KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2019/1583

af 25. september 2019

om ændring af gennemførelsesforordning (EU) 2015/1998 af om detaljerede foranstaltninger til gennemførelse af de fælles grundlæggende normer for luftfartssikkerhed for så vidt angår cybersikkerhedsforanstaltninger

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 af 11. marts 2008 om fælles bestemmelser om sikkerhed (security) inden for civil luftfart og om ophævelse af forordning (EF) nr. 2320/2002 ([1]), særlig artikel 1 og artikel 4, stk. 3, og

ud fra følgende betragtninger:

(1) Et af de vigtigste formål med forordning (EF) nr. 300/2008 er at tilvejebringe grundlaget for en ensartet fortolkning af bilag 17 (sikkerhedsbilaget) til konventionen angående international civil luftfart ([2]) af 7. december 1944, 10 udgave, 2017, som alle EU-medlemsstaterne har undertegnet.

(2) Midlerne til at nå målene er a) fastsættelse af fælles bestemmelser og fælles grundlæggende normer for luftfartssikkerhed og b) mekanismer til overvågning af overholdelse.

(3) Formålet med at ændre gennemførelsesbestemmelserne er at støtte medlemsstaterne i at sikre fuld overholdelse af den seneste ændring (ændring nr. 16) til bilag 17 til konventionen angående international civil luftfart, hvorved der i kapitel 3.1.4 er indført nye normer vedrørende nationale organisationer og den kompetente myndighed og i kapitel 4.9.1 nye normer vedrørende forebyggende cybersikkerhedsforanstaltninger.

(4) Ved at gennemføre disse normer i de EU-dækkende gennemførelsesbestemmelser på luftfartssikkerhedsområdet sikres det, at de kompetente myndigheder fastlægger og gennemfører procedurer for, når det er relevant, på praktisk vis og rettidigt at udveksle relevante oplysninger med henblik på at bistå de øvrige nationale myndigheder og organer, lufthavnsoperatører, luftfartsselskaber og andre berørte enheder med at gennemføre effektive sikkerhedsrisikovurderinger relateret til deres aktiviteter og på den måde støtte disse enheder i at gennemføre effektive sikkerhedsrisikovurderinger relateret til andre områder, som f.eks. cybersikkerhed, og gennemføre foranstaltninger til imødegåelse af cybertrusler.

(5) I Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet), fastsættes der foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i Unionen ([3]) med det formål at forbedre det indre markeds funktion. De foranstaltninger, der følger af NIS-direktivet og denne forordning, bør koordineres på nationalt plan for at undgå huller og overlappende forpligtelser.

(6) Kommissionens gennemførelsesforordning (EU) 2015/1998 ([4]) bør derfor ændres.

(7) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra Komitéen for Civil Luftfartssikkerhed, der er nedsat ved artikel 19, stk. 1, i forordning (EF) nr. 300/2008 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Bilaget til gennemførelsesforordning (EU) 2015/1998 ændres som angivet i bilaget til nærværende forordning.

([1]) EUT L 97 af 9.4.2008, s. 72.
([2]) https://icao.int/publications/pages/doc7300.aspx.
([3]) 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 (EUT L 194 af 19.7.2016, s. 1).
([4]) Kommissionens gennemførelsesforordning (EU) 2015/1998 af 5. november 2015 om detaljerede foranstaltninger til gennemførelse af de fælles grundlæggende normer for luftfartssikkerhed (EUT L 299 af 14.11.2015, s. 1).

Artikel 2

Denne forordning træder i kraft den 31. december 2020.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 25. september 2019.

På Kommissionens vegne

Jean-Claude JUNCKER

Formand

BILAG

I bilaget til gennemførelsesforordning (EU) 2015/1998 foretages følgende ændringer:

1) Som punkt 1.0.6 tilføjes:

»1.0.6. Den kompetente myndighed fastlægger og gennemfører procedurer med henblik på, når det er relevant, på praktisk vis og rettidigt at udveksle relevante oplysninger for at bistå andre nationale myndigheder og organer, lufthavnsoperatører, luftfartsselskaber og andre berørte enheder med gennemførelsen af effektive sikkerhedsrisikovurderinger relateret til deres aktiviteter.«

2) Som punkt 1.7 tilføjes:

»1.7. IDENTIFIKATION OG BESKYTTELSE AF KRITISKE INFORMATIONS- OG KOMMUNIKATIONSTEKNOLOGISYSTEMER OG DATA I DEN CIVILE LUFTFART MOD CYBERTRUSLER

1.7.1. Den kompetente myndighed sikrer, at lufthavnsoperatører, luftfartsselskaber og enheder som defineret i det nationale sikkerhedsprogram for civil luftfart identificerer og beskytter deres kritiske informations- og kommunikationsteknologisystemer og data mod cyberangreb, som kan påvirke den civile luftfartssikkerhed.

1.7.2. Lufthavnsoperatører, luftfartsselskaber og enheder identificerer i deres sikkerhedsprogram eller ethvert relevant dokument, som der krydshenvises til i sikkerhedsprogrammet, de kritiske informations- og kommunikationsteknologisystemer og data, der er omhandlet i punkt 1.7.1.

Sikkerhedsprogrammet, eller ethvert relevant dokument, som der krydshenvises til i sikkerhedsprogrammet, skal indeholde en detaljeret beskrivelse af de foranstaltninger, som skal sikre beskyttelse mod, detektion af, reaktion på og genopretning efter cyberangreb som omhandlet i punkt 1.7.1.

1.7.3. De detaljerede foranstaltninger til beskyttelse af sådanne systemer og data mod ulovlige indgreb bestemmes, udarbejdes og gennemføres i overensstemmelse med en risikovurdering foretaget af lufthavnsoperatøren, luftfartsselskabet eller enheden, alt efter omstændighederne.

1.7.4. Hvis en bestemt myndighed eller et bestemt organ er kompetent med hensyn til foranstaltninger mod cybertrusler i en enkelt medlemsstat, kan myndigheden eller organet udpeges som kompetent med hensyn til koordinering og/eller overvågning af de cyberrelaterede bestemmelser i denne forordning.

1.7.5. Hvis lufthavnsoperatører, luftfartsselskaber og enheder som defineret i det nationale sikkerhedsprogram for civil luftfart er omfattet af særskilte cybersikkerhedskrav, der følger af anden EU-lovgivning eller national lovgivning, kan den kompetente myndighed erstatte overholdelse af kravene i nærværende forordning med overholdelse af de krav, der følger af nævnte anden EU-lovgivning eller national lovgivning. Den kompetente myndighed koordinerer med eventuelle andre relevante kompetente myndigheder for at sikre koordinerede eller kompatible tilsynsordninger.«

3) Punkt 11.1.2 affattes således:

»11.1.2 Følgende personale have gennemgået en udvidet eller en standard baggrundskontrol med et tilfredsstillende resultat:

a) personer, som ansættes til at gennemføre eller være ansvarlige for at gennemføre screening, adgangskontrol eller anden sikkerhedskontrol andre steder end i et security-beskyttet område

b) personer, der har uledsaget adgang til luftfragt og luftpost, luftfartsselskabers post og materialer, forsyninger til flyvningen og lufthavnsleverancer, som den krævede sikkerhedskontrol er gennemført for

c) personer med administratorrettigheder eller uovervåget og ubegrænset adgang til kritiske informations- og kommunikationsteknologisystemer og data, der anvendes til civile luftfartssikkerhedsformål som omhandlet i punkt 1.7.1. i overensstemmelse med det nationale sikkerhedsprogram for civil luftfart, eller som på anden måde er blevet identificeret i risikovurderingen i overensstemmelse med punkt 1.7.3.

Medmindre andet fremgår af denne forordning, fastsætter den kompetente myndighed i overensstemmelse med de gældende nationale regler, hvorvidt der gennemføres en udvidet eller en standard baggrundskontrol.«

4) Som punkt 11.2.8 tilføjes:

»11.2.8. Uddannelse af personer, der spiller en rolle, eller som har ansvar i forbindelse med cybertrusler

11.2.8.1. Personer, der gennemfører de foranstaltninger, der er omhandlet i punkt 1.7.2, skal have de færdigheder og evner, der kræves for at udføre de opgaver, de har fået pålagt, effektivt. De skal gøres opmærksomme på relevante cyberrisici efter need to know-princippet.

11.2.8.2. Personer, der har adgang til data eller systemer, skal modtage passende og specifik jobrelateret uddannelse, der står i et rimeligt forhold til deres rolle og ansvar, og de skal gøres opmærksomme på relevante risici, hvis deres jobfunktion kræver det. Den kompetente myndighed eller den myndighed eller det organ, der er omhandlet i punkt 1.7.4, specificerer eller godkender indholdet af kurset.«