SUNDHEDS- OG ÆLDREMINISTERIET

Sundheds- og Ældreministeriet

Enhed: SUNDOK
Sagsbeh.: DEPMAHA
Koordineret med:
Sagsnr.: 1706260
Dok. nr.: 528257
Dato: 08-02-2018

NOTAT

Høringsnotat vedr. forslag til lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren

1. Høringen

Et udkast til lovforslag har i perioden den 18. oktober 2017 til den 15. november 2017 været sendt i høring hos følgende myndigheder, organisationer mv.:

3F, Ansatte Tandlægers Organisation, Brancheforeningen for Private Hospitaler og Klinikker, Danmarks Apotekerforening, Danmarks Optikerforening, Dansk Erhverv, Dansk Industri, Dansk IT – Råd for IT-og persondatasikkerhed, Dansk Kiropraktor Forening, Dansk Psykolog Forening, Dansk Psykoterapeutforening, Dansk Socialrådgiverforening, Dansk Standard, Dansk Sygeplejeråd, Dansk Tandplejerforening, Danske Bandagister, Danske Bioanalytikere, Danske Dental Laboratorier, Danske Fodterapeuter, Danske Fysioterapeuter, Danske Patienter, Danske Regioner, Datatilsynet, De Offentlige Tandlæger, Den Danske Dyrlægeforening, Ergoterapeutforeningen, Farmakonomforeningen, FOA, Forbrugerrådet, Foreningen af Kliniske Diætister, Foreningen af Speciallæger, Forsikring & Pension, Færøernes Landsstyre, Grønlands Selvstyre, Jordemoderforeningen, KL, Konkurrence- og Forbrugerstyrelsen, Københavns Universitet, Landsforeningen af Kliniske Tandteknikere, Lægeforeningen, Lægemiddelstyrelsen, Organisationen af Lægevidenskabelige Selskaber, Patienterstatningen, Praktiserende Lægers Organisation, Praktiserende Tandlægers Organisation, Psykologanævnet, Radiograf Rådet, Region Hovedstaden, Region Midtjylland, Region Nordjylland, Region Sjælland, Region Syddanmark, Rigsadvokaten, Rigsombudsmanden på Færøerne, Rigsombudsmanden på Grønland, Rigspolitiet, Roskilde Universitet, Rådet for Digital Sikkerhed, Socialpædagogernes Landsforbund, Statens Serum Institut, Styrelsen for Patientsikkerhed, Sundhedsdatastyrelsen, Sundhedsstyrelsen, Sundhedsstyrelsen, Strålebeskyttelse, Syddanmarks Universitet, Tandlægeforeningen, Tandlægeforeningens Tandskadeerstatning, Yngre Læger, Ældre Sagen, Aalborg Universitet, Aarhus Universitet.

2. Høringssvar og kommentarer

Der er modtaget høringssvar med bemærkninger fra følgende høringsparter samt organisationer/myndigheder:

Datatilsynet, Færøernes Landsstyre (Heilsu- og innlendismálaráðið– på Færøerne), Grønlands Selvstyre (Departement for Sundhed – Grønland), IT-Politisk Forening, Lægeforeningen, Region Midtjylland og Region Syddanmark.

Følgende høringsparter samt organisationer/myndigheder, som er opført på høringslisten, har oplyst, at de ikke har bemærkninger til lovforslaget:

Danske Kiropraktor Forening, Dansk Psykolog Forening, Farmakonomforeningen, FOA, Forbrugerrådet Tænk, Patienterstatningen, Rigsombudsmanden på Grønland og Ældre Sagen.

Høringssvar med indholdsmæssige bemærkninger gennemgås nedenfor. Sundheds- og Ældreministeriets kommentarer til disse høringssvar er anført i *kursiv*.

3. Specielle bemærkninger

I det følgende foretages en gennemgang af de i høringssvarene væsentligste bemærkninger til de enkelte elementer i lovforslaget.

3.1. Definitioner

Region Syddanmark har anført, at begrebet *hændelse* nationalt bør defineres på samme måde, da der ellers vil kunne opstå forskellige krav til underretning af hændelser alt efter, hvilken sektor en operatør af en væsentlig tjeneste er omfattet af. Det vurderer Region Syddanmark uhensigtsmæssigt.

Region Midtjylland har påpeget, at lovforslaget anvender begreber som op*eratør af en væsentlig tjeneste* og *udbyder af digitale tjenester* uden at uddybe disse begreber i bemærkningerne til lovforslaget.

Lægeforeningen har anført, at det er uklart hvilke systemer lovforslaget omfatter og efterlyser eksempler, som vil give en bedre forståelse af omfanget af lovforslaget. Særligt efterlyses en nærmere beskrivelse af en *operatør af en væsentlig tjeneste*.

Sundheds- og Ældreministeriet kan oplyse, at det i Danmark er vurderet hensigtsmæssigt at implementere Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (herefter NIS-direktivet) sektorvist for at sikre, at der ved implementeringen opnås en målrettet implementering, hvor lovkravene er nøje tilpasset de enkelte sektorers særlige forhold. NIS-direktivet har et bredt anvendelsesområde, men forudsætningen for en målrettet og erhvervsvenlig direktivimplementering, hvor danske virksomheder ikke pålægges unødvendige byrder, er, at nye lovgivningskrav nøje tilpasses de enkelte sektorer. Ved implementeringen af NIS-direktivet videreføres sektoransvaret derfor, således at de enkelte ressortmyndigheder inden for eget område fortsat har ansvaret for at fastsætte og håndhæve de nødvendige regler om sikkerhed for net- og informationssystemer.

NIS-direktivets artikler, herunder anvendte definitioner, vil i de enkelte sektorer, hvor det er relevant, blive implementeret på ensartet vis, men grundet de enkelte sektorers forskelle kan udmøntningen af bestemmelserne forekomme forskellig.

For så vidt angår operatører af væsentlige tjenester skal Sundheds- og Ældreministeriet bemærke, at det fremgår af § 3, stk. 3, i det endelige lovforslag, at sundhedsministeren fastsætter nærmere regler om kriterierne for at være en operatør af en væsentlig tjeneste. Det er således hensigten at udstede en bekendtgørelse, der nærmere præciserer, hvad der skal forstås ved en operatør af en væsentlig tjeneste.

For så vidt angår Region Midtjyllands bemærkning om, at begrebet udbyder af digitale tjenester ikke uddybes i bemærkningerne til lovforslaget, kan ministeriet oplyse, at

lovforslaget udelukkende fastsætter krav til operatører af væsentlige tjenester. Udbydere af digitale tjenester reguleres af Erhvervsministeriet.

3.2. Lovforslagets forhold til databeskyttelsesforordningen

Region Midtjylland har efterlyst en beskrivelse af lovforslagets kobling til databeskyttelsesforordningen, herunder bl.a. forordningens kobling til lovforslagets definitioner.

Region Syddanmark har påpeget, at indholdet i lovforslagets afsnit vedrørende sikkerhedskrav er tæt på enslydende eller sammenfaldende med databeskyttelsesforordningens artikler om behandlingssikkerhed.

Datatilsynet har bemærket, at hvis der behandles personoplysninger i net- og informationssystemer, som er omfattet af lovforslaget, skal den til enhver tid gældende lovgivning om behandling af personoplysninger i øvrigt iagttages.

Sundheds- og Ældreministeriet kan oplyse, at lovforslaget ikke regulerer behandling af personoplysninger.

Sundheds- og Ældreministeriet skal bemærke, at det følger af artikel 2, stk. 1 i NIS-direktivet, at behandling af personoplysninger i henhold til NIS-direktivet udføres i overensstemmelse med direktiv 95/46/EF (herefter databeskyttelsesdirektivet).

Ministeriet har, i lyset af de indkomne høringssvar, i bemærkningerne i det endelige lovforslag præciseret, at den offentlige og private sektor er – indtil den 24. maj 2018 – omfattet af lov nr. 429 af 31. maj 2000 med senere ændringer (herefter persondataloven) og tilhørende bekendtgørelser, når der behandles personoplysninger. Databeskyttelsesdirektivet ophæves den 25. maj 2018, jf. Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (herefter databeskyttelsesforordningen), som finder anvendelse fra den 25. maj 2018. Efter den 25. maj 2018 vil det være reglerne i databeskyttelsesforordningen, suppleret af lovforslag til databeskyttelsesloven, lov om retshåndhævende myndigheders behandling af personoplysninger samt diverse særregler, herunder bl.a. regler i sundhedsloven m.v., der regulerer området for behandling af personoplysninger.

3.3 Sikkerhedskrav

Datatilsynet har bemærket, at hvis der behandles personoplysninger i net- og informationssystemer følger det ligeledes af persondataloven, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbrug eller i øvrigt behandles i strid med loven. Det gælder ligeledes efter databeskyttelsesforordningen, at der gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

Sundheds- og Ældreministeriet har i bemærkningerne til det endelige lovforslag præciseret, at såfremt en operatør af en væsentlig tjeneste behandler personoplysninger, vil de relevante sikkerhedskrav, der følger af databeskyttelsesforordningen skulle iagttages.

3.4 Tilsyn

Lægeforeningen har anført, at Sundhedsdatastyrelsen kan risikere at få en dobbeltrolle som både tilsynsmyndighed og operatør af en væsentlig tjeneste. Derfor anfører Lægeforeningen, at tilsynet med Sundhedsdatastyrelsen f.eks. bør ligge hos Datatilsynet eller Digitaliseringsstyrelsen.

Region Midtjylland har efterspurgt en begrundelse for, hvorfor Sundhedsdatastyrelsen skal fungere som tilsynsmyndighed på sundhedsområdet.

Region Syddanmark har anført, at dokumentation om sikkerhedsforanstaltninger, som led i Sundhedsdatastyrelsens tilsyn med operatører af væsentlige tjenester, i form og indhold bør svare til de dokumentationskrav, der gælder i databeskyttelsesforordningen.

IT-Politisk Forening har anført, at hvis hver sektor har sin egen tilsynsmyndighed, vil tilsynsressourcerne kunne blive spredt unødigt, og synergieffekter mellem forskellige tilsynsområder vil kunne blive vanskelige at udnytte.

Sundheds- og Ældreministeriet har i det endelig lovforslag præciseret, at lovforslagets beføjelser - der i høringsversionen tilkom Sundhedsdatastyrelsen – nu er blevet tillagt sundhedsministeren. Dog foreslås det med § 9 i det endelige lovforslag, at sundhedsministeren kan bemyndige Sundhedsdatastyrelsen til at varetage opgaver, der i loven er tillagt ministeren.

Ministeriet har i bemærkningerne til det endelige lovforslag præciseret, at det er hensigten, at delegere lovforslagets beføjelser til Sundhedsdatastyrelsen, da Sundhedsdatastyrelsen i forvejen har opgaver vedrørende bl.a. digitalisering, sundhedsdata og it-arkitektur i sundhedsvæsenet, herunder opgaver vedrørende informationssikkerhed.

Til Lægeforeningens høringssvar skal det bemærkes, at det i bemærkningerne til det endelige lovforslaget er blevet præciseret, at i det omfang Sundhedsdatastyrelsen selv er en operatør af en væsentlig tjeneste, vil sundhedsministeren dog selv skulle varetage de opgaver, der i lovforslaget er tillagt ministeren, herunder bl.a. føre tilsyn med Sundhedsdatastyrelsen.

For så vidt angår IT-Politisk Forenings bemærkninger om unødig spredning af tilsynsressourcer kan ministeriet oplyse, at det i Danmark er vurderet hensigtsmæssigt at implementere NIS-direktivet sektorvist for på denne måde at opnå en målrettet og erhvervsvenlig implementering samt en implementering, hvor lovkravene nøje er tilpasset de enkelte sektorer. Det bemærkes i øvrigt, at Center for Cybersikkerhed som nationalt centralt kontaktpunkt og CSIRT vil skulle varetage en række tværgående funktioner, herunder monitorering af hændelser på nationalt plan samt formidling af information om risici og hændelser til sektormyndighederne og andre relevante interessenter. Dermed er det hensigten, at der vil ske en koordination og erfaringsudveksling på tværs af sektorerne.

3.5 Underretning og offentliggørelse af hændelser

IT-Politiske Forening har anført, at det ikke fremgår af lovforslaget, hvorledes en underretning, der indeholder personoplysninger, skal håndteres. Foreningen har endvidere påpeget, at der kan forekomme tilfælde, hvor Sundhedsdatastyrelsen i forlængelse af en hændelse vil skulle videregive personoplysninger til Center for Cybersikkerhed.

Region Syddanmark har bemærket, at en hændelse, der berører en operatørs net- og informationssystem ligeledes kan udgøre et brud på persondatasikkerheden, hvorfor der skal ske underretning til Sundhedsdatastyrelsen og Datatilsynet. Dette vurderer regionen uhensigtsmæssigt.

Datatilsynet har påpeget, at det er uklart, i hvilket omfang oplysninger til offentligheden i forbindelse med en offentliggørelse af en hændelse vil kunne indeholde personoplysninger. Tilsynet har i øvrigt henledt opmærksomhed på, at der i databeskyttelsesforordningen er regler om anmeldelse af brud på persondatasikkerheden. Tilsynet har i den forbindelse bemærket at et samarbejde med Datatilsynet kan blive relevant i forbindelse med en underretning om en hændelse til Sundhedsdatastyrelsen.

Sundheds- og Ældreministeriet har i bemærkningerne til det endelige lovforslaget præciseret, at underretninger om hændelser vil skulle ske parallelt til sundhedsministeren og Center for Cybersikkerhed.

Sundheds- og Ældreministeriet har i bemærkningerne til det endelige lovforslag præciseret, at lovforslaget ikke regulerer videregivelse af personoplysninger. Såfremt sundhedsministeren, vil få behov for at videregive personoplysninger, skal videregivelsen ske i overensstemmelse med gældende ret, herunder reglerne i databeskyttelsesforordningen, forslag til databeskyttelsesloven, lov om retshåndhævende myndigheders behandling af personoplysninger og forvaltningsloven.

Ministeriet har endvidere i bemærkningerne til det endelige lovforslag præciseret, at i tilfælde af brud på persondatasikkerheden, vil der fra den 25. maj 2018, hvor databeskyttelsesforordningen finder anvendelse, skulle ske anmeldelse af brud på persondatasikkerheden til den relevante tilsynsmyndighed, dvs. Datatilsynet, uden unødig forsinkelse og om muligt senest 72 timer efter at den dataansvarlige er blevet bekendt med bruddet, jf. forordningens artikel 33, stk. 1.

I forhold til Datatilsynets bemærkning om, at et samarbejde med Datatilsynet kan blive relevant i forbindelse med en underretning om en hændelse til sundhedsministeren, kan ministeriet bekræfte, at der kan forekomme tilfælde, hvor en hændelse i henhold til lovforslaget tillige vil udgøre et brud persondatasikkerheden, hvorfor der vil skulle ske underretning til henholdsvis sundhedsministeren og Datatilsynet.

Ministeriet har i bemærkningerne til det endelige lovforslaget præciseret, at en underretning til sundhedsministeren vil skulle ske gennem en fællesoffentlig indberetningsløsning. Det tilstræbes at udvikle en effektiv og enkel indberetningsløsning.

Ministeriet har i bemærkningerne til det endelige lovforslaget præciseret, at såfremt der sker offentliggørelse af personoplysninger vil offentliggørelsen skulle ske i overensstemmelse med reglerne i databeskyttelsesforordningen, forslag til databeskyttelsesloven og lov om retshåndhævende myndigheders behandling af personoplysninger.

3.6 CSIRT og nationalt centralt kontaktpunkt

IT-Politisk Forening har i høringssvaret gjort opmærksom på, det af lovforslaget ikke fremgår, hvem der skal varetage funktionen som CSIRT og nationalt centralt kontaktpunkt.

Sundheds- og Ældreministeriet har i det endelige lovforslag præciseret, at Center for Cybersikkerhed varetager funktionen som henholdsvis nationalt centralt kontaktpunkt og Computer Security Incident Response Team (CSIRT).

3.7 Sanktioner

Region Midtjylland har anført, at de forventer, at sanktionsbestemmelsen vil lægge sig op af Databeskyttelsesloven.

IT-Politisk Forening har anført, at de i forhold til offentlige myndigheder ikke ser nogen mulighed for at gøre undtagelser vedrørende økonomiske sanktioner.

Sundheds- og Ældreministeriet har i det endelige lovforslag præciseret rammerne for straf, herunder at offentlige myndigheder ikke er omfattet af strafbestemmelsen.

3.8 Ikrafttrædelse m.v.

Grønlands Selvstyre (Departement for Sundhed – Grønland) har oplyst, at den foreslåede lov ikke skal gælde for Grønland, men ved kongelig anordning skal kunne sættes helt eller delvist i kraft for Grønland med de afvigelser, som de grønlandske forhold tilsiger.

Færøernes Landsstyre (Heilsu- og innlendismálaráðið) har oplyst, at Færøerne har overtaget lovgivningskompetencen vedrørende diverse sagsområder på sundhedsområdet. Lovforslaget skal således ikke gælde for Færøerne.

Sundheds- og Ældreministeriet har i det endelige lovforslag præciseret, at den foreslåede lov ikke gælder for Færøerne og Grønland. Baggrunden for den foreslåede ordning er, at Grønland har overtaget sundhedsvæsenet i Grønland, og Færøerne har overtaget de relevante dele af sundhedsområdet på Færøerne.