Advokatrådet

ADVOKAT SAMFUNDET

Forsvarsministeriet

KRONPRINSESSEGADE 28
1306 KØBENHAVN K
TLF. 33 96 97 98
DATO: 21.08.2024
SAGSNR.: 2024-2135

Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Ved e-mail af 5. juli 2024 har Forsvarsministeriet anmodet om Advokatrådets bemærkninger til ovennævnte lovforslag.

Advokatrådet har følgende bemærkninger:

Generelle forhold

Det angives i lovforslaget, at Forsvarsministeriet har lagt afgørende vægt på, at gennemførelsen af NIS 2-direktivet sker i overensstemmelse med regeringens principper for implementering af erhvervsrettet EU-regulering, hvorefter den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen. Dette sker efter det anførte for at sikre, at danske virksomheder ikke pålægges flere byrder end andre europæiske virksomheder.

Advokatrådet støtter generelt hensigten om at sikre, at implementeringen af erhvervsrettet regulering i dansk ret ikke går videre, end hvad den relevante EU-regulering forudsætter. Hensynet til at sikre minimumsimplementering bør dog ikke hindre, at lovgivningen – herunder navnlig lovgivning underlagt så betydelig strafsanktionering, som det er tilfældet efter det foreliggende lovforslag – udformes på en måde, der gør det muligt for de omfattede virksomheder at fastlægge, hvilke retlige forpligtelser, de er underlagt, samt hvordan de konkret skal indrette sig for at efterleve reglerne og undgå strafsanktionering mv.

I den forbindelse bemærkes det, at hovedparten af lovforslagets krav rettet mod omfattede enheder indeholder bredt udformede krav, der ordret gennemfører NIS 2-direktivet. F.eks. indeholder lovforslaget 32 definitioner. Bemærkningerne til disse definitioner ses kun i begrænset omfang at indeholde fortolkningsbidrag, ud over henvisninger til den underliggende EU-regulering, der gør det muligt for omfattede enheder at anvende begreberne, og dermed lovforslaget, i praksis. En række af lovforslagets øvrige bestemmelser ses også alene at indeholde en ordret

gengivelse af direktivets ordlyd, og indeholder kun i meget begrænset omfang bidrag, der kan understøtte de omfattede enheders konkrete fortolkning og afgrænsning af, hvilke forpligtelser de er underlagt.

Advokatrådet anerkender i sagens natur, at den danske stat som led i implementeringen af NIS 2-direktivet er EU-retligt forpligtet til at udforme ordlyden af de relevante bestemmelser i overensstemmelse med direktivets ordlyd. Ligesom det anerkendes, at et område af så dynamisk og omskiftelig karakter som cybersikkerhed til en vis grad må lovreguleres generelt og neutralt. Med henblik på at sikre de omfattede enheder en acceptabel grad af klarhed om, hvilke tiltag de er forpligtet til at implementere for at efterleve lovforslaget, finder Advokatrådet dog, at det er af afgørende betydning, at den direktivnære implementering ledsages med bemærkninger, der mere entydigt fastsætter de specifikke begreber og krav de omfattede enheder er underlagt. I fraværet af mere udbyggede lovbemærkninger overlades de enkelte enheder og kompetente myndigheder til selv at fastlægge deres forståelse af lovforslagets praktiske betydning.

Advokatrådet har i den forbindelse noteret, at der efter lovforslagets § 6, stk. 3, kan udstedes sektorspecifikke bekendtgørelser med mere konkretiserede krav til de foranstaltninger, som enhederne skal træffe i medfør af den foreslåede bestemmelse i stk. 1. Af bemærkningerne til bestemmelsen anføres det, at regler fastsat efter denne bestemmelse bl.a. vil skulle være i overensstemmelse med regeringens principper om minimumsimplementering.

Som anført finder Advokatrådet, at hensynet til alene at foretage en minimumsimplementering ikke bør hindre, at de i praksis meget relevante – og strafbelagte – krav i § 6, stk. 1, blot gentages i de sektorspecifikke bekendtgørelser. Advokatrådet tilskynder derfor til, at der i lovforslagets bemærkninger nærmere beskrives, hvilken grad af præcisering de regeludstedende myndigheder kan og bør sikre som led i udstedelsen af de sektorspecifikke bekendtgørelser. Derudover bemærkes det, at såvel kravene i lovforslagets § 6, samt lovforslagets øvrige bestemmelser, der pålægger enheder forpligtelser, i praksis bør understøttes af konkret og handlingsanvisende vejledninger mv. fra de relevante myndigheder for også derigennem at sikre de omfattede enheder betryggende mulighed for at efterleve reglerne. Dette vurderes samtidig at ville lette de relevante myndigheders håndhævelse af og tilsyn med lovforslagets krav.

Advokatrådet opfordrer til, at udarbejdelsen af sådanne vejledninger mv. prioriteres højt af de relevante myndigheder og udstedes i rimelig tid inden reglerne finder anvendelse.

I forlængelse af ovenstående bemærkes det, at lovmodellen for implementering af NIS 2-direktivet forudsætter, at der udpeges en række kompetente myndigheder på tværs af de omfattede sektorer, der - for hver deres sektor - skal varetage tilsyns-

og myndighedsopgaver. Det fremgår af lovforslagets bemærkninger, at det forudsættes, at der vil være en tæt koordination mellem de kompetente myndigheder i forbindelse med tilrettelæggelsen af tilsynsarbejdet, således at der i videst muligt omfang anlægges en fælles tilgang. Det er endvidere fastsat, at Center for Cybersikkerhed (CFCS) vil varetage funktionen som CSIRT i forhold til alle de af direktivet omfattede sektorer og forestå forhandlingen af bekendtgørelser efter lovforslagets § 6, stk. 3.

Advokatrådet tilslutter sig det anførte om, at denne model forudsætter en meget effektiv koordinering mellem de kompetente myndigheder. Advokatrådet bemærker i den forbindelse, at det – netop for at sikre en fælles tilgang og effektiv vejledning mv. af de berørte enheder – vil være af afgørende betydning, at myndighederne etablerer en ordning, der sikrer, at eventuelle uoverensstemmelser mellem kompetente myndigheders fortolkning, vurdering af trusselsbilledet mv. identificeres og udredes af myndighederne. Lovforslaget bør på den baggrund nærmere beskrive, hvordan det i praksis vil blive sikret, at f.eks. enheder, der har aktiviteter inden for flere omfattede sektorer, ikke mødes af divergerende krav, fortolkninger mv. fra to eller flere kompetente myndigheder.

Retssikkerhedsmæssige forhold

Lovens anvendelsesområde

Det fremgår af lovforslagets generelle bemærkninger, at lovforslaget vurderes at omfatte omkring 2.000 virksomheder. Lovforslagets § 1 fastsætter anvendelsesområdet med en generel henvisning til NIS 2-direktivets artikel 2. Samtidig indeholder lovforslagets bemærkninger – med henvisning til NIS 2-direktivet – flere opregninger af hvilke typer af enheder, der, alt efter deres størrelse og sektor, er omfattet af lovforslaget. Eksempelvis angives det, at følgende sektorer er omfattet udover de sektorer, der i dag er omfattet af NIS 1-reglerne: 1) Spildevand, 2) forvaltning af informations- og kommunikationstjenester (IKT-tjenester) (business-to-business), 3) offentlig forvaltning, 4) rummet, 5) post- og kurertjenester, 6) affaldshåndtering, 7) fremstilling, produktion og distribution af kemikalier, 8) produktion, tilvirkning og distribution af fødevarer, 9) forskning og 10) fremstilling med delsektorerne: a) Fremstilling af medicinsk udstyr og medicinsk udstyr til vitrodiagnostik, b) fremstilling af computere og elektroniske og optiske produkter, c) fremstilling af elektrisk udstyr, d) fremstilling af maskiner og udstyr ikke andetsteds nævnt, e) fremstilling af motorkøretøjer, påhængsvogne og sættevogne og f) fremstilling af andre transportmidler.

Endvidere opregnes der i bemærkningerne, de typer af enheder, som vil være omfattet af lovforslaget, uanset deres størrelse.

Det fremgår af bemærkningerne til § 1, at det efter den foreslåede bestemmelse vil være enhedernes ansvar at vurdere, om de er omfattet af lovens anvendelsesområde, idet enheder, der er omfattet af anvendelsesområdet i artikel 2 i NIS 2-direktivet, vil være umiddelbart omfattet af lovens anvendelsesområde. Enheder vil i overensstemmelse med forvaltningslovens § 7 i fornødent omfang kunne få vejledning og bistand fra de kompetente myndigheder.

Det anføres videre, at i en situation, hvor en enhed fejlagtigt måtte vurdere, at denne er eller ikke er omfattet af lovens anvendelsesområde, vil de kompetente myndigheder ved en forvaltningsakt kunne konstatere, hvorvidt enheden er omfattet af lovens anvendelsesområde.

Afgrænsningen af hvilke enheder, der anses for væsentlige, fremgår af lovforslagets § 4. I § 4, stk. 4, er der hjemmel til, at vedkommende minister inden for sit område kan fastsætte nærmere regler om kriterier for, hvornår enheder er omfattet af stk. 3, nr. 5. Det fremgår af bemærkningerne til stk. 4, at hjemlen til at fastsætte nærmere regler om hvilke enheder, der er omfattet af § 4, stk. 3, nr. 5, idet denne bestemmelse har et forholdsvist skønsmæssigt og kvalitativt præg, hvilket kan gøre det vanskeligt for de enkelte enheder at vurdere, om de betragtes som omfattet af lovens krav.

Advokatrådet finder, at ordningen for afgrænsning af hvilke enheder, der er omfattet af lovforslaget efter § 1, ligeledes efterlader en betydelig grad af usikkerhed om lovforslagets anvendelsesområde. Vurderingen af om en enhed – der møder lovforslagets øvrige krav – f.eks. er beskæftiget med ”rummet” eller ”fremstilling af elektronisk udstyr” giver ikke mulighed for entydigt at fastslå om, og hvorfor, aktivitet knyttet til et angivet område bevirker, at enheder er omfattet af lovforslagets krav. Hensynet anført i bemærkningerne til § 4, stk. 4, om at bestemmelsen i § 4, stk. 3, nr. 5, har et forholdsvist skønsmæssigt og kvalitativt præg synes således ligeledes at være aktuelt i forhold til afgrænsningen af dele af anvendelsesområdet fastsat i lovforslagets § 1. Den foreslåede ordning efter § 1, bør således, efter Advokatrådets vurdering, omfatte et egentligt retskrav for en enhed til, efter anmodning, at modtage en afgørelse fra den relevante sektorspecifikke myndighed om, hvorvidt den er omfattet eller ej. Alternativt bør der fastsættes en hjemmel svarende til bestemmelsen i § 4, stk. 4, hvorefter vedkommende minister inden for sit område kan fastsætte nærmere regler om kriterier for, hvornår enheder er omfattet af § 1.

Anvendelse af kriterier for omfattede enheders størrelse

Det fremgår af lovforslaget, at det – inden for de relevante sektorer – finder anvendelse for små virksomheder i kategorien SMV’er, der defineres som virksomheder, der beskæftiger under 50 personer, og som har en årlig omsætning

eller en samlet årlig balance på ikke over 10 mio. euro.

Advokatrådet anbefaler, at det præciseres fra hvilket tidspunkt SMV'er, der først efter lovens ikrafttræden opfylder disse betingelser, anses for omfattet af lovforslaget, herunder om tidspunktet fastsættes baseret på indeværende eller afsluttede regnskabsår. Endvidere bør der angives, hvad retsvirkningen er – og hvornår den indtræffer – hvis en virksomhed ikke længere opfylder de angivne kriterier.

Leverandører

Det fremgår af lovforslagets § 6, stk. 1, nr. 4, at væsentlige og vigtige enheder som minimum skal tage højde for forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.

Af bemærkningerne til bestemmelsen fremgår det, med henvisning til direktivet, at enheder i den forbindelse skal tage hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder, og den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer.

Af NIS 2-direktivets præambelbetragtning 84-85 fremgår bl.a. følgende:

"Væsentlige og vigtige enheder bør navnlig tilskyndes til at indarbejde foranstaltninger til styring af cybersikkerhedsrisici i kontraktlige arrangementer med deres direkte leverandører og tjenesteudbydere. Disse enheder kunne overveje risici hidrørende fra leverandører og tjenesteudbydere i andre led.

Væsentlige og vigtige enheder bør derfor vurdere og tage hensyn til den generelle kvalitet og modstandsdygtighed af produkter og tjenester, de heri integrerede foranstaltninger til styring af cybersikkerhedsrisici og deres leverandørers og tjenesteudbyderes cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer. Væsentlige og vigtige enheder bør navnlig tilskyndes til at indarbejde foranstaltninger til styring af cybersikkerhedsrisici i kontraktlige arrangementer med deres direkte leverandører og tjenesteudbydere. Disse enheder kunne overveje risici hidrørende fra leverandører og tjenesteudbydere i andre led."

Advokatrådet bemærker, at omfattede enheder i vidt omfang benytter leverandører som led i driften og understøttelsen af net- og informationssystemer omfattet af § 6. I praksis er der således allerede forud for direktivets implementering stor fokus på disse spørgsmål blandt de enheder og leverandører, der forventer at være omfattet af lovforslaget. Henset til lovforslagets og NIS 2-direktivets generelle udformning,

må der i praksis derfor forventes at opstå spørgsmål om det præcise omfang og karakteren, af de krav, enhederne skal stille til deres leverandører. Herunder i hvilket omfang enheden skal påtage sig et nærmere ansvar for at føre tilsyn med leverandørers cybersikkerhedspraksis mv. Lovforslaget og NIS 2-direktivet ses kun i begrænset omfang at beskrive det nærmere omfang af såvel enhedernes, som leverandørers ansvar for forsyningskædesikkerhed mv., herunder hvordan konkrete krav nærmere afgrænses.

Advokatrådet opfordrer derfor til, at lovforslaget nærmere behandler den præcise afgrænsning af indholdet og ansvaret for forsyningskædesikkerhed mv., og beskriver hvilke forventninger de kompetente myndigheder har til "styring af cybersikkerhedsrisici i kontraktlige arrangementer", jf. NIS 2-direktivets præambel.

Strafbestemmelser mv.

Det følger af lovforslagets § 23, stk. 1, nr. 2, at den kompetente myndighed kan træffe afgørelse om midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos enheden at udøve ledelsesfunktioner i den pågældende enhed.

Efter bestemmelsens stk. 2, kan midlertidige suspensioner eller forbud, som er pålagt i medfør af stk. 1, kun anvendes, indtil enheden træffer de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningerne blev anvendt.

Efter bestemmelsens stk. 3 kan en afgørelse efter stk. 1 forlanges indbragt for domstolene af enheden eller den fysiske person, afgørelsen vedrører. Den myndighed, som vedkommende minister bemyndiger hertil, anlægger i givet fald sag inden for rammerne af den civile retspleje mod den enhed eller person, som har forlangt sagen indbragt.

Det fremgår af lovforslagets bemærkninger, at Forsvarsministeriet har vurderet, at de eksisterende muligheder for rettighedsfrakendelse i straffeloven ikke er tilstrækkelige til at sikre korrekt og tilstrækkelig gennemførelse af den pågældende bestemmelse i direktivet. Det skyldes navnlig, at rettighedsfrakendelse i medfør af straffelovens § 79 alene kan ske i forbindelse med dom for strafbart forhold, og hvis det udviste forhold begrunder en nærliggende fare for misbrug af stillingen.

Advokatrådet finder, at den foreslåede særregel – som den danske stat er EU-retligt forpligtet til at indføre – om midlertidig frakendelse af retten til at udøve ledelsesfunktioner i den pågældende enhed, aktualiserer visse retssikkerhedsmæssige overvejelser.

Som lovforslaget er affattet, er adgangen til at forbyde en person at udøve

ledelsesfunktioner ikke direkte knyttet til den pågældende persons egen adfærd, men fungerer som et middel til at foranledige den pågældende enhed til at træffe de nødvendige foranstaltninger til at afhjælpe manglerne eller opfylde den kompetente myndigheds krav.

Advokatrådet anbefaler, at det nærmere behandles i lovforslaget, om et forbud kan meddeles en person, uden at den pågældende konkret har foretaget dadelværdige forhold eller forsømmelser (objektivt ansvar) eller om anvendelsen af et forbud forudsætter, at den pågældende konkret har været vidende om eller deltaget i beslutninger, der vedrører de forhold, som forbuddet søger at adressere.

Advokatrådet finder det positivt – ud fra en retssikkerhedsmæssig betragtning – at en afgørelse om midlertidig frakendelse, kan forlanges indbragt for domstolene. Dette ses også at være i overensstemmelse med Justitsministeriets vejledning om lovkvalitet, jf. dennes afsnit 6.3. Det bemærkes i den forbindelse, at det fremgår af Justitsministeriets vejledning, at der normalt bør være adgang for den pågældende til, eventuelt inden for en vis frist, at forlange spørgsmålet indbragt for domstolene ved den administrative myndigheds foranstaltning. Henset til, at rettighedsfrakendelsen efter lovforslaget er midlertidig, og således alene kan anvendes indtil enheden træffer de nødvendige tiltag, vil adgangen til domstolsprøvelse – i lyset af domstolenes samlede sagsbehandlingstid for behandlingen af civile sager i 1. instans ofte er over ét år – imidlertid i praksis kun have reel betydning i tilfælde, hvor afhjælpningen af de relevante forhold hos enheden overstiger domstolens samlede sagsbehandlingstid. Adgangen til domstolsprøvelse vil således i de fleste – hvis ikke alle – tilfælde, alene have relevans for en prøvelse af en rettighedsfrakendelse, der efterfølgende er bortfaldet.

Endvidere bemærkes det, at lovforslaget ikke ses at fastsætte, at en begæring om, at en afgørelse om midlertidig frakendelse, indbringes for domstolene har opsættende virkning, medmindre retten bestemmer andet. Efter Justitsministeriets vejledning om lovkvalitet, jf. ovenfor, bør dette ellers i almindelighed være tilfældet.

Advokatrådet antager, at fraværet af en bestemmelse om, at indbringelse for domstolene skal have opsættende virkning, skyldes, at der i lovforslaget alene er tale om en midlertidig frakendelse af retten til at udøve ledelsesfunktioner i den pågældende enhed, hvorfor opsættende virkningen i vidt omfang vil bevirke, at frakendelsen ikke når at få effekt, før forholdet er afhjulpet og frakendelsen derfor bortfalder. Da en midlertidig frakendelse i alle tilfælde vil være særdeles bebyrdende for de omfattede personer, og potentielt kunne have varige omdømmemæssige konsekvenser og påvirke den pågældendes adgang til senere at genindtræde i den samme eller tilsvarende stillinger, bør lovforslaget sikre en passende varetagelse af de berørte personers retssikkerhed.

På denne baggrund anbefaler Advokatrådet, at Forsvarsministeriet overvejer alternative måder at sikre de berørte personer og enheders retsstilling. Dette kunne være i form af en lovfastsat adgang for de berørte til at opnå prøvelse gennem administrativ rekurs inden for en passende kort frist, der henset til sagernes karakter, ikke bør overstige 3 uger.

Endvidere bør der – som et supplement til ovenstående – fastsættes en udvidet partshøringspligt i sager efter lovforslagets § 23, således at afgørelse alene kan træffes, når der er partshørt over såvel sagens faktum, myndighedens bevismæssige og retlige vurdering og den påtænkte sanktion.

Forholdet til anden lovgivning mv.

Forholdet til databeskyttelsesretten

Det anføres generelt i lovforslaget, at det er Forsvarsministeriets opfattelse, at behandling af almindelige personoplysninger i forbindelse med overholdelsen af registreringsforpligtelserne i §§ 9 og 10 og underretningsforpligtelserne i §§ 12 og 13, samt i forbindelse med myndighedernes anvendelse af tilsyns- og håndhævelsesforanstaltninger efter reglerne i kapitel 6 for private virksomheder vil kunne ske i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra c og e.

For så vidt angår spørgsmålet om videregivelse af personoplysninger til CSIRT'en og det centrale kontaktpunkt, fremgår det af lovforslaget, at private virksomheder vil kunne videregive almindelige personoplysninger efter databeskyttelsesforordningens artikel 6, stk. 1, litra f. Det anføres i den forbindelse, at det fremgår af databeskyttelsesforordningens præambelbetragtning 49, at behandling af personoplysninger – i det omfang, det er strengt nødvendigt og forholdsmæssigt for at sikre net- og informationssikkerheden – der foretages af eksempelvis Computer Emergency Response Teams (CERT'er), udgør en legitim interesse for den berørte dataansvarlige.

Efter Advokatrådets vurdering kan der rejses spørgsmål om, hvorvidt videregivelse af personoplysninger til CSIRT og det centrale kontaktpunkt navnlig efter lovforslagets § 19, i alle tilfælde kan baseres på interesseafvejningsreglen i databeskyttelsesforordningens artikel 6, stk. 1, litra f. Navnlig henset til, at det – som anført ovenfor – følger af databeskyttelsesforordningens præambelbetragtning nr. 49, at videregivelse forudsætter, at det er "strengt nødvendigt og forholdsmæssigt for at sikre net- og informationssikkerheden".

Den meget omfattende deling af oplysninger, der er en forudsætning for et effektivt samarbejde på tværs af omfattede enheder, vurderes således at omfatte deling af

oplysninger – herunder personoplysninger – uden at det på forhånd kan fastlægges i hvilket omfang oplysningerne konkret har relevans for modtagerne, navnlig når formålet med delingen er at varsle fællesskaber af væsentlige og vigtige enheder og, hvor det er relevant, deres leverandører eller tjenesteudbydere, jf. bemærkningerne til lovforslagets § 19. Dette gælder f.eks. ved deling af oplysninger om nærved hændelser, kompromitteringsindikatorer, IP-adresser mv.

Endvidere bemærkes det, at det følger af lovforslagets § 1, stk. 6, at offentlige og private enheder kan, uanset om de er omfattet af lovens anvendelsesområde, give frivillig underretning til CSIRT'en efter § 14 og deltage i den frivillige udveksling af oplysninger mellem enheder i cybersikkerhedsfællesskaber efter § 19.

Efter de specielle bemærkninger til § 19 vil bestemmelsen kunne omfatte udveksling af relevante cybersikkerhedsoplysninger indbyrdes, herunder oplysninger om cybertrusler, nærved hændelser, sårbarheder, teknikker og procedurer, kompromitteringsindikatorer, fjendtlige taktikker, specifikke oplysninger vedrørende trusselsaktører, cybersikkerhedsadvarsler og anbefalinger vedrørende konfiguration af cybersikkerhedsværktøjer til opdagelse af cyberangreb.

Det databeskyttelsesretlige grundlag for udveksling af oplysninger mellem enheder efter lovforslagets § 19, ses ikke nærmere behandlet i lovforslaget. Sådanne enheder vil efter Advokatrådets umiddelbare vurdering ikke kunne basere deres videregivelse af personoplysninger på databeskyttelsesforordningens artikel 6, stk. 1, litra c.

Advokatrådet anbefaler derfor, at der – for at sikre så klare og betryggende rammer som muligt for de berørte enheder – mere entydigt fastsættes i lovforslaget, at den ofte brede og omfattende videregivelse af oplysninger, herunder af personoplysninger i form af IP-adresser mv., som et effektivt samarbejde om cybersikkerhed forudsætter, kan finde sted til CSIRT'en og det centrale kontaktpunkt, og at lovforslaget i databeskyttelsesforordningens forstand fastsætter en retlig forpligtelse, jf. artikel 6, stk. 1, litra c, for alle enheder til at dele oplysninger, herunder enheder, der ellers ikke er omfattet af lovforslaget, jf. lovforslagets § 1, stk. 6.

Advokatrådet skal endvidere anbefale, at lovforslaget – under hensyntagen til de ovenfor anførte betragtninger om at sikre en betryggende ramme for udvekslingen af personoplysninger – tilføjes en redegørelse for hjemmelsgrundlaget for udveksling af personoplysninger efter § 19.

Håndtering af klassificerede oplysninger mv.

Lovforslagets §§ 12 og 13, fastsætter en række forpligtelser for omfattede enheder til at underrette den relevante kompetente myndighed og CSIRT'en om væsentlige

hændelser.

Det fremgår bl.a. af lovforslagets bemærkninger, at der ved vurderingen af, om offentligheden skal informeres, skal sikres, at dette sker uden at kompromittere fortrolige oplysninger.

Advokatrådet bemærker, at underretninger – efter omstændighederne – kan vedrøre hændelser, der, med varierende grader af sikkerhed, kan attribueres til ondsindede tredjestatsaktører.

Lovforslaget ses dog ikke at behandle, hvordan enheder, der eventuelt på baggrund af oplysninger fra CSIRT'en, må lægge til grund, at en aktuel hændelse afdækker en tredjestatsaktørs forsøg på f.eks. at opnå adgang til, eller kompromittere, net- og informationssystemer, skal behandle nærmere oplysninger herom. Det bemærkes i den forbindelse, at såfremt CSIRT'en konkret vurderer, at oplysninger om den pågældende hændelse omfatter oplysninger, der er, eller bør være, klassificerede efter Justitsministeriets cirkulære nr. 10338 af 17. december 2014 (sikkerhedscirkulæret), vil hovedparten af de omfattede enheder ikke være omfattet af cirkulæret, og dermed ikke være forpligtet til at behandle oplysningerne i overensstemmelse hermed. Lovforslaget ses samtidig ikke at hjemle adgang for CSIRT'en eller de kompetente myndigheder, til at pålægge omfattede enheder eksempelvis tavshedspligt mv. i forhold til oplysninger om hændelsen.

Med henblik på at sikre, at der er klarhed om, hvordan omfattede enheder skal forholde sig ved underretninger om hændelser, der af myndighederne anses for at vedrøre klassificerede forhold mv., opfordrer Advokatrådet til, at det nærmere reguleres i lovforslaget, såfremt Forsvarsministeriet forventer, at der i konkrete tilfælde kan opstå behov for at underretninger og opfølgningen på hændelser behandles under iagttagelse af særlige foranstaltninger. Det bør i den forbindelse overvejes, om der bør fastsættes en adgang til, at CSIRT'en, eller den kompetente myndighed, kan beslutte, at navnlig forpligtelserne i lovforslagets §§ 12 og 13, konkret skal fraviges med henblik på at sikre, at særlige fortrolighedshensyn kan varetages inden for lovgivningens rammer.

Med venlig hilsen

Andrew Hjuler Crichton
Generalsekretær