INSTITUT FOR
MENNESKE
RETTIGHEDER

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
DIREKTE 3269 8805
RFJ@HUMANRIGHTS.DK
MENNESKERET.DK

J. NR. 540.10/30403/RFJ/MAF

4. MARTS 2014

Forsvarsministeriet
fmn@fmn.dk
pah@fmn.dk
hvs@govcert.dk

HØRING OVER UDKAST TIL FORSLAG TIL LOV OM CENTER FOR CYBERSIKKERHED SAMT EVALUERING AF GOVCERT-LOVEN

Forsvarsministeriet har ved e-mail af 4. februar 2014 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til høring over udkast til forslag til lov om Center for Cybersikkerhed samt evaluering af GovCERT-loven.

Med udkast til forslag til lov om Center for Cybersikkerhed etableres et samlet lovgrundlag for Center for Cybersikkerhed. Lovforslaget er baseret på en evaluering af den statslige varslingstjeneste for internettrusler (GovCERT), som varetages af Center for Cybersikkerhed. Evalueringen er foretaget af Forsvarsministeriet, men det fremgår ikke tydeligt af evalueringen eller lovforslaget, hvordan evalueringen er foretaget eller hvem, der er blevet hørt. Det fremgår dog, at tilsynet for GovCERT, som blev nedsat i september 2013 endnu ikke har afgivet sin første beretning, og derfor ikke har været en del af evalueringen. I evalueringen konkluderes det, at GovCERT har bidraget væsentligt til cybersikkerheden i Danmark, men at der samtidig er behov for at revidere lovgrundlaget for GovCERT, for at sikre GovCERTs evne til at bidrage til sikringen mod væsentlige angreb mod danske interesser.

Instituttet har følgende bemærkninger:

Instituttet finder det positivt at lovforslaget etablerer en lovregulering af Center for Cybersikkerhed, GovCERT og varslingstjenesten for internettrusler på forsvarsministeriets område (MILCERT). Instituttet finder endvidere, at forebyggelse af cyberangreb er et tungtvejende hensyn for danske myndigheder og virksomheder.

KORT OM MENNESKERETTEN

Retten til et beskyttet privatliv og familieliv reguleres bl.a. i Den Europæiske Menneskerettighedskonventions artikel 8 (EMRK) og i FN´s konvention om borgerlige og politiske rettigheder (ICCPR), artikel 17. Artikel 7 og 8 i EU's charter om grundlæggende rettigheder beskytter henholdsvis retten til respekt for privatliv og familieliv og beskyttelse af personoplysninger.

EMRK art. 8 har følgende ordlyd:
"Stk.1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.
Stk. 2. Ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder."

Videregivelse og anden behandling af oplysninger om enkeltpersoners private forhold, hører ind under beskyttelsesområdet i artikel 8. Statens mulighed for at foretage indgreb i retten til respekt for privatliv forudsætter opfyldelsen af tre indgrebsbetingelser, som er hjemmel i national ret, forfølgelsen af et anerkendelsesværdigt formål og et krav om nødvendighed i et demokratisk samfund.

Ved kravet om, at et indgreb skal være nødvendigt i et demokratisk samfund søges det sikret, at der består en rimelig balance i afvejningen mellem borgerens og samfundets interesser. Derudover følger det af nødvendighedskravet, at et indgrebs begrundelse skal findes i et påtrængende samfundsmæssigt behov. Undersøgelsen af, om nødvendighedskravet er opfyldt, skal suppleres af en proportionalitetsvurdering. Denne vurdering skal skabe sikkerhed for, at indgreb foretages med et middel, der må anses for proportionalt i forhold til målet, dvs. at det middel, der bringes i anvendelse, skal stå i et rimeligt forhold til det mål, som søges opnået.

EU's Persondatadirektiv (95/46/EC), fastsætter rammer for behandling af personoplysninger. Artikel 8 i direktivet fastsætter som udgangspunkt et forbud mod behandling af personoplysninger. Dette udgangspunkt kan dog fraviges, hvis den, som oplysninger vedrører, giver samtykke til behandlingen, ligesom der oplistes andre situationer, hvor udgangspunktet kan fraviges, se herved artikel 8, stk. 3. Direktivet er implementeret ved den danske persondatalov.

ORGANISATORISK PLACERING AF GOVCERT

Da lovgivningen, som regulerer GovCERT, blev vedtaget, var GovCERT en del af den daværende IT- og Telestyrelse under det daværende Videnskabsministerium (nu Uddannelses- og Forskningsministeriet) Ved kongelig resolution af 3. oktober 2011 blev ressortansvaret for GovCERT overført til Forsvarsministeriet og med oprettelsen af Center for Cybersikkerhed den 18. december 2012 blev GovCERT en del af Forsvarets Efterretningstjeneste. Placeringen under Forsvarets Efterretningstjeneste betyder, at GovCERT ikke er omfattet af persondataloven, offentlighedsloven og forvaltningsloven. Som en konsekvens af, at persondataloven ikke gælder for Center for Cybersikkerhed, udstedte Forsvarsministeriet den 13. maj 2013 retningslinier for behandling af personoplysninger m.v. i Center for Cybersikkerhed. Desuden er nogle principper fra persondataloven indskrevet i forslag til lov om Center for Cybersikkerhed.

Med lovforslagets § 8 videreføres undtagelsen af Center for Cybersikkerheds og dermed også GovCERTs virksomhed fra offentlighedsloven, forvaltningsloven og persondataloven. Endvidere udvides GovCERTs grundlag for dataindsamling, da kredsen af virksomheder, der kan tilslutte sig GovCERT, udvides fra virksomheder, der er beskæftiget med kritisk infrastruktur, til en bredere gruppe af virksomheder beskæftiget med samfundsvigtige funktioner. Samfundsvigtige funktioner beskrives i bemærkningerne til lovforslaget som funktioner, der er særligt vigtige for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed, herunder funktioner inden for sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet.

Det fremgår af lovforslaget, at begrundelsen for at placere Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste var at opnå synergieffekter. Institut for Menneskerettigheder finder det imidlertid betænkeligt, at den organisatoriske placering af GovCERT medfører, at GovCERT ikke er omfattet af særligt persondataloven og dermed heller ikke Datatilsynets tilsynsvirksomhed. Evalueringen af GovCERT-loven fremhæver ikke et behov for at fritage GovCERT fra persondataloven, som er af stor betydning i forhold til at sikre en forsvarlig behandling af personoplysninger. Endvidere bemærker instituttet, at der generelt ikke var behov for at undtage GovCERT fra offentlighedsloven, persondataloven og forvaltningsloven, da GovCERT organisatorisk var underlagt IT- og Telestyrelsen.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at GovCERT omfattes

af persondataloven, offentlighedsloven og forvaltningsloven, for eksempel gennem en ændret organisatorisk placering af GovCERT.

INTERN VIDEREGIVELSE AF DATA

GovCERT-lovens § 6 regulerede videregivelse af pakkedata fra GovCERT til MILCERT under Forsvarets Efterretningstjeneste. Videregivelse af pakkedata knyttet til en sikkerhedshændelse forudsatte, at IT- og Telestyrelsen skønnede det nødvendigt for at beskytte nationale digitale infrastrukturer mod sikkerhedsmæssige trusler.
Placeringen af både MILCERT og GovCERT i Center for Cybersikkerhed under Forsvarets Efterretningstjeneste medfører, at der nu som udgangspunkt er fri adgang til at udveksle data mellem GovCERT og den øvrige del af Forsvarets Efterretningstjeneste, jf. almindelige forvaltningsretlige principper. Det fremgår af lovforslaget, at Forsvarsministeriet har til hensigt at udstede administrative retningslinier, der sikrer, at intern udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige Efterretningstjeneste sker med respekt for retssikkerheden og den personlige frihed.

Institut for Menneskerettigheder finder det betænkeligt, at der med lovforslaget ikke på lovniveau sikres en varetagelse af retssikkerhedsmæssige hensyn ved videregivelse af oplysninger fra GovCERT til Forsvarets Efterretningstjeneste. Data, som GovCERT er i besiddelse af som den statslige varslingstjeneste for danske myndigheder og en lang række private virksomheder, vil således i høj grad kunne inddrages i Forsvarets Efterretningstjenestes øvrige arbejde inden for det militære område.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at der i lovforslaget indføres et krav om, at videregivelse af data fra GovCERT til resten af Forsvarets Efterretningstjeneste forudsætter, at det konkret vurderes nødvendigt for at beskytte den nationale digitale infrastrukturer mod sikkerhedsmæssige trusler.

EKSTERN VIDEREGIVELSE AF DATA

Lovforslagets § 16 regulerer Center for Cybersikkerheds mulighed for ekstern videregivelse af data. Ved begrundet mistanke om en sikkerhedshændelse kan både pakke- og trafikdata videregives til politiet. Trafikdata kan desuden videregives til blandt andet danske myndigheder og udenlandske netsikkerhedstjenester, hvis det vurderes nødvendigt for udførelsen af netsikkerhedstjenestens opgaver.

Det fremhæves i lovforslaget, at en af Center for Cybersikkerheds vigtigste forebyggende aktiviteter er udsendelse af

sikkerhedsvarslinger, hvor myndigheder, virksomheder, andre netsikkerhedstjenester m.v. underrettes om særligt alvorlige sikkerhedshændelser. Det fremhæves endvidere, at et effektivt internationalt samarbejde forudsætter, at Danmark også kan give oplysninger, som kan bidrage til at stoppe grænseoverskridende cyberangreb.

Institut for Menneskerettigheder anerkender behovet for at videregive oplysninger til blandt andet udenlandske netsikkerhedstjenester. Instituttet finder imidlertid også, at muligheden for at videregive oplysninger bør begrænses mest muligt. Instituttet bemærker i den forbindelse at lovforslaget primært fremhæver behovet for at videregive oplysninger vedrørende sikkerhedshændelser. Instituttet finder således, at det bør overvejes, om muligheden for videregivelse af oplysninger bør begrænses yderligere.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at det overvejes at begrænse muligheden for videregivelse af oplysninger i lovforslagets § 16, nr. 2 til trafikdata, der vedrører en konkret sikkerhedshændelse.

SLETTEFRISTER

Med lovforslaget udvides fristerne for sletning af data, som ikke knytter sig til en sikkerhedshændelse. Ifølge den nuværende GovCERT-lov kan pakkedata, som ikke knytter sig til en sikkerhedshændelse opbevares i højst 14 dage. Trafikdata, der ikke knytter sig til en sikkerhedshændelse, kan opbevares i højst 12 måneder. I evalueringen af GovCERT-loven fremhæves generelt et behov for længere frister for opbevaring af data. Ifølge lovforslagets § 17, stk. 2, nr. 2, behandles trafik- og pakkedata nu ens, og det foreslås, at opbevaring af sådanne data udvides til højst 13 måneder.

Instituttet finder, at særligt udvidelsen af muligheden for at opbevare pakkedata, som ikke knytter sig til en sikkerhedshændelse, fra 14 dage til 13 måneder er en betydelig udvidelse af adgangen til at opbevare historiske data. Af hensyn til den enkeltes ret til privatliv finder instituttet, at fristerne for sletning af data bør sikre, at oplysninger ikke opbevares længere end højst nødvendigt. Samtidig bør oplysninger kunne opbevares længe nok til, at opgaverne forbundet med GovCERT kan varetages forsvarligt. Instituttet finder det ikke sandsynliggjort i lovforslaget, at en så betydelig udvidelse af adgangen til at opbevare historiske data er et nødvendigt og proportionalt indgreb i den enkeltes ret til privatliv.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at lovforslagets slettefrist på 13 måneder for pakkedata, som ikke knytter sig til en sikkerhedshændelse, sænkes.

Det fremgår desuden af lovforslagets § 17, stk. 4, at data, som er videregivet i medfør af § 16 ikke er omfattet af slettefristerne. I lovforslaget pålægges Center for Cybersikkerhed heller ikke at stille krav om sletning af data hos myndigheder m.v., som modtager data iht. lovforslagets § 16. Ved videregivelse af data, heriblandt til udenlandske myndigheder, er hverken Center for Cybersikkerhed eller modtageren således ifølge lovforslaget forpligtet til at slette de pågældende data.

Det fremhæves i lovforslaget, at Center for Cybersikkerhed i sagens natur ikke har mulighed for at sikre, at der efterfølgende sker sletning af data hos en modtager af disse data. Ved videregivelse af oplysninger til politiet til brug for en eventuel straffesag anses det endvidere for uhensigtsmæssigt, at sådanne oplysninger risikerer at blive slettet af Center for Cybersikkerhed, inden en sådan sag er afsluttet. Det fremhæves desuden i lovforslagets bemærkninger, at danske myndigheder og virksomheder, som modtager data fra Center for Cybersikkerhed vil være underlagt persondatalovens databehandlingsregler.

Institut for Menneskerettigheder finder det ikke tilstrækkeligt godtgjort i lovforslaget, at videregivelse af data ikke kan ske med betingelse om sletning af disse data efter en nærmere angivet periode. Såfremt data videregives til dansk politi til brug for en eventuel straffesag, finder instituttet endvidere, at sletning bør kunne ske, når politiets behandling af sagen er afsluttet.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at der i lovforslagets § 17 indføres krav om sletning af data, som videregives til politiet iht. lovforslagets § 16, nr. 1, når formålet med videregivelsen er ophørt.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at Center for Cybersikkerhed pålægges at indføre krav om sletning af data, som videregives iht. lovforslagets § 16, nr. 2.

TILSYNET MED GOVCERT

GovCERTs organisatoriske placering under Center for Cybersikkerhed medfører, at GovCERT er undtaget fra Datatilsynets tilsynsvirksomhed. I den nuværende GovCERT-lov er der etableret et GovCERT-tilsyn. Med

lovforslaget overføres tilsynet med GovCERT imidlertid til Tilsynet med Efterretningstjenesterne, som blev oprettet 1. januar 2014.

Institut for Menneskerettigheder finder som tidligere anført, at GovCERT bør være underlagt persondataloven og herunder tilsyn fra Datatilsynets vedrørende deres behandling af personoplysninger. Såfremt det nuværende forslag opretholdes, hvorefter tilsynet med GovCERT overgår til Tilsynet med Efterretningstjenesterne, bør det sikres, at kompetencen i dette nye tilsyn afspejler den nye opgavevaretagelse.

Det nuværende GovCERT-tilsyn består af en formand, der er jurist og fire sagkyndige medlemmer, der repræsenterer juridisk, it-revisionsmæssig og sikkerhedsmæssig sagkundskab. Det fremgår ikke af lovforslagets bemærkninger, om denne sagkundskab sikres i Tilsynet med Efterretningstjenesterne.

Ved overførslen af tilsynsopgaven fra GovCERT-tilsynet til Tilsynet med Efterretningstjenesterne finder instituttet, at det bør sikres, at en sagkundskab svarende til GovCERT-tilsynets er repræsenteret i Tilsynet med Efterretningstjenesterne.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at det sikres, at Tilsynet med Efterretningstjenesterne besidder de fornødne juridiske, it-revisionsmæssige og sikkerhedsmæssige sagkundskab til at foretage et effektivt tilsyn med GovCERT.

Der henvises til sagsnr. 2013/003214.

Venlig hilsen

Rikke Frank Jørgensen og Martin Futtrup