kun vil kunne blive analyseret af GovCERT, hvis der er begrundet mistanke om en sikkerhedshændelse, og at det kun er den relevante del af de indsamlede data, som kan analyseres."

Endvidere fremgår følgende:

> "Længden af fristerne i § 3 er fastsat på baggrund af en proportionalitetsafvejning af hensynet til GovCERT's virke set i forhold til hensynet til privat livets fred. Det er i visse situationer væsentligt for GovCERT at kunne sammenholde nyindsamlede data med ældre data for f.eks. at kunne analysere et it-angreb nærmere. Heroverfor står hensynet til de berørte borgeres privatliv. Denne afvejning har resulteret i de nævnte frister, som også er fastsat under inddragelse af erfaringer fra andre landes CERT'er."

Af bemærkningerne til § 3 fremgår bl.a. følgende:

> "Det vurderes, at de foreslåede maksimale opbevaringsperioder er de kortest mulige i forhold til formålet med GovCERT. Det er i den forbindelse væsentligt at være opmærksom på, at GovCERT med vedtagelsen af lovforslaget alene 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 privat livets fred."

Datatilsynet har noteret sig, at der er foretaget en proportionalitetsafvejning og på den baggrund beskrevet sletterutiner.

Det står imidlertid ikke Datatilsynet klart, hvorfor det er nødvendigt at opbevare pakkedata i op til 14 dage, hvis der ikke er tegn på sikkerhedshændelser. Datatilsynet skal anbefale, at det i bemærkningerne præciseres, hvorfor det overhovedet er nødvendigt at opbevare pakkedata i situationer, hvor der ikke er tegn på sikkerhedshændelser, samt at det præciseres, hvorfor perioden på 14 dage er valgt, når det samtidig fremgår af bemærkningerne, at pakkedata som udgangspunkt kun vil blive opbevaret i 6 dage.

**3.** Lovforslaget indeholder under de almindelige bemærkninger et afsnit 2 med overskriften "Gældende ret". I afsnittet omtales visse af persondatalovens regler.

Frem for denne omtale af visse, men ikke alle relevante regler vil Datatilsynet foreslå, at der i afsnittet om gældende ret blot gives en mere overordnet og generel henvisning til persondataloven og det efterfølgende afsnit om forholdet til persondataloven.

I den forbindelse skal Datatilsynet bemærke, at også andre love end persondataloven kan have betydning for GovCERT. Datatilsynet skal navnlig pege på reglerne om meddelelseshemmeligheden, jf. herunder også lovforslagets senere afsnit herom.

Hertil kommer, at persondataloven på teleområdet suppleres af særregler i telelovgivningen, som gennemfører det særlige databeskyttelsesdirektiv vedrørende elektronisk kommunikation (e-databeskyttelsesdirektivet, direktiv

2002/58/EF). Datatilsynet går ud fra, at IT- og Telestyrelsen har overvejet, om dette kan være relevant.

**4.** Udkastes § 6 har følgende ordlyd:

> "**§ 6.** Ministeren for videnskab, teknologi og udvikling nedsætter et uafhængigt tilsyn, der følger den statslige varslingstjeneste for internet truslers virksomhed.
> Stk. 2. Tilsynet består af en dommer som formand og fire sagkyndige medlemmer. Formanden og medlemmerne af tilsynet beskikkes af ministeren for videnskab, teknologi og udvikling. Ministeren for videnskab, teknologi og udvikling skal ved beskikkelsen af tilsynets medlemmer lægge vægt på, at tilsynet samlet repræsenterer juridisk, it-revisionsmæssig og sikkerhedsmæssig sagkundskab.
> Stk. 3. Medlemmerne beskikkes for fire år ad gangen og kan genbeskikkes.
> Stk. 4. Ministeren for videnskab, teknologi og udvikling fastsæt ter rammerne for tilsynets virksomhed. Ministeren for videnskab, teknologi og udvikling kan herunder beslut te, 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 i forbindelse med tilsynets virksomhed."

Det fremgår af bemærkningerne til § 6, at formålet med bestemmelsen er at pålægge Ministeren for videnskab, teknologi og udvikling at nedsætte et uafhængigt tilsyn, der skal følge GovCERT's virksomhed, og at Ministeren for videnskab, teknologi og udvikling fastsætter nærmere regler for tilsynets virksomhed.

Det fremgår endvidere af bemærkningerne til § 6, at det er hensigten, at tilsynet skal forestås af en dommer 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 – i lighed med ordningen, der er kendt fra Wamberg-udvalget, der fører tilsyn med Politiets Efterretningstjenestes og Forsvarets Efterretningstjenestes behandling af personoplysninger. Det er endvidere ifølge bemærkningerne en forudsætning, at tilsynets medlemmer kan sikkerhedsgodkendes.

Ifølge bemærkningerne til § 6 har Datatilsynet samtidig hermed fuld inspektionskompetence i forhold til de registrerede og opbevarede oplysninger, jf. persondatalovens § 62, stk. 2, om behandling, der foretages for den offentlige forvaltning, og at bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige sektor, finder anvendelse.

Det fremgår endvidere af udkastet til lovforslag pkt. 3.5., at lovforslaget for at sikre, at GovCERTs behandling af personoplysninger er i overensstemmelse med lovforslaget og gældende ret i øvrigt, indeholder en bestemmelse om, at Ministeren for Videnskab, Teknologi og Udvikling nedsætter et uafhængigt tilsyn, som skal følge GovCERTs virksomhed. Tilsynet vil bl.a. kunne bestå i en årlig afrapportering til Ministeren for Videnskab, Teknologi og Udvikling om GovCERTs virksomhed. Tilsynet skal ifølge udkastet have en dommer som formand.

Det fremgår endvidere af udkastet, pkt. 3.6.4., at en registreret person kan klage til Datatilsynet over GovCERTs behandling af personoplysninger vedrørende den pågældende, jf. persondatalovens § 40 og kapitel 16.

Det fremgår af PIA'en[4] for GovCERT, s. 21, at GovCERT er underlagt tilsyn af Rigsrevisionen, Datatilsynet og et uafhængigt tilsyn. IT- og Telestyrelsen har oplyst, at lovforslaget ikke har til hensigt at afskære Datatilsynets kompetence.

Datatilsynet ser positivt på tiltag, som kan understrege og forankre ansvaret for behandlingen af personoplysninger hos den dataansvarlige. Datatilsynet har således senest i forbindelse med sin udtalelse til Justitsministeriet vedrørende Kommissionens oplæg om beskyttelse af personoplysninger[5], tilkendegivet, at der er behov for at sætte beskyttelse af persondata, herunder overholdelse af gældende lovgivning, på dagsordenen i alle projekter, og at gøre projekterne ansvarlige for at udvikle løsningerne i den ønskede retning. Datatilsynet kan i den anledning også henvise til Artikel 29-gruppens udtalelse 3/2010[6] om princippet om ansvarlighed.

Efter Datatilsynets opfattelse vil det imidlertid være meget uhensigtsmæssigt, hvis GovCERTs behandling af personoplysninger er underlagt tilsyn fra to forskellige tilsynsorganer – begge med en dommer som formand. Datarådet har således haft en højesteretsdommer som formand siden sin etablering.

I det foreliggende udkast fremstår det endvidere uklart, hvilke opgaver, ansvar og kompetencer det særlige tilsyn med GovCERT tilsigtes at skulle have – sammenholdt med de opgaver og kompetencer, som Datatilsynet har efter persondataloven. Det bemærkes i den forbindelse, at Datatilsynet ikke har kompetence i forhold til efterretningstjenesternes behandling af personoplysninger. På dette område føres tilsynet af det såkaldte Wamberg-udvalg, som også omtales i lovforslagets bemærkninger.

Datatilsynet mener, at den foreslåede tilsynsmodel bør genovervejes. Under henvisning til, at der skal ske en omfattende behandling af personoplysninger af særlig teknisk karakter, kan der være gode grunde til at overveje en tilsynsmodel, som giver et mere intensivt tilsyn end det, som Datatilsynet vil kunne føre efter persondataloven.

Efter persondatalovens regler – og inden for de nuværende ressourcemæssige rammer – vil Datatilsynet således på ingen måde kunne følge GovCERTs daglige virksomhed, lave årlig afrapportering mv.

---

[4] Privatlivsimplikationsanalyse (PIA) for GovCERT IDS (Intrusion Detection System), som er tilgængelig på www.digitaliser.dk

[5] Datatilsynets j.nr. 2010-111-0063, som er tilgængelig på Datatilsynets hjemmeside

[6] Udtalelsen er tilgængelig på Artikel 29-gruppens hjemmeside: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_da.pdf

Hvis der etableres et særligt tilsyn på dette område, bør det fremgå klart af lovforslaget og dets bemærkninger, at det særlige tilsyn træder i stedet for Datatilsynet. Det bør samtidig sikres, at et sådant særligt tilsyn har de kompetencer og beføjelser, som forudsættes efter databeskyttelsesdirektivets regler[7].

**5.** Lovforslagets afsnit om forholdet til persondataloven ses ikke at forholde sig til persondatalovens § 27 om overførsel af oplysninger til tredjelande.

Datatilsynet skal anbefale, at forholdet til persondatalovens § 27 tydeliggøres i lovforslaget. Tilsynet skal i den forbindelse pege på, at det for så vidt angår udkastets § 5 om videregivelse af oplysninger til politiet ikke fremgår, om der alene kan videregives oplysninger til dansk politi, eller om bestemmelsen også vil omfatte udenlandske politimyndigheder.

Opmærksomheden henledes endvidere på udkastets § 5, stk. 2, idet det ikke fremgår af bestemmelsen eller bemærkningerne, om der kan videregives oplysninger til CERT'er uden for EU. I så fald må forholdet til persondatalovens § 27 også i denne sammenhæng tydeliggøres.

Datatilsynet skal i den forbindelse henlede opmærksomheden på, at det følger af persondatalovens § 27, stk. 3, nr. 4, at der kan overføres oplysninger til tredjelande, hvis overførslen er nødvendig eller følger af lov eller bestemmelser fastsat i henhold til lov for at beskytte en vigtig samfundsmæssig interesse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

**6.** Datatilsynet skal henlede opmærksomheden på, at GovCERTs anmeldelse til Datatilsynet (jf. j.nr. 2010-54-0870) skal tilrettes i overensstemmelse med et eventuelt vedtaget lovforslag. Dette kan gøres elektronisk via Datatilsynets hjemmeside.

**7.** Datatilsynet skal endelig for god ordens skyld bemærke, at det følger af persondatalovens § 57, at der ved udarbejdelse af bekendtgørelser, cirkulærer eller lignende retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger, skal indhentes en udtalelse fra Datatilsynet.

Med venlig hilsen

Janni Christoffersen
Direktør

[7] Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, se især artikel 28 og betragtning 62-64

IT- og Telestyrelsen
Att.: GovCERT
Holsteinsgade 63
København Ø

Danish ICT and Electronics Federation

## Høring vedrørende udkast til lovforslag om den statslige varslingstjeneste for internettruslers (GovCERT) behandling af personoplysninger

IT- og Telestyrelsen har ved mail af 11. februar anmodet DI ITEK om eventuelle bemærkninger til "Lovforslag om den statslige varslingstjeneste for internettruslers (GovCERT) behandling af personoplysninger. DI ITEK takker for muligheden for at afgive kommentarer og har nedenstående bemærkninger til lovforslaget.

Internettet er af afgørende betydning for, at det danske samfund kan indrettes og fungere effektivt og give borgerne adgang til en bred vifte af nyttige og spændende tjenester. Det er imidlertid i denne sammenhæng vigtigt, at borgerne kan færdes trygt på nettet. Dannelsen af en GovCERT i Danmark er et af flere elementer, som bibringer til at understøtte denne tryghed i den betydning, at GovCERT kan bidrage til at sikre tilgængelighed, fortrolighed og integritet på den danske del af nettet. Henset til hvad der er sket andre steder i verden – f.eks. Estland – og hvad Danmark selv har oplevet af angreb rettet mod dansk infrastruktur, er dannelsen af GovCERT er vigtigt skridt i retning af at forbedre landets informationssikkerhed. Dannelsen af GovCERT på nuværende tidspunkt er også at udvise rettidig omhu i forhold til den angreb, som kan komme i fremtiden. Det er vigtigt, at Danmark får en myndighed, som kan indgå i det internationale samarbejde for at bekæmpe it-kriminalitet. Det er med stor glæde, at vi kan konstatere, at den danske GovCERT blev funktionsdygtig i december 2010.

Imidlertid rummer dannelsen af en GovCERT også visse muligheder for at skabe utryghed for danske borgere. GovCERTens setup er baseret på IDS (p. 10) med henblik på at få indblik i pakkedata og trafikdata, som tilgår statslige myndigheder m.fl. Det betyder, at GovCERT principielt set kan få adgang til al elektronisk kommunikation mellem borgerne og myndighederne. Principielt set vil man kunne se skatteoplysninger, sundhedsoplysninger og sociale oplysninger på de enkelte borgere. Jo flere der har adgang til disse oplysninger, jo større usikkerhed er der omkring data, og jo større utryghed kan der være for borgerne.

Utrygheden kan forværres af, at GovCERT ud fra en sagligheds- og proportionalitetsvurdering undtages mange af de bestemmelser, der normalt bidrager til borgernes retssikkerhed og skaber tryghed for behandling af persondata hos borgerne.

Postadresse/Postal address
1787 København V
Danmark
(+45) 3377 3377
itek@di.dk
itek.di.dk

Besøgsadresser/Visiting addresses
Hannemanns Allé 25
København S
Sundkrogskaj 20
København Ø

CVR: 16 07 75 93

Undtagelserne omfatter bl.a. Grundlovens § 72 (p. 22) og Den Europæiske Menneskerettighedskonvention artikel 8 (p. 23) der begge vedrører meddelelseshemmeligheden, Lov om behandling af personoplysnings bestemmelser om samtykke til behandling (p. 21), oplysningspligt (p. 22), indsigtsret (p.22) og indsigelsesret (p. 22).

DI ITEK er enig i, at der er et stort behov for at sikre beskyttelse af statslige institutioner primært og desuden af kommuner, regioner og kritisk infrastruktur sektorer bedst muligt. Derfor er det nødvendigt at iværksætte tiltag, som dem GovCERT beskæftiger sig med. Det er tilsvarende i den konkrete sag nødvendigt med nogle vide reguleringsmæssige rammer, for at GovCERT operationelt kan fungere. Loven lægger også op til en god beskyttelse ved:

- at beskytte data fornuftigt
- at begrænse adgangen til data mest muligt
- at have et godt præcist afgrænset formål
- at slette data så hurtigt som muligt
- at lagre de data, som er relevante, i en fornuftig periode
- at sikre ekstern kontrol gennem et selvstændigt Tilsyn
- at Datatilsynet desuden kan lave tilsyn.

Endelig kommer det faktum at borgere, som ønsker sig særlig sikkerhed kan kryptere deres meddelelser, som så kommer igennem GovCERT IDS uden at blive læst. På denne baggrund finder DI ITEK det nødvendigt at bakke op bag det nuværende lovforslag.

I takt med at teknologierne i samfundet modnes kan der dog være behov for at modernisere loven. Generelt bør der arbejdes på, at man kan skabe tillid til en part i en kommunikation uden at denne er identificeret. Når f.eks. denne type teknologi er tilstrækkeligt modnet vil kommunikation mellem to trustede parter kunne undtages IDS. På den måde kan man gøre overvågningen mindre indgribende set over den samlede mængde af kommunikation, som overvåges. Generelt er det vigtigt, at overvågningen holdes på et minimum. DI ITEK anbefaler derfor, at loven suppleres med en evalueringsforpligtelse, hvor det f.eks. hvert andet år vurderes, om GovCERT kan foretage mindre indgribende tekniske analyse, end den nuværende IDS på al kommunikation.

DI ITEK står gerne til rådighed for uddybende kommentarer.

Med venlig hilsen

Henning Mortensen
Chefkonsulent
DI ITEK

**Høringssvar – DK-CERT (UNI-C)**

IT- og Telestyrelsen

Med henvisning til styrelsens høring af 11. februar 2011 vedrørende udkast til lovforslag om den statslige varslingstjeneste for internettruslers (GovCERT) behandling af personoplysninger skal vi oplyse, at UNI-C (DKCert) ikke har bemærkninger til det fremsendt udkast.

Med venlig hilsen

Erik A. Larsen
Fuldmægtig

UNI•C
Koncern it
Vermundsgade 5,
2100 København Ø
Direkte tlf. 3587 8532
UNI•C tlf. 3587 8889
Erik.larsen@uni-c.dk

Domstolsstyrelsen

Ministeriet for Videnskab, Teknologi og Udvikling
Bredgade 43
1260 København K

Store Kongensgade 1-3
1264 København K
Tlf. +45 70 10 33 22
Fax +45 7010 4455
post@domstolsstyrelsen.dk
CVR nr. 21-65-95-09
EAN-nr.5798000161184

J. nr. 2011-4102-0008-2

Sagsbeh. Rune Sorvad Kock
Dir.tlf.
Mail rsk@domstolsstyrelsen.dk

10. marts 2011

**Høring vedrørende udkast til lovforslag om den statslige varslingstjeneste for internettruslers behandling af personoplysninger**

Ministeriet for Videnskab, Teknologi og Udvikling
har i en e-mail af 14. februar 2011 anmodet Domstolsstyrelsen om eventuelle bemærkninger til udkast til lovforslag om den statslige varslingstjeneste for internettruslers behandling af personoplysninger.

Det fremgår af lovforslagets § 6, at ministeren for videnskab, teknologi og udvikling nedsætter et uafhængigt tilsyn, som ifølge stk. 2 skal bestå af en formand som er dommer, der beskikkes af ministeren for videnskab, teknologi og udvikling.

Domstolsstyrelsen skal i den anledning bemærke, at Ministeriet for Videnskab, Teknologi og Udvikling i den forbindelse bør være opmærksom på om lovforslagets § 6, stk. 2, er i overensstemmelse med reglerne i retsplejelovens § 47 a, stk. 3, vedrørende udpegning af dommere til offentligt eller privat råd eller nævn.

I øvrigt skal Domstolsstyrelsen henlede ministeriets opmærksomhed på Justitsministeriets skrivelse fra december 2000, hvori justitsministeren anmodede samtlige ministerier om, at ministerierne for fremtiden i forbindelse med oprettelse af nye nævn alene indsætter bestemmelser om dommermedvirken efter en vurdering af, om sådanne bestemmelser er tilstrækkeligt velbegrundede.

Bibeskæftigelsesnævnet får kopi af dette brev til orientering.

Med venlig hilsen

Niels Juhl

**Høringssvar - Erhvervs- og Byggestyrelsen**

Vi har ingen kommentarer til denne her høring.

Med venlig hilsen

Trine M. T. Hansen
Sekretær
Erhvervs- og Byggestyrelsen
Dahlerups Pakhus
Langelinie Allé 17
2100 København Ø
Tlf. 35 46 66 21

FINANSRÅDET

IT- og Telestyrelsen
Holsteinsgade 63, 4. sal
2100 København Ø

Att. info@govcert.itst.dk

# Høringssvar til lovforslag om GovCERTs behandling af personoplysninger

28. februar 2011

Finanssektorens Hus
Amaliegade 7
1256 København K

Telefon 3370 1000
Fax 3393 0260

mail@finansraadet.dk
www.finansraadet.dk

Journalnr. 466/01
Dok. nr. 278196-v1

Ved brev af 11. februar 2011 har IT- og Telestyrelsen sendt ovennævnte udkast i officiel høring og anmodet om Finansrådets bemærkninger.

Finansrådet bifalder beslutningen om at etablere et statsligt CERT i Danmark, og det glæder os at se, at det har været muligt at etablere en funktionsduelig enhed så hurtigt efter beslutningen om etablering.

Finansrådet støtter lovforslaget, som giver GovCERT hjemmel til at behandle personoplysninger, som led i arbejdet omkring varsling og informationsindsamling samt reduktion af de risici, der er forbundet med anvendelse af internettet. Dette svarer til god praksis i andre tilsvarende varslingstjenester.

Vi er enige i vurderingen af, at behandling af personoplysninger er påkrævet for, at varslingstjenestens formål kan opfyldes (lovforslag side 8). Opgaven omkring it-sikkerhed og kriminalitetsbekæmpelse er af væsentlig samfundsmæssig betydning, men over for dette står hensynene til privacy, som ikke må glemmes. Af denne grund har Finansrådet med tilfredshed noteret, at der er sket formel registrering i Datatilsynets fortegnelse, og der er givet retningslinjer for sikker og adækvat behandling af personoplysningerne.

I takt med, at Internettet spiller en stadig større rolle i samfundet, er it-sikkerhed blevet en væsentlig samfundsmæssig opgave. Mange forsyningsmæssige, logistiske og økonomiske opgaver varetages allerede igennem internetanvendelse, og udviklingen går imod stadigt øget anvendelse af elektroniske tjenester såvel i det private som i det offentlige regi. Af samme grund er det af største betydning, at borgere og virksomheder trygt kan anvende Internettet.

I forhold til den opgave GovCERT skal varetage, vil Finansrådet henlede opmærksomheden på, at truslerne mod den offentlige infrastruktur i fremtiden også kan få en anden karakter end de trusler, som har dannet grundlaget for lovforslaget. Finansrådet tænker specielt på angreb med avanceret kriminelt software, som eksempelvis trojanere, der går efter specifikke, fortrolige oplysninger. Derfor er det relevant allerede nu at overveje, hvordan GovCERT kan håndtere dette i fremtiden.

Ud over lovforslaget vedrørende GovCERTs behandling af personoplysninger vil Finansrådet gerne henlede opmærksomheden på Memorandum of Understanding mellem medlemmerne af DK-CERT, GovCERT og ISP Sikkerhedsforum vedrørende bekæmpelse af botnets. Initiativet viser et fremsynet syn på it-sikkerhed, hvor centrale tiltag bliver mulige igennem samarbejde. Finansrådet støtter dette samarbejde.

Journalnr. 466/01
Dok. nr. 278196-v1

Med venlig hilsen

Henriette Rolskov

Direkte 3370 1102
her@finansraadet.dk

**Høringssvar - Forbrugerrådet**

Forbrugerrådet har af ressourcemæssige årsager ikke mulighed for at forholde os til lovforslag om den statslige varsligstjeneste for internettruslers (GovCERT) behandling af personoplysninger. Forbrugerrådet kan således ikke tages til indtægt for at støtte forslaget eller for at gøre det modsatte.

Med venlig hilsen

Anette Høyrup
Jurist
Forbrugerrådet

Danish Consumer Council
Fiolstræde 17, Postboks 2188, 1017 København K, Danmark

**Høringssvar – IT-Politisk Forening**

IT-Politisk Forening påskønner, at GovCert har været meget åbne omkring både tjenestens funktion og dette lovforslag i høring.

IT-Politisk forening mener, at loven bør sikre at:

Den statslige varslingtjeneste ikke er bemyndiget til at opsamle eller tilgå datatrafik, hvor hverken afsender eller modtager frivilligt og eksplicit har tilsluttet sig tjenesten.

Selvom det ikke er GovCerts nuværende sigte, finder IT-Politisk Forening det vigtigt, at danske internetbrugere ikke kan blive overvåget af en statslig tjeneste, selvom internetudbydere skulle tilslutte sig varslingstjenesten.

IT-Pol mener ikke, at definitionerne af pakke- og trafikdata er tilstrækkeligt præcise. Alt efter hvilket lag i modellen for computernetværk, man behandler, kan det samme data være pakke- eller trafikdata. For eksempel er email-adresser pakkedata i TCP-forbindelser, men trafikdata i højere lag. IT-Politisk Forening mener at data, som fx email-adresser, hjemmesideadresser, o.lign, bør betragtes som pakkedata. Det er især vigtigt fordi trafikdata kan udleveres til varslingstjenester i andre lande (jvf § 5).

--
Niels Elgaard Larsen
Formand
IT-Politisk Forening

Miljøministeriet
Kort & Matrikelstyrelsen

Digital forvaltning og GIS
J.nr. 072-00017
Ref. tmj
Den 7. marts 2011

Høring af Forslag til Lov om den statslige varslingstjeneste for internet-truslers behandling af personoplysninger.

Lovforslaget tildeler den statslige varslingstjeneste for internettrusler beføjelser (§5), som kan være ret vidtgående m.h.t. opbevaring og videregivelse af personoplysninger. Et uvildigt tilsyn er da også foreslået.

I bemærkninger til lovforslagets enkelte bestemmelser om § 6 fremgår det, at man ønsker at pålægge ministeren for VTU, at nedsætte et uafhængigt tilsyn, der skal føre tilsyn med GovCert. Et sådant udvalg kunne f.eks være det eksisterende Wamberg udvalg, hvormed uvildigheden styrkes yderligere, idet det ikke er udpeget af VTU alene.

Af lovforslaget fremgår det, at der er tale om overvågning af kommunikation til og fra offentlig myndighed. Der vil således også kunne indgå privatpersoner i den kommunikation, der påtænkes overvåget.

I bemærkningerne til lovforslaget pkt. 3.4. fremgår det, at udveksling af trafikdata også omhandler ip-adresser. Er ip-adresser ikke at regne for personoplysninger ifølge Datatilsynet?

I pkt. 3.4.1 tales om videregivelse af oplysninger for iværksættelse af modforanstaltninger. F.eks. blokering af kommunikation med specifik ip-adressse. Den pågældende ip-adresse kunne tilhøre en privatperson, der kan være uvidende om eventuelt misbrug af ip-adressen. Er der hjemmel til en sådan foranstaltning? Hvordan informeres om, at en ip-adresse er lukket, og baggrunden for lukningen?

Af bemærkninger til lovforslagets enkelte bestemmelser er der om § 3 nævnt, at der ikke vil blive registreret trafikoplysninger fra hjemmearbejdspladser. Rent teknisk er det næppe muligt, at skelne imellem hjemmearbejdspladserne og de pc-arbejdspladser, der befinder sig i ministeriets forskellige lokaliteter. Hvordan ses dette problem varetaget?

I afsnittet om forholdet til den Europæiske Menneskerettighedskonvention anføres det, at det forudsættes, at den ansatte i forbindelse afsendelse af private e-mail giver samtykke til GovCert behandling af data. Hvordan ses dette i sammenhæng med bemærkninger til lovforslagets enkelte bestemmelser § 3, hvor det fremgår, at der kun vil blive registreret trafikdata?

Af § 5 fremgår det, at ”trafikdata kan videregives til danske myndigheder, tilsluttede private virksomheder og tilsvarende varslingstjenester i andre lande i henhold til varslingstjenestens formål”. Samme sted fremgår det, at

”pakke- og trafikdata, der knytter sig til en konkret sikkerhedshændelse, kan videregives til politiet”. Hvordan forventes informationen til de berørte parter udført? Ligger der en forventning om, at de enkelte ministerier skal varetage denne opgave?

Der ser ud til at være en forglemmelse, i bemærkningerne afsnit 3.7 om Grundlovens § 72. I det sidste afsnit i bemærkninger til lovforslagets enkelte bestemmelser, at proportionalitetsprincippet i forhold til § 72 er overvejet og henviser til et afsnit X.X, et afsnit der ikke ser ud til at findes.

Med venlig hilsen

Annette Dindorp
Souschef

POLITIETS EFTERRETNINGSTJENESTE
DANISH SECURITY AND INTELLIGENCE SERVICE

It og Telestyrelsen

info@govcert.itst.dk

Politiets Efterretningstjeneste
Klausdalsbrovej 1
DK-2860 Søborg
Telefon: +45 33 14 88 88
Telefax: +45 45 15 01 90
E-mail: pet@pet.dk
Web: www.pet.dk

Dato: 4. marts 2011
Jour. Nr. 2011-20-616

Ved e-mail af 11. februar 2011 har IT og Telestyrelsen anmodet om Politiets Efterretningstjenestes eventuelle bemærkninger til udkast til lovforslag om den statslige varslingstjeneste for internettruslers behandling af personoplysninger.

Politiets Efterretningstjeneste kan i den forbindelse oplyse, at udkastet ikke giver efterretningstjenesten anledning til bemærkninger.

Med venlig hilsen

Henrik Pass
politiassessor

København d. 13. marts 2011

Til IT- og Telestyrelsen

## Høring vedrørende udkast til lovforslag om den statslige varslingstjeneste for internettruslers (GovCERT) behandling af personoplysninger

PROSA takker for indbydelsen til at deltage i høringssvar om GovCert, ligesom PROSA gerne vil rose de initiativer, der blev taget i processen, hvor der var arrangementer med muligheder for at drøfte forslaget nærmere.

Med dette svar er det vores håb, at vi kan bidrage til den endelige udformning af GovCert – også selv om vores bidrag kommer noget sent.

PROSA har støttet oprettelsen af GovCert, og ser dets etablering som et meget positivt bidrag til at øge sikkerheden overfor varierede og stigende trusler fra kriminelle via internettet.

Vi noterer, at en Cert oprettes for at kunne øge informationer og varslinger om it-trusler og dermed give et forbedret risikobillede og bidrage til reaktioner fra de it-ansvarlige på trusler. Det er væsentligt for os at fremhæve, at GovCert hverken er en politimyndighed, en del af efterretningstjenester eller lignende.

GovCert udvider den almindelige indsamling af informationer fra indberetninger og offentlig kilder ved at organisere en systematisk indhentning af information direkte fra trafik på internettet. Dette tiltag vil utvivlsomt kunne forbedre viden om trusselsbillede og give mulighed for hurtigere at kunne varsle trusler og aktuelle angreb.

I loven står der konkret:

> "...§ 5. Den statslige varslingstjeneste kan kun videregive data, der er indsamlet som led i varslingstjenestens aktiviteter, i følgende tilfælde:
> 1) Pakkedata og trafikdata, der knytter sig til en konkret sikkerhedshændelse, kan videregives til politiet.
> 2) Trafikdata kan videregives til danske myndigheder, tilsluttede private virksomheder og tilsvarende varslingstjenester i andre lande i henhold til varslingstjenestens formål..."

Det interessante i denne forbindelse er, hvad substansen faktisk er omkring "... kun (at) videregive data, der er indsamlet som led i varslingstjenestens aktiviteter...". Sagen er jo, at varslingstjenesten potentielt bliver i stand til at behandle og gennemgå AL trafik, der transporteres på internettet. Hvordan mon "varslingstjenestens aktiviteter" afgrænses - er der reelt kun tale om tekniske trusler mod infrastrukturen, der omfattes af de i paragraf 1 nævnte "... statslige varslingstjeneste for internettrusler...".

PROSA anbefaler, at det til § 5 indskærpes, at

- GovCert kun må kigge i pakkedata, hvis der foreligger begrundet mistanke om noget kriminelt.
- GovCert kun må udlevere data, hvis der foreligger en dommerkendelse på baggrund af dansk lov.

I de efterfølgende "Bemærkninger til lovforslaget" står der på side 8, at:

> "...GovCERTs opgaver kan opsummeres således:
> - Indhentning af information om sikkerhedshændelser og aktiviteter i net og systemer
> i staten.
> - Analyse og vurdering af internet - sikkerhedsniveauet 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..."

Det som bekymrer Prosa er, om der reelt er tale om, at der (ad bagvejen) kan skabes det nødvendige grundlag for, at GovCert (for den danske regering) gennemlæser indholdet af al internet-trafik, der passerer udstyr, placeret på dansk område (det ligner Echelon eller et supersæt af de svenske regler, som tillader, at indholdet af al internettrafik ud og ind af Sverige gennemlæses). Når først indholdet af al trafik på internettet gennemlæses, kan der let etableres kriterier for udtræk baseret på f.eks. søgeord.

På side 9 står, omkring de personoplysninger som skal benyttes i denne forbindelse, at:

> "...Begreberne personoplysning og behandling skal forstås i overensstemmelse med definitionerne i persondatalovens § 3, stk. 1, nr. 1 og 2. I relation til dette lovforslag er det særligt relevant at bemærke, at ip-adresser betragtes som personoplysninger, hvorfor persondataloven også finder anvendelse på trafikdata, som bl.a. omfatter ip-adresser, jf. definitionen heraf i lovforslagets § 2, nr. 2..."

På denne baggrund er det klart, at GovCert faktisk vil have behov for selv at kunne benytte og videregive de ip-adresser, der indgår i internettrafik som en del af en sikkerhedshændelse - det er jo adresserne på afsenderne af al trafik på nettet.

Loven giver en meget bred adgang til at behandle og videregive sådanne personoplysninger. Men lovforslaget burde ikke give en sådan bred adgang til personoplysninger.

Ved indsamling af data om internet-datatrafik indsamles trafikdata og pakkedata. Personoplysninger kan optræde i denne indsamling af data. Dette bør anerkendes – men er ikke anderledes end, at personoplysninger behandles af netværkstjenester, som opbevarer og videresender data. Denne indsamling sker på GovCerts uklassificerede net og anvendes til

monitorering, og der sker ikke en behandling, hvor personer får adgang til disse personoplysninger.

Lovforslaget tager sigte på den behandling af personoplysninger, som kan ske, når data overføres til det klassificerede net til nærmere behandling.

Ved overførsel af data til nærmere analyse på det klassificerede netværk vil PROSA fremhæve, at udgangspunktet må være, at personoplysninger slettes eller anonymiseres/krypteres således, at der ikke sker en behandling af persondata. PROSA må afvise, at der med lovforslaget åbnes en generel adgang for GovCert og dets medarbejdere til at få indsigt i personoplysninger. Det er vores vurdering, at GovCert udmærket vil kunne varetage sit formål uden at have adgang til personoplysninger, og at en fremgangsmåde, hvor disse slettes eller anonymiseres/krypteres, ikke vil hindre GovCert i at opfylde sit formål som varslingstjeneste generelt og ved konkrete angrebs-hændelser.

Vi er opmærksomme på, at der kan opstå enkelte hændelser, hvor de fastlagte procedurer og den tekniske behandling vil fejle, og medarbejdere hos GovCert kan blive bekendt med personoplysninger. Der bør indrømmes en undtagelse for Persondataloven straffebestemmelser i sådanne tilfælde under forudsætning af,

- at adgang til personoplysninger straks afbrydes, og
- at personoplysningerne ikke videregives eller behandles på anden vis

For at sikre kontrol med denne undtagelse vil PROSA foreslå, at der indføres en anmeldelsesordning således, at den enkelte medarbejder og GovCert forpligtes til at anmelde enhver hændelse, hvor der har været (kortvarig) tilgang til personoplysninger (udover ip-adresser) til Datatilsynet.

Datatilsynets opgave er

- at sikre, at der er tale om enkeltstående hændelse, som afviger fra reglen om, at personoplysninger slettes eller anonymiseres/krypteres og
- at følge op på, om GovCerts procedurer er tilstrækkelige

Eventuelle anmeldelser indgår desuden i Datatilsynets øvrige tilsynsvirksomhed og offentliggøres på tilsynets hjemmeside og i årsberetningen.

Der er ingen saglig begrundelse for at behandle personoplysninger for at kunne varetage GovCerts formål og opgaver. Hvis GovCert bliver opmærksom på mulige kriminelle forhold, eller at der ud fra indhold i datakommunikationen kan spores kriminelle, må sagen overdrages til politiet. GovCerts opgave vil alene være at konsolidere data, så de kan indgå i politiets efterforskning. Politiets efterforskning må basere sig på eksisterende retsprincipper, herunder indhentning af fornøden retskendelse. Behov for hurtig reaktion må løses ved at etablere et samarbejde mellem politi og GovCert, som fastholder arbejdsfordeling mellem anmelder og politi.

PROSA anbefaler, at det blev mere nøje specificeret, hvilke personlysninger dette drejede sig om (altså: er det alene ip-numre, eller er der andre personoplysninger?). Personoplysninger (inden i datapakkerne) bør krypteres, så de ikke kommer i hænderne på udenforstående.

PROSA kan endvidere ikke støtte oprettelsen af et kontroludvalg, der, som det hedder i bemærkningerne, har inspiration af Wamberg-udvalget.

Det "uafhængige tilsyn" beskrives i loven:

> "§ 6. Ministeren for videnskab, teknologi og udvikling nedsætter et uafhængigt tilsyn, der følger den statslige varslingstjeneste for internet truslers virksomhed.
> Stk. 2. Tilsynet består af en dommer som formand og fire sagkyndige medlemmer. Formanden og medlemmerne af tilsynet beskikkes af ministeren for videnskab, teknologi og udvikling. Ministeren for videnskab, teknologi og udvikling skal ved beskikkelsen af tilsynets medlemmer lægge vægt på, at tilsynet samlet repræsenterer juridisk, it -revisionsmæssig og sikkerhedsmæssig sagkundskab.
> Stk. 3. Medlemmerne beskikkes for fire år ad gangen og kan genbeskikkes.
> Stk. 4. Ministeren for videnskab, teknologi og udvikling fastsætter rammerne for tilsynets virksomhed. Ministeren for videnskab, teknologi og udvikling kan herunder beslutte, at tilsynet skal udarbejde en årsberetning om den statslige varslingstjeneste for internet truslers virksomhed.
> Stk. 5. IT- og Telestyrelsen stiller sekretariatsbistand til rådighed for tilsynet..."

Dette tilsyn minder om det Wamberg-udvalg, der i 1964 blev nedsat af Folketinget for at tilse arbejdet i PET. Dette tilsyn har bestemt ikke været nogen stor succes - det har fungeret så dårligt, at det som bekendt blev nødvendigt at nedsætte en særlig kommission, der skulle gennemgå PET's arbejde gennem tiden. Sporene fra Wamberg-udvalget og anvendelsen af lukkede kontroludvalg skræmmer. De giver ingen garanti for retssikkerheden. Tilsynet bør placeres hos Datatilsynet, der beretter om dette på deres hjemmeside og i årsberetningen. Der bør i forbindelse med behov for det særlige tilsyn af GovCert tilføres Datatilsynet fornødne resurser.

PROSA vil derfor anbefale, at der bliver udarbejdet en specificering af de konkrete og specificerede personoplysninger (altså en positivliste som indeholder ip-numre), der må behandles og videregives.

PROSA deltager gerne i en udredning, som kan sikre GovCert et troværdigt grundlag, der, som beskrevet ovenfor, bl.a. må indebære, at der ikke er en generel tilgang til personoplysninger.

Venlig hilsen

Niels Bertelsen
Formand
PROSA

RIGSREVISIONEN

Landgreven 4
Postboks 9009
1022 København K

Tlf. 33 92 84 00
Fax 33 11 04 15

rr@rigsrevisionen.dk
www.rigsrevisionen.dk

IT- og Telestyrelsen

Sendt pr. e-mail til: info@govcert.itst.dk

2. marts 2011

Kontor: C5

J.nr.: 2011-5902-9

**Høring vedr. lovforslag om GovCERT**

Rigsrevisionen har gennemgået forslag til lov om den statslige varslingstjeneste for internettruslers behandling af personoplysninger. Lovforslaget blev som udkast fremsendt til høring ved IT- og Telestyrelsens brev af 11. februar 2011.

Rigsrevisionen har ikke bemærkninger til lovforslaget.

Med venlig hilsen
Ingolf Holm Clausen
Specialkonsulent

**Høringssvar - Telia**

Til IT- og Telestyrelsen -

IT- og Telestyrelsen (ITST) har ved brev af 11. februar 2011 iværksat bred offentlig høring af udkast til lovforslag om den statslige varslingstjeneste for internettruslers (GovCERT) behandling af personoplysninger. I denne anledning skal Telia afgive følgende bemærkninger, idet man overordnet klart støtter udkastets sigte.

Telia finder det tilfredsstillende, at udgangspunktet for private virksomheders eventuelle tilslutning til den statslige varslingstjeneste er frivillighed baseret på et påregneligt grundlag, jf. regler fastsat af ministeren i medfør af den foreslåede § 1, stk. 3. Som de specifikke bemærkninger til udkastets § 1, stk. 3, er formuleret (”selv finansiere tjenestens ydelser”), fremstår sigtet ikke ganske klart. Efter Telias opfattelse vil private virksomheders beslutning om tilslutning som minimum forudsætte, at tilslutningsvilkår bliver gennemsigtige og prissætningen rimelig. Telia skal herudover opfordre ITST til at arbejde aktivt for at der fastsættes vilkår og priser, der vil give kritiske infrastrukturvirksomheder klare incitamenter for tilslutning.

Udkastet lægger med bestemmelsen i § 3, stk. 2, nr. 1, op til, at pakke- og trafikdata, der knytter sig til en konkret sikkerhedshændelse, højst kan opbevares i tre år. Af de særlige bemærkninger til denne bestemmelse fremgår, at den maksimale opbevaringstid i de fleste tilfælde vil være væsentligt kortere end tre år. Det er efter Telias opfattelse bemærkelsesværdigt, at der således lægges op til mulighed for to års længere opbevaringstid for sådanne pakke- eller trafikdata end efter logningsbekendtgørelsen. Da der i sådanne data må formodes at findes data hidrørende fra begge sider af en kommunikation, er der dermed åbnet for potentielt at gemme forholdsvis følsomme personoplysninger i usædvanlig lang tid. Telia noterer, at der tilsyneladende ligger en it-teknisk vurdering, som Telia ikke mener at have fået adgang til, som beslutningsgrundlag for dette oplæg. Den givne vurdering er efter Telias opfattelse overraskende: Erfaringer fra tidligere sikkerhedshændelser skulle bestemt have givet anledning til at opstille generelle beskrivelser af og betragtninger om hændelsesforløbet, således at sådanne hændelser kan identificeres, inden en frist på et år er overskredet. Det er især nødvendigt at lave et sådant (anonymiseret) 'fingeraftryk' af en hændelse, hvis information om den skal publiceres eller blot kommunikeres til en lukket kreds og dermed burde det være overflødigt at gemme data relateret til den faktiske hændelse. Telia opfordrer derfor til at både mængden af data og den maksimale opbevaringsperiode genovervejes.

Telia forstår og støtter udkastets oplæg om etablering af et uafhængigt tilsyn, jf. § 6, stk. 1, henset til den potentielle informationsmængde, der kan vise sig nødvendig at håndtere og disse datas i nogen grad personhenførbare karakter. De anførte hensyn vejer efter Telias opfattelse så tungt, at udkastets § 6, stk. 4, må genovervejes. Uafhængigheden kunne tale for, at i hvert fald tilsynets forretningsorden ikke fastsættes af ministeren, men af tilsynets medlemmer selv, ligesom tilsynet selv frit må afgøre, hvor hyppig rapportering til ministeren man finder hensigtsmæssig. Uanset et eventuelt fastsat krav om årsberetning må dette ikke i praksis udvikle sig til en begrænsning for tilsynets rapporteringsadgang. Endvidere bør det være op til tilsynet selv at vurdere, om adressaten for årsberetning eller anden

rapportering alene skal være ministeren, eller om offentliggørelse i en videre udstrækning muligvis vil fremme lovens formål.

Dette høringssvar sendes alene i elektronisk version - og fristoverskridelsen beklages.

Med venlig hilsen/Best regards
Michael Green
Legal advisor, Legal and External Affairs
Mobile +45 28275046 Telephone +45 82337000
Michael.Green@teliasonera.com
Telia Danmark, Part of TeliaSonera Group, Head Office
Holmbladsgade 139, DK-2300 Copenhagen, Denmark
www.teliasonera.com
www.telia.dk

**Høringssvar – Tor Bloch**

Jeg har tre bemærkninger til udkastet til lovforslaget - alle med henblik på at fremme "good governance" og sikre transparens.

1. Ad §3. At GovCERT holder et detailleret regnskab med brugen af muligheden for at analysere pakkedata "i tilfælde af begrundet mistanke om en stedfunden eller forventet sikkerhedshændelse" således at (i det mindste) GovCERT selv og det uafhængige tilsyn er informerede om mængden af sådanne tilfælde af "begrundet mistanke", der var berettigede relativt til mængden der ikke var det. En flerårig trend-analyse i denne forbindelse kunne vise sig at være nyttig - navnlig hvis den kan sammenholdes med antallet af tilfælde, hvor man har afholdt sig fordi den begrundede mistanke ikke var kraftig nok.

2. Ad. §6 stk.2 og 3. At der lovmæssigt sikres en rimelig grad af fornyelse af det uafhængige tilsyn. Selv om det kræver en vis indsigt i de relevante problemstillinger at sidde i et sådant tilsyn så er det også af stor værdi at have en tilgang af nye kompetencer og ikke falde hen i en etableret rutine. Det kan for eksempel sikres gennem en fornyelse af 1 eller 2 medlemmer i hver ny 4-årig periode (med en passende start-ordning) suppleret med en regel om at formandsskabet ikke kan udøves mere end to (tre???) på hinanden følgende perioder af den samme person.

3. Ad §6 stk. 4. At en årsberetning fra GovCERT sikres lovmæssigt i selv teksten og ikke blot fremstår som en mulighed. Transparens, transparens, transparens...

Med venlig hilsen og tak for muligheden for at kommentere efter det meget oplysende møde forleden.

Tor Bloch
Parcelvej 114
2830 Virum
Tel. 26 36 7812.

(Credentials: Mag. Scient. fra KU, derefter mange år ved CERN, École Polytechnique mest som opbygger og leder af supercomputer centre. Senere i industri (både start-up og store firmaer) og i perioden 1996-2001 videnskabelig direktør på UNI-C med bl.a. overordnet ansvar for DK-CERT, Danmarks deltagelse i Nordunet mv. Har arbejdet med NATO's civile program omkring internettet i partner lande (bl.a. formandskabet for den rådgivende ekspertkomité i et par år), p.t. en del projekt evaluering for EU's rammeprogrammer og involvering i kvalitetsstyringen på dansk side for Sundhedsministeriet (SDSD, nu NSI) i et større eHealth projekt: epSOS)