KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2019/1583

av den 25 september 2019

om ändring av genomförandeförordning (EU) 2015/1998 om detaljerade bestämmelser för genomförande av de gemensamma grundläggande standarderna avseende luftfartsskydd, vad gäller cybersäkerhetsåtgärder

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 ([1]), särskilt artiklarna 1 och 4.3, och

av följande skäl:

(1) Ett av huvudsyftena med förordning (EG) nr 300/2008 är att ge en grund för en gemensam tolkning av bilaga 17 (säkerhetsbilagan) till konventionen angående internationell civil luftfart ([2]) av den 7 december 1944, tionde upplagan, 2017, som är undertecknad av alla EU-medlemsstater.

(2) Dessa syften ska uppnås genom a) fastställande av gemensamma regler och gemensamma grundläggande standarder för luftfartsskydd, och b) mekanismer för övervakning av att reglerna efterlevs.

(3) Syftet med att ändra genomförandelagstiftningen är att stödja medlemsstaterna i säkerställandet av full efterlevnad av den senaste ändringen (ändring 16) av bilaga 17 till konventionen angående internationell civil luftfart, där det i kapitel 3.1.4 infördes nya standarder med avseende på nationell organisation och berörd myndighet, och i kapitel 4.9.1 nya standarder med avseende på förebyggande cybersäkerhetsåtgärder.

(4) Ett införlivande av dessa standarder med EU-omfattande genomförandelagstiftning om luftfartsskydd säkerställer att berörda myndigheter fastställer och genomför förfaranden för att i rätt tid och på ett lämpligt och praktiskt sätt kunna utbyta relevant information för att bistå andra nationella myndigheter och organ, flygplatsoperatörer, lufttrafikföretag och andra berörda verksamhetsutövare, så att de kan utföra effektiva säkerhetsriskbedömningar i sin verksamhet, och på så sätt stödja dessa enheter i utförandet av effektiva säkerhetsriskbedömningar avseende bl.a. cybersäkerhet och i genomförandet av åtgärder mot cyberhot.

(5) Europaparlamentets och rådets direktiv (EU) 2016/1148 ([3]) omfattar åtgärder för att uppnå en hög gemensam nivå av säkerhet i nätverks- och informationssystem i unionen och på så sätt bidra till en fungerande inre marknad. Åtgärderna enligt det direktivet och åtgärderna enligt denna förordning bör samordnas på nationell nivå så att luckor och överlappningar av skyldigheter undviks.

(6) Kommissionens genomförandeförordning (EU) 2015/1998 ([4]) bör därför ändras i enlighet med detta.

(7) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté för luftfartsskyddet inom den civila luftfarten som inrättats enligt artikel 19.1 i förordning (EG) nr 300/2008.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Bilagan till genomförandeförordning (EU) 2015/1998 ska ändras i enlighet med bilagan till denna förordning.

([1]) EUT L 97, 9.4.2008, s. 72.
([2]) https://icao.int/publications/pages/doc7300.aspx
([3]) Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).
([4]) Kommissionens genomförandeförordning (EU) 2015/1998 av den 5 november 2015 om detaljerade bestämmelser för genomförande av de gemensamma grundläggande standarderna avseende luftfartsskydd (EUT L 299, 14.11.2015, s. 1).

Artikel 2

Denna förordning träder i kraft den 31 december 2020.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 25 september 2019.

På kommissionens vägnar
Violeta BULC
Ledamot av kommissionen

BILAGA

Bilagan till genomförandeförordning (EU) 2015/1998 ska ändras på följande sätt:

1. Följande punkt 1.0.6 ska läggas till:

"1.0.6 Den berörda myndigheten ska fastställa och genomföra förfaranden för att i rätt tid och på ett lämpligt och praktiskt sätt kunna utbyta relevant information för att bistå andra nationella myndigheter och organ, flygplatsoperatörer, lufttrafikföretag och andra berörda verksamhetsutövare, så att de kan utföra effektiva säkerhetsriskbedömningar i sin verksamhet."

2. Följande punkt 1.7 ska läggas till:

"1.7 IDENTIFIERING OCH SKYDD AV DEN CIVILA LUFTFARTENS KRITISKA INFORMATIONS- OCH KOMMUNIKATIONSTEKNIKSYSTEM OCH DATA MOT CYBERHOT

1.7.1 Den berörda myndigheten ska säkerställa att flygplatsoperatörer, lufttrafikföretag och verksamhetsutövare enligt definitionen i det nationella säkerhetsprogrammet för civil luftfart identifierar och skyddar sina kritiska informations- och kommunikationstekniksystem och data från cyberattacker som skulle kunna påverka skyddet av den civila luftfarten.

1.7.2 Flygplatsoperatörer, lufttrafikföretag och verksamhetsutövare ska i sina säkerhetsprogram, eller i relevanta dokument som det hänvisas till i säkerhetsprogrammet, identifiera de kritiska informations- och kommunikationstekniksystem och data som används för civil luftfart enligt beskrivningen i 1.7.1.

Säkerhetsprogrammet, eller de relevanta dokument som det hänvisas till i säkerhetsprogrammet, ska i detalj redogöra för åtgärderna för att säkerställa skydd, detektion, respons och återhämtning vid cyberattacker, enligt beskrivningen i 1.7.1.

1.7.3 De detaljerade åtgärderna för att skydda sådana system och data från olagliga handlingar ska identifieras, utvecklas och genomföras i enlighet med en riskbedömning som görs av flygplatsoperatören, lufttrafikföretaget eller verksamhetsutövaren, såsom lämpligt.

1.7.4 Om en specifik myndighet eller ett specifikt organ har behörighet när det gäller åtgärder som avser cyberhot i en enskild medlemsstat får denna myndighet eller detta organ utses som behörig enhet för samordningen och/eller övervakningen av de cyberrelaterade bestämmelserna i denna förordning.

1.7.5 Om flygplatsoperatörer, lufttrafikföretag och verksamhetsutövare enligt definitionen i det nationella säkerhetsprogrammet för civil luftfart omfattas av separata cybersäkerhetskrav som härrör från annan EU-lagstiftning eller nationell lagstiftning får den berörda myndigheten ersätta uppfyllandet av kraven i denna förordning med uppfyllandet av de krav som finns i den andra EU-lagstiftningen eller nationella lagstiftningen. Den berörda myndigheten ska samordna sitt arbete med eventuella andra berörda myndigheter för att säkerställa samordnade eller förenliga tillsynsordningar."

3. Punkt 11.1.2 ska ersättas med följande:

"11.1.2 Följande personal ska med tillfredsställande resultat ha genomgått en utökad säkerhetsprövning eller vanlig säkerhetsprövning:

a) Personer som rekryteras för att utföra, eller ansvara för genomförandet av, säkerhetskontroll, tillträdeskontroll eller andra säkerhetsåtgärder på annat område än på ett behörighetsområde.

b) Personer som har oeskorterad tillgång till flygfrakt och post, lufttrafikföretagens post och materiel, förnödenheter som används ombord och varuleveranser till flygplatser som varit föremål för de föreskrivna säkerhetsåtgärderna.

c) Personer vilka har administratörsrättigheter eller oövervakad och obegränsad åtkomst till kritiska informations- och kommunikationstekniksystem och data som används för det civila luftfartsskyddets syften enligt 1.7.1 i enlighet med det nationella säkerhetsprogrammet för civil luftfart, eller vilka på annat sätt identifierats i riskbedömningen enligt 1.7.3.

Om inte annat anges i denna förordning är det den behöriga myndigheten som, i enlighet med den gällande nationella lagstiftningen, bestämmer om den obligatoriska säkerhetsprövningen ska vara en utökad säkerhetsprövning eller en vanlig säkerhetsprövning."

4. Följande punkt 11.2.8 ska läggas till:

”11.2.8 Utbildning av personer med roller och ansvarsområden relaterade till cyberhot

11.2.8.1 Personer som genomför de åtgärder som anges i punkt 1.7.2 ska ha de färdigheter och kunskaper som krävs för att utföra dessa uppgifter på ett effektivt sätt. De ska få information om relevanta cyberrisker när de behöver denna information.

11.2.8.2 Personer som har tillgång till data eller system ska ges ändamålsenlig och specifik jobbrelaterad utbildning som står i proportion till deras roll och ansvar, inklusive information om relevanta risker när deras arbetsuppgifter så kräver. Den berörda myndigheten, eller den myndighet eller det organ som avses i punkt 1.7.4, ska specificera eller godkänna kursinnehållet.”