Transport-, Bygnings- og Boligministeriet

DEPARTEMENTET

Komiténotat

Dato 29. april 2019
J. nr. 2019-1359

Transport, Bygnings- og Boligministeriet
Frederiksholms Kanal 27 F
1220 København K

Telefon 41 71 27 00
trm@trm.dk
www.trm.dk

Bank Danske Bank
reg. 0216 kt. 4069 065880
EAN 5798000893429
CVR 43265717

Kommissionens forslag til ændring af gennemførelsesforordning (EU) nr. 2015/1998 om detaljerede foranstaltninger til gennemførelse af de fælles grundlæggende normer for luftfarssikkerhed

1. Resumé

Europa-Kommissionen sendte den 12. februar 2019 et forslag til ændring af gennemførelsesforordning (EU) nr. 2015/1998 om detaljerede foranstaltninger til gennemførelse af de fælles grundlæggende normer for luftfartssikkerhed i høring.

Forslaget indfører som noget nyt regulering vedrørende cybersecurity i gennemførelsesforordningen. Forslaget indebærer, at lufthavne, operatører og enheder skal identificere deres kritiske informations- og kommunikationsteknologisystemer samt data vedrørende civil luftfart. Herefter skal lufthavne, operatører og enheder træffe sikkerhedsforanstaltninger til beskyttelse af sådanne systemer og data mod cyberangreb, der kan udgøre en trussel mod den civile luftfart. Sikkerhedsforanstaltningerne skal bestemmes ud fra en risikovurdering, som lufthavnene, operatørerne og enhederne udarbejder. Hvilke luftfartsenheder, der forpligtes af de foreslåede cyberregler, skal defineres af Trafik-, Bygge- og Boligstyrelsen i det nationale sikkerhedsprogram for civil luftfart.

Forslaget har til formål at sikre en fælles europæisk implementering af de nye cyberrelaterede bestemmelser i ICAO's Annex 17 blandt medlemsstaterne i EU.

Der er på nuværende tidspunkt ikke foretaget en analyse af de økonomiske konsekvenser af forslaget, men et øget kontrolkrav som følge af forslaget kan medføre statsfinansielle konsekvenser i form af afledte nationale udgifter såvel som øgede udgifter for de virksomheder, der pålægges øgede opgaver og tiltag. De eventuelle økonomiske konsekvenser af forslaget vil også afhænge af, hvilke og hvor mange luftfartsenheder, der i det nationale sikkerhedsprogram for civil luftfart, vil blive defineret som værende forpligtet til at iværksætte cybersikkerhedsforanstaltninger.

Forslaget forventes at blive sat til afstemning i AVSEC-komitéen på det kommende møde den 12. juni 2019.

Forslaget er direkte gældende i dansk ret og skal således ikke efterfølgende implementeres.

En vedtagelse af forslaget skønnes at medvirke til at sikre, at det høje beskyttelsesniveau i Danmark inden for den civile luftfart i Danmark også fremadrettet vil ligge på et højt niveau.

Regeringen agter at støtte forslaget.

2. Baggrund

Europa-Kommissionen har den 12. februar 2019 sendt et forslag til ændring af gennemførelsesforordning 2015/1998 om detaljerede foranstaltninger til gennemførelse af de fælles grundlæggende normer for luftfartssikkerhed i høring.

Forordningsforslaget er fremsat med hjemmel i Europa-Parlamentets og Rådets forordning (EF) Nr. 300/2008 om fælles bestemmelser om sikkerhed inden for civil luftfart og om ophævelse af forordning (EF) nr. 2320/2002.

Forslaget behandles efter undersøgelsesproceduren, jf. artikel 5 i Europa-Parlamentets og Rådets forordning (EU) Nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser.

Hvis udvalget (AVSEC-komitéen) afgiver en positiv udtalelse, vedtager Kommissionen forslaget. Hvis udvalget afgiver en negativ udtalelse, eller hvis udvalget ikke afgiver en udtalelse, vedtager Kommissionen ikke forslaget – alternativt kan formanden dog enten forelægge en ændret udgave af udkastet for det samme udvalg inden for to måneder efter afstemningen eller forelægge udkastet for appeludvalget til yderligere drøftelse inden for en måned efter afstemningen. Appeludvalget er et komitologiudvalg, som består af medlemsstaternes repræsentanter, men med en højere grad af repræsentation. Det har Kommissionen i formandssædet. Kommissionen kan forelægge en sag for appeludvalget, hvis det ikke har været muligt at gennemføre en foreslået gennemførelsesretsakt, fordi udvalget/AVSEC-komitéen har stemt imod.

Forslaget forventes at blive sat til afstemning i AVSEC-Komitéen på det kommende møde den 12. juni 2019.

Efter gældende ret er det et krav, at samtlige luftfartsenheder skal udarbejde en sikkerhedsplan, der skal godkendes af Trafik-, Bygge- og Boligstyrelsen. Det nye i forslaget består derfor i, at de enheder, som er defineret i det nationale sikkerhedsprogram for civil luftfart, skal udarbejde en risikovurdering samt ændre sikkerhedsplanen i overensstemmelse med risikovurderingen. Både risikovurdering og ændringerne i sikkerhedsplanen skal godkendes af Trafik-, Bygge- og Boligstyrelsen.

En risikovurdering er en systematisk måde at identificere risici og sårbarheder på samt opstille passende sikkerhedsforanstaltninger til at imødegå de identificerede risici, således at sandsynlighed og konsekvens minimeres. Det er en omfattende og tidskrævende proces at udarbejde en risikovurdering, særligt for de enheder der ikke er trænet i eller er vant til at udarbejde dem.

Det er et krav i det danske nationale sikkerhedsprogram for civil luftfart, at lufthavne skal udarbejde risikovurderinger med henblik på at bestemme omfanget af overvågnings- og patruljeringsaktiviteter. Det er også et krav, at de lufthavne, der anvender demarkerede områder, godkendes hertil på baggrund af en risikovurdering. Endelig er det et krav, at byggeprojekter på lufthavnens område godkendes på baggrund af en risikovurdering. I enkelte tilfælde stilles der desuden krav om, at luftfartsselskaber skal udarbejde risikovurderinger, navnlig i tilfælde af opstilling af check-in-pulte uden for lufthavnens område samt ved undtagelse om kravet om rescreening af indskrevet bagage, der er blevet til uledsaget bagage.

Udarbejdelse af risikovurderinger vil således være en ny øvelse for størstedelen af de luftfartsenheder, der berøres af forslaget, hvis det vedtages, idet det i praksis stort set kun er lufthavne, der arbejder med risikovurderinger i dag.

3. Formål og indhold

Formålet med ændringerne i gennemførelsesforordningen er at tilvejebringe grundlaget for en ensartet fortolkning blandt EU-medlemsstaterne af cybersecuritybestemmelserne i Annex 17 til Chicago-konventionen angående international civil luftfart, der trådte i kraft den 16. november 2018. Det bemærkes i den forbindelse, at forslaget efter seneste revision læner sig meget op ad ordlyden i Annex 17-bestemmelserne.

En forskel er imidlertid, at Annex 17 fastlægger krav om, at de enheder, der skal iværksætte cybersikkerhedsforanstaltninger, skal defineres i det nationale sikkerhedsprogram for civil luftfart eller i "anden relevant national dokumentation". Denne formulering i Annex 17 er hidtil fortolket således, at NIS-direktivets implementering i dansk ret inden for transportsektoren ved lov nr. 441 af 8. maj 2018 om sikkerhed i net- og informationssystemer i transportsektoren samt bekendtgørelse nr. 1042 af 6. august 2018 om sikkerhed i net- og informationssystemer i transportsektoren, sikrer efterlevelse af ICAO-standarden i Annex 17. Denne tolkning lader til at være i overensstemmelse med introduktionen til standarden i Annex 17, som fastslår, at bestemmelsen åbner op for en fleksibel national implementering af et cybersecurity-setup. Formuleringen er imidlertid fjernet i EU-Kommissionens forslag, således at de forpligtede luftfartsenheder skal defineres i det nationale sikkerhedsprogram for civil luftfart, og det betyder, at kredsen af forpligtede enheder er bredere end NIS-operatørerne.

Ifølge forslaget skal den kompetente myndighed fastsætte og implementere procedurer for deling af relevante oplysninger til andre myndigheder og luftfartsenheder med henblik på at støtte disse i at udføre effektive risikovurderinger inden for deres respektive områder.

Herudover skal den kompetente myndighed sikre, at lufthavne, operatører og enheder, som er defineret i det nationale sikkerhedsprogram for civil luftfart, identificerer og beskytter deres kritiske informations- og kommunikationsteknologisystemer samt data vedrørende civil luftfart.

Ifølge forslaget skal de ovenfor nævnte lufthavne, operatører og enheder i deres sikkerhedsplaner identificere deres kritiske informations- og kommunikationsteknologisystemer samt data vedrørende civil luftfart. Sikkerhedsplanen skal indeholde en detaljeret beskrivelse af sikkerhedsforanstaltninger af beskyttende, detekterende, responderende og genoprettende karakter i forbindelse med cyberangreb, som kan true den civile luftfart.

Sikkerhedsforanstaltningerne, der skal beskytte systemerne mod ulovlige handlinger, skal identificeres, udvikles og implementeres på baggrund af en risikovurdering, som udarbejdes af lufthavnen, operatøren eller enheden.

Ifølge forslaget kan en specifik myndighed, som er kompetent i relation til cybertrusler, udpeges som kompetent for så vidt angår koordineringen og monitoreringen af de foreslåede cyberrelaterede bestemmelser.

Forslaget indfører mulighed for, at den kompetente myndighed eller den myndighed, der er udpeget som kompetent for så vidt angår koordinering og monitorering jf. ovenfor, kan stille krav om, at personer, der spiller en rolle i forbindelse med kritisk informations- og kommunikationsteknologisystemer, skal have gennemgået en baggrundskontrol med tilfredsstillende resultat.

Pr. 31. december 2020 stilles der krav om, at personer, der i medfør af det nationale sikkerhedsprogram har administratorrettigheder til eller har uledsaget adgang til kritisk informations- og kommunikationsteknologisystemer samt data vedrørende civil luftfart, skal have gennemgået en udvidet eller standard baggrundskontrol med et tilfredsstillende resultat.

Ifølge forslaget skal personer, der implementerer sikkerhedsforanstaltninger i de berørte enheders sikkerhedsplaner, besidde de for jobbet nødvendige evner og færdigheder. Personale og eksterne entreprenører skal gøres opmærksom på relevante cyberrisici på behørig vis.

Herudover skal personer, der har adgang til data eller systemer, modtage passende og specifik uddannelse, der svarer til deres rolle og ansvar, herunder blive gjort opmærksom på cyberrisici, når deres funktion kræver det. Den kompetente myndighed skal specificere og godkende uddannelsen.

4. Europaparlamentets udtalelser

Europa-Parlamentet skal ikke høres.

5. Nærhedsprincippet

Der er tale om en gennemførelsesforordning til en allerede vedtagen retsakt. Det er derfor regeringens vurdering, at det følger heraf, at forslaget er i overensstemmelse med nærhedsprincippet.

6. Gældende dansk ret

Gennemførelsesforordninger er direkte gældende i dansk ret.

7. Konsekvenser

Lovgivningsmæssige konsekvenser

Gennemførelsesforordningen har direkte juridisk virkning og ændringerne hertil skal derfor ikke implementeres i dansk lovgivning.

Økonomiske konsekvenser

Statsfinansielle konsekvenser

Der er på nuværende tidspunkt ikke foretaget en analyse af de statsfinansielle konsekvenser af forslaget, men det må forventes, at forordningsforslaget vil nødvendiggøre et øget godkendelses- og ressourceforbrug for de berørte myndigheder som følge af et øget kontrolkrav. Forslaget kan således indebære økonomiske konsekvenser i form af afledte nationale udgifter. Omfanget heraf vil afhænge af, hvor vidtgående en rolle, myndighederne forventes at spille samt hvor mange luftfartsenheder, der vil blive forpligtet til at iværksætte cybersikkerhedsforanstaltninger.

Samfundsøkonomiske konsekvenser

Forslaget vurderes at ville påføre de berørte myndigheder ekstra opgaver, jf. ovenfor, og vil påføre de berørte virksomheder, der pålægges ekstra opgaver og tiltag ekstra omkostninger, jf. nedenfor, således at forslaget samlet må forventes at have negative samfundsøkonomiske konsekvenser. Det kan på det foreliggende grundlag ikke opgøres hvor store.

Erhvervsøkonomiske konsekvenser

Forslaget forventes at påføre de virksomheder, der pålægges ekstra opgaver og tiltag ekstra omkostninger forbundet hermed. Det er på nuværende tidspunkt

ikke muligt at opgøre det samlede omfang, da det vil afhænge af, hvilke aktører inden for luftfarten, der ender med at blive omfattet af forordningen.

Andre konsekvenser og beskyttelsesniveauet

En vedtagelse af forslaget skønnes at medvirke til at sikre, at det høje beskyttelsesniveau i Danmark inden for den civile luftfart i Danmark også fremadrettet vil ligge på et højt niveau. Det er ikke muligt at vurdere, i hvilket omfang forslaget isoleret set medvirker til at øge beskyttelsesniveauet i de berørte virksomheder over for det øgede antal cybertrusler.

En vedtagelse af forslaget skønnes ikke at berøre beskyttelsesniveauet i Danmark for så vidt angår miljø, sundhed og forbrugerbeskyttelse. Det samme gør sig gældende, hvis forslaget ikke vedtages.

Regeringen finder, at operatører af væsentlige transporttjenester inden for området for civil luftfart (de såkaldte NIS-operatører), som er udpeget hertil af Trafik- Bygge- og Boligstyrelsen, allerede pr. definition efterlever formålet med reglerne i forslaget, i det omfang de opfylder kravene i den danske implementering af EU-direktiv 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet).

Disse operatører er allerede forpligtet til at træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger til at styre risiciene for sikkerheden i net- og informationssystemer, som de anvender til den del af deres aktiviteter, hvor en hændelse vil få væsentlige forstyrrende virkninger for leveringen af den nævnte transporttjeneste. Ligeledes skal operatører af væsentlige transporttjenester træffe passende foranstaltninger for at minimere konsekvensen af en hændelse, der kan have negativ indvirkning på de net- og informationssystemer, som anvendes til leveringen af en væsentlig transporttjeneste.

Disse passende foranstaltninger sikres i transportsektoren ved, at operatøren af en væsentlig transporttjeneste opnår akkrediteret certificering i overensstemmelse med en internationalt anerkendt standard for styring af sikkerheden i net- og informationssystemer, for eksempel DS/EN ISO/IEC 27001 eller tilsvarende.

8. Høring

Forslaget er sendt i høring i EU-specialudvalget for Transport, Bygning og Bolig den 22. februar 2019 med frist den 28. februar 2019. Der er ikke modtaget høringssvar.

Forslaget er sendt i høring hos de større danske lufthavne, de danske luftfartsselskaber samt de danske fragtagenter, der udfører screening, den 27. februar med frist den 5. marts. Der er ikke modtaget høringssvar.

9. Generelle forventninger til andre landes holdninger

Det er forventningen, at størstedelen af medlemsstaterne vil stemme for forslaget.

10. Regeringens foreløbige generelle holdning

Regeringen støtter grundlæggende EU-Kommissionens ønske om at styrke den civile luftfart mod cybertrusler.

Regeringen agter at støtte forslaget.

11. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt for Folketingets Europaudvalg.