DATATILSYNET

Sundheds- og Ældreministeriet
Holbergsgade 6
1057 København K

Sendt til: sum@sum.dk og padl@sum.dk

15. november 2017

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

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

J.nr. 2017-112-0790
Dok.nr. 451160
Sagsbehandler
Signe Vestergård Abildskov
Direkte 3319 3212

Vedrørende høring over udkast til forslag til lov om krav til sikkerheden for net- og informationssystemer inden for sundhedssektoren – Sundheds- og Ældreministeriets sagsnr.: 1706260

Ved e-mail af 18. oktober 2017 har Sundheds- og Ældreministeriet anmodet om Datatilsynets eventuelle bemærkninger til ovennævnte udkast.

Det fremgår af ministeriets høringsbrev, at lovforslaget inden for sundhedssektoren implementerer dele af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (herefter "NIS-direktivet").

1. Anvendelsesområde

Det fremgår af udkastets § 1, at loven gælder for operatører, der leverer væsentlige tjenester inden for sundhedssektoren med henblik på at sikre et højt sikkerhedsniveau i disses net- og informationssystemer.

Det følgende fremgår bl.a. af bemærkningerne til udkastets § 1:

> "Ved *net- og informationssystemer* forstås enten a) et elektronisk kommunikationsnet som defineret i telelovens § 2, nr. 4, dvs. et elektronisk kommunikationsnet i form af en radiofrekvens- eller kabelbaseret teleinfrastruktur, der anvendes til formidling af elektroniske kommunikationstjenester, b) enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller c) digitale data, som lagres, behandles, fremfindes eller overføres ved brug af elementer i førnævnte punkt a) og b) med henblik på deres drift, brug, beskyttelse og vedligeholdelse. Definitionen af net- og informationssystemer bygger på NIS-direktivets artikel 4, nr. 1."

Datatilsynet henviser til, at persondataloven[1] ifølge lovens § 1, stk. 1, bl.a. gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.

Datatilsynet skal i øvrigt gøre opmærksom på, at databeskyttelsesforordningen[2] finder anvendelse fra den 25. maj 2018, og at persondataloven samtidig ophæves. Databeskyttelsesforordningen finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

På den baggrund skal Datatilsynet bemærke, at hvis der behandles personoplysninger i net- og informationssystemerne, som er omfattet af udkastet, skal den til enhver tid gældende lovgivning om behandling af personoplysninger i øvrigt iagttages. Datatilsynet kan til orientering oplyse, at personoplysninger er enhver form for information om en identificeret eller identificerbar fysisk person, jf. databeskyttelsesforordningens artikel 4, nr. 1.

2. Sikkerhedskrav

Det fremgår af udkastets § 3, at operatører af væsentlige tjenester skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at sikre et højt sikkerhedsniveau for net- og informationssystemer, som anvendes til deres aktiviteter og med disse foranstaltninger opretholde et sikkerhedsniveau, der står i forhold til risikoen.

Datatilsynet bemærker, at hvis der behandles personoplysninger i net- og informationssystemer følger det ligeledes af persondatalovens § 41, stk. 3, 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, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Der gælder ligeledes en forpligtelse efter databeskyttelsesforordningens artikel 32 til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

3. Underretning om hændelser

Det følger bl.a. af udkastets § 4, at operatører af væsentlige tjenester hurtigst muligt skal underrette Sundhedsdatastyrelsen om hændelser, der har væsentlige konsekvenser for kontinuiteten af de tjenester, som de leverer.

Det følgende fremgår til udkastets § 2, stk. 1:

> "Ved *hændelse* forstås enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer. Definitionen af hændelse bygger på NIS-direktivets artikel 4, nr. 7. I vurderingen af, hvorvidt en hændel-

[2] 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

> se har væsentlig forstyrrende virkning, skal en række faktorer indgå, som f.eks. det antal brugere, der er afhængige af tjenesten til private eller erhvervsmæssige formål samt hændelsens betydning for patientsikkerheden. Til eksempel kan antallet af patienter under operatørens virke pr. år inddrages i vurderingen af, hvorvidt en hændelse har væsentlig forstyrrende virkning. I vurderingen af en hændelses omfang og varighed på økonomiske og samfundsmæssige aktiviteter eller den offentlige sikkerhed, vil ligeledes kunne indgå, hvor lang tid, der skønnes at ville gå, før afbrydelsen af tjenesten vil have negative konsekvenser."

Datatilsynet skal herefter gøre opmærksom på, at der også i databeskyttelsesforordningens artikel 33 er regler om anmeldelse af brud på persondatasikkerhed. Disse sikkerhedsbrud skal anmeldes til Datatilsynet uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet på persondatasikkerhed.[3]

Det fremgår af NIS-direktivets artikel 8, stk. 6, at de kompetente myndigheder – Sundhedsdatastyrelsen i sundhedssektoren – og det centrale kontaktpunkt konsulterer og samarbejder, hvor det er passende og i henhold til national ret, med de relevante nationale retshåndhævende myndigheder og de nationale databeskyttelsesmyndigheder.

Datatilsynet går således ud fra, at et sådan samarbejde med Datatilsynet kan bliver relevant i forbindelse med en underretning til Sundhedsdatastyrelsen af en hændelse.

4. Offentliggørelse af hændelser

Det fremgår af udkastets § 4, stk. 5, at Sundhedsdatastyrelsen efter høring af den underrettende operatør kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Det fremgår af bemærkningerne til udkastets § 4, stk. 5, at offentliggørelse skal ske efter høring af operatøren, og Sundhedsdatastyrelsen skal foretage en afvejning af offentlighedens interesse i at blive informeret om de pågældende trusler over for operatørens interesse i ikke at lide kommerciel skade.

Det står ikke Datatilsynet klart, i hvilket omfang der i de omtalte oplysninger til offentligheden vil kunne indgå personoplysninger.

Datatilsynet kan i den forbindelse oplyse, at enhver form for information om en identificeret eller identificerbar fysisk person er personoplysninger, jf. persondatalovens § 3, nr. 1.

---

[3] Det følger af § 27 i L 68 Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, at Datatilsynet i overensstemmelse med databeskyttelsesforordningens kaptiel VI-VII fører tilsyn med enhver behandling, der omfattes af databeskyttelsesloven, databeskyttelsesforordningen og anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger, jf. dog lovens kapitel 11.

Oplysninger vedrørende enkeltmandsejede virksomheder anses for personoplysninger omfattet af persondataloven.

Det fremgår af udkastets § 8, at det bl.a. er strafbart ikke at efterkomme kravene i udkastets § 3, stk. 1 og 2, om sikkerhedskrav.

Efter persondatalovens § 8, stk. 2, må oplysninger om strafbare forhold som udgangspunkt ikke videregives (herunder offentliggøres). Der kan imidlertid alene ske videregivelse af oplysninger om strafbare forhold, såfremt én af betingelserne i lovens § 8, stk. 2, nr. 1-4, er opfyldt.

I den forbindelse finder Datatilsynet anledning til at bemærke, at udvalget om offentlige myndigheders offentliggørelse af kontrolresultater mv. i sin betænkning[4] har anført, at der efter udvalgets opfattelse kun i sjældne tilfælde bør indføres ordninger med systematisk offentliggørelse vedrørende fysiske personer af oplysninger omfattet af persondatalovens § 8 (betænkningens kapitel 4, punkt 3).

Det følger endvidere af databeskyttelsesforordningens artikel 10, at behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger på grundlag af artikel 6, stk. 1, kun må foretages under kontrol af en offentlig myndighed, eller hvis behandling har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for registreredes rettigheder og frihedsrettigheder.

Datatilsynet bemærker i den forbindelse, at det er anført i Betænkning om Databeskyttelsesforordningen (2016/679) og de retlige rammer for dansk lovgivning, at det må antages umiddelbart at være muligt at videreføre de særlige regler i gældende ret for offentlige myndigheders behandling og videregivelse af oplysninger om strafbare forhold efter persondatalovens § 8, stk. 1-3, på baggrund af forordningens artikel 6, stk. 1, litra e, jf. artikel 6, stk. 2 og 3 (betænkningens punkt 3.10.4.).

I forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter "databeskyttelsesloven")[5] er der også lagt op til, at § 8, stk. 1-3 videreføres fra den 25. maj 2018, når persondataloven ophæves.

Sundhedsdatastyrelsen må således sikre sig, at sådanne oplysninger ikke i strid med persondataloven, databeskyttelsesforordningen og databeskyttelsesloven offentliggøres i medfør af udkastets § 4, stk. 5.

---

[4] Betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv.

[5] L 68 Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

5. Afsluttende bemærkninger
For så vidt angår bemyndigelsesbestemmelserne i udkastet til lovforslagets § 2, stk. 4, § 3, stk. 3, § 4, stk. 6, og § 6, stk. 4, skal Datatilsynet for god ordens skyld henlede opmærksomheden på persondatalovens § 57. Det følger heraf, at der skal indhentes en udtalelse fra Datatilsynet i forbindelse med udfærdigelse af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelse af privatlivet i forbindelse med behandling af oplysninger.

Kopi af dette brev er dags dato sendt til Justitsministeriet, Lovafdelingen, til orientering.

Med venlig hilsen

Signe Vestergård Abildskov

From: Chilli Fredslund
Sent: Tue, 14 Nov 2017 13:37:46 +0100
To: DEP Sundheds- og Ældreministeriet;Anne-Sofie Duelund Lassesen
Subject: Sv: HØRING: Udkast til lovforslag om krav til sikkerhed for net- og informationssystemer i sundhedssektoren (F2 DP Id nr.: 1585286)

Til rette vedkommende.

Dansk Psykolog Forening har ikke som udgangspunkt kommentarer til lovforslaget, men understreger at vi på baggrund af psykologers håndtering af persondata og personfølsomme data i sine virksomheder, er optaget af, at net- og informationssikkerheden på sundhedsområdet holder et så højt niveau som muligt.

I lyset af, at operatører i dag ikke er underlagt retlig regulering i forhold til net- og informationssikkerhed, og i lyset af at sundhedssektoren i høj grad er afhængig af velfungerende og sikre systemer, ser Dansk Psykolog Forening derfor positivt på lovforslaget.

Med venlig hilsen

Chilli Fredslund
-- Studentermedhjælper --

DANSK PSYKOLOG FORENING

Stockholmsgade 27 | 2100 København Ø | cfr@dp.dk |
Web: www.dp.dk |www.psykologeridanmark.dk |www.facebook.com/DanskPsykologForening.dk

---

Til: 'aeldresagen@aeldresagen.dk' (aeldresagen@aeldresagen.dk), info@danskerhverv.dk (info@danskerhverv.dk), PLO (plo@dadl.dk), Lægeforeningen (DADL) (dadl@dadl.dk), kl@kl.dk (kl@kl.dk), Region Hovedstaden (regionh@regionh.dk), kontakt@regionmidtjylland.dk (kontakt@regionmidtjylland.dk), info@danskepatienter.dk (info@danskepatienter.dk), 'ku@ku.dk' (ku@ku.dk), 'kontakt@sundhedsdata.dk' (kontakt@sundhedsdata.dk), 'info@digitalsikkerhed.dk' (info@digitalsikkerhed.dk), 'politi@politi.dk' (politi@politi.dk), 'ro@gl.stm.dk' (ro@gl.stm.dk), 'ro@fo.stm.dk' (ro@fo.stm.dk), 'rigsadvokaten@ankl.dk' (rigsadvokaten@ankl.dk), 'info@privatehospitaler.dk' (info@privatehospitaler.dk), 'pebl@patienterstatningen.dk' (pebl@patienterstatningen.dk), info@dansktp.dk (info@dansktp.dk), Radiograf Rådet (kontakt@radiograf.dk (kontakt@radiograf.dk), YL (yl@dadl.dk), Tandlægeforeningen (TF) (info@tandlaegeforeningen.dk), Sundhedsstyrelsen (sst@sst.dk), Sundhedsstyrelsen (sst@sst.dk), DP (dp@dp.dk), 'aau@auu.dk' (aau@auu.dk), jordemoderforeningen.dk (sek@jordemoderforeningen.dk), 'ruc@ruc.dk' (ruc@ruc.dk), SIS Institutpostkasse (sis@sis.dk), 'serum@ssi.dk' (serum@ssi.dk), 'web@tf-tandskade.dk' (web@tf-tandskade.dk), region@rn.dk (region@rn.dk), pob@patientombuddet.dk (pob@patientombuddet.dk), info@fodterapeut.dk (info@fodterapeut.dk), 'sdu@sdu.dk' (sdu@sdu.dk), Lægemiddelstyrelsen DKMA (dkma@dkma.dk), 'kfst@kfst.dk' (kfst@kfst.dk), 'hoeringer@fbr.dk' (hoeringer@fbr.dk), 'hmr@hmr.fo' (hmr@hmr.fo), 'fp@forsikringogpension.dk' (fp@forsikringogpension.dk), 'dit@dit.dk' (dit@dit.dk), 'do@optikerforeningen.dk' (do@optikerforeningen.dk), danske.bandagister@mail.dk (danske.bandagister@mail.dk), dbio@dbio.dk (dbio@dbio.dk), 'govsec@nanoq.gl' (govsec@nanoq.gl), Datatilsynet (dt@datatilsynet.dk), ast@ast.dk (ast@ast.dk), Danske Regioner (DR) (regioner@regioner.dk), 'dansk.standard@ds.dk' (dansk.standard@ds.dk), 'apotekerforeningen@apotekerforeningen.dk'

(apotekerforeningen@apotekerforeningen.dk), Ansatte Tandlægers Organisation (info@ato.dk (info@ato.dk), 3F (3f@3f.dk (3f@3f.dk), ddd (ddd@ddd.dk), Foreningen af Speciallæger (fas@dadl.dk), DKF og Kiropraktoren (dkf@danskkiropraktorforening.dk), DOFT (info@deoffentligetandlaeger.dk), 'info@danske-dental.dk' (info@danske-dental.dk), 'pto@pto.dk' (pto@pto.dk), 'lvs@dadl.dk' (lvs@dadl.dk), 'info@lkt.dk' (info@lkt.dk), 'kontakt@dpfo.dk' (kontakt@dpfo.dk), 'kontakt@rsyd.dk' (kontakt@rsyd.dk), 'regionsjaelland@regionsjaelland.dk' (regionsjaelland@regionsjaelland.dk), ff@farmakonom.dk (ff@farmakonom.dk), 'foa@foa.dk' (foa@foa.dk), dsr@dsr.dk (dsr@dsr.dk), ds@socialraadgiverne.dk (ds@socialraadgiverne.dk), Di@Di.Dk (Di@Di.Dk), 'etf@etf.dk' (etf@etf.dk), 'fysio@fysio.dk' (fysio@fysio.dk), FaKD (post@diaetist.dk), Aarhus Universitet (au@au.dk), SI@SI.Dk (SI@SI.Dk)

Fra: Maja Holm Andreasen (MAHA@sum.dk)

Titel: HØRING: Udkast til lovforslag om krav til sikkerhed for net- og informationssystemer i sundhedssektoren

Sendt: 18-10-2017 22:34:20

Til høringsparterne

Se venligst vedhæftede høringsbrev, høringsliste og udkast til lovforslag om krav til sikkerhed for net- og informationssystemer i sundhedssektoren.

Med venlig hilsen

Maja Holm Andreasen
Fuldmægtig, Sundhedsøkonomi

Mail: maha@sum.dk

Telefon: 72 26 94 23

Sundheds- og Ældreministeriet ● Holbergsgade 6 ●
1057 København K ● Tlf. 7226 9000 ● Fax 7226 9001 ● www.sum.dk

SUNDHEDS- OG ÆLDREMINISTERIET

From: Pia Saxild
Sent: Wed, 15 Nov 2017 15:17:46 +0100
To: DEP Sundheds- og Ældreministeriet
Cc: Anne-Sofie Duelund Lassesen
Subject: SV: HØRING: Udkast til lovforslag om krav til sikkerhed for net- og informationssystemer i sundhedssektoren

Forbrugerrådet Tænk har af ressourcemæssige årsager ikke mulighed for at forholde os til udkast til lovforslag om krav til sikkerhed for net- og informationssystemer i sundhedssektoren. Forbrugerrådet Tænk kan således ikke tages til indtægt for at støtte forslaget eller for at gøre det modsatte.

Med venlig hilsen

Sine Jensen
Seniorrådgiver, sundhedspolitik

Forbrugerrådet Tænk
T +45 7741 7737 / sj@fbr.dk / taenk.dk
Fiolstræde 17 B / Postboks 2188 / 1017 København K

Vær med i kampen. Bevar forbrugernes stemme. Skriv under her.

Fra: Maja Holm Andreasen [mailto:MAHA@sum.dk]
Sendt: 18. oktober 2017 22:34
Til: 'regioner@regioner.dk'; 'kl@kl.dk'; 'regionh@regionh.dk'; 'regionsjaelland@regionsjaelland.dk'; 'kontakt@rsyd.dk'; 'kontakt@regionmidtjylland.dk'; 'region@rn.dk'; '3f@3f.dk'; 'info@ato.dk'; 'apotekerforeningen@apotekerforeningen.dk'; 'do@optikerforeningen.dk'; 'dkf@danskkiropraktorforening.dk'; 'dp@dp.dk'; 'kontakt@dpfo.dk'; 'ds@socialraadgiverne.dk'; 'dsr@dsr.dk'; 'info@dansktp.dk'; 'danske.bandagister@mail.dk'; 'dbio@dbio.dk'; 'info@fodterapeut.dk'; 'fysio@fysio.dk'; 'info@deoffentligetandlaeger.dk'; 'ddd@ddd.dk'; 'etf@etf.dk'; 'ff@farmakonom.dk'; 'foa@foa.dk'; 'post@diaetist.dk'; 'fas@dadl.dk'; 'sek@jordemoderforeningen.dk'; 'info@lkt.dk'; 'dadl@dadl.dk'; 'lvs@dadl.dk'; 'plo@dadl.dk'; 'pto@pto.dk'; 'ast@ast.dk'; 'kontakt@radiograf.dk'; 'sl@sl.dk'; 'info@tandlaegeforeningen.dk'; 'yl@dadl.dk'; 'info@danskepatienter.dk'; 'aeldresagen@aeldresagen.dk'; 'info@privatehospitaler.dk'; 'info@danskerhverv.dk'; 'di@di.dk'; 'dit@dit.dk'; 'dansk.standard@ds.dk'; 'info@danske-dental.dk'; Forbrugerrådet Tænk Hoeringer; 'fp@forsikringogpension.dk'; 'web@tf-tandskade.dk'; 'dt@datatilsynet.dk'; 'hmr@hmr.fo'; 'govsec@nanoq.gl'; 'kfst@kfst.dk'; Lægemiddelstyrelsen DKMA; 'pebl@patienterstatningen.dk'; 'rigsadvokaten@ankl.dk'; 'ro@fo.stm.dk'; 'ro@gl.stm.dk'; 'politi@politi.dk'; 'info@digitalsikkerhed.dk'; 'serum@ssi.dk'; Sundhedsstyrelsen Institutionspostkasse; 'kontakt@sundhedsdata.dk'; SIS Institutpostkasse; Sundhedsstyrelsen Institutionspostkasse; 'pob@patientombuddet.dk'; 'ku@ku.dk'; 'au@au.dk'; 'sdu@sdu.dk'; 'ruc@ruc.dk'; 'aau@auu.dk'
Emne: HØRING: Udkast til lovforslag om krav til sikkerhed for net- og informationssystemer i sundhedssektoren

Til høringsparterne

Se venligst vedhæftede høringsbrev, høringsliste og udkast til lovforslag om krav til sikkerhed for net- og informationssystemer i sundhedssektoren.

Med venlig hilsen

Maja Holm Andreasen
Fuldmægtig, Sundhedsøkonomi

Mail: maha@sum.dk

Telefon: 72 26 94 23

Sundheds- og Ældreministeriet ● Holbergsgade 6 ●
1057 København K ● Tlf. 7226 9000 ● Fax 7226 9001 ● www.sum.dk

---

SUNDHEDS- OG ÆLDREMINISTERIET

From: Birita Ludvíksdóttir
Sent: Wed, 29 Nov 2017 13:26:28 +0000
To: Maja Holm Andreasen
Cc: Turid Arge;Jan Simonsen
Subject: VS: Udkast til lovforslag om krav til sikkerhed for net- og informationssystemer i sundhedssektoren
Attachments: image003.png, image004.png, image005.png

Til Sundhedsministeriet,

Heilsu- og Innlendismálaráðið har modtaget nedenforstående lovforslag i høring og har disse bemærkninger:

Ved lov nr. 316 af 17.05.1995 om sundhedsvæsenet på Færøerne har Færøerne overtaget lovgivningskompetencen vedrørende diverse sagsområder på sundhedsområdet. Heilsu- og Innlendismálaráðið vurderer, at lovforslag om krav til sikkerhed for net- og informationssystemer i sundhedssektoren er en del af denne lov, dvs. at såfremt vi skal have lignende regler på Færøerne, skal disse have hjemmel i lov nr. 316/1995 om sundhedsvæsenet på Færøerne. Disse regler udfærdiges i lagtingslov.

Det anbefales derfor, at der i § 10 i lovforslaget for Færøernes vedkommende skal stå: "Loven gælder ikke for Færøerne".

Vinaliga/Sincerely

Birita Ludvíksdóttir
Løgfrøðiligur ráðgevi/Legal adviser

<image003.png> Heilsu- og Innlendismálaráðið/
Ministry of Health and the Interior
Eirargarður 2 • 100 Tórshavn • Faroe Islands
Tel. +298 304050 • Mobile +298 734066
birita.ludviksdottir@himr.fo • www.himr.fo

Fra: Maja Holm Andreasen [mailto:MAHA@sum.dk]
Sendt: 18. oktober 2017 21:34
Til: 'regioner@regioner.dk' <regioner@regioner.dk>; 'kl@kl.dk' <kl@kl.dk>; 'regionh@regionh.dk' <regionh@regionh.dk>; 'regionsjaelland@regionsjaelland.dk' <regionsjaelland@regionsjaelland.dk>; 'kontakt@rsyd.dk' <kontakt@rsyd.dk>; 'kontakt@regionmidtjylland.dk' <kontakt@regionmidtjylland.dk>; 'region@rn.dk' <region@rn.dk>; '3f@3f.dk' <3f@3f.dk>; 'info@ato.dk' <info@ato.dk>; 'apotekerforeningen@apotekerforeningen.dk' <apotekerforeningen@apotekerforeningen.dk>; 'do@optikerforeningen.dk' <do@optikerforeningen.dk>; 'dkf@danskkiropraktorforening.dk' <dkf@danskkiropraktorforening.dk>; 'dp@dp.dk' <dp@dp.dk>; 'kontakt@dpfo.dk' <kontakt@dpfo.dk>; 'ds@socialraadgiverne.dk' <ds@socialraadgiverne.dk>; 'dsr@dsr.dk' <dsr@dsr.dk>; 'info@dansktp.dk' <info@dansktp.dk>; 'danske.bandagister@mail.dk' <danske.bandagister@mail.dk>; 'dbio@dbio.dk' <dbio@dbio.dk>; 'info@fodterapeut.dk' <info@fodterapeut.dk>; 'fysio@fysio.dk' <fysio@fysio.dk>; 'info@deoffentligetandlaeger.dk' <info@deoffentligetandlaeger.dk>; 'ddd@ddd.dk' <ddd@ddd.dk>; 'etf@etf.dk' <etf@etf.dk>; 'ff@farmakonom.dk' <ff@farmakonom.dk>; 'foa@foa.dk' <foa@foa.dk>; 'post@diaetist.dk' <post@diaetist.dk>; 'fas@dadl.dk' <fas@dadl.dk>; 'sek@jordemoderforeningen.dk'

<sek@jordemoderforeningen.dk>; 'info@lkt.dk' <info@lkt.dk>; 'dadl@dadl.dk' <dadl@dadl.dk>; 'lvs@dadl.dk' <lvs@dadl.dk>; 'plo@dadl.dk' <plo@dadl.dk>; 'pto@pto.dk' <pto@pto.dk>; 'ast@ast.dk' <ast@ast.dk>; 'kontakt@radiograf.dk' <kontakt@radiograf.dk>; 'sl@sl.dk' <sl@sl.dk>; 'info@tandlaegeforeningen.dk' <info@tandlaegeforeningen.dk>; 'yl@dadl.dk' <yl@dadl.dk>; 'info@danskepatienter.dk' <info@danskepatienter.dk>; 'aeldresagen@aeldresagen.dk' <aeldresagen@aeldresagen.dk>; 'info@privatehospitaler.dk' <info@privatehospitaler.dk>; 'info@danskerhverv.dk' <info@danskerhverv.dk>; 'di@di.dk' <di@di.dk>; 'dit@dit.dk' <dit@dit.dk>; 'dansk.standard@ds.dk' <dansk.standard@ds.dk>; 'info@danske-dental.dk' <info@danske-dental.dk>; 'hoeringer@fbr.dk' <hoeringer@fbr.dk>; 'fp@forsikringogpension.dk' <fp@forsikringogpension.dk>; 'web@tf-tandskade.dk' <web@tf-tandskade.dk>; 'dt@datatilsynet.dk' <dt@datatilsynet.dk>; Heilsu- og innlendismálaráðið <himr@himr.fo>; 'govsec@nanoq.gl' <govsec@nanoq.gl>; 'kfst@kfst.dk' <kfst@kfst.dk>; Lægemiddelstyrelsen DKMA <dkma@dkma.dk>; 'pebl@patienterstatningen.dk' <pebl@patienterstatningen.dk>; 'rigsadvokaten@ankl.dk' <rigsadvokaten@ankl.dk>; 'ro@fo.stm.dk' <ro@fo.stm.dk>; 'ro@gl.stm.dk' <ro@gl.stm.dk>; 'politi@politi.dk' <politi@politi.dk>; 'info@digitalsikkerhed.dk' <info@digitalsikkerhed.dk>; 'serum@ssi.dk' <serum@ssi.dk>; Sundhedsstyrelsen Institutionspostkasse <SST@SST.DK>; 'kontakt@sundhedsdata.dk' <kontakt@sundhedsdata.dk>; SIS Institutpostkasse <sis@sis.dk>; Sundhedsstyrelsen Institutionspostkasse <SST@SST.DK>; 'pob@patientombuddet.dk' <pob@patientombuddet.dk>; 'ku@ku.dk' <ku@ku.dk>; 'au@au.dk' <au@au.dk>; 'sdu@sdu.dk' <sdu@sdu.dk>; 'ruc@ruc.dk' <ruc@ruc.dk>; 'aau@auu.dk' <aau@auu.dk>
Emne: HØRING: Udkast til lovforslag om krav til sikkerhed for net- og informationssystemer i sundhedssektoren

Til høringsparterne

Se venligst vedhæftede høringsbrev, høringsliste og udkast til lovforslag om krav til sikkerhed for net- og informationssystemer i sundhedssektoren.

Med venlig hilsen
<image004.png>

Maja Holm Andreasen
Fuldmægtig, Sundhedsøkonomi

Mail: maha@sum.dk

Telefon: 72 26 94 23

Sundheds- og Ældreministeriet • Holbergsgade 6 •
1057 København K • Tlf. 7226 9000 • Fax 7226 9001 • www.sum.dk
<image004.png>

<image005.png>

Maja Holm Andreasen

Fra: Louise Restorff Jacobsen <lrja@nanoq.gl>
Sendt: 22. januar 2018 14:06
Til: Maja Holm Andreasen
Emne: Sv: Vedr. hjemtaget ansvarsområder (Nanoq - ID nr.: 7109132)

Sag: 1706260
Sagsdokument: 526343; 529733

Kære Maja.

Tak for en behagelig samtale.

Departementet skal venligst anmode om, at Grønland bliver inkluderet i lovforslagets § 12, således at loven ikke gælder for Færøerne og Grønland, men kan ved kongelig anordning sættes i kraft.

Inussiarnersumik Inuulluaqqusillunga
Med venlig hilsen
Best regards

Louise Restorff Jacobsen
Inatsisileritooq
Jurist
Legal Officer

NAALAKKERSUISUT
GOVERNMENT OF GREENLAND

Peqqissutsimut Naalakkersusisoqarfik
Departementet for Sundhed
Ministry of Health

P.O. Box xx . 3900 Nuuk
Oq./Tel.: +299 346619

lrja@nanoq.gl
www.naalakkersuisut.gl

Sundheds- og Ældreministeriet
Holbergsgade 6
1057 København K

Sendt per email til **sum@sum.dk**
med kopi til **padl@sum.dk**

IT-Politisk Forening
c/o Jesper Lund
Carl Bernhards Vej 15, 2.tv
1817 Frederiksberg C

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 15. november 2017

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

Regeringen har valgt at gennemføre NIS-direktivet med sektorspecifikke love, hvor en eksisterende institution under det pågældende ministerium får tilsynsopgaven som kompetent myndighed. For Sundheds- og Ældreministeriets område får Sundhedsdatastyrelsen denne opgave.

NIS-direktivets artikel 8, stk. 1 overlader det til medlemsstaterne at fastsætte, om der skal være en eller flere kompetente myndigheder. En kompetent myndighed for hvert ministeriums område er som sådan inden for rammerne af artikel 8, stk. 1. Hvis der kommer 4-5 kompetente myndigheder i Danmark (jf. sektoropdelingen i bilag II i NIS-direktivet), kan tilsynsressourcerne blive spredt mere end godt er, og synergieffekter mellem forskellige tilsynsområder kan blive vanskelige at udnytte.

Et væsentligt element i NIS-direktivet er at medlemsstaterne skal vedtage en samlet national strategi for sikkerheden i net- og informationssystemer, og der skal være en effektiv informationsudveksling på tværs af sektorer på nationalt plan samt mellem EU-landene på internationalt plan. De tværgående opgaver vil blive varetaget af de(n) danske CSIRT-enhed(er) og det centrale kontaktpunkt, jf. NIS-direktivet. De organisatoriske rammer for disse enheder er ikke omtalt i lovforslaget, men det

fremgår af Forsvarsministeriets lovudkast vedrørende ”Lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.” at Center for Cybersikkerhed skal have disse roller (som eneste danske CSIRT og det centrale kontaktpunkt).

Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, som generelt opererer under andre rammebetingelser end civile myndigheder, for eksempel med betydelige undtagelser fra offentlighedsloven, forvaltningsloven og persondataloven. IT-Politisk Foreninger finder det meget betænkeligt, at Center for Cybersikkerhed via gennemførelsen af NIS-direktivet får en så betydelig rolle i forhold til cybersikkerheden i den offentlige og private sektor. Af principielle årsager mener vi, at de(n) danske CSIRT(er) og det centrale kontaktpunkt bør være civile myndigheder.

Det gælder ikke mindst i de situationer, hvor det kan blive nødvendigt at behandle personoplysninger i forbindelse med underretning af den kompetente myndighed om hændelser, jf. NIS-direktivets artikel 14, stk. 3. Dette punkt uddybes nedenfor.

Bemærkninger til lovforslagets paragraffer

Lovforslaget følger strukturen og terminologien i NIS-direktivet i forhold til operatører af væsentlige tjenester. Visse bestemmelser skal dog fastsættes i bekendtgørelser, eksempelvis definitionen af ”væsentligt forstyrrende virkning”, der skal være inden for rammerne af NIS-direktivets artikel 6. De specielle bemærkninger til lovforslagets § 2 henviser til NIS-direktivet på dette punkt.

Af hensyn til retssikkerheden for offentlige og private enheder (herunder fysiske personer), som kan blive udpeget som operatør af væsentlige tjenester mod deres vilje med deraf følgende uønskede administrative byrder, vil IT-Politisk Forening anbefale, at kriterierne for ”væsentligt forstyrrende virkning” skrives direkte ind i lovforslaget, så vidt muligt med en stillingtagen til hvilke sektorspecifikke forhold der kan være relevante på Sundheds- og Ældreministeriets område, jf. NIS-direktivets artikel 6, stk. 2.

Ifølge § 8, stk. 2 i lovforslaget udestår stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder. IT-Politisk Forening skal hertil bemærke, at det efter NIS-direktivets artikel 21 er et krav, at sanktioner skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. Der er ikke nogen mulighed for at gøre undtagelser i forhold til offentlige myndigheder på dette punkt.

Behandling af personoplysninger i forbindelse med underretning om hændelser

Lovforlagets § 4, stk. 1, jf. NIS-direktivets artikel 14, stk. 3, fastsætter en pligt til hurtigt at underrette Sundhedsdatastyrelsen (den kompetente myndighed) om hændelser, der har væsentlig betydning for kontinuiteten af de leverede tjenester. Underretningen skal indeholde oplysninger, som gør det muligt for Sundhedsdatastyrelsen at klarlægge eventuelle grænseoverskridende konsekvenser af hændelsen.

I nogle tilfælde vil de nødvendige oplysninger i forbindelse med underretningen om en hændelse indeholde personoplysninger. Det kunne være IP-adresser, men også oplysninger fra et IT-systems databaser, som er forsøgt hacket (exfiltreret) og måske optræder i logfiler. Dette spørgsmål omtales ikke i lovforslagets bemærkninger. Der er således ingen overvejelser om hjemmel i persondataloven til videregivelse af disse personoplysninger og hvordan eventuelle videregivne personoplysninger skal behandles af Sundhedsdatastyrelsen.

Efter IT-Politisk Forenings opfattelse bør der fastsættes lovregler (eventuelt i bekendtgørelsesform), som begrænser behandlingen af personoplysninger til det strengt nødvendige for at klarlægge omfanget af hændelsen og dens eventuelle grænseoverskridende konsekvenser. Der bør desuden være et eksplicit krav om at disse personoplysninger skal slettes eller anonymiseres hurtigst muligt.

Efter lovforslaget skal der alene ske underretning til den kompetente myndighed (Sundhedsdatastyrelsen). Når der ikke sker underretning af CSIRT'en i forbindelse med en

hændelse, kræver NIS-direktivets artikel 10, stk. 2, at CSIRT'en skal have adgang til oplysninger om hændelser, der er underrettet af operatører af væsentlige tjenester. Denne adgang vil potentielt indebære en yderligere videregivelse af personoplysninger, i det tilfælde fra Sundhedsdatastyrelsen til Center for Cybersikkerhed.

NIS-direktivets artikel 2, stk. 1 kræver, at behandling af personoplysninger i henhold til direktivet sker i overensstemmelse med direktiv 95/46/EF, og fra 25. maj 2018 databeskyttelsesforordningen (EU) 2016/679. Ifølge den nuværende persondatalov, og det forslag til ny databeskyttelseslov som Justitsministeren har fremsat 25. oktober 2017 (L 68), er Forsvarets Efterretningstjeneste (FE) undtaget fra de EU-retlige regler om databeskyttelse. Undtagelsen er for FE som institution, og vil derfor også gælde, når FE udøver aktiviteter inden for EU-retten, eksempelvis cybersikkerhedsopgaver i forbindelse med NIS-direktivet.

Hvis den fuldstændige undtagelse fra databeskyttelses-forordningen opretholdes for Center for Cybersikkerhed (under FE), vil det efter IT-Politisk Forenings opfattelse ikke være muligt at gennemføre NIS-direktivet på en korrekt måde. Beskyttelsen af personoplysninger i den danske gennemførelse af direktivet vil ikke kunne leve op til kravet i NIS-direktivets artikel 2 (samt artikel 8 i Charter om Grundlæggende Rettigheder).

Lægeforeningen

Høringssvar

Høring over udkast til forslag til lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren

Lægeforeningen finder det betænkeligt, at det ikke fremgår af lovforslaget præcist, hvilke typer af systemer lovforslaget omhandler.
Lægeforeningens svar bygger på en forventning om, at loven ikke medfører administrative eller økonomiske byrder for vores medlemmer.
Lægeforeningen lægger vægt på at undgå en dobbeltrolle for Sundhedsdatastyrelsen og imødeser, at en anden myndighed tillægges opgaven med at føre tilsyn.

Lægeforeningen har lagt til grund for dette høringssvar, at vores medlemmer ikke bliver pålagt nye administrative eller økonomiske byrder som følge af loven, hverken direkte fx ved at medlemmer skal indberette oplysninger til de centrale myndigheder, de ikke indberetter i dag, eller indirekte ved at enkeltmedlemmers it-operatører skal indberette oplysninger de ikke indberetter i dag til de centrale myndigheder.

Lægeforeningen finder det uklart, hvilke systemer loven omfatter og efterlyser eksempler på konkrete systemer inden for de tre kategorier opregnet i bemærkningerne til § 1, der er omfattet af lovforslaget hhv. ikke er omfattet. En sådan oversigt kunne angive eksempler og give en bedre forståelse af omfanget af loven. Vi finder det hensigtsmæssigt, at systemkategorierne uddybes i den kommende bekendtgørelse til loven. Endvidere er begrebet "operatør", der anvendes i lovforslaget, ikke nærmere defineret.

Endelig finder vi det betænkeligt, at Sundhedsdatastyrelsen, der driver mange af sundhedsvæsenets it-systemer, kunne risikere at skulle have en dobbeltrolle og både skal være ansvarlig for systemernes sikkerhed (som operatør) og skal føre tilsyn med systemernes sikkerhed. Tilsynet med sikkerheden af Sundhedsdatastyrelsens systemer bør således ligge hos en anden myndighed, eksempelvis Datatilsynet eller Digitaliseringsstyrelsen.

Med venlig hilsen

Andreas Rudkjøbing
Formand for Lægeforeningen

Sundhedspolitik & Koordinering

Jr. 2017-7927
Den 14. november 2017

Domus Medica
Kristianiagade 12
2100 København Ø

Tlf.: 3544 8500
E-post: dadl@dadl.dk
www.laeger.dk

Regionshuset
Viborg

Regionssekretariatet
Skottenborg 26
Postboks 21
DK-8800 Viborg
Tel. +45 7841 0000
kontakt@rm.dk
www.rm.dk

Region Midtjylland bemærkninger til udkast til forslag til lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren

Dato 14-11-2017
Sagsbehandler Tina Leutholtz
TINLEU@rm.dk
Tel. +4520330891
Sagsnr. 1-10-70-102-17

Region Midtjylland har fra Sundheds- og Ældreministeriet modtaget anmodning om bemærkninger til ovenstående lovforslag.

Regionen er opmærksom på, at lovforslaget er en udmøntning af NIS-direktivet.

Indledningsvis bemærkes, at regionen finder lovudkastet svært læseligt. Et konkret eksempel herpå er, at lovforslaget anvender begreber, som ikke forklares i bemærkningerne, f.eks. *operatører* af væsentlige tjenester (overskrift i lovforslagets kapitel 2) og *udbydere* af digitale tjenester (§ 4, stk. 3). Regionen savner, at bemærkningerne indeholder et afsnit, som nærmere forklarer og definerer begreberne. Det ville være ønskeligt, om man i den forbindelse kobler til Databeskyttelsesforordningen.

Regionen savner en begrundelse for, at Sundhedsdatastyrelsen skal fungere som tilsynsmyndighed på området. I dag fungerer Datatilsynet og Rigsrevisionen som tilsynsmyndigheder på området, med lidt forskellige fokusområder. Vi ser gerne, at bemærkningerne forholder sig til, hvorfor man introducerer endnu en tilsynsmyndighed på området.

Afslutningsvis undrer regionen sig over, at lovforslaget i § 8, stk. 2 endnu ikke er medtaget. Vi forventer, at udkastet til bestemmelsen skal lægge sig om af Databeskyttelsesloven, idet grundlaget for sanktioner vel er det samme her?

/ 14.11.2017
MGW og TLE

Region Syddanmark

Afdeling: Informationssikkerhed

Journal nr.: 46/775

Dato: 15. november 2017

Udarbejdet af: Morten Kjeldgaard og Troels Hjortebjerg Pedersen
E-mail: Morten.Kjeldgaard@rsyd.dk / Troels.hjortebjerg.pedersen@rsyd.dk
Telefon: 2046 0747 / 4022 0253

Att.: Sundheds- og Ældreministeriet
Høringssvar fra Region Syddanmark

Vedr. høring over udkast til forslag til lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren

Generelle bemærkninger:
Region Syddanmark vurderer, at der i udformningen af lovforslaget er flere steder med sammenfald eller tæt på enslydende indhold sammenlignet med Persondataforordningen (GDPR) omkring informationssikkerhedsbrud.

Det er Region Syddanmarks antagelse, at for de it-systemer, hvor man ifølge lovforslaget får rollen som operatør, vil regionen i praksis skulle rapportere, dokumentere mv. for det samme system til to forskellige myndigheder. Det være sig Datatilsynet og Sundhedsdatastyrelsen. *Region Syddanmark vurderer dette som værende uhensigtsmæssigt.*

Det bør præciseres, om de generelle krav GDPR stiller til rapportering mv. til Datatilsynet, på de områder som er omfattet af nærværende lovforslag, hermed overgår til Sundhedsdatastyrelsen, eller om der vil være krav om parallel rapportering mv. til to myndigheder.

Såfremt man ønsker, at der skal være parallel rapportering og dokumentation, er det væsentligt at dette udføres på en måde, hvor form og indhold følger den samme struktur. Det gælder særligt for nedenstående forhold.

Krav til dokumentation og tilsyn:
Af lovforslaget fremgår, at Sundhedsdatastyrelsen kan efterspørge dokumentation mv. for de i Region Syddanmark udarbejdede sikkerhedspolitikker på området[1].
Region Syddanmark antager, at den dokumentation som kan forlanges udleveret, vil være at betragte som enslydende med dokumentationskravene fra GDPR i både form og indhold.
Region Syddanmark anfører, at det vil være uhensigtsmæssigt, såfremt der vil blive stillet krav til forskellige måder at dokumentere og rapportere på inden for samme område.

Væsentlige hændelser:
Af lovforslaget fremgår, at operatører skal underrette Sundhedsdatastyrelsen om hændelser, der har væsentlige konsekvenser for kontinuiteten af tjenester[2].
Region Syddanmark antager, at "væsentlige hændelser" vil blive defineret på samme måde nationalt. Og dermed være enslydende for alle myndigheder som arbejder med området.

[1] § 6., stk. 1.-4.
[2] § 4., stk. 1.

Region Syddanmark anfører, at såfremt definition af ”væsentlige hændelser” og beslægtede begreber ikke sker på nationalt niveau, vil der være risiko for forskellige krav til rapportering af væsentlige hændelser, alt efter den myndighed der skal rapporteres til. Herunder rapportering af væsentlige hændelser i det samme it-system.
Efter Region Syddanmarks opfattelse vil dette være uhensigtsmæssigt.