KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2019/1583

(2019. gada 25. septembris),

ar ko attiecībā uz kiberdrošības pasākumiem groza Īstenošanas regulu (ES) 2015/1998, ar ko nosaka sīki izstrādātus pasākumus kopīgu pamatstandartu īstenošanai aviācijas drošības jomā

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2008. gada 11. marta Regulu (EK) Nr. 300/2008 par kopīgiem noteikumiem civilās aviācijas drošības jomā un ar ko atceļ Regulu (EK) Nr. 2320/2002 ([1]), un jo īpaši tās 1. pantu un 4. panta 3. punktu,

tā kā:

(1) Viens no galvenajiem Regulas (EK) Nr. 300/2008 mērķiem ir nodrošināt pamatu, kas vajadzīgs, lai vienoti interpretētu 17. pielikumu (Drošības pielikums) 1944. gada 7. decembra Konvencijai par starptautisko civilo aviāciju ([2]) (10. redakcija, 2017. gads), kuru parakstījušas visas ES dalībvalstis.

(2) Mērķu sasniegšanas līdzekļi ir a) kopīgu noteikumu un kopīgu pamatstandartu noteikšana aviācijas drošības jomā un b) atbilstības uzraudzības mehānismi.

(3) Īstenošanas tiesību aktu grozīšanas mērķis ir palīdzēt dalībvalstīm nodrošināt pilnīgu atbilstību jaunākajiem Konvencijas par starptautisko civilo aviāciju 17. pielikuma grozījumiem (grozījums Nr. 16), ar ko tika ieviesti jauni standarti 3.1.4. nodaļā, kas attiecas uz valsts organizāciju un pilnvaroto iestādi, un 4.9.1. nodaļā, kas attiecas uz preventīviem kiberdrošības pasākumiem.

(4) Transponējot šos standartus ES mēroga aviācijas drošības tiesību aktu īstenošanā, tiks nodrošināts, ka pilnvarotās iestādes izstrādā un īsteno procedūras, lai vajadzības gadījumā praktiski un laikus apmainītos ar informāciju, kas nepieciešama, lai palīdzētu citām valsts iestādēm un aģentūrām, lidostu ekspluatantiem, gaisa pārvadātājiem un citām iesaistītajām struktūrām veikt efektīvus drošības riska novērtējumus attiecībā uz to darbībām, un tādā veidā palīdzētu šīm struktūrām veikt efektīvus drošības riska novērtējumus, kas saistīti cita starpā ar kiberdrošību, un īstenot pasākumus kiberdraudu novēršanai.

(5) Eiropas Parlamenta un Padomes Direktīvā (ES) 2016/1148 ([3]) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (TID direktīva) ir noteikti pasākumi, kuru mērķis ir panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību Savienībā, lai uzlabotu iekšējā tirgus darbību. Lai novērstu nepilnības un pienākumu dublēšanos, no TID direktīvas un šīs regulas izrietošie pasākumi būtu jākoordinē valstu līmenī.

(6) Tādēļ Padomes Īstenošanas regula (ES) 2015/1998 ([4]) būtu attiecīgi jāgroza.

(7) Šajā regulā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi ar Regulas (EK) Nr. 300/2008 19. panta 1. punktu izveidotā Civilās aviācijas drošības komiteja,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Īstenošanas regulas (ES) 2015/1998 pielikumu groza saskaņā ar šīs regulas pielikumu.

([1]) OV L 97, 9.4.2008., 72. lpp.
([2]) https://icao.int/publications/pages/doc7300.aspx
([3]) Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).
([4]) Padomes 2015. gada 5. novembra Īstenošanas regula (ES) 2015/1998, ar ko nosaka sīki izstrādātus pasākumus kopīgu pamatstandartu īstenošanai aviācijas drošības jomā (OV L 299, 14.11.2015., 1. lpp.).

2. pants

Šī regula stājas spēkā 2020. gada 31. decembrī.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2019. gada 25. septembrī

Komisijas vārdā –
priekšsēdētājs
Jean-Claude JUNCKER

PIELIKUMS

Īstenošanas regulas (ES) 2015/1998 pielikumu groza šādi:

1) pievieno šādu 1.0.6. punktu:

"1.0.6. Pilnvarotā iestāde izveido un īsteno procedūras, lai vajadzības gadījumā praktiski un laikus apmainītos ar attiecīgo informāciju, kas nepieciešama, lai palīdzētu citām valsts iestādēm un aģentūrām, lidostu ekspluatantiem, gaisa pārvadātājiem un citiem attiecīgiem tiesību subjektiem veikt efektīvus drošības riska novērtējumus attiecībā uz to darbībām.";

2) pievieno šādu 1.7. punktu:

"1.7. CIVILĀS AVIĀCIJAS KRITISKO INFORMĀCIJAS UN KOMUNIKĀCIJAS TEHNOLOĢIJU SISTĒMU UN DATU IDENTIFICĒŠANA UN AIZSARDZĪBA PRET KIBERDRAUDIEM

1.7.1. Pilnvarotā iestāde nodrošina, ka lidostu ekspluatanti, gaisa pārvadātāji un tiesību subjekti, kā definēts valsts civilās aviācijas drošības programmā, identificē un aizsargā savas kritiskās informācijas un komunikācijas tehnoloģiju sistēmas un datus pret kiberuzbrukumiem, kuri varētu ietekmēt civilās aviācijas drošību.

1.7.2. Lidostu ekspluatanti, gaisa pārvadātāji un tiesību subjekti savā drošības programmā vai jebkurā attiecīgā dokumentā, uz ko ir atsauce drošības programmā, identificē kritiskās informācijas un komunikācijas tehnoloģiju sistēmas un datus, kas aprakstīti 1.7.1. punktā.

Drošības programmā vai jebkurā attiecīgā dokumentā, uz ko ir atsauce drošības programmā, sīki izklāsta pasākumus, ar kuriem nodrošina aizsardzību pret kiberuzbrukumiem, kas aprakstīti 1.7.1. punktā, kā arī šādu kiberuzbrukumu atklāšanu, reaģēšanu uz tiem un atgūšanos no tiem.

1.7.3. Sīki izstrādātos pasākumus, ar kuriem aizsargā šādas sistēmas un datus no nelikumīgas iejaukšanās, identificē, izstrādā un īsteno saskaņā ar riska novērtējumu, ko veic attiecīgi lidostas ekspluatants, gaisa pārvadātājs vai tiesību subjekts.

1.7.4. Ja konkrētas iestādes vai aģentūras kompetencē ir pasākumi, kas saistīti ar kiberdraudiem vienā dalībvalstī, šo iestādi vai aģentūru var iecelt par kompetentu šajā regulā paredzēto ar kibertelpu saistīto noteikumu koordinācijai un/vai uzraudzībai.

1.7.5. Ja lidostu ekspluatantiem, gaisa pārvadātājiem un tiesību subjektiem, kas definēti valsts civilās aviācijas drošības programmā, piemēro atsevišķas kiberdrošības prasības, kas izriet no citiem ES vai valsts tiesību aktiem, pilnvarotā iestāde var aizstāt atbilstību šīs regulas prasībām ar atbilstību citu ES tiesību aktu vai valsts tiesību aktu elementiem. Pilnvarotā iestāde saskaņo darbību ar citām attiecīgajām kompetentajām iestādēm, lai nodrošinātu koordinētu vai saderīgu pārraudzības režīmu.";

3) pielikuma 11.1.2. punktu aizstāj ar šādu:

"11.1.2. Turpmāk minētais personāls ir sekmīgi izturējis uzlabotu vai standarta iepriekšējās darbības pārbaudi:

a) personas, ko pieņem darbā, lai tās īstenotu pārbaudes, piekļuves kontroli un citus drošības kontroles pasākumus vai atbildētu par drošības kontroli citur, nevis ierobežotas iekļuves drošības zonā;

b) personas, kam atļauts bez pavadības piekļūt gaisa kravai un pastam, gaisa pārvadātāja pastam un gaisa pārvadātāja materiāliem, lidojuma laikā patērējamiem krājumiem un lidostas krājumiem, kam veiktas vajadzīgās drošības kontroles;

c) personas, kurām ir administratora tiesības vai atļauja bez pavadības un neierobežoti piekļūt kritiskajām informācijas un komunikācijas tehnoloģiju sistēmām un datiem, ko izmanto civilās aviācijas drošībai, kā aprakstīts 1.7.1. punktā saskaņā ar valsts aviācijas drošības programmu, vai kuras ir citādi identificētas riska novērtējumā saskaņā ar 1.7.3. punktu.

Ja šajā regulā nav noteikts citādi, pilnvarotā iestāde saskaņā ar spēkā esošajiem valsts noteikumiem nosaka, vai persona jāpakļauj pastiprinātai vai parastai iepriekšējās darbības pārbaudei.";

4) pievieno šādu 11.2.8. punktu:

"11.2.8. To personu apmācība, kuru uzdevumi un atbildība saistīta ar kiberdraudiem

11.2.8.1. Personām, kas īsteno 1.7.2. punktā noteiktos pasākumus, ir prasmes un iemaņas, kas vajadzīgas, lai efektīvi pildītu savus uzdevumus. Tās informē par attiecīgiem kiberriskiem, pamatojoties uz vajadzību pēc informācijas.

11.2.8.2. Personas, kurām ir piekļuve datiem vai sistēmām, saņem atbilstošu un īpašu apmācību saistībā ar darbu, kas ir samērīga ar viņu lomu un pienākumiem, tostarp tiek informētas par attiecīgajiem riskiem, ja to prasa darba pienākumi. Pilnvarotā iestāde, vai iestāde vai aģentūra, kā noteikts 1.7.4. punktā, nosaka vai apstiprina kursa saturu."