II

(Neleģislatīvi akti)

REGULAS

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2023/203

(2022. gada 27. oktobris),

ar ko paredz Eiropas Parlamenta un Padomes Regulas (ES) 2018/1139 piemērošanas noteikumus saistībā ar prasībām, kas attiecas uz tādu informācijas drošības risku pārvaldību, kuri spēj ietekmēt aviācijas drošumu, un kas noteiktas organizācijām, uz kurām attiecas Komisijas Regulas (ES) Nr. 1321/2014, (ES) Nr. 965/2012, (ES) Nr. 1178/2011, (ES) 2015/340, Komisijas Īstenošanas regulas (ES) 2017/373 un (ES) 2021/664, un kompetentajām iestādēm, uz kurām attiecas Komisijas Regulas (ES) Nr. 748/2012, (ES) Nr. 1321/2014, (ES) Nr. 965/2012, (ES) Nr. 1178/2011, (ES) 2015/340 un (ES) Nr. 139/2014, Komisijas Īstenošanas regulas (ES) 2017/373 un (ES) 2021/664, un ar ko groza Komisijas Regulas (ES) Nr. 1178/2011, (ES) Nr. 748/2012, (ES) Nr. 965/2012, (ES) Nr. 139/2014, (ES) Nr. 1321/2014, (ES) 2015/340 un Komisijas Īstenošanas regulas (ES) 2017/373 un (ES) 2021/664

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2018/1139 (2018. gada 4. jūlijs) par kopīgiem noteikumiem civilās aviācijas jomā un ar ko izveido Eiropas Savienības Aviācijas drošības aģentūru, un ar ko groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 2111/2005, (EK) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 un Direktīvas 2014/30/ES un 2014/53/ES un atceļ Eiropas Parlamenta un Padomes Regulas (EK) Nr. 552/2004 un (EK) Nr. 216/2008 un Padomes Regulu (EEK) Nr. 3922/91 [1], un jo īpaši tās 17. panta 1. punkta b) apakšpunktu, 27. panta 1. punkta a) apakšpunktu, 31. panta 1. punkta b) apakšpunktu, 43. panta 1. punkta b) apakšpunktu, 53. panta 1. punkta a) apakšpunktu un 62. panta 15. punkta c) apakšpunktu,

tā kā:

(1) Saskaņā ar Regulas (ES) 2018/1139 II pielikuma 3.1. punkta b) apakšpunktā noteiktajām pamatprasībām lidojumderīguma uzturēšanas vadības organizācijām un tehniskās apkopes organizācijām ir jāievieš un jāuztur pārvaldības sistēma drošuma risku pārvaldībai.

(2) Turklāt saskaņā ar Regulas (ES) 2018/1139 IV pielikuma 3.3. punkta b) apakšpunktā un 5. punkta b) apakšpunktā noteiktajām pamatprasībām pilotu mācību organizācijām, salona apkalpes mācību organizācijām, aviācijas medicīnas centriem, kas paredzēti apkalpei, un lidojumu simulācijas trenažieru iekārtu operatoriem ir jāievieš un jāuztur pārvaldības sistēma drošuma risku pārvaldībai.

(3) Bez tam saskaņā ar Regulas (ES) 2018/1139 V pielikuma 8.1. punkta c) apakšpunktā noteiktajām pamatprasībām gaisa kuģu ekspluatantiem ir jāievieš un jāuztur pārvaldības sistēma drošuma risku pārvaldībai.

(4) Kā arī saskaņā ar Regulas (ES) 2018/1139 VIII pielikuma 5.1. punkta c) apakšpunktā un 5.4. punkta b) apakšpunktā noteiktajām pamatprasībām gaisa satiksmes pārvaldības un aeronavigācijas pakalpojumu sniedzējiem, "U-space" pakalpojumu sniedzējiem un vienotiem kopīgo informācijas pakalpojumu sniedzējiem, kā arī mācību organizācijām un aviācijas medicīnas centriem, kas paredzēti gaisa satiksmes vadības dispečeriem, ir jāievieš un jāuztur pārvaldības sistēma drošuma risku pārvaldībai.

[1] OV L 212, 22.8.2018. 1. lpp.

(5) Minētos drošuma riskus var izraisīt dažādi cēloņi, piemēram, konstrukcijas un tehniskās apkopes nepilnības, cilvēka darbības aspekti, vidiskie apdraudējumi un informācijas drošības apdraudējumi. Tāpēc Eiropas Savienības Aviācijas drošības aģentūras ("Aģentūra") un iepriekš norādītajos apsvērumos minēto valsts kompetento iestāžu un organizāciju ieviestajās pārvaldības sistēmās būtu jāņem vērā ne tikai drošuma riski, kuri izriet no nejaušiem notikumiem, bet arī drošuma riski, ko izraisa informācijas drošības apdraudējumi, ja pastāvošās nepilnības var izmantot indivīdi, kuru nolūki ir ļaunprātīgi. Šie informācijas drošības riski civilās aviācijas vidē pastāvīgi pieaug, jo aizvien vairāk un vairāk palielinās pašreizējo informācijas sistēmu savstarpējā savienotība un šīs sistēmas aizvien biežāk kļūst par ļaunprātīgu personu mērķi.

(6) Ar šīm informācijas sistēmām saistītie riski neaprobežojas tikai ar iespējamiem uzbrukumiem kibertelpai, bet ietver arī apdraudējumus, kas var ietekmēt procesus un procedūras, kā arī cilvēku darbību.

(7) Lai risinātu digitālās informācijas un datu drošības jautājumus, ievērojams skaits organizāciju jau izmanto starptautiskos standartus, piemēram, ISO 27001. Tomēr šajos standartos var nebūt pilnībā ņemtas vērā visas civilās aviācijas īpatnības. Tāpēc ir lietderīgi noteikt prasības tādu informācijas drošības risku pārvaldībai, kuri spēj ietekmēt aviācijas drošumu.

(8) Ir ļoti svarīgi, lai šīs prasības attiektos uz visām aviācijas jomām un to saskarnēm, jo aviācija ir savstarpēji ļoti cieši savienotu sistēmu sistēma. Tāpēc tās būtu jāpiemēro visām organizācijām un kompetentajām iestādēm, uz kurām attiecas Komisijas Regulām (ES) Nr. 748/2012 ([2]), (ES) Nr. 1321/2014 ([3]), (ES) Nr. 965/2012 ([4]), (ES) Nr. 1178/2011 ([5]), (ES) 2015/340 ([6]), (ES) Nr. 139/2014 ([7]) un Īstenošanas regula (ES) 2021/664 ([8]), kā arī tām organizācijām un kompetentajām iestādēm, kurām jau ir jābūt pārvaldības sistēmai saskaņā ar spēkā esošajiem Savienības tiesību aktiem aviācijas drošuma jomā. Tomēr dažas organizācijas būtu jāizslēdz no šīs regulas darbības jomas, lai nodrošinātu pienācīgu samērīgumu ar mazākiem informācijas drošības riskiem, ko tās rada aviācijas sistēmai.

(9) Šajā regulā noteiktajām prasībām būtu jānodrošina konsekventa īstenošana visās aviācijas jomās, vienlaikus minimāli ietekmējot Savienības aviācijas drošuma tiesību aktus, kas jau ir piemērojami minētajās jomās.

([2]) Komisijas Regula (ES) Nr. 748/2012 (2012. gada 3. augusts), ar ko paredz īstenošanas noteikumus par sertifikāciju attiecībā uz gaisa kuģu un ar tiem saistīto ražojumu, daļu un ierīču lidojumderīgumu un atbilstību vides aizsardzības prasībām, kā arī projektēšanas un ražošanas organizāciju sertifikāciju (OV L 224, 21.8.2012., 1. lpp.).

([3]) Komisijas Regula (ES) Nr. 1321/2014 (2014. gada 26. novembris) par gaisa kuģu un aeronavigācijas ražojumu, daļu un ierīču lidojumderīguma uzturēšanu un šo uzdevumu izpildē iesaistīto organizāciju un personāla apstiprināšanu (OV L 362, 17.12.2014., 1. lpp.).

([4]) Komisijas Regula (ES) Nr. 965/2012 (2012. gada 5. oktobris), ar ko nosaka tehniskās prasības un administratīvās procedūras saistībā ar gaisa kuģu ekspluatāciju atbilstīgi Eiropas Parlamenta un Padomes Regulai (EK) Nr. 216/2008 (OV L 296, 25.10.2012., 1. lpp.).

([5]) Komisijas Regula (ES) Nr. 1178/2011 (2011. gada 3. novembris), ar ko nosaka tehniskās prasības un administratīvās procedūras attiecībā uz civilās aviācijas gaisa kuģa apkalpi atbilstīgi Eiropas Parlamenta un Padomes Regulai (EK) Nr. 216/2008 (OV L 311, 25.11.2011., 1. lpp.).

([6]) Komisijas Regula (ES) 2015/340 (2015. gada 20. februāris), ar ko nosaka tehniskās prasības un administratīvās procedūras saistībā ar gaisa satiksmes vadības dispečeru licencēm un sertifikātiem atbilstīgi Eiropas Parlamenta un Padomes Regulai (EK) Nr. 216/2008, groza Komisijas Īstenošanas regulu (ES) Nr. 923/2012 un atceļ Komisijas Regulu (ES) Nr. 805/2011 (OV L 63, 6.3.2015., 1. lpp.).

([7]) Komisijas Regula (ES) Nr. 139/2014 (2014. gada 12. februāris), ar ko nosaka prasības un administratīvās procedūras saistībā ar lidlaukiem atbilstīgi Eiropas Parlamenta un Padomes Regulai (EK) Nr. 216/2008 (OV L 44, 14.2.2014., 1. lpp.).

([8]) Komisijas Īstenošanas regula (ES) 2021/664 (2021. gada 22. aprīlis) par "U-space" tiesisko regulējumu (OV L 139, 23.4.2021., 161. lpp.).

(10) Šajā regulā noteiktajām prasībām nebūtu jāskar informācijas drošības un kiberdrošības prasības, kas noteiktas Komisijas Īstenošanas regulas (ES) 2015/1998 ([9]) pielikuma 1.7. punktā un Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/1148 ([10]) 14. pantā.

(11) Drošības prasības, kas noteiktas Eiropas Parlamenta un Padomes Regulas (ES) 2021/696 ([11])) V sadaļas "Programmas drošība" 33.–43. pantā, uzskata par līdzvērtīgām šajā regulā noteiktajām prasībām, izņemot šīs regulas II pielikuma IS.I.OR.230. punktu, kas jāievēro.

(12) Lai nodrošinātu juridisko noteiktību, šajā regulā definētā termina "informācijas drošība" interpretācija, kas atspoguļo tā vispārējo lietojumu civilajā aviācijā visā pasaulē, būtu jāuzskata par saskanīgu ar Direktīvas (ES) 2016/1148 4. panta 2. punktā definētā termina "tīklu un informācijas sistēmu drošība" interpretāciju. Šajā regulā izmantotā informācijas drošības definīcija nebūtu jāinterpretē kā atšķirīga no Direktīvā (ES) 2016/1148 noteiktās tīklu un informācijas sistēmu drošības definīcijas.

(13) Lai novērstu juridisko prasību dublēšanos gadījumā, kad uz organizācijām, uz kurām attiecas šī regula, jau attiecas drošības prasības, kuras izriet no (10) un 11. apsvērumā minētajiem Savienības tiesību aktiem un kuru iedarbība ir līdzvērtīga šajā regulā paredzētajiem noteikumiem, atbilstība minētajām drošības prasībām būtu jāuzskata par atbilstību šajā regulā noteiktajām prasībām.

(14) Organizācijām, uz kurām attiecas šī regula un uz kurām jau attiecas drošības prasības, kas izriet no Īstenošanas regulas (ES) 2015/1998 vai Regulas (ES) 2021/696, vai šīm abām regulām, būtu jāizpilda arī šīs regulas II pielikuma (IS.I.OR.230. punkta "Sistēma ārējai ziņošanai par informācijas drošību") prasības, jo nevienā no minētajām regulām nav noteikumu, kas attiektos uz ārējo ziņošanu par informācijas drošības incidentiem.

(15) Pabeigtības labad būtu jāgroza Regulas (ES) Nr. 1178/2011, (ES) Nr. 748/2012, (ES) Nr. 965/2012, (ES) Nr. 139/2014, (ES) Nr. 1321/2014, (ES) 2015/340 un Īstenošanas regulas (ES) 2017/373 ([12]) un (ES) 2021/664, lai ieviestu šajā regulā noteiktās informācijas drošības pārvaldības sistēmas prasības kopā ar tajā noteiktajām pārvaldības sistēmām un lai noteiktu kompetento iestāžu prasības attiecībā uz to organizāciju uzraudzību, kuras īsteno minētās informācijas pārvaldības prasības.

(16) Lai sniegtu organizācijām pietiekamu laiku, kas vajadzīgs, lai nodrošinātu atbilstību jaunajiem noteikumiem un procedūrām, šī regula būtu jāsāk piemērot trīs gadus pēc tās stāšanās spēkā, izņemot attiecībā uz Eiropas Ģeostacionārās navigācijas pārklājuma dienesta (*EGNOS*) aeronavigācijas pakalpojumu sniedzēju, kurš noteikts Īstenošanas regulā (ES) 2017/373 un kuram, ņemot vērā *EGNOS* sistēmas un pakalpojumu notiekošo drošības akreditāciju saskaņā ar Regulu (ES) 2021/696, tā būtu jāpiemēro no 2026. gada 1. janvāra.

(17) Šajā regulā noteikto prasību pamatā ir Atzinums Nr. 03/2021 ([13]), ko Aģentūra izdevusi saskaņā ar Regulas (ES) 2018/1139 75. panta 2. punkta b) un c) apakšpunktu un 76. panta 1. punktu.

([9]) Komisijas Īstenošanas regula (ES) 2015/1998 (2015. gada 5. novembris), ar ko nosaka sīki izstrādātus pasākumus kopīgu pamatstandartu īstenošanai aviācijas drošības jomā (OV L 299, 14.11.2015., 1. lpp.).

([10]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

([11]) Eiropas Parlamenta un Padomes Regula (ES) 2021/696 (2021. gada 28. aprīlis), ar ko izveido Savienības kosmosa programmu un Eiropas Savienības Kosmosa programmas aģentūru un atceļ Regulas (ES) Nr. 912/2010, (ES) Nr. 1285/2013 un (ES) Nr. 377/2014 un Lēmumu Nr. 541/2014/ES (OV L 170, 12.5.2021., 69. lpp.).

([12]) Komisijas Īstenošanas regula (ES) 2017/373 (2017. gada 1. marts), ar ko nosaka kopīgas prasības gaisa satiksmes pārvaldības/aeronavigācijas pakalpojumu sniedzējiem un citu gaisa satiksmes pārvaldības tīkla funkciju nodrošinātājiem un to uzraudzībai, ar ko atceļ Regulu (EK) Nr. 482/2008, Īstenošanas regulas (ES) Nr. 1034/2011, (ES) Nr. 1035/2011 un (ES) 2016/1377 un groza Regulu (ES) Nr. 677/2011 (OV L 62, 8.3.2017., 1. lpp.).

([13]) https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

(18) Šajā regulā noteiktās prasības ir saskaņā ar atzinumu, kuru sniegusi Komiteja kopīgo drošības noteikumu piemērošanai civilās aviācijas jomā, kas izveidota ar Regulas (ES) 2018/1139 127. pantu,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Priekšmets

Šajā regulā ir izklāstītas prasības, kas organizācijām un kompetentajām iestādēm ir jāizpilda, lai:

a) identificētu un pārvaldītu informācijas drošības riskus, kuri spēj ietekmēt informācijas un komunikācijas tehnoloģiju sistēmas un datus, ko izmanto civilajā aviācijā;

b) atklātu informācijas drošības notikumus un identificētu tos notikumus, kas uzskatāmi par informācijas drošības incidentiem, kuri spēj ietekmēt aviācijas drošumu;

c) reaģētu uz minētajiem informācijas drošības incidentiem un novērstu to sekas.

2. pants

Darbības joma

1. Šo regulu piemēro šādām organizācijām:

a) tehniskās apkopes organizācijām, uz kurām attiecas Regulas (ES) Nr. 1321/2014 II pielikuma (145. daļas) A iedaļa, izņemot tās, kas iesaistītas tikai gaisa kuģu tehniskajā apkopē saskaņā ar Regulas (ES) Nr. 1321/2014 Vb pielikumu (ML daļu);

b) lidojumderīguma uzturēšanas vadības organizācijām (*CAMO*), uz kurām attiecas Regulas (ES) Nr. 1321/2014 Vc pielikuma (*CAMO daļas*) A iedaļa, izņemot tās, kas iesaistītas tikai gaisa kuģu lidojumderīguma uzturēšanas vadībā saskaņā ar Regulas (ES) Nr. 1321/2014 Vb pielikumu (ML daļu);

c) gaisa kuģu ekspluatantiem, uz kuriem attiecas Regulas (ES) Nr. 965/2012 III pielikums (*Part-ORO*), izņemot tos, kas iesaistīti tikai šādu gaisa kuģu ekspluatācijā:

   i) *ELA2* gaisa kuģi, kas definēti Regulas (ES) Nr. 748/2012 1. panta 2. punkta j) apakšpunktā;

   ii) viendzinēja propelleru lidmašīnas, kuru maksimālā operatīvā pasažieru vietu konfigurācija nav lielāka par piecām pasažieru vietām un kuras nav klasificētas kā komplekss motorizēts gaisa kuģis, kad notiek pacelšanās un nosēšanās vienā un tajā pašā lidlaukā vai ekspluatācijas vietā, un kuras ekspluatē saskaņā ar vizuālo lidojumu noteikumiem (*VFR*), kas piemērojami pa dienu;

   iii) viendzinēja helikopteri, kuru maksimālā operatīvā pasažieru vietu konfigurācija nav lielāka par piecām pasažieru vietām un kuri nav klasificēti kā komplekss motorizēts gaisa kuģis, kad notiek pacelšanās un nosēšanās vienā un tajā pašā lidlaukā vai ekspluatācijas vietā, un kurus ekspluatē saskaņā ar *VFR*, kas piemērojami pa dienu.

d) apstiprinātām mācību organizācijām (*ATO*), uz kurām attiecas Regulas (ES) Nr. 1178/2011 VII pielikums (*ORA* daļa), izņemot tās, kas iesaistītas tikai Regulas (ES) Nr. 748/2012 1. panta 2. punkta j) apakšpunktā definēto *ELA2* gaisa kuģu mācību pasākumos vai iesaistītas tikai teorētiskās mācībās;

e) aviācijas medicīnas centriem, kuri paredzēti apkalpei un uz kuriem attiecas Regulas (ES) Nr. 1178/2011 VII pielikums (*ORA* daļa);

f) lidojumu simulācijas trenažieru iekārtu (*FSTD*) operatoriem, uz kuriem attiecas Regulas (ES) Nr. 1178/2011 VII pielikums (*ORA* daļa), izņemot tos, kas iesaistīti tikai Regulas (ES) Nr. 748/2012 1. panta 2. punkta j) apakšpunktā definēto *ELA2* gaisa kuģu *FSTD* ekspluatācijā;

g) gaisa satiksmes vadības dispečeru mācību organizācijām (*ATCO TO*) un gaisa satiksmes vadības dispečeru (*ATCO*) aviācijas medicīnas centriem, uz kuriem attiecas Regulas (ES) 2015/340 III pielikums (ATCO.OR daļa);

h) organizācijām, uz kurām attiecas Īstenošanas regulas (ES) 2017/373 III pielikums (*Part-ATM/ANS.OR*), izņemot šādus pakalpojumu sniedzējus:

i) aeronavigācijas pakalpojumu sniedzēji, kuri ir saņēmuši ierobežotu sertifikātu saskaņā ar minētā pielikuma ATM/ANS.OR.A.010. punktu;

ii) lidojumu informācijas pakalpojumu sniedzēji, kuri savu darbību ir deklarējuši saskaņā ar minētā pielikuma ATM/ANS.OR.A.015. punktu;

i) "U-space" pakalpojumu sniedzējiem un vienotiem kopīgo informācijas pakalpojumu sniedzējiem, uz kuriem attiecas Īstenošanas regula (ES) 2021/664.

2. Šo regulu piemēro kompetentajām iestādēm, tajā skaitā Eiropas Savienības Aviācijas drošības aģentūrai ("Aģentūra"), kas minētas šīs regulas 6. pantā un Komisijas Deleģētās regulas (ES) 2022/1645 ([14]) 5. pantā.

3. Šo regulu piemēro arī kompetentajai iestādei, kas ir atbildīga par gaisa kuģa tehniskās apkopes licenču izsniegšanu, pagarināšanu, apmaiņu, apturēšanu vai atsaukšanu saskaņā ar Regulas (ES) Nr. 1321/2014 III pielikumu (66. daļu).

4. Šī regula neskar informācijas drošības un kiberdrošības prasības, kas noteiktas Īstenošanas regulas (ES) 2015/1998 pielikuma 1.7. punktā un Direktīvas (ES) 2016/1148 14. pantā.

3. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "informācijas drošība" ir tīklu un informācijas sistēmu konfidencialitātes, integritātes, autentiskuma un darbgatavības saglabāšana;

2) "informācijas drošības notikums" ir identificēta sistēmas, pakalpojuma vai tīkla stāvokļa rašanās, norādot uz iespējamu informācijas drošības politikas neievērošanu vai informācijas drošības kontroles kļūdu, vai iepriekš nezināma situācija, kas var būt svarīga informācijas drošībai;

3) "incidents" ir jebkāds notikums, kas faktiski nelabvēlīgi ietekmē tīklu un informācijas sistēmu drošību, kā definēts Direktīvas (ES) 2016/1148 4. panta 7. punktā;

4) "informācijas drošības risks" ir risks, kas informācijas drošības notikuma iespējamības dēļ apdraud organizācijas civilās aviācijas darbības, aktīvus, indivīdus un citas organizācijas. Informācijas drošības riski ir saistīti ar apdraudējumu spēju izmantot informācijas aktīva vai informācijas aktīvu grupas ievainojamības;

([14]) Komisijas Deleģētā regula (ES) 2022/1645 (2022. gada 14. jūlijs), ar ko paredz noteikumus par Eiropas Parlamenta un Padomes Regulas (ES) 2018/1139 piemērošanu attiecībā uz prasībām par tādu informācijas drošības risku pārvaldību, kuri spēj ietekmēt aviācijas drošumu, kas noteiktas organizācijām, uz kurām attiecas Komisijas Regulas (ES) Nr. 748/2012 un (ES) Nr. 139/2014, un ar ko groza Komisijas Regulas (ES) Nr. 748/2012 un (ES) Nr. 139/2014 (OV L 248, 26.9.2022., 18. lpp.).

5) "apdraudējums" ir informācijas drošības pārkāpuma iespējamība, kas pastāv, ja ir subjekts, apstāklis, darbība vai notikums, kas varētu radīt kaitējumu;

6) "ievainojamība" ir aktīva vai sistēmas, procedūru, projekta, īstenošanas vai informācijas drošības pasākumu nepilnība vai trūkums, ko varētu izmantot un izraisīt informācijas drošības politikas neievērošanu vai pārkāpumu.

4. pants

Prasības organizācijām un kompetentajām iestādēm

1. Šīs regulas 2. panta 1. punktā minētajām organizācijām jānodrošina atbilstība šīs regulas II pielikuma (IS.I.OR daļas) prasībām.

2. Šīs regulas 2. panta 2. un 3. punktā minētajām kompetentajām iestādēm jānodrošina atbilstība šīs regulas I pielikuma (IS.AR daļas) prasībām.

5. pants

No citiem Savienības tiesību aktiem izrietošās prasības

1. Ja 2. panta 1. punktā minētā organizācija atbilst drošības prasībām, kas noteiktas saskaņā ar Direktīvas (ES) 2016/1148 14. pantu un ir līdzvērtīgas šajā regulā noteiktajām prasībām, atbilstību minētajām drošības prasībām uzskata par atbilstību šajā regulā noteiktajām prasībām.

2. Ja 2. panta 1. punktā minētā organizācija ir ekspluatants vai struktūra, kas minēta dalībvalstu valsts civilās aviācijas drošības programmās, kuras noteiktas saskaņā ar Eiropas Parlamenta un Padomes Regulas (EK) Nr. 300/2008 ([15]) 10. pantu, Īstenošanas regulas (ES) 2015/1998 pielikuma 1.7. punktā ietvertās kiberdrošības prasības uzskata par līdzvērtīgām šajā regulā noteiktajām prasībām, izņemot šīs regulas II pielikuma IS.I.OR.230. punktā noteiktās prasības, kuras ir jāizpilda, kā paredzēts.

3. Ja 2. panta 1. punktā minētā organizācija ir Regulā (ES) 2021/696 minētais Eiropas Ģeostacionārās navigācijas pārklājuma dienesta (*EGNOS*) aeronavigācijas pakalpojumu sniedzējs, minētās regulas V sadaļas 33.–43. pantā ietvertās drošības prasības uzskata par līdzvērtīgām šajā regulā noteiktajām prasībām, izņemot šīs regulas II pielikuma IS.I.OR.230. punktā noteiktās prasības, kuras ir jāizpilda, kā paredzēts.

4. Komisija pēc apspriešanās ar Aģentūru un Direktīvas (ES) 2016/1148 11. pantā minēto sadarbības grupu var izdot vadlīnijas šajā regulā un Direktīvā (ES) 2016/1148 noteikto prasību līdzvērtības novērtēšanai.

6. pants

Kompetentā iestāde

1. Neskarot uzdevumus, kas uzticēti Regulas (ES) 2021/696 36. pantā minētajai Drošības akreditācijas padomei (*SAB*), iestāde, kuras pienākums ir apliecināt un pārraudzīt atbilstību šai regulai, ir:

a) attiecībā uz 2. panta 1. punkta a) apakšpunktā minētajām organizācijām – kompetentā iestāde, kas izraudzīta saskaņā ar Regulas (ES) Nr. 1321/2014 II pielikumu (145. daļu);

b) attiecībā uz 2. panta 1. punkta b) apakšpunktā minētajām organizācijām – kompetentā iestāde, kas izraudzīta saskaņā ar Regulas (ES) Nr. 1321/2014 Vc pielikumu (*CAMO* daļu);

([15]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 300/2008 (2008. gada 11. marts) par kopīgiem noteikumiem civilās aviācijas drošības jomā un ar ko atceļ Regulu (EK) Nr. 2320/2002 (OV L 97, 9.4.2008., 72. lpp.).

c) attiecībā uz 2. panta 1. punkta c) apakšpunktā minētajām organizācijām – kompetentā iestāde, kas izraudzīta saskaņā ar Regulas (ES) Nr. 965/2012 III pielikumu (*Part-ORO*);

d) attiecībā uz 2. panta 1. punkta d)–f) apakšpunktā minētajām organizācijām – kompetentā iestāde, kas izraudzīta saskaņā ar Regulas (ES) Nr. 1178/2011 VII pielikumu (*ORA* daļu);

e) attiecībā uz 2. panta 1. punkta g) apakšpunktā minētajām organizācijām – kompetentā iestāde, kas izraudzīta saskaņā ar Regulas (ES) 2015/340 6. panta 2. punktu;

f) attiecībā uz 2. panta 1. punkta h) apakšpunktā minētajām organizācijām – kompetentā iestāde, kas izraudzīta saskaņā ar Īstenošanas regulas (ES) 2017/373 4. panta 1. punktu;

g) attiecībā uz 2. panta 1. punkta i) apakšpunktā minētajām organizācijām – kompetentā iestāde, kas izraudzīta saskaņā ar Īstenošanas regulas (ES) 2021/664 14. panta 1. vai 2. punktu.

2. Dalībvalstis šīs regulas vajadzībām var izraudzīties neatkarīgu un autonomu struktūru, kas pildītu 1. punktā minētajām kompetentajām iestādēm uzticētās funkcijas un pienākumus. Šādā gadījumā nosaka pasākumus koordinācijai starp minēto struktūru un kompetentajām iestādēm, kas minētas 1. punktā, lai nodrošinātu visu to prasību efektīvu pārraudzību, kuras organizācijai ir jāizpilda.

3. Aģentūra, pilnībā ievērojot piemērojamos noteikumus par slepenību, personas datu aizsardzību un klasificētas informācijas aizsardzību, sadarbojas ar Eiropas Savienības Kosmosa programmas aģentūru (*EUSPA*) un *SAB*, kas minēta Regulas (ES) 2021/696 36. pantā, lai nodrošinātu *EGNOS* aeronavigācijas pakalpojumu sniedzējam piemērojamo prasību efektīvu uzraudzību.

7. pants

Attiecīgās informācijas iesniegšana tīklu un informācijas drošības (TID) kompetentajās iestādēs

Šajā regulā norādītās kompetentās iestādes bez nepamatotas kavēšanās informē vienoto kontaktpunktu, kurš izraudzīts saskaņā ar Direktīvas (ES) 2016/1148 8. pantu, sniedzot visu attiecīgo informāciju, kas iekļauta paziņojumos, kurus saskaņā ar šīs regulas II pielikuma IS.I.OR.230. punktu un Deleģētās regulas (ES) 2022/1645 I pielikuma IS.D.OR.230. punktu ir iesnieguši pamatpakalpojumu sniedzēji, kas identificēti saskaņā ar Direktīvas (ES) 2016/1148 5. pantu.

8. pants

Grozījumi Regulā (ES) Nr. 1178/2011

Regulas (ES) Nr. 1178/2011 VI pielikumu (*ARA* daļu) un VII pielikumu (*ORA* daļu) groza saskaņā ar šīs regulas III pielikumu.

9. pants

Grozījumi Regulā (ES) Nr. 748/2012

Regulas (ES) Nr. 748/2012 I pielikumu (21. daļu) groza saskaņā ar šīs regulas IV pielikumu.

10. pants

Grozījumi Regulā (ES) Nr. 965/2012

Regulas (ES) Nr. 965/2012 II pielikumu (*Part-ARO*) un III pielikumu (*Part-ORO*) groza saskaņā ar šīs regulas V pielikumu.

11. pants

Grozījumi Regulā (ES) Nr. 139/2014

Regulas (ES) Nr. 139/2014 II pielikumu (*Part-ADR.AR*) groza saskaņā ar šīs regulas VI pielikumu.

12. pants

Grozījumi Regulā (ES) Nr. 1321/2014

Regulas (ES) Nr. 1321/2014 II pielikumu (145. daļu), III pielikumu (66. daļu) un Vc pielikumu (*CAMO daļu*) groza saskaņā ar šīs regulas VII pielikumu.

13. pants

Grozījumi Regulā (ES) 2015/340

Regulas (ES) 2015/340 II pielikumu (*ATCO.AR daļu*) un III pielikumu (*ATCO.OR* daļu) groza saskaņā ar šīs regulas VIII pielikumu.

14. pants

Grozījumi Īstenošanas regulā (ES) 2017/373

Īstenošanas regulas (ES) 2017/373 II pielikumu (*Part-ATM/ANS.AR*) un III pielikumu (*Part-ATM/ANS.OR*) groza saskaņā ar šīs regulas IX pielikumu.

15. pants

Grozījumi Īstenošanas regulā (ES) 2021/664

Īstenošanas regulu (ES) 2021/664 groza šādi:

1) regulas 15. panta 1. punkta f) apakšpunktu aizstāj ar šādu:

"f) īsteno un uztur drošības pārvaldības sistēmu saskaņā ar Īstenošanas regulas (ES) 2017/373 III pielikuma D apakšiedaļas ATM/ANS.OR.D.010. punktu un informācijas drošības pārvaldības sistēmu saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikumu (IS.I.OR daļu);"

2) regulas 18. pantam pievieno šādu l) punktu:

"l) izveido, īsteno un uztur informācijas drošības pārvaldības sistēmu saskaņā ar Īstenošanas regulas (ES) 2023/203 I pielikumu (IS.AR daļu)."

16. pants

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

To piemēro no 2026. gada 22. februāra.

Tomēr attiecībā uz *EGNOS* aeronavigācijas pakalpojumu sniedzēju, uz kuru attiecas Īstenošanas regula (ES) 2017/373, to piemēro no 2026. gada 1. janvāra.

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

Briselē, 2022. gada 27. oktobrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

I PIELIKUMS

INFORMĀCIJAS DROŠĪBA – PRASĪBAS IESTĀDĒM

[IS.AR DAĻA]

IS.AR.100. Darbības joma

IS.AR.200. Informācijas drošības pārvaldības sistēma (IDPS)

IS.AR.205. Informācijas drošības riska novērtējums

IS.AR.210. Informācijas drošības riska risināšana

IS.AR.215. Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana

IS.AR.220. Informācijas drošības pārvaldības darbību līguma slēgšana

IS.AR.225. Prasības personālam

IS.AR.230. Reģistrācija

IS.AR.235. Pastāvīgi uzlabojumi

IS.AR.100. Darbības joma

Šajā daļā ir noteiktas pārvaldības prasības, kas jāizpilda šīs regulas 2. panta 2. punktā minētajām kompetentajām iestādēm.

Prasības, kas šīm kompetentajām iestādēm jāizpilda, veicot sertifikācijas, uzraudzības un izpildes darbības, ir ietvertas šīs regulas 2. panta 1. punktā un Deleģētās regulas (ES) 2022/1645 2. pantā minētajās regulās.

IS.AR.200. Informācijas drošības pārvaldības sistēma (IDPS)

a) Lai sasniegtu 1. pantā noteiktos mērķus, kompetentā iestāde izveido, īsteno un uztur informācijas drošības pārvaldības sistēmu (IDPS), kas nodrošina, ka kompetentā iestāde:

1) izveido informācijas drošības politiku, kurā izklāstīti kompetentās iestādes vispārējie principi, kas attiecas uz informācijas drošības risku iespējamo ietekmi uz aviācijas drošumu;

2) identificē un pārskata informācijas drošības riskus saskaņā ar IS.AR.205. punktu;

3) nosaka un īsteno informācijas drošības riska risināšanas pasākumus saskaņā ar IS.AR.210. punktu;

4) saskaņā ar IS.AR.215. punktu nosaka un īsteno pasākumus, kas vajadzīgi, lai atklātu informācijas drošības notikumus, identificē tos notikumus, kuri uzskatāmi par incidentiem, kas spēj ietekmēt aviācijas drošumu, un reaģē uz minētajiem informācijas drošības incidentiem un novērš to sekas;

5) ja tiek slēgts līgums ar citām organizācijām par jebkuru daļu no IS.AR.200. punktā aprakstītajām darbībām, nodrošina atbilstību IS.AR.220. punktā ietvertajām prasībām;

6) nodrošina atbilstību prasībām, kas IS.AR.225. punktā noteiktas attiecībā uz personālu;

7) nodrošina atbilstību IS.AR.230. punktā ietvertajām reģistrācijas prasībām;

8) uzrauga savas organizācijas atbilstību šīs regulas prasībām un sniedz atsauksmes par konstatējumiem IS.AR.225. punkta a) apakšpunktā minētajai personai, lai nodrošinātu korektīvo pasākumu efektīvu īstenošanu;

9) aizsargā jebkuras tādas informācijas konfidencialitāti, kas kompetentajai iestādei varētu būt pieejama saistībā ar organizācijām, uz kurām attiecas tās uzraudzība, un kas saņemta, izmantojot organizācijas ārējās ziņošanas sistēmas, kuras izveidotas saskaņā ar šīs regulas II pielikuma (IS.I.OR daļas) IS.I.OR.230. punktu un Deleģētās regulas (ES) 2022/1645 I pielikuma (IS.D.OR daļas) IS.D.OR.230. punktu;

10) ziņo Aģentūrai par izmaiņām, kas ietekmē kompetentās iestādes spēju veikt uzdevumus un pildīt pienākumus, kas tai noteikti šajā regulā;

11) nosaka un īsteno procedūras, kuras ļauj pienācīgi, praktiski un laikus apmainīties ar attiecīgo informāciju, kas nepieciešama, lai palīdzētu citām kompetentajām iestādēm un aģentūrām, kā arī organizācijām, uz kurām attiecas šī regula, veikt efektīvus drošības riska novērtējumus saistībā ar to darbībām.

b) Lai nodrošinātu pastāvīgu atbilstību 1. pantā minētajām prasībām, kompetentā iestāde īsteno pastāvīgu uzlabojumu procesu saskaņā ar IS.AR.235. punktu.

c) Kompetentā iestāde dokumentē visus galvenos procesus, procedūras, funkcijas un pienākumus, kas vajadzīgi, lai izpildītu IS.AR.200. punkta a) apakšpunkta prasības, un izveido minētās dokumentācijas grozījumu veikšanas procesu.

d) Procesi, procedūras, funkcijas un pienākumi, ko kompetentā iestāde noteikusi, lai izpildītu IS.AR.200. punkta a) apakšpunkta prasības, atbilst tās darbību veidam un sarežģītībai, pamatojoties uz šīm darbībām raksturīgo informācijas drošības risku novērtējumu, un tos var integrēt citās esošās pārvaldības sistēmās, kuras kompetentā iestāde jau ir ieviesusi.

IS.AR.205. Informācijas drošības riska novērtējums

a) Kompetentā iestāde identificē visus savas organizācijas elementus, kas varētu būt pakļauti informācijas drošības riskiem. Tas ietver:

1) kompetentās iestādes darbības, objektus un resursus, kā arī kompetentās iestādes sniegtos, nodrošinātos, saņemtos vai uzturētos pakalpojumus;

2) iekārtas, sistēmas, datus un informāciju, kas veicina 1. punktā minēto elementu darbību.

b) Kompetentā iestāde identificē saskarnes, kas tās organizācijai ir ar citām organizācijām un varētu radīt savstarpēju pakļautību informācijas drošības riskiem.

c) Attiecībā uz a) un b) apakšpunktā minētajiem elementiem un saskarnēm kompetentā iestāde identificē informācijas drošības riskus, kas varētu spēt ietekmēt aviācijas drošumu.

Attiecībā uz katru identificēto risku kompetentā iestāde:

1) nosaka riska līmeni saskaņā ar kompetentās iestādes iepriekšnoteiktu klasifikāciju;

2) katru risku un tā līmeni sasaista ar attiecīgo elementu vai saskarni, kas identificēta saskaņā ar a) un b) apakšpunktu.

Iepriekšnoteiktajā klasifikācijā, kas minēta 1. punktā, ņem vērā apdraudējuma scenārija īstenošanās iespējamību un to, cik smagi tā sekas ietekmētu drošumu. Izmantojot minēto klasifikāciju un ņemot vērā to, vai kompetentajā iestādē ir strukturēts un atkārtojams darbības riska pārvaldības process, kompetentajai iestādei jāspēj noteikt, vai risks ir pieņemams, vai arī tas ir jārisina saskaņā ar IS.AR.210. punktu.

Lai veicinātu riska novērtējumu savstarpējo salīdzināmību, riska līmeņa noteikšanā saskaņā ar 1. punktu ņem vērā attiecīgo informāciju, kas iegūta koordinācijā ar b) apakšpunktā minētajām organizācijām.

d) Kompetentā iestāde saskaņā ar a), b) un c) apakšpunktu veikto riska novērtējumu pārskata un atjaunina jebkurā no šādiem gadījumiem:

1) mainās elementi, uz kuriem attiecas informācijas drošības riski;

2) mainās saskarnes starp kompetentās iestādes organizāciju un citām organizācijām vai citu organizāciju paziņotie riski;

3) mainās informācija vai zināšanas, ko izmanto risku identificēšanai, analīzei un klasifikācijai;

4) ir gūta pieredze, kas izriet no informācijas drošības incidentu analīzes.

IS.AR.210. Informācijas drošības riska risināšana

a) Kompetentā iestāde izstrādā pasākumus, ar kuriem novērst nepieņemamus riskus, kas identificēti saskaņā ar IS.AR.205. punktu, laikus īsteno tos un pārbauda to pastāvīgu rezultativitāti. Šie pasākumi kompetentajai iestādei ļauj:

1) saglabāt kontroli pār apstākļiem, kas veicina apdraudējuma scenārija faktisku īstenošanos;

2) apdraudējuma scenārija īstenošanās gadījumā samazināt sekas aviācijas drošumam;

3) novērst riskus.

Šie pasākumi nerada jaunus iespējami nepieņemamus riskus, kas apdraud aviācijas drošumu.

b) Personu, kas minēta IS.AR.225. punkta a) apakšpunktā, un citu ietekmēto kompetentās iestādes personālu informē par saskaņā ar IS.AR.205. punktu veiktā riska novērtējuma rezultātiem, attiecīgajiem apdraudējuma scenārijiem un īstenojamajiem pasākumiem.

Kompetentā iestāde arī informē organizācijas, ar kurām tai ir saskarne saskaņā ar IS.AR.205. punkta b) apakšpunktu, par visiem kompetentās iestādes un organizācijas dalītajiem riskiem.

IS.AR.215. Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana

a) Pamatojoties uz saskaņā ar IS.AR.205. punktu veiktā riska novērtējuma rezultātiem, kā arī rezultātiem, kas gūti riska risināšanā saskaņā ar IS.AR.210. punktu, kompetentā iestāde īsteno pasākumus, kuru mērķis ir atklāt notikumus, kas norāda uz nepieņemamu risku iespējamo īstenošanos un spēj ietekmēt aviācijas drošumu. Šie atklāšanas pasākumi kompetentajai iestādei ļauj:

1) konstatēt novirzes no iepriekšnoteiktām funkcionālās veiktspējas bāzlīnijām;

2) jebkādas novirzes gadījumā dot brīdinājumus, lai aktivizētu pienācīgus reaģēšanas pasākumus.

b) Kompetentā iestāde īsteno pasākumus, kuru mērķis ir reaģēt uz visiem notikuma apstākļiem, kas konstatēti saskaņā ar a) apakšpunktu un var attīstīties vai ir attīstījušies par informācijas drošības incidentu. Šie reaģēšanas pasākumi kompetentajai iestādei ļauj:

1) sākt savas organizācijas reaģēšanu uz a) apakšpunkta 2. punktā minētajiem brīdinājumiem, aktivizējot iepriekšnoteiktus resursus un darbību gaitu;

2) ierobežot uzbrukuma izvēršanos un novērst apdraudējuma scenārija pilnīgu īstenošanos;

3) vadīt IS.AR.205. punkta a) apakšpunktā noteikto skarto elementu atteices režīmu.

c) Kompetentā iestāde īsteno pasākumus, kuru mērķis ir novērst informācijas drošības incidentu sekas, tostarp ārkārtas pasākumus vajadzības gadījumā. Šie seku novēršanas pasākumi kompetentajai iestādei ļauj:

1) novērst incidentu izraisījušo apstākli vai ierobežot to līdz pieļaujamam līmenim;

2) atjaunošanās laikā, ko iepriekš noteikusi tās organizācija, atjaunot IS.AR.205. punkta a) apakšpunktā noteikto skarto elementu drošu stāvokli.

IS.AR.220. Informācijas drošības pārvaldības darbību līguma slēgšana

Ja kompetentā iestāde noslēdz līgumu ar citām organizācijām par kādu daļu no IS.AR.200. punktā minētajām darbībām, tā nodrošina, ka darbības, par kurām noslēgts līgums, atbilst šīs regulas prasībām un ka nolīgtā organizācija darbojas tās uzraudzībā. Kompetentā iestāde nodrošina, ka riski, kas saistīti ar darbībām, par kurām noslēgts līgums, tiek pienācīgi pārvaldīti.

IS.AR.225. Prasības personālam

Kompetentajai iestādei:

a) ir persona, kurai ir pilnvaras izveidot un uzturēt šīs regulas īstenošanai vajadzīgās organizatoriskās struktūras, politiku, procesus un procedūras.

Šai personai:

1) ir pilnvaras, kas nepieciešamas, lai pilnībā piekļūtu resursiem, kuri vajadzīgi, lai kompetentā iestāde varētu veikt visus šajā regulā paredzētos uzdevumus;

2) ir deleģētas pilnvaras, kas vajadzīgas, lai veiktu piešķirtos pienākumus;

b) ir ieviests process, ar ko nodrošināt, ka tai pietiek dežurējošo darbinieku šajā pielikumā izklāstīto darbību veikšanai;

c) ir ieviests process, ar ko nodrošināt, ka b) apakšpunktā minētajiem darbiniekiem ir savu uzdevumu veikšanai vajadzīgā kompetence;

d) ir ieviests process, ar ko nodrošināt, ka darbinieki atzīst pienākumus, kas saistīti ar tiem uzticētajām funkcijām un uzdevumiem;

e) ir jānodrošina, ka tiek pienācīgi noteikta to darbinieku identitāte un uzticamība, kuriem ir piekļuve informācijas sistēmām un datiem, uz ko attiecas šīs regulas prasības.

IS.AR.230. Reģistrācija

a) Kompetentā iestāde reģistrē savas informācijas drošības pārvaldības darbības.

1) Kompetentā iestāde nodrošina, ka ir arhivēti un izsekojami šādi ieraksti:

i) līgumi par darbībām, kas minēti IS.AR.200. punkta a) apakšpunkta 5. punktā;

ii) ieraksti par galvenajiem procesiem, kas minēti IS.AR.200. punkta d) apakšpunktā;

iii) ieraksti par IS.AR.205. punktā minētajā riska novērtējumā identificētajiem riskiem kopā ar saistītajiem IS.AR.210. punktā minētajiem riska risināšanas pasākumiem;

iv) ieraksti par tiem informācijas drošības notikumiem, kuri varētu būt jāizvērtē atkārtoti, lai atklātu vēl neatklātus informācijas drošības incidentus vai ievainojamības.

2) Ierakstus, kas minēti 1. punkta i) apakšpunktā, glabā vismaz 5 gadus pēc tam, kad līgums ir grozīts vai izbeigts.

3) Ierakstus, kas minēti 1. punkta ii) un iii) apakšpunktā, glabā vismaz 5 gadus.

4) Ierakstus, kas minēti 1. punkta iv) apakšpunktā, glabā tik ilgi, līdz šie informācijas drošības notikumi ir atkārtoti izvērtēti saskaņā ar kompetentās iestādes izveidotā procedūrā noteiktu periodiskumu.

b) Kompetentā iestāde reģistrē savu informācijas drošības pārvaldības darbībās iesaistīto darbinieku kvalifikāciju un pieredzi.

1) Ierakstus par darbinieka kvalifikāciju un pieredzi glabā tik ilgi, kamēr persona strādā kompetentajā iestādē, un vismaz 3 gadus pēc tam, kad persona ir aizgājusi no darba kompetentajā iestādē.

2) Darbiniekiem pēc pieprasījuma dod piekļuvi viņu individuālajiem datiem. Turklāt pēc darbinieka pieprasījuma kompetentā iestāde darbiniekam izsniedz viņa individuālo datu kopiju, kad darbinieks aiziet no darba kompetentajā iestādē.

c) Ierakstu formātu nosaka kompetentās iestādes procedūrās.

d) Ierakstus information being identified, when required, according to its security classification level. glabā veidā, kas nodrošina aizsardzību pret bojājumiem, pārveidošanu un zādzību, vajadzības gadījumā informāciju identificējot atbilstīgi tās drošības klasifikācijas līmenim. Kompetentā iestāde nodrošina, ka ierakstus glabā, izmantojot līdzekļus, kas nodrošina integritāti, autentiskumu un atļautu piekļuvi.

IS.AR.235. Pastāvīgi uzlabojumi

a) Kompetentā iestāde, izmantojot atbilstīgus darbības rādītājus, novērtē savas IDPS efektivitāti un gatavību. Minēto novērtēšanu veic, pamatojoties uz kompetentās iestādes iepriekšnoteiktu kalendāro grafiku vai pēc informācijas drošības incidenta.

b) Ja pēc novērtēšanas, kas veikta saskaņā ar a) apakšpunktu, tiek konstatēti trūkumi, kompetentā iestāde īsteno uzlabošanas pasākumus, kuri vajadzīgi, lai nodrošinātu, ka IDPS joprojām atbilst piemērojamajām prasībām un uztur informācijas drošības riskus pieņemamā līmenī. Turklāt kompetentā iestāde atkārtoti izvērtē tos IDPS elementus, kurus ietekmē pieņemtie pasākumi.

II PIELIKUMS

INFORMĀCIJAS DROŠĪBA – PRASĪBAS ORGANIZĀCIJĀM

[IS.I.OR DAĻA]

IS.I.OR.100. Darbības joma

IS.I.OR.200. Informācijas drošības pārvaldības sistēma (IDPS)

IS.I.OR.205. Informācijas drošības riska novērtējums

IS.I.OR.210. Informācijas drošības riska risināšana

IS.I.OR.215. Sistēma iekšējai ziņošanai par informācijas drošību

IS.I.OR.220. Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana

IS.I.OR.225. Reaģēšana uz kompetentās iestādes paziņotajiem konstatējumiem

IS.I.OR.230. Sistēma ārējai ziņošanai par informācijas drošību

IS.I.OR.235. Informācijas drošības pārvaldības darbību līguma slēgšana

IS.I.OR.240. Prasības personālam

IS.I.OR.245. Reģistrācija

IS.I.OR.250. Informācijas drošības pārvaldības rokasgrāmata (IDPR)

IS.I.OR.255. Informācijas drošības pārvaldības sistēmas izmaiņas

IS.I.OR.260. Pastāvīgi uzlabojumi

IS.I.OR.100. Darbības joma

Šajā daļā ir paredzētas prasības, kas jāizpilda šīs regulas 2. panta 1. punktā minētajām organizācijām.

IS.I.OR.200. Informācijas drošības pārvaldības sistēma (IDPS)

a) Lai sasniegtu 1. pantā noteiktos mērķus, organizācija izveido, īsteno un uztur informācijas drošības pārvaldības sistēmu (IDPS), kas nodrošina, ka organizācija:

   1) izveido informācijas drošības politiku, kurā izklāstīti organizācijas vispārējie principi, kas attiecas uz informācijas drošības risku iespējamo ietekmi uz aviācijas drošumu;

   2) identificē un pārskata informācijas drošības riskus saskaņā ar IS.I.OR.205. punktu;

   3) nosaka un īsteno informācijas drošības riska risināšanas pasākumus saskaņā ar IS.I.OR.210. punktu;

   4) īsteno sistēmu iekšējai ziņošanai par informācijas drošību saskaņā ar IS.I.OR.215. punktu;

   5) saskaņā ar IS.I.OR.220. punktu nosaka un īsteno pasākumus, kas vajadzīgi, lai atklātu informācijas drošības notikumus, identificē tos notikumus, kuri uzskatāmi par incidentiem, kas spēj ietekmēt aviācijas drošumu, neskarot izņēmumus, kuri atļauti saskaņā ar IS.I.OR.205. punkta e) apakšpunktu, reaģē uz minētajiem informācijas drošības incidentiem un novērš to sekas;

6) īsteno kompetentās iestādes paziņotos pasākumus kā tūlītēju reakciju uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu;

7) lai reaģētu uz kompetentās iestādes paziņotajiem konstatējumiem, veic atbilstīgus pasākumus saskaņā ar IS.I.OR.225. punktu;

8) lai kompetentā iestāde varētu veikt atbilstīgus pasākumus, īsteno ārējās ziņošanas sistēmu saskaņā ar IS.I.OR.230. punktu;

9) ja tiek slēgts līgums ar citām organizācijām par jebkuru daļu no IS.I.OR.200. punktā minētajām darbībām, nodrošina atbilstību IS.I.OR.235. punktā ietvertajām prasībām;

10) nodrošina atbilstību prasībām, kas IS.I.OR.240. punktā noteiktas attiecībā uz personālu;

11) nodrošina atbilstību IS.I.OR.245. punktā noteiktajām reģistrācijas prasībām;

12) uzrauga organizācijas atbilstību šīs regulas prasībām un sniedz atsauksmes par konstatējumiem atbildīgajam vadītājam, lai nodrošinātu korektīvo pasākumu efektīvu īstenošanu;

13) neskarot ziņošanai par incidentiem piemērojamās prasības, aizsargā jebkuras tādas informācijas konfidencialitāti, ko organizācija, iespējams, ir saņēmusi no citām organizācijām, atkarībā no tās sensitivitātes līmeņa.

b) Lai nodrošinātu pastāvīgu atbilstību 1. pantā minētajām prasībām, organizācija īsteno pastāvīgu uzlabojumu procesu saskaņā ar IS.I.OR.260. punktu.

c) Organizācija saskaņā ar IS.I.OR.250. punktu dokumentē visus galvenos procesus, procedūras, funkcijas un pienākumus, kas vajadzīgi, lai izpildītu IS.I.OR.200. punkta a) apakšpunkta prasības, un izveido minētās dokumentācijas grozījumu veikšanas procesu. Šo procesu, procedūru, funkciju un pienākumu izmaiņas pārvalda saskaņā ar IS.I.OR.255. punktu.

d) Procesi, procedūras, funkcijas un pienākumi, ko organizācija noteikusi, lai izpildītu IS.I.OR.200. punkta a) apakšpunkta prasības, atbilst tās darbību veidam un sarežģītībai, pamatojoties uz šīm darbībām raksturīgo informācijas drošības risku novērtējumu, un tos var integrēt citās esošās pārvaldības sistēmās, ko organizācija jau ir ieviesusi.

e) Neskarot pienākumu nodrošināt atbilstību Regulā (ES) Nr. 376/2014 ietvertajām ziņošanas prasībām un IS.I.OR.200. punkta a) apakšpunkta 13. punktā izklāstītajām prasībām, kompetentā iestāde var organizācijai dot atļauju neīstenot prasības, kas minētas a) līdz d) apakšpunktā, un saistītās prasības, kas ietvertas IS.I.OR.205. līdz IS.I.OR.260. punktā, ja organizācija minētajai iestādei pārliecinoši pierāda, ka tās darbības, objekti un resursi, kā arī tās sniegtie, nodrošinātie, saņemtie un uzturētie pakalpojumi ne attiecīgajai organizācijai, ne citām organizācijām nerada informācijas drošības riskus, kas spēj ietekmēt aviācijas drošumu. Atļauja pamatojas uz dokumentētu informācijas drošības riska novērtējumu, ko organizācija vai trešā persona veikusi saskaņā ar IS.I.OR.205. punktu un ko pārskatījusi un apstiprinājusi tās kompetentā iestāde.

Pēc piemērojamā pārraudzības revīzijas cikla un ikreiz, kad tiek ieviestas izmaiņas organizācijas darbības jomā, kompetentā iestāde pārskatīs minētās atļaujas turpmāko derīgumu.

IS.I.OR.205. Informācijas drošības riska novērtējums

a) Organizācija identificē visus tās elementus, kas varētu būt pakļauti informācijas drošības riskiem. Tas ietver:

1) organizācijas darbības, objektus un resursus, kā arī organizācijas sniegtos, nodrošinātos, saņemtos vai uzturētos pakalpojumus;

2) iekārtas, sistēmas, datus un informāciju, kas veicina 1. punktā uzskaitīto elementu darbību.

b) Organizācija identificē saskarnes, kas tai ir ar citām organizācijām un varētu radīt savstarpēju pakļautību informācijas drošības riskiem.

c) Attiecībā uz a) un b) apakšpunktā minētajiem elementiem un saskarnēm organizācija identificē informācijas drošības riskus, kas varētu spēt ietekmēt aviācijas drošumu. Attiecībā uz katru identificēto risku organizācija:

1) nosaka riska līmeni saskaņā ar organizācijas iepriekšnoteiktu klasifikāciju;

2) katru risku un tā līmeni sasaista ar attiecīgo elementu vai saskarni, kas identificēta saskaņā ar a) un b) apakšpunktu.

Iepriekšnoteiktajā klasifikācijā, kas minēta 1. punktā, ņem vērā apdraudējuma scenārija īstenošanās iespējamību un to, cik smagi tā sekas ietekmētu drošumu. Pamatojoties uz minēto klasifikāciju un ņemot vērā to, vai organizācijā ir strukturēts un atkārtojams darbības riska pārvaldības process, organizācijai jāspēj noteikt, vai risks ir pieņemams, vai arī tas ir jārisina saskaņā ar IS.I.OR.210. punktu.

Lai veicinātu riska novērtējumu savstarpējo salīdzināmību, riska līmeņa noteikšanā saskaņā ar 1. punktu ņem vērā attiecīgo informāciju, kas iegūta koordinācijā ar b) apakšpunktā minētajām organizācijām.

d) Organizācija saskaņā ar a), b) un attiecīgā gadījumā c) vai e) apakšpunktu veikto riska novērtējumu pārskata un atjaunina jebkurā no šādām situācijām:

1) mainās elementi, uz kuriem attiecas informācijas drošības riski;

2) mainās saskarnes starp attiecīgo organizāciju un citām organizācijām vai citu organizāciju paziņotie riski;

3) mainās informācija vai zināšanas, ko izmanto risku identificēšanai, analīzei un klasifikācijai;

4) ir gūta pieredze, kas izriet no informācijas drošības incidentu analīzes.

e) Atkāpjoties no c) apakšpunkta, organizācijas, kurām jāatbilst Īstenošanas regulas (ES) 2017/373 III pielikuma (*Part-ATM/ANS.OR*) C apakšdaļas prasībām, analīzi par ietekmi uz aviācijas drošumu aizstāj ar analīzi par ietekmi uz organizāciju pakalpojumiem saskaņā ar drošības atbalsta novērtējumu, kas paredzēts ATM/ANS.OR.C.005. punktā. Šo drošības atbalsta novērtējumu dara pieejamu gaisa satiksmes pakalpojumu sniedzējiem, kuriem tās sniedz pakalpojumus, un šie gaisa satiksmes pakalpojumu sniedzēji ir atbildīgi par to, lai tiktu izvērtēta ietekme uz aviācijas drošumu.

IS.I.OR.210. Informācijas drošības riska risināšana

a) Organizācija izstrādā pasākumus, ar kuriem novērst nepieņemamus riskus, kas identificēti saskaņā ar IS.I.OR.205. punktu, laikus īsteno tos un pārbauda to pastāvīgu rezultativitāti. Šie pasākumi organizācijai ļauj:

1) saglabāt kontroli pār apstākļiem, kas veicina apdraudējuma scenārija faktisku īstenošanos;

2) samazināt ietekmi uz aviācijas drošumu, kas saistīta ar apdraudējuma scenārija īstenošanos;

3) novērst riskus.

Šie pasākumi nerada jaunus iespējami nepieņemamus riskus, kas apdraud aviācijas drošumu.

b) Personu, kas minēta IS.I.OR.240. punkta a) un b) apakšpunktā, un citu ietekmēto organizācijas personālu informē par saskaņā ar IS.I.OR.205. punktu veiktā riska novērtējuma rezultātiem, attiecīgajiem apdraudējuma scenārijiem un īstenojamajiem pasākumiem.

Organizācija arī informē organizācijas, ar kurām tai ir saskarne saskaņā ar IS.I.OR.205. punkta b) apakšpunktu, par visiem abu organizāciju dalītajiem riskiem.

IS.I.OR.215. Sistēma iekšējai ziņošanai par informācijas drošību

a) Organizācija izveido iekšējās ziņošanas sistēmu, ar ko var apkopot un izvērtēt informācijas drošības notikumus, tostarp notikumus, par kuriem jāziņo saskaņā ar IS.I.OR.230. punktu.

b) Minētā sistēma un IS.I.OR.220. punktā minētais process organizācijai ļauj:

1) noteikt, kuri no notikumiem, par kuriem ziņots saskaņā ar a) apakšpunktu, ir uzskatāmi par informācijas drošības incidentiem vai ievainojamībām, kas spēj ietekmēt aviācijas drošumu;

2) noskaidrot saskaņā ar 1. punktu noteikto informācijas drošības incidentu un ievainojamību cēloņus un veicinošos faktorus un pievērsties tiem informācijas drošības riska pārvaldības procesā saskaņā ar IS.I.OR.205. un IS.I.OR.220. punktu;

3) nodrošināt, ka tiek izvērtēta visa zināmā un būtiskā informācija saistībā ar informācijas drošības incidentiem un ievainojamībām, kas noteikti saskaņā ar 1. punktu;

4) nodrošināt, ka tiek ieviesta metode informācijas iekšējai izplatīšanai pēc vajadzības.

c) Visām nolīgtām organizācijām, kuras var pakļaut attiecīgo organizāciju informācijas drošības riskiem, kas spēj ietekmēt aviācijas drošumu, ir pienākums ziņot organizācijai par informācijas drošības notikumiem. Minētos ziņojumus iesniedz, izmantojot procedūras, kas īpaši noteiktas līgumos, un tos izvērtē saskaņā ar b) apakšpunktu.

d) Organizācija izmeklēšanas jomā sadarbojas ar visām citām organizācijām, kas sniedz būtisku ieguldījumu organizācijas darbību informācijas drošībā.

e) Organizācija var minēto ziņošanas sistēmu integrēt ar citām ziņošanas sistēmām, ko tā jau ir ieviesusi.

IS.I.OR.220. Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana

a) Pamatojoties uz saskaņā ar IS.I.OR.205. punktu veiktā riska novērtējuma rezultātiem, kā arī rezultātiem, kas gūti riska risināšanā saskaņā ar IS.I.OR.210. punktu, organizācija īsteno pasākumus, kuru mērķis ir atklāt incidentus un ievainojamības, kas norāda uz nepieņemamu risku iespējamo īstenošanos un spēj ietekmēt aviācijas drošumu. Šie atklāšanas pasākumi organizācijai ļauj:

1) konstatēt novirzes no iepriekšnoteiktām funkcionālās veiktspējas bāzlīnijām;

2) jebkādas novirzes gadījumā dot brīdinājumus, lai aktivizētu pienācīgus reaģēšanas pasākumus.

b) Organizācija īsteno pasākumus, kuru mērķis ir reaģēt uz visiem notikuma apstākļiem, kas konstatēti saskaņā ar a) apakšpunktu un var attīstīties vai ir attīstījušies par informācijas drošības incidentu. Šie reaģēšanas pasākumi organizācijai ļauj:

1) sākt reaģēšanu uz a) apakšpunkta 2. punktā minētajiem brīdinājumiem, aktivizējot iepriekšnoteiktus resursus un darbību gaitu;

2) ierobežot uzbrukuma izvēršanos un novērst apdraudējuma scenārija pilnīgu īstenošanos;

3) vadīt IS.I.OR.205. punkta a) apakšpunktā noteikto skarto elementu atteices režīmu.

c) Organizācija īsteno pasākumus, kuru mērķis ir novērst informācijas drošības incidentu sekas, tostarp ārkārtas pasākumus vajadzības gadījumā. Šie seku novēršanas pasākumi organizācijai ļauj:

1) novērst incidentu izraisījušo apstākli vai ierobežot to līdz pieļaujamam līmenim;

2) atjaunošanās laikā, ko iepriekš noteikusi organizācija, sasniegt IS.I.OR.205. punkta a) apakšpunktā noteikto skarto elementu drošu stāvokli.

IS.I.OR.225. Reaģēšana uz kompetentās iestādes paziņotajiem konstatējumiem

a) Saņēmusi kompetentās iestādes iesniegto paziņojumu par konstatējumiem, organizācija:

1) noskaidro neatbilstības pamatcēloni vai cēloņus un veicinošos faktorus;

2) izstrādā korektīvo pasākumu plānu;

3) pierāda kompetentajai iestādei, ka neatbilstība ir novērsta.

b) Šā punkta a) apakšpunktā minētās darbības veic laikposmā, par kuru panākta vienošanās ar kompetento iestādi.

IS.I.OR.230. Sistēma ārējai ziņošanai par informācijas drošību

a) Organizācija ievieš informācijas drošības ziņošanas sistēmu, kas atbilst Regulā (ES) Nr. 376/2014 un tās deleģētajos un īstenošanas aktos noteiktajām prasībām, ja minētā regula ir piemērojama organizācijai.

b) Neskarot Regulā (ES) Nr. 376/2014 noteiktos pienākumus, organizācija nodrošina, ka par visiem informācijas drošības incidentiem un ievainojamībām, kas var radīt būtisku risku aviācijas drošumam, tiek ziņots tās kompetentajai iestādei. Turklāt:

1) ja šāds incidents vai ievainojamība ietekmē gaisa kuģi vai ar to saistītu sistēmu vai sastāvdaļu, organizācija par to ziņo arī projekta apstiprinājuma turētājam;

2) ja šāds incidents vai ievainojamība ietekmē organizācijas izmantotu sistēmu vai sastāvdaļu, organizācija par to ziņo organizācijai, kas atbild par sistēmas vai sastāvdaļas projektēšanu.

c) Organizācija par b) apakšpunktā minētajiem apstākļiem ziņo šādi:

1) tiklīdz organizācija ir uzzinājusi par apstākli, tā iesniedz paziņojumu kompetentajai iestādei un attiecīgā gadījumā projekta apstiprinājuma turētājam vai organizācijai, kas atbild par sistēmas vai sastāvdaļas projektēšanu;

2) ja vien ārkārtas apstākļi to neliedz, cik drīz vien iespējams, bet ne vēlāk kā 72 stundas pēc tam, kad organizācija ir uzzinājusi par apstākli, tā iesniedz ziņojumu kompetentajai iestādei un attiecīgā gadījumā projekta apstiprinājuma turētājam vai organizācijai, kas atbild par sistēmas vai sastāvdaļas projektēšanu.

Ziņojumu sagatavo kompetentās iestādes noteiktā formā, un tajā iekļauj visu attiecīgo informāciju par apstākli, kas zināma organizācijai;

3) iesniedz paveiktā darba pārbaudes ziņojumu kompetentajai iestādei un attiecīgā gadījumā projekta apstiprinājuma turētājam vai organizācijai, kas atbild par sistēmas vai sastāvdaļas projektēšanu, ziņojumā sīki izklāstot informāciju par darbībām, ko organizācija ir veikusi vai plāno veikt, lai novērstu incidenta sekas, un par darbībām, ko tā plāno veikt, lai nākotnē novērstu līdzīgus informācijas drošības incidentus.

Paveiktā darba pārbaudes ziņojumu iesniedz, tiklīdz minētās darbības ir noteiktas, un to sagatavo kompetentās iestādes noteiktā formā.

IS.I.OR.235. Informācijas drošības pārvaldības darbību līguma slēgšana

a) Ja organizācija noslēdz līgumu ar citām organizācijām par kādu daļu no IS.I.OR.200. punktā minētajām darbībām, organizācija nodrošina, ka darbības, par kurām noslēgts līgums, atbilst šīs regulas prasībām un ka nolīgtā organizācija darbojas tās uzraudzībā. Organizācija nodrošina, ka riski, kas saistīti ar darbībām, par kurām noslēgts līgums, tiek pienācīgi pārvaldīti.

b) Organizācija nodrošina, ka kompetentajai iestādei pēc pieprasījuma tiek dota piekļuve nolīgtajai organizācijai, lai kompetentā iestāde varētu pārliecināties par pastāvīgu atbilstību piemērojamajām prasībām, kas noteiktas šajā regulā.

IS.I.OR.240. Prasības personālam

a) Organizācijas atbildīgajam vadītājam, kas norīkots saskaņā ar Regulām (ES) Nr. 1321/2014, (ES) Nr. 965/2012, (ES) Nr. 1178/2011, (ES) 2015/340, Īstenošanas regulu (ES) 2017/373 vai Īstenošanas regulu (ES) 2021/664, ko piemēro, kā minēts šīs regulas 2. panta 1. punktā, ir organizācijas dotas pilnvaras nodrošināt, ka visas šajā regulā paredzētās darbības ir iespējams finansēt un veikt. Minētā persona:

1) nodrošina, ka ir pieejami visi šīs regulas prasību izpildei vajadzīgie resursi;

2) izveido informācijas drošības politiku, kas minēta IS.I.OR.200. punkta a) apakšpunkta 1. punktā, un veicina tās īstenošanu;

3) pierāda pamatizpratni par šo regulu.

b) Atbildīgais vadītājs ieceļ personu vai personu grupu, kas nodrošina, ka organizācija atbilst šīs regulas prasībām, un nosaka viņu pilnvaru apjomu. Minētā persona vai personu grupa ir tieši pakļauta atbildīgajam vadītājam, un tai ir pienākumu izpildei atbilstošas zināšanas, agrāka darbība un pieredze. Procedūrās nosaka, kas aizvieto konkrētu personu tās ilgstošas prombūtnes laikā.

c) Atbildīgais vadītājs ieceļ personu vai personu grupu, kas atbild par IS.I.OR.200. punkta a) apakšpunkta 12. punktā minētās atbilstības uzraudzības funkcijas pārvaldību.

d) Ja organizācijas informācijas drošības organizatoriskās struktūras, politika, procesi un procedūras ir kopīgas ar citām organizācijām vai savas organizācijas jomām, kas nav apstiprinājuma vai deklarācijas daļa, atbildīgais vadītājs var deleģēt savas darbības kopīgai atbildīgajai personai.

Lai nodrošinātu informācijas drošības pārvaldības pienācīgu integrāciju organizācijā, šādā gadījumā nosaka pasākumus koordinācijai starp organizācijas atbildīgo vadītāju un kopīgo atbildīgo personu.

e) Atbildīgajam vadītājam vai d) apakšpunktā minētajai kopīgajai atbildīgajai personai ir organizācijas dotas pilnvaras izveidot un uzturēt IS.I.OR.200. punkta īstenošanai vajadzīgās organizatoriskās struktūras, politiku, procesus un procedūras.

f) Organizācijā ir ieviests process, ar ko nodrošināt, ka tai pietiek dežurējošo darbinieku šajā pielikumā izklāstīto darbību veikšanai.

g) Organizācijā ir ieviests process, ar ko nodrošināt, ka f) apakšpunktā minētajiem darbiniekiem ir savu uzdevumu veikšanai vajadzīgā kompetence.

h) Organizācijā ir ieviests process, ar ko nodrošināt, ka darbinieki atzīst pienākumus, kas saistīti ar tiem uzticētajām funkcijām un uzdevumiem.

i) Organizācija nodrošina, ka tiek pienācīgi noteikta to darbinieku identitāte un uzticamība, kuriem ir piekļuve informācijas sistēmām un datiem, uz ko attiecas šīs regulas prasības.

IS.I.OR.245. Reģistrācija

a) *Organizācija reģistrē savas informācijas drošības pārvaldības darbības.*

1) Organizācija nodrošina, ka ir arhivēti un izsekojami šādi ieraksti:

i) visi saņemtie apstiprinājumi un visi saistītie informācijas drošības riska novērtējumi saskaņā ar IS.I.OR.200. punkta e) apakšpunktu;

ii) līgumi par darbībām, kas minēti IS.I.OR.200. punkta a) apakšpunkta 9. punktā;

iii) ieraksti par galvenajiem procesiem, kas minēti IS.I.OR.200. punkta d) apakšpunktā;

iv) ieraksti par IS.I.OR.205. punktā minētajā riska novērtējumā identificētajiem riskiem kopā ar saistītajiem IS.I.OR.210. punktā minētajiem riska risināšanas pasākumiem;

v) ieraksti par informācijas drošības incidentiem un ievainojamībām, par ko ziņots saskaņā ar IS.I.OR.215. un IS.I.OR.230. punktā minētajām ziņošanas sistēmām;

vi) ieraksti par informācijas drošības notikumiem, kuri varētu būt jāizvērtē atkārtoti, lai atklātu vēl neatklātus informācijas drošības incidentus vai ievainojamības.

2) Ierakstus, kas minēti 1. punkta i) apakšpunktā, glabā vismaz 5 gadus pēc tam, kad apstiprinājums ir zaudējis derīgumu.

3) Ierakstus, kas minēti 1. punkta ii) apakšpunktā, glabā vismaz 5 gadus pēc tam, kad līgums ir grozīts vai izbeigts.

4) Ierakstus, kas minēti 1. punkta iii), iv) un v) apakšpunktā, glabā vismaz 5 gadus.

5) Ierakstus, kas minēti 1. punkta vi) apakšpunktā, glabā tik ilgi, līdz šie informācijas drošības notikumi ir atkārtoti izvērtēti saskaņā ar organizācijas izveidotā procedūrā noteiktu periodiskumu.

b) *Organizācija reģistrē savu informācijas drošības pārvaldības darbībās iesaistīto darbinieku kvalifikāciju un pieredzi.*

1) Ierakstus par darbinieka kvalifikāciju un pieredzi glabā tik ilgi, kamēr persona strādā organizācijā, un vismaz 3 gadus pēc tam, kad persona ir aizgājusi no darba organizācijā.

2) Darbiniekiem pēc pieprasījuma dod piekļuvi viņu individuālajiem datiem. Turklāt pēc darbinieka pieprasījuma organizācija darbiniekam izsniedz viņa individuālo datu kopiju, kad darbinieks aiziet no darba organizācijā.

c) Ierakstu formātu nosaka organizācijas procedūrās.

d) Ierakstus information being identified, when required, according to its security classification level. glabā veidā, kas nodrošina aizsardzību pret bojājumiem, pārveidošanu un zādzību, vajadzības gadījumā informāciju identificējot atbilstīgi tās drošības klasifikācijas līmenim. Organizācija nodrošina, ka ierakstus glabā, izmantojot līdzekļus, kas nodrošina integritāti, autentiskumu un atļautu piekļuvi.

IS.I.OR.250. Informācijas drošības pārvaldības rokasgrāmata (IDPR)

a) Organizācija kompetentajai iestādei dara pieejamu informācijas drošības pārvaldības rokasgrāmatu (IDPR) un attiecīgā gadījumā visas saistītās rokasgrāmatas un procedūras, uz kurām ir sniegtas atsauces, un rokasgrāmatā ir:

1) atbildīgā vadītāja parakstīts apliecinājums par to, ka organizācija savā darbībā vienmēr ievēros šā pielikuma un IDPR prasības. Ja atbildīgais vadītājs nav organizācijas izpilddirektors, tad izpilddirektors apstiprina šo apliecinājumu ar savu parakstu;

2) IS.I.OR.240. punkta b) un c) apakšpunktā minētās personas vai minēto personu amats, vārds un uzvārds, pienākumi, pakļautība, atbildība un pilnvaras;

3) attiecīgā gadījumā IS.I.OR.240. punkta d) apakšpunktā minētās kopīgās atbildīgās personas amats, vārds un uzvārds, pienākumi, pakļautība, atbildība un pilnvaras;

4) organizācijas informācijas drošības politika, kas minēta IS.I.OR.200. punkta a) apakšpunkta 1. punktā;

5) vispārīgs apraksts par darbinieku skaitu un kategorijām un par sistēmu, kas ieviesta personāla pieejamības plānošanai, kā prasīts IS.I.OR.240. punktā;

6) galveno personu, kas atbild par IS.I.OR.200. punkta īstenošanu, tostarp personas vai personu, kas atbild par IS.I.OR.200. punkta a) apakšpunkta 12. punktā minēto atbilstības uzraudzības funkciju, amats, vārds un uzvārds, pienākumi, pakļautība, atbildība un pilnvaras;

7) struktūrshēma, kurā parādītas ar 2. un 6. punktā minētajām personām saistītās pakļautības un atbildības ķēdes;

8) IS.I.OR.215. punktā minētās iekšējās ziņošanas sistēmas apraksts;

9) procedūras, kas precizē, kā organizācija nodrošina atbilstību šai daļai, un jo īpaši:

i) IS.I.OR.200. punkta c) apakšpunktā minētā dokumentācija;

ii) procedūras, kas nosaka, kā organizācija kontrolē visas IS.I.OR.200. punkta a) apakšpunkta 9. punktā minētās darbības, par kurām noslēgts līgums;

iii) IDPR grozījumu procedūra, kas minēta c) apakšpunktā;

10) sīka informācija par pašreizējiem apstiprinātajiem alternatīvajiem atbilstības nodrošināšanas līdzekļiem.

b) Kompetentā iestāde apstiprina IDPR sākotnējo izdevumu un saglabā tās eksemplāru. IDPR vajadzības gadījumā groza, lai organizācijas IDPS apraksts vienmēr būtu atjaunināts. Visu IDPR grozījumu eksemplāru iesniedz kompetentajai iestādei.

c) IDPR grozījumus pārvalda saskaņā ar organizācijas izveidotu procedūru. Visus grozījumus, kas nav iekļauti šīs procedūras darbības jomā, un visus grozījumus, kas saistīti ar IS.I.OR.255. punkta b) apakšpunktā minētajām izmaiņām, apstiprina kompetentā iestāde.

d) Organizācija IDPR var integrēt ar citiem tās rīcībā esošiem pārvaldības pašraksturojumiem vai rokasgrāmatām, ja ir dota skaidra savstarpēja atsauce, kas norāda, kuras pārvaldības pašraksturojuma vai rokasgrāmatas daļas atbilst dažādām šajā pielikumā ietvertajām prasībām.

IS.I.OR.255. Informācijas drošības pārvaldības sistēmas izmaiņas

a) IDPS izmaiņas var pārvaldīt un paziņot kompetentajai iestādei saskaņā ar organizācijas izstrādātu procedūru. Šo procedūru apstiprina kompetentā iestāde.

b) Attiecībā uz IDPS izmaiņām, uz kurām neattiecas a) apakšpunktā minētā procedūra, organizācija iesniedz pieteikumu un saņem kompetentās iestādes dotu apstiprinājumu.

Attiecībā uz šīm izmaiņām:

1) pirms šādu izmaiņu veikšanas iesniedz pieteikumu, lai kompetentajai iestādei dotu iespēju pārliecināties par pastāvīgu atbilstību šai regulai un vajadzības gadījumā grozīt organizācijas sertifikātu un tam pievienotos attiecīgos apstiprinājuma noteikumus;

2) organizācija kompetentajai iestādei dara pieejamu visu informāciju, ko tā pieprasa izmaiņu izvērtēšanai;

3) izmaiņas īsteno tikai pēc kompetentās iestādes oficiāla apstiprinājuma saņemšanas;

4) kamēr šādas izmaiņas tiek ieviestas, organizācija darbojas saskaņā ar nosacījumiem, ko noteikusi kompetentā iestāde.

IS.I.OR.260. Pastāvīgi uzlabojumi

a) Organizācija, izmantojot atbilstīgus darbības rādītājus, novērtē IDPS efektivitāti un gatavību. Minēto novērtēšanu veic, pamatojoties uz organizācijas iepriekšnoteiktu kalendāro grafiku vai pēc informācijas drošības incidenta.

b) Ja pēc novērtēšanas, kas veikta saskaņā ar a) apakšpunktu, tiek konstatēti trūkumi, organizācija īsteno uzlabošanas pasākumus, kuri vajadzīgi, lai nodrošinātu, ka IDPS joprojām atbilst piemērojamajām prasībām un uztur informācijas drošības riskus pieņemamā līmenī. Turklāt organizācija atkārtoti izvērtē tos IDPS elementus, kurus ietekmē pieņemtie pasākumi.

III PIELIKUMS

Regulas (ES) Nr. 1178/2011 VI pielikumu (ARA daļu) un VII pielikumu (ORA daļu) groza šādi:

1) regulas VI pielikumu (ARA daļu) groza šādi:

a) ARA.GEN.125. punktam pievieno šādu c) apakšpunktu:

"c) Dalībvalsts kompetentā iestāde pēc iespējas ātrāk sniedz Aģentūrai drošuma ziņā svarīgo informāciju, kas izriet no informācijas drošības ziņojumiem, kurus tā saņēmusi saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.230. punktu.";

b) aiz ARA.GEN.135. punkta iekļauj šādu ARA.GEN.135.A punktu:

"**ARA.GEN.135.A Tūlītēja reakcija uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu**

a) Kompetentā iestāde ievieš sistēmu, kas nepieciešama, lai pienācīgi vāktu, analizētu un izplatītu organizāciju paziņoto informāciju, kura saistīta ar informācijas drošības incidentiem un ievainojamībām, kas spēj ietekmēt aviācijas drošumu. To veic, saskaņojot ar visām citām attiecīgajām iestādēm, kas ir atbildīgas par informācijas drošību vai kiberdrošību dalībvalstī, lai sekmētu ziņošanas sistēmu koordināciju un saderību.

b) Aģentūra ievieš sistēmu, kura nepieciešama, lai pienācīgi analizētu visu attiecīgo drošuma ziņā svarīgo informāciju, kas saņemta saskaņā ar ARA.GEN.125. punkta c) apakšpunktu, un bez nepamatotas kavēšanās sniedz dalībvalstīm un Komisijai visu informāciju, tajā skaitā par ieteikumiem vai veicamajiem korektīvajiem pasākumiem, kura tām nepieciešama, lai laikus reaģētu uz informācijas drošības incidentu vai ievainojamību, kas spēj ietekmēt aviācijas drošumu, tajā skaitā saistībā ar ražojumiem, daļām, neuzstādītām ierīcēm, personām vai organizācijām, uz kurām attiecas Regula (ES) 2018/1139 un tās deleģētie un īstenošanas akti.

c) Pēc a) un b) apakšpunktā minētās informācijas saņemšanas kompetentā iestāde veic attiecīgus pasākumus, kuri nepieciešami, lai novērstu informācijas drošības incidenta vai ievainojamības iespējamo ietekmi uz aviācijas drošumu.

d) Par pasākumiem, kas veikti saskaņā ar c) apakšpunktu, nekavējoties paziņo visām personām vai organizācijām, kurām jānodrošina atbilstība šiem pasākumiem saskaņā ar Regulu (ES) 2018/1139 un tās deleģētajiem un īstenošanas aktiem. Dalībvalsts kompetentā iestāde par šiem pasākumiem informē arī Aģentūru un, ja nepieciešama kopīga rīcība, arī citu iesaistīto dalībvalstu kompetentās iestādes.";

c) pielikuma ARA.GEN.200. punktam pievieno šādu e) apakšpunktu:

"e) Lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu, pārvaldības sistēma, ko izveido un uztur kompetentā iestāde, atbilst ne tikai a) apakšpunktā noteiktajām prasībām, bet arī Īstenošanas regulas (ES) 2023/203 I pielikumam (IS.AR daļai).";

d) pielikuma ARA.GEN.205. punktu groza šādi:

i) virsrakstu aizstāj ar šādu:

"**ARA.GEN.205 Uzdevumu sadale**";

ii) pievieno šādu c) apakšpunktu:

"c) Attiecībā uz organizācijas atbilstības ORA.GEN.200.A punktam sertificēšanu un uzraudzību kompetentā iestāde var piešķirt uzdevumus kvalificētajām vienībām saskaņā ar a) apakšpunktu vai jebkurai attiecīgajai iestādei, kas atbild par informācijas drošību vai kiberdrošību dalībvalstī. Uzdevumu sadalē kompetentā iestāde nodrošina, ka:

1) kvalificētā vienība vai attiecīgā iestāde koordinē un ņem vērā visus ar aviācijas drošumu saistītos aspektus;

2) kvalificētās vienības vai attiecīgās iestādes veikto sertificēšanas un uzraudzības darbību rezultāti ir iekļauti organizācijas vispārējos sertificēšanas un uzraudzības dokumentos;

3) tās informācijas drošības pārvaldības sistēma, kas izveidota saskaņā ar ARA.GEN.200. punkta e) apakšpunktu, aptver visus tās vārdā veiktos sertificēšanas un pastāvīgās uzraudzības uzdevumus.";

e) pielikuma ARA.GEN.300. punktam pievieno šādu g) apakšpunktu:

"g) Attiecībā uz organizācijas atbilstības ORA.GEN.200.A punktam sertificēšanu un uzraudzību kompetentā iestāde papildus a) līdz f) apakšpunkta ievērošanai pārskata visus apstiprinājumus, kas piešķirti saskaņā ar šīs regulas IS.I.OR.200. punkta e) apakšpunktu vai Deleģētās regulas (ES) 2022/1645 IS.D.OR.200. punkta e) apakšpunktu, pēc piemērojamā pārraudzības revīzijas cikla un ikreiz, kad tiek ieviestas izmaiņas organizācijas darbības jomā.";

f) aiz ARA.GEN.330. punkta iekļauj šādu ARA.GEN.330.A punktu:

"**ARA.GEN.330.A Informācijas drošības pārvaldības sistēmas izmaiņas**

a) Attiecībā uz izmaiņām, kas pārvaldītas un paziņotas kompetentajai iestādei saskaņā ar procedūru, kura noteikta Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta a) apakšpunktā, kompetentā iestāde iekļauj šādu izmaiņu pārbaudi savā pastāvīgajā uzraudzībā saskaņā ar ARA.GEN.300. punktā norādītajiem principiem. Ja tiek konstatēta neatbilstība, kompetentā iestāde informē par to organizāciju, pieprasa veikt papildu izmaiņas un rīkojas saskaņā ar ARA.GEN.350. punktu.

b) Attiecībā uz citām izmaiņām, kam nepieciešams apstiprināšanas pieteikums saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta b) apakšpunktu:

1) saņēmusi pieteikumu par izmaiņām, kompetentā iestāde pirms apstiprinājuma izdošanas pārbauda organizācijas atbilstību piemērojamajām prasībām;

2) kompetentā iestāde nosaka nosacījumus, saskaņā ar kuriem organizācija var darboties izmaiņu ieviešanas laikā;

3) ja kompetentā iestāde ir pārliecināta, ka organizācija atbilst piemērojamajām prasībām, tā apstiprina izmaiņas.";

2) regulas VII pielikumu (ORA daļu) groza šādi:

aiz ORA.GEN.200. punkta iekļauj šādu ORA.GEN.200.A punktu:

"**ORA.GEN.200.A Informācijas drošības pārvaldības sistēma**

Papildus ORA.GEN.200. punktā noteiktajai pārvaldības sistēmai organizācija izveido, īsteno un uztur informācijas drošības pārvaldības sistēmu saskaņā ar Īstenošanas regulu (ES) 2023/203, lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu."

IV PIELIKUMS

Regulas (ES) Nr. 748/2012 I pielikumu (21. daļu) groza šādi:

1) satura rādītāju groza šādi:

a) aiz 21.B.20. punkta virsraksta iekļauj šādu virsrakstu:

"21.B.20.A Tūlītēja reakcija uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu";

b) pielikuma 21.B.30. punkta virsrakstu aizstāj ar šādu:

"21.B.30. Uzdevumu sadale";

c) aiz 21.B.240. punkta virsraksta iekļauj šādu virsrakstu:

"21.B.240.A Informācijas drošības pārvaldības sistēmas izmaiņas";

d) aiz 21.B.435. punkta virsraksta iekļauj šādu virsrakstu:

"21.B.435.A Informācijas drošības pārvaldības sistēmas izmaiņas";

2) pielikuma 21.B.15. punktam pievieno šādu c) apakšpunktu:

"c) Dalībvalsts kompetentā iestāde pēc iespējas ātrāk sniedz Aģentūrai drošuma ziņā svarīgo informāciju, kas izriet no informācijas drošības ziņojumiem, kurus tā saņēmusi saskaņā ar Deleģētās regulas (ES) 2022/1645 pielikuma (IS.D.OR daļas) IS.D.OR.230. punktu.";

3) aiz 21.B.20. punkta iekļauj šādu 21.B.20.A punktu:

"**21.B.20.A Tūlītēja reakcija uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu**

a) Kompetentā iestāde ievieš sistēmu, kas nepieciešama, lai pienācīgi vāktu, analizētu un izplatītu organizāciju paziņoto informāciju, kura saistīta ar informācijas drošības incidentiem un ievainojamībām, kas spēj ietekmēt aviācijas drošumu. To veic, saskaņojot ar visām citām attiecīgajām iestādēm, kas ir atbildīgas par informācijas drošību vai kiberdrošību dalībvalstī, lai sekmētu ziņošanas sistēmu koordināciju un saderību.

b) Aģentūra ievieš sistēmu, kura nepieciešama, lai pienācīgi analizētu visu attiecīgo drošuma ziņā svarīgo informāciju, kas saņemta saskaņā ar 21.B.15. punkta c) apakšpunktu, un bez nepamatotas kavēšanās sniedz dalībvalstīm un Komisijai visu informāciju, tajā skaitā par ieteikumiem vai veicamajiem korektīvajiem pasākumiem, kura tām nepieciešama, lai laikus reaģētu uz informācijas drošības incidentu vai ievainojamību, kas spēj ietekmēt aviācijas drošumu, tajā skaitā saistībā ar ražojumiem, daļām, neuzstādītām ierīcēm, personām vai organizācijām, uz kurām attiecas Regula (ES) 2018/1139 un tās deleģētie un īstenošanas akti.

c) Pēc a) un b) apakšpunktā minētās informācijas saņemšanas kompetentā iestāde veic attiecīgus pasākumus, kuri nepieciešami, lai novērstu informācijas drošības incidenta vai ievainojamības iespējamo ietekmi uz aviācijas drošumu.

d) Par pasākumiem, kas veikti saskaņā ar c) apakšpunktu, nekavējoties paziņo visām personām vai organizācijām, kurām jānodrošina atbilstība šiem pasākumiem saskaņā ar Regulu (ES) 2018/1139 un tās deleģētajiem un īstenošanas aktiem. Dalībvalsts kompetentā iestāde par šiem pasākumiem informē arī Aģentūru un, ja nepieciešama kopīga rīcība, arī citu iesaistīto dalībvalstu kompetentās iestādes.";

4) pielikuma 21.B.25. punktam pievieno šādu e) apakšpunktu:

"e) Lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu, pārvaldības sistēma, ko izveido un uztur kompetentā iestāde, atbilst ne tikai a) apakšpunktā noteiktajām prasībām, bet arī Īstenošanas regulas (ES) 2023/203 I pielikumam (IS.AR daļai).";

5) pielikuma 21.B.30. punktu groza šādi:

a) virsrakstu aizstāj ar šādu:

"**21.B.30. Uzdevumu sadale";**

b) pievieno šādu c) apakšpunktu:

"c) Attiecībā uz organizācijas atbilstības 21.A.139.A un 21.A.239.A punktam sertificēšanu un uzraudzību kompetentā iestāde var piešķirt uzdevumus kvalificētajām vienībām saskaņā ar a) apakšpunktu vai jebkurai attiecīgajai iestādei, kas atbild par informācijas drošību vai kiberdrošību dalībvalstī. Uzdevumu sadalē kompetentā iestāde nodrošina, ka:

1) kvalificētā vienība vai attiecīgā iestāde koordinē un ņem vērā visus ar aviācijas drošumu saistītos aspektus;

2) kvalificētās vienības vai attiecīgās iestādes veikto sertificēšanas un uzraudzības darbību rezultāti ir iekļauti organizācijas vispārējos sertificēšanas un uzraudzības dokumentos;

3) tās informācijas drošības pārvaldības sistēma, kas izveidota saskaņā ar 21.B.25. punkta e) apakšpunktu, aptver visus tās vārdā veiktos sertificēšanas un pastāvīgās uzraudzības uzdevumus.";

6) pielikuma 21.B.221. punktam pievieno šādu g) apakšpunktu:

"g) Attiecībā uz organizācijas atbilstības 21.A.139.A punktam sertificēšanu un uzraudzību kompetentā iestāde papildus a) līdz f) apakšpunkta ievērošanai pārskata visus apstiprinājumus, kas piešķirti saskaņā ar šīs regulas IS.I.OR.200. punkta e) apakšpunktu vai Deleģētās regulas (ES) 2022/1645 IS.D.OR.200. punkta e) apakšpunktu, pēc piemērojamā pārraudzības revīzijas cikla un ikreiz, kad tiek ieviestas izmaiņas organizācijas darbības jomā.";

7) aiz 21.B.240. punkta iekļauj šādu 21.B.240.A punktu:

"**21.B.240.A Informācijas drošības pārvaldības sistēmas izmaiņas**

a) Attiecībā uz izmaiņām, kas pārvaldītas un paziņotas kompetentajai iestādei saskaņā ar procedūru, kura noteikta Deleģētās regulas (ES) 2022/1645 pielikuma (IS.D.OR daļas) IS.D.OR.255. punkta a) apakšpunktā, kompetentā iestāde iekļauj šādu izmaiņu pārbaudi savā pastāvīgajā uzraudzībā saskaņā ar 21.B.221. punktā norādītajiem principiem. Ja tiek konstatēta neatbilstība, kompetentā iestāde informē par to organizāciju, pieprasa veikt papildu izmaiņas un rīkojas saskaņā ar 21.B.225. punktu.

b) Attiecībā uz citām izmaiņām, kam nepieciešams apstiprināšanas pieteikums saskaņā ar Deleģētās regulas (ES) 2022/1645 pielikuma (IS.D.OR daļas) IS.D.OR.255. punkta b) apakšpunktu:

1) saņēmusi pieteikumu par izmaiņām, kompetentā iestāde pirms apstiprinājuma izdošanas pārbauda organizācijas atbilstību piemērojamajām prasībām;

2) kompetentā iestāde nosaka nosacījumus, saskaņā ar kuriem organizācija var darboties izmaiņu ieviešanas laikā;

3) ja kompetentā iestāde ir pārliecināta, ka organizācija atbilst piemērojamajām prasībām, tā apstiprina izmaiņas.";

8) pielikuma 21.B.431. punktam pievieno šādu d) apakšpunktu:

"d) Attiecībā uz organizācijas atbilstības 21.A.239.A punktam sertificēšanu un uzraudzību kompetentā iestāde papildus a) līdz c) apakšpunkta ievērošanai arī ievēro šādus principus:

1) kompetentā iestāde pārbauda saskarnes un saistītos riskus, ko saskaņā ar Deleģētās regulas (ES) 2022/1645 pielikuma (IS.D.OR daļas) IS.D.OR.205. punkta b) apakšpunktu ir noteikusi katra organizācija, kuru tā uzrauga;

2) ja tiek konstatētas neatbilstības savstarpējās saskarnēs un saistītajos riskos, ko noteikušas dažādas organizācijas, kompetentā iestāde tās pārskata kopā ar ietekmētajām organizācijām un, ja nepieciešams, veic attiecīgus konstatējumus, lai nodrošinātu korektīvo pasākumu īstenošanu;

3) ja dokumentācija, kas pārskatīta saskaņā ar 2. punktu, atklāj būtiskus riskus attiecībā uz saskarnēm ar organizācijām, kuras tajā pašā dalībvalstī uzrauga cita kompetentā iestāde, šo informāciju paziņo attiecīgajai kompetentajai iestādei.";

9) aiz 21.B.435. punkta iekļauj šādu 21.B.435.A punktu:

"**21.B.435.A Informācijas drošības pārvaldības sistēmas izmaiņas**

a) Attiecībā uz izmaiņām, kas pārvaldītas un paziņotas kompetentajai iestādei saskaņā ar procedūru, kura noteikta Deleģētās regulas (ES) 2022/1645 pielikuma (IS.D.OR daļas) IS.D.OR.255. punkta a) apakšpunktā, kompetentā iestāde iekļauj šādu izmaiņu pārbaudi savā pastāvīgajā uzraudzībā saskaņā ar 21.B.431. punktā norādītajiem principiem. Ja tiek konstatēta neatbilstība, kompetentā iestāde informē par to organizāciju, pieprasa veikt papildu izmaiņas un rīkojas saskaņā ar 21.B.433. punktu.

b) Attiecībā uz citām izmaiņām, kam nepieciešams apstiprināšanas pieteikums saskaņā ar Deleģētās regulas (ES) 2022/1645 pielikuma (IS.D.OR daļas) IS.D.OR.255. punkta b) apakšpunktu:

1) saņēmusi pieteikumu par izmaiņām, kompetentā iestāde pirms apstiprinājuma izdošanas pārbauda organizācijas atbilstību piemērojamajām prasībām;

2) kompetentā iestāde nosaka nosacījumus, saskaņā ar kuriem organizācija var darboties izmaiņu ieviešanas laikā;

3) ja kompetentā iestāde ir pārliecināta, ka organizācija atbilst piemērojamajām prasībām, tā apstiprina izmaiņas."

V PIELIKUMS

Regulas (ES) Nr. 965/2012 II pielikumu (*Part-ARO*) un III pielikumu (*Part-ORO*) groza šādi:

1) regulas II pielikumu (*Part-ARO*) groza šādi:

a) ARO.GEN.125. punktam pievieno šādu c) apakšpunktu:

"c) Dalībvalsts kompetentā iestāde pēc iespējas ātrāk sniedz Aģentūrai drošuma ziņā svarīgo informāciju, kas izriet no informācijas drošības ziņojumiem, kurus tā saņēmusi saskaņā ar Īstenošanas regulas (ES) 2023/203 5 II pielikuma (IS.I.OR daļas) IS.I.OR.230. punktu.";

b) aiz ARO.GEN.135. punkta iekļauj šādu ARO.GEN.135.A punktu:

"**ARO.GEN.135.A Tūlītēja reakcija uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu**

a) Kompetentā iestāde ievieš sistēmu, kas nepieciešama, lai pienācīgi vāktu, analizētu un izplatītu organizāciju paziņoto informāciju, kura saistīta ar informācijas drošības incidentiem un ievainojamībām, kas spēj ietekmēt aviācijas drošumu. To veic, saskaņojot ar visām citām attiecīgajām iestādēm, kas ir atbildīgas par informācijas drošību vai kiberdrošību dalībvalstī, lai sekmētu ziņošanas sistēmu koordināciju un saderību.

b) Aģentūra ievieš sistēmu, kura nepieciešama, lai pienācīgi analizētu visu attiecīgo drošuma ziņā svarīgo informāciju, kas saņemta saskaņā ar ARO.GEN.125. punkta c) apakšpunktu, un bez nepamatotas kavēšanās sniedz dalībvalstīm un Komisijai visu informāciju, tajā skaitā par ieteikumiem vai veicamajiem korektīvajiem pasākumiem, kura tām nepieciešama, lai laikus reaģētu uz informācijas drošības incidentu vai ievainojamību, kas spēj ietekmēt aviācijas drošumu, tajā skaitā saistībā ar ražojumiem, daļām, neuzstādītām ierīcēm, personām vai organizācijām, uz kurām attiecas Regula (ES) 2018/1139 un tās deleģētie un īstenošanas akti.

c) Pēc a) un b) apakšpunktā minētās informācijas saņemšanas kompetentā iestāde veic attiecīgus pasākumus, kuri nepieciešami, lai novērstu informācijas drošības incidenta vai ievainojamības iespējamo ietekmi uz aviācijas drošumu.

d) Par pasākumiem, kas veikti saskaņā ar c) apakšpunktu, nekavējoties paziņo visām personām vai organizācijām, kurām jānodrošina atbilstība šiem pasākumiem saskaņā ar Regulu (ES) 2018/1139 un tās deleģētajiem un īstenošanas aktiem. Dalībvalsts kompetentā iestāde par šiem pasākumiem informē arī Aģentūru un, ja nepieciešama kopīga rīcība, arī citu iesaistīto dalībvalstu kompetentās iestādes.";

c) pielikuma ARO.GEN.200. punktam pievieno šādu e) apakšpunktu:

"e) Lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu, pārvaldības sistēma, ko izveido un uztur kompetentā iestāde, atbilst ne tikai a) apakšpunktā noteiktajām prasībām, bet arī Īstenošanas regulas (ES) 2023/203 I pielikumam (IS.AR daļai).";

d) pielikuma ARO.GEN.205. punktu groza šādi:

i) virsrakstu aizstāj ar šādu:

"**ARO.GEN.205. Uzdevumu sadale**";

ii) pievieno šādu c) apakšpunktu:

"c) Attiecībā uz organizācijas atbilstības ORO.GEN.200.A punktam sertificēšanu un uzraudzību kompetentā iestāde var piešķirt uzdevumus kvalificētajām vienībām saskaņā ar a) apakšpunktu vai jebkurai attiecīgajai iestādei, kas atbild par informācijas drošību vai kiberdrošību dalībvalstī. Uzdevumu sadalē kompetentā iestāde nodrošina, ka:

1) kvalificētā vienība vai attiecīgā iestāde koordinē un ņem vērā visus ar aviācijas drošumu saistītos aspektus;

2) kvalificētās vienības vai attiecīgās iestādes veikto sertificēšanas un uzraudzības darbību rezultāti ir iekļauti organizācijas vispārējos sertificēšanas un uzraudzības dokumentos;

3) tās informācijas drošības pārvaldības sistēma, kas izveidota saskaņā ar ARO.GEN.200. punkta e) apakšpunktu, aptver visus tās vārdā veiktos sertificēšanas un pastāvīgās uzraudzības uzdevumus.";

e) pielikuma ARO.GEN.300. punktam pievieno šādu g) apakšpunktu:

"g) Attiecībā uz organizācijas atbilstības ORO.GEN.200.A punktam sertificēšanu un uzraudzību kompetentā iestāde papildus a) līdz f) apakšpunkta ievērošanai pārskata visus apstiprinājumus, kas piešķirti saskaņā ar šīs regulas IS.I.OR.200. punkta e) apakšpunktu vai Deleģētās regulas (ES) 2022/1645 IS.D.OR.200. punkta e) apakšpunktu, pēc piemērojamā pārraudzības revīzijas cikla un ikreiz, kad tiek ieviestas izmaiņas organizācijas darbības jomā.";

f) aiz ARO.GEN.330. punkta iekļauj šādu ARO.GEN.330.A punktu:

"**ARO.GEN.330.A Informācijas drošības pārvaldības sistēmas izmaiņas**

a) Attiecībā uz izmaiņām, kas pārvaldītas un paziņotas kompetentajai iestādei saskaņā ar procedūru, kura noteikta Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta a) apakšpunktā, kompetentā iestāde iekļauj šādu izmaiņu pārbaudi savā pastāvīgajā uzraudzībā saskaņā ar ARO.GEN.300. punktā norādītajiem principiem. Ja tiek konstatēta neatbilstība, kompetentā iestāde informē par to organizāciju, pieprasa veikt papildu izmaiņas un rīkojas saskaņā ar ARO.GEN.350. punktu.

b) Attiecībā uz citām izmaiņām, kam nepieciešams apstiprināšanas pieteikums saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta b) apakšpunktu:

1) saņēmusi pieteikumu par izmaiņām, kompetentā iestāde pirms apstiprinājuma izdošanas pārbauda organizācijas atbilstību piemērojamajām prasībām;

2) kompetentā iestāde nosaka nosacījumus, saskaņā ar kuriem organizācija var darboties izmaiņu ieviešanas laikā;

3) ja kompetentā iestāde ir pārliecināta, ka organizācija atbilst piemērojamajām prasībām, tā apstiprina izmaiņas.";

2) regulas III pielikumu (*Part-ORO*) groza šādi:

aiz ORO.GEN.200. punkta iekļauj šādu ORO.GEN.200.A punktu:

"**ORO.GEN.200.A Informācijas drošības pārvaldības sistēma**

Papildus ORO.GEN.200. punktā noteiktajai pārvaldības sistēmai operators izveido, īsteno un uztur informācijas drošības pārvaldības sistēmu saskaņā ar Īstenošanas regulu (ES) 2023/203, lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu."

VI PIELIKUMS

Regulas (ES) Nr. 139/2014 II pielikumu (*Part-ADR.AR*) groza šādi:

1) ADR.AR.A.025. punktam pievieno šādu c) apakšpunktu:

"c) Dalībvalsts kompetentā iestāde pēc iespējas ātrāk sniedz Aģentūrai drošuma ziņā svarīgo informāciju, kas izriet no informācijas drošības ziņojumiem, kurus tā saņēmusi saskaņā ar Deleģētās regulas (ES) 2022/1645 pielikuma (IS.D.OR daļas) IS.D.OR.230. punktu.";

2) aiz ADR.AR.A.030. punkta iekļauj šādu ADR.AR.A.030.A punktu:

"**ADR.AR.A.030.A Tūlītēja reakcija uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu**

a) Kompetentā iestāde ievieš sistēmu, kas nepieciešama, lai pienācīgi vāktu, analizētu un izplatītu organizāciju paziņoto informāciju, kura saistīta ar informācijas drošības incidentiem un ievainojamībām, kas spēj ietekmēt aviācijas drošumu. To veic, saskaņojot ar visām citām attiecīgajām iestādēm, kas ir atbildīgas par informācijas drošību vai kiberdrošību dalībvalstī, lai sekmētu ziņošanas sistēmu koordināciju un saderību.

b) Aģentūra ievieš sistēmu, kura nepieciešama, lai pienācīgi analizētu visu attiecīgo drošuma ziņā svarīgo informāciju, kas saņemta saskaņā ar ADR.AR.A.025. punkta c) apakšpunktu, un bez nepamatotas kavēšanās sniedz dalībvalstīm un Komisijai visu informāciju, tajā skaitā par ieteikumiem vai veicamajiem korektīvajiem pasākumiem, kura tām nepieciešama, lai laikus reaģētu uz informācijas drošības incidentu vai ievainojamību, kas spēj ietekmēt aviācijas drošumu, tajā skaitā saistībā ar ražojumiem, daļām, neuzstādītām ierīcēm, personām vai organizācijām, uz kurām attiecas Regula (ES) 2018/1139 un tās deleģētie un īstenošanas akti.

c) Pēc a) un b) apakšpunktā minētās informācijas saņemšanas kompetentā iestāde veic attiecīgus pasākumus, kuri nepieciešami, lai novērstu informācijas drošības incidenta vai ievainojamības iespējamo ietekmi uz aviācijas drošumu.

d) Par pasākumiem, kas veikti saskaņā ar c) apakšpunktu, nekavējoties paziņo visām personām vai organizācijām, kurām jānodrošina atbilstība šiem pasākumiem saskaņā ar Regulu (ES) 2018/1139 un tās deleģētajiem un īstenošanas aktiem. Dalībvalsts kompetentā iestāde par šiem pasākumiem informē arī Aģentūru un, ja nepieciešama kopīga rīcība, arī citu iesaistīto dalībvalstu kompetentās iestādes.";

3) pielikuma ADR.AR.B.005. punktam pievieno šādu d) apakšpunktu:

"d) Lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu, pārvaldības sistēma, ko izveido un uztur kompetentā iestāde, atbilst ne tikai a) apakšpunktā noteiktajām prasībām, bet arī Īstenošanas regulas (ES) 2023/203 I pielikumam (IS.AR daļai).";

4) pielikuma ADR.AR.B.010. punktu groza šādi:

i) virsrakstu aizstāj ar šādu:

"**ADR.AR.B.010 Uzdevumu sadale**";

ii) pievieno šādu c) apakšpunktu:

"c) Attiecībā uz organizācijas atbilstības ADR.OR.D.005.A punktam sertificēšanu un uzraudzību kompetentā iestāde var piešķirt uzdevumus kvalificētajām vienībām saskaņā ar a) apakšpunktu vai jebkurai attiecīgajai iestādei, kas atbild par informācijas drošību vai kiberdrošību dalībvalstī. Uzdevumu sadalē kompetentā iestāde nodrošina, ka:

1) kvalificētā vienība vai attiecīgā iestāde koordinē un ņem vērā visus ar aviācijas drošumu saistītos aspektus;

2) kvalificētās vienības vai attiecīgās iestādes veikto sertificēšanas un uzraudzības darbību rezultāti ir iekļauti organizācijas vispārējos sertificēšanas un uzraudzības dokumentos;

3) tās informācijas drošības pārvaldības sistēma, kas izveidota saskaņā ar ADR.AR.B.005. punkta e) apakšpunktu, aptver visus tās vārdā veiktos sertificēšanas un pastāvīgās uzraudzības uzdevumus.";

5) pielikuma ADR.AR.C.005. punktam pievieno šādu f) apakšpunktu:

"f) Attiecībā uz organizācijas atbilstības ADR.OR.D.005.A punktam sertificēšanu un uzraudzību kompetentā iestāde papildus a) līdz e) apakšpunkta ievērošanai pārskata visus apstiprinājumus, kas piešķirti saskaņā ar šīs regulas IS.I.OR.200. punkta e) apakšpunktu vai Deleģētās regulas (ES) 2022/1645 IS.D.OR.200. punkta e) apakšpunktu, pēc piemērojamā pārraudzības revīzijas cikla un ikreiz, kad tiek ieviestas izmaiņas organizācijas darbības jomā.";

6) aiz ADR.AR.C.040. punkta iekļauj šādu ADR.AR.C.040.A punktu:

"**ADR.AR.C.040.A Informācijas drošības pārvaldības sistēmas izmaiņas**

a) Attiecībā uz izmaiņām, kas pārvaldītas un paziņotas kompetentajai iestādei saskaņā ar procedūru, kura noteikta Deleģētās regulas (ES) 2022/1645 pielikuma (IS.D.OR daļas) IS.D.OR.255. punkta a) apakšpunktā, kompetentā iestāde iekļauj šādu izmaiņu pārbaudi savā pastāvīgajā uzraudzībā saskaņā ar ADR.AR.C.005. punktā norādītajiem principiem. Ja tiek konstatēta neatbilstība, kompetentā iestāde informē par to organizāciju, pieprasa veikt papildu izmaiņas un rīkojas saskaņā ar ADR.AR.C.055. punktu.

b) Attiecībā uz citām izmaiņām, kam nepieciešams apstiprināšanas pieteikums saskaņā ar Deleģētās regulas (ES) 2022/1645 pielikuma (IS.D.OR daļas) IS.D.OR.255. punkta b) apakšpunktu:

1) saņēmusi pieteikumu par izmaiņām, kompetentā iestāde pirms apstiprinājuma izdošanas pārbauda organizācijas atbilstību piemērojamajām prasībām;

2) kompetentā iestāde nosaka nosacījumus, saskaņā ar kuriem organizācija var darboties izmaiņu ieviešanas laikā;

3) ja kompetentā iestāde ir pārliecināta, ka organizācija atbilst piemērojamajām prasībām, tā apstiprina izmaiņas."

VII PIELIKUMS

Regulas (ES) Nr. 1321/2014 II pielikumu (145. daļu), III pielikumu (66. daļu) un Vc pielikumu (*CAMO daļu*) groza šādi:

1) II pielikumu (145. daļu) groza šādi:

a) satura rādītāju groza šādi:

i) aiz 145.A.200. punkta virsraksta iekļauj šādu virsrakstu:

"145.A.200.A Informācijas drošības pārvaldības sistēma";

ii) aiz 145.B.135. punkta virsraksta iekļauj šādu virsrakstu:

"145.B.135.A Tūlītēja reakcija uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu";

iii) pielikuma 145.B.205. punkta virsrakstu aizstāj ar šādu:

"145.B.205. Uzdevumu sadale";

iv) aiz 145.B.330. punkta virsraksta iekļauj šādu virsrakstu:

"145.B.330.A Informācijas drošības pārvaldības sistēmas izmaiņas";

b) aiz 145.A.200. punkta iekļauj šādu 145.A.200.A punktu:

"145.A.200.A **Informācijas drošības pārvaldības sistēma**

Lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu, papildus 145.A.200. punktā noteiktajai pārvaldības sistēmai tehniskās apkopes organizācija izveido, īsteno un uztur informācijas drošības pārvaldības sistēmu saskaņā ar Īstenošanas regulu (ES) 2023/203.";

c) pielikuma 145.B.125. punktam pievieno šādu c) apakšpunktu:

"c) Dalībvalsts kompetentā iestāde pēc iespējas ātrāk sniedz Aģentūrai drošuma ziņā svarīgo informāciju, kas izriet no informācijas drošības ziņojumiem, kurus tā saņēmusi saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.230. punktu.";

d) aiz 145.B.135. punkta iekļauj šādu 145.B.135.A punktu:

"145.B.135.A **Tūlītēja reakcija uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu**

a) Kompetentā iestāde ievieš sistēmu, kas nepieciešama, lai pienācīgi vāktu, analizētu un izplatītu organizāciju paziņoto informāciju, kura saistīta ar informācijas drošības incidentiem un ievainojamībām, kas spēj ietekmēt aviācijas drošumu. To veic, saskaņojot ar visām citām attiecīgajām iestādēm, kas ir atbildīgas par informācijas drošību vai kiberdrošību dalībvalstī, lai sekmētu ziņošanas sistēmu koordināciju un saderību.

b) Aģentūra ievieš sistēmu, kura nepieciešama, lai pienācīgi analizētu visu attiecīgo drošuma ziņā svarīgo informāciju, kas saņemta saskaņā ar 145.B.125. punkta c) apakšpunktu, un bez nepamatotas kavēšanās sniedz dalībvalstīm un Komisijai visu informāciju, tajā skaitā par ieteikumiem vai veicamajiem korektīvajiem pasākumiem, kura tām nepieciešama, lai laikus reaģētu uz informācijas drošības incidentu vai ievainojamību, kas spēj ietekmēt aviācijas drošumu, tajā skaitā saistībā ar ražojumiem, daļām, neuzstādītām ierīcēm, personām vai organizācijām, uz kurām attiecas Regula (ES) 2018/1139 un tās deleģētie un īstenošanas akti.

c) Pēc a) un b) apakšpunktā minētās informācijas saņemšanas kompetentā iestāde veic attiecīgus pasākumus, kuri nepieciešami, lai novērstu informācijas drošības incidenta vai ievainojamības iespējamo ietekmi uz aviācijas drošumu.

d) Par pasākumiem, kas veikti saskaņā ar c) apakšpunktu, nekavējoties paziņo visām personām vai organizācijām, kurām jānodrošina atbilstība šiem pasākumiem saskaņā ar Regulu (ES) 2018/1139 un tās deleģētajiem un īstenošanas aktiem. Dalībvalsts kompetentā iestāde par šiem pasākumiem informē arī Aģentūru un, ja nepieciešama kopīga rīcība, arī citu iesaistīto dalībvalstu kompetentās iestādes.";

e) pielikuma 145.B.200. punktam pievieno šādu e) apakšpunktu:

"e) Lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu, pārvaldības sistēma, ko izveido un uztur kompetentā iestāde, atbilst ne tikai a) apakšpunktā noteiktajām prasībām, bet arī Īstenošanas regulas (ES) 2023/203 I pielikumam (IS.AR daļai).";

f) pielikuma 145.B.205. punktu groza šādi:

i) virsrakstu aizstāj ar šādu:

"145.B.205. **Uzdevumu sadale**";

ii) pievieno šādu c) apakšpunktu:

"c) Attiecībā uz organizācijas atbilstības 145.A.200.A punktam sertificēšanu un uzraudzību kompetentā iestāde var piešķirt uzdevumus kvalificētajām vienībām saskaņā ar a) apakšpunktu vai jebkurai attiecīgajai iestādei, kas atbild par informācijas drošību vai kiberdrošību dalībvalstī. Uzdevumu sadalē kompetentā iestāde nodrošina, ka:

1) kvalificētā vienība vai attiecīgā iestāde koordinē un ņem vērā visus ar aviācijas drošumu saistītos aspektus;

2) kvalificētās vienības vai attiecīgās iestādes veikto sertificēšanas un uzraudzības darbību rezultāti ir iekļauti organizācijas vispārējos sertificēšanas un uzraudzības dokumentos;

3) tās informācijas drošības pārvaldības sistēma, kas izveidota saskaņā ar 145.B.200. punkta e) apakšpunktu, aptver visus tās vārdā veiktos sertificēšanas un pastāvīgās uzraudzības uzdevumus.";

g) pielikuma 145.B.300. punktam pievieno šādu g) apakšpunktu:

"g) Attiecībā uz organizācijas atbilstības 145.A.200.A punktam sertificēšanu un uzraudzību kompetentā iestāde papildus a) līdz f) apakšpunkta ievērošanai pārskata visus apstiprinājumus, kas piešķirti saskaņā ar šīs regulas IS.I.OR.200. punkta e) apakšpunktu vai Deleģētās regulas (ES) 2022/1645 IS.D.OR.200. punkta e) apakšpunktu, pēc piemērojamā pārraudzības revīzijas cikla un ikreiz, kad tiek ieviestas izmaiņas organizācijas darbības jomā.";

h) aiz 145.B.330. punkta iekļauj šādu 145.B.330.A punktu:

"145.B.330.A **Informācijas drošības pārvaldības sistēmas izmaiņas**

a) Attiecībā uz izmaiņām, kas pārvaldītas un paziņotas kompetentajai iestādei saskaņā ar procedūru, kura Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta a) apakšpunktā, kompetentā iestāde iekļauj šādu izmaiņu pārbaudi savā pastāvīgajā uzraudzībā saskaņā ar 145.B.300. punktā norādītajiem principiem. Ja tiek konstatēta neatbilstība, kompetentā iestāde informē par to organizāciju, pieprasa veikt papildu izmaiņas un rīkojas saskaņā ar 145.B.350. punktu.

b) Attiecībā uz citām izmaiņām, kam nepieciešams apstiprināšanas pieteikums saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta b) apakšpunktu:

1) saņēmusi pieteikumu par izmaiņām, kompetentā iestāde pirms apstiprinājuma izdošanas pārbauda organizācijas atbilstību piemērojamajām prasībām;

2) kompetentā iestāde nosaka nosacījumus, saskaņā ar kuriem organizācija var darboties izmaiņu ieviešanas laikā;

3) ja kompetentā iestāde ir pārliecināta, ka organizācija atbilst piemērojamajām prasībām, tā apstiprina izmaiņas.";

2) III pielikumu (66. daļu) groza šādi:

a) satura rādītājā aiz 66.B.10. punkta virsraksta iekļauj šādu virsrakstu:

"66.B.15. Informācijas drošības pārvaldības sistēma";

b) aiz 66.B.10. punkta iekļauj šādu 66.B.15. punktu:

"66.B.15. **Informācijas drošības pārvaldības sistēma**

Lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu, kompetentā iestāde izveido, īsteno un uztur informācijas drošības pārvaldības sistēmu saskaņā ar Īstenošanas regulas (ES) 2023/203 I pielikumu (IS.AR daļu).";

3) regulas Vc pielikumu (*CAMO daļu*) groza šādi:

a) satura rādītāju groza šādi:

i) aiz CAMO.A.200. punkta virsraksta iekļauj šādu virsrakstu:

"CAMO.A.200A. Informācijas drošības pārvaldības sistēma";

ii) aiz CAMO.B.135. punkta virsraksta iekļauj šādu virsrakstu:

"CAMO.B.135.A Tūlītēja reakcija uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu";

iii) pielikuma CAMO.B.205. punkta virsrakstu aizstāj ar šādu:

"CAMO.B.205. Uzdevumu sadale";

iv) aiz CAMO.B.330. punkta virsraksta iekļauj šādu virsrakstu:

"CAMO.B.330.A Informācijas drošības pārvaldības sistēmas izmaiņas";

b) aiz CAMO.A.200. punkta iekļauj šādu CAMO.A.200.A punktu:

"CAMO.A.200.A **Informācijas drošības pārvaldības sistēma**

Papildus CAMO.A.200. punktā noteiktajai pārvaldības sistēmai organizācija izveido, īsteno un uztur informācijas drošības pārvaldības sistēmu saskaņā ar Īstenošanas regulu (ES) 2023/203, lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu.";

c) CAMO.B.125. punktam pievieno šādu c) apakšpunktu:

"c) Dalībvalsts kompetentā iestāde pēc iespējas ātrāk sniedz Aģentūrai drošuma ziņā svarīgo informāciju, kas izriet no informācijas drošības ziņojumiem, kurus tā saņēmusi saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.230. punktu.";

d) aiz CAMO.B.135. punkta iekļauj šādu CAMO.B.135.A punktu:

"CAMO.B.135.A **Tūlītēja reakcija uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu**

a) Kompetentā iestāde ievieš sistēmu, kas nepieciešama, lai pienācīgi vāktu, analizētu un izplatītu organizāciju paziņoto informāciju, kura saistīta ar informācijas drošības incidentiem un ievainojamībām, kas spēj ietekmēt aviācijas drošumu. To veic, saskaņojot ar visām citām attiecīgajām iestādēm, kas ir atbildīgas par informācijas drošību vai kiberdrošību dalībvalstī, lai sekmētu ziņošanas sistēmu koordināciju un saderību.

b) Aģentūra ievieš sistēmu, kura nepieciešama, lai pienācīgi analizētu visu attiecīgo drošuma ziņā svarīgo informāciju, kas saņemta saskaņā ar CAMO.B.125. punkta c) apakšpunktu, un bez nepamatotas kavēšanās sniedz dalībvalstīm un Komisijai visu informāciju, tajā skaitā par ieteikumiem vai veicamajiem korektīvajiem pasākumiem, kura tām nepieciešama, lai laikus reaģētu uz informācijas drošības incidentu vai ievainojamību, kas spēj ietekmēt aviācijas drošumu, tajā skaitā saistībā ar ražojumiem, daļām, neuzstādītām ierīcēm, personām vai organizācijām, uz kurām attiecas Regula (ES) 2018/1139 un tās deleģētie un īstenošanas akti.

c) Pēc a) un b) apakšpunktā minētās informācijas saņemšanas kompetentā iestāde veic attiecīgus pasākumus, kuri nepieciešami, lai novērstu informācijas drošības incidenta vai ievainojamības iespējamo ietekmi uz aviācijas drošumu.

d) Par pasākumiem, kas veikti saskaņā ar c) apakšpunktu, nekavējoties paziņo visām personām vai organizācijām, kurām jānodrošina atbilstība šiem pasākumiem saskaņā ar Regulu (ES) 2018/1139 un tās deleģētajiem un īstenošanas aktiem. Dalībvalsts kompetentā iestāde par šiem pasākumiem informē arī Aģentūru un, ja nepieciešama kopīga rīcība, arī citu iesaistīto dalībvalstu kompetentās iestādes.";

e) pielikuma CAMO.B.200. punktam pievieno šādu e) apakšpunktu:

"e) Lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu, pārvaldības sistēma, ko izveido un uztur kompetentā iestāde, atbilst ne tikai a) apakšpunktā noteiktajām prasībām, bet arī Īstenošanas regulas (ES) 2023/203 I pielikumam (IS.AR daļai).";

f) pielikuma CAMO.B.205. punktu groza šādi:

i) virsrakstu aizstāj ar šādu:

"CAMO.B.205 **Uzdevumu sadale**";

ii) pievieno šādu c) apakšpunktu:

"c) Attiecībā uz organizācijas atbilstības CAMO.A.200.A punktam sertificēšanu un uzraudzību kompetentā iestāde var piešķirt uzdevumus kvalificētajām vienībām saskaņā ar a) apakšpunktu vai jebkurai attiecīgajai iestādei, kas atbild par informācijas drošību vai kiberdrošību dalībvalstī. Uzdevumu sadalē kompetentā iestāde nodrošina, ka:

1) kvalificētā vienība vai attiecīgā iestāde koordinē un ņem vērā visus ar aviācijas drošumu saistītos aspektus;

2) kvalificētās vienības vai attiecīgās iestādes veikto sertificēšanas un uzraudzības darbību rezultāti ir iekļauti organizācijas vispārējos sertificēšanas un uzraudzības dokumentos;

3) tās informācijas drošības pārvaldības sistēma, kas izveidota saskaņā ar CAMO.B.200. punkta e) apakšpunktu, aptver visus tās vārdā veiktos sertificēšanas un pastāvīgās uzraudzības uzdevumus.";

g) pielikuma CAMO.B.300. punktam pievieno šādu g) apakšpunktu:

"g) Attiecībā uz organizācijas atbilstības CAMO.A.200.A punktam sertificēšanu un uzraudzību kompetentā iestāde papildus a) līdz f) apakšpunkta ievērošanai pārskata visus apstiprinājumus, kas piešķirti saskaņā ar šīs regulas IS.I.OR.200. punkta e) apakšpunktu vai Deleģētās regulas (ES) 2022/1645 IS.D.OR.200. punkta e) apakšpunktu, pēc piemērojamā pārraudzības revīzijas cikla un ikreiz, kad tiek ieviestas izmaiņas organizācijas darbības jomā.";

h) aiz CAMO.B.330. punkta iekļauj šādu CAMO.B.330.A punktu:

"CAMO.B.330.A **Informācijas drošības pārvaldības sistēmas izmaiņas**

a) Attiecībā uz izmaiņām, kas pārvaldītas un paziņotas kompetentajai iestādei saskaņā ar procedūru, kura noteikta Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta a) apakšpunktā, kompetentā iestāde iekļauj šādu izmaiņu pārbaudi savā pastāvīgajā uzraudzībā saskaņā ar CAMO.B.300. punktā norādītajiem principiem. Ja tiek konstatēta neatbilstība, kompetentā iestāde informē par to organizāciju, pieprasa veikt papildu izmaiņas un rīkojas saskaņā ar CAMO.B.350. punktu.

b) Attiecībā uz citām izmaiņām, kam nepieciešams apstiprināšanas pieteikums saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta b) apakšpunktu:

1) saņēmusi pieteikumu par izmaiņām, kompetentā iestāde pirms apstiprinājuma izdošanas pārbauda organizācijas atbilstību piemērojamajām prasībām;

2) kompetentā iestāde nosaka nosacījumus, saskaņā ar kuriem organizācija var darboties izmaiņu ieviešanas laikā;

3) ja kompetentā iestāde ir pārliecināta, ka organizācija atbilst piemērojamajām prasībām, tā apstiprina izmaiņas."

VIII PIELIKUMS

Regulas (ES) 2015/340 II pielikumu (ATCO.AR daļu) un III pielikumu (ATCO.OR daļu) groza šādi:

1) II pielikumu (ATCO.AR daļu) groza šādi:

a) ATCO.AR.A.020. punktam pievieno šādu c) apakšpunktu:

"c) Dalībvalsts kompetentā iestāde pēc iespējas ātrāk sniedz Aģentūrai drošuma ziņā svarīgo informāciju, kas izriet no informācijas drošības ziņojumiem, kurus tā saņēmusi saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.230. punktu.";

b) aiz ATCO.AR.A.025. punkta iekļauj šādu ATCO.AR.A.025.A punktu:

"**ATCO.AR.A.025.A Tūlītēja reakcija uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu**

a) Kompetentā iestāde ievieš sistēmu, kas nepieciešama, lai pienācīgi vāktu, analizētu un izplatītu organizāciju paziņoto informāciju, kura saistīta ar informācijas drošības incidentiem un ievainojamībām, kas spēj ietekmēt aviācijas drošumu. To veic, saskaņojot ar visām citām attiecīgajām iestādēm, kas ir atbildīgas par informācijas drošību vai kiberdrošību dalībvalstī, lai sekmētu ziņošanas sistēmu koordināciju un saderību.

b) Aģentūra ievieš sistēmu, kura nepieciešama, lai pienācīgi analizētu visu attiecīgo drošuma ziņā svarīgo informāciju, kas saņemta saskaņā ar ATCO.AR.A.020. punktu, un bez nepamatotas kavēšanās sniedz dalībvalstīm un Komisijai visu informāciju, tajā skaitā par ieteikumiem vai veicamajiem korektīvajiem pasākumiem, kura tām nepieciešama, lai laikus reaģētu uz informācijas drošības incidentu vai ievainojamību, kas spēj ietekmēt aviācijas drošumu, tajā skaitā saistībā ar ražojumiem, daļām, neuzstādītām ierīcēm, personām vai organizācijām, uz kurām attiecas Regula (ES) 2018/1139 un tās deleģētie un īstenošanas akti.

c) Pēc a) un b) apakšpunktā minētās informācijas saņemšanas kompetentā iestāde veic attiecīgus pasākumus, kuri nepieciešami, lai novērstu informācijas drošības incidenta vai ievainojamības iespējamo ietekmi uz aviācijas drošumu.

d) Par pasākumiem, kas veikti saskaņā ar c) apakšpunktu, nekavējoties paziņo visām personām vai organizācijām, kurām jānodrošina atbilstība šiem pasākumiem saskaņā ar Regulu (ES) 2018/1139 un tās deleģētajiem un īstenošanas aktiem. Dalībvalsts kompetentā iestāde par šiem pasākumiem informē arī Aģentūru un, ja nepieciešama kopīga rīcība, arī citu iesaistīto dalībvalstu kompetentās iestādes.";

c) pielikuma ATCO.AR.B.001. punktam pievieno šādu e) apakšpunktu:

"e) Lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu, pārvaldības sistēma, ko izveido un uztur kompetentā iestāde, atbilst ne tikai a) apakšpunktā noteiktajām prasībām, bet arī Īstenošanas regulas (ES) 2023/203 I pielikumam (IS.AR daļai).";

d) pielikuma ATCO.AR.B.005. punktu groza šādi:

i) virsrakstu aizstāj ar šādu:

"**ATCO.AR.B.005 Uzdevumu sadale**";

ii) pievieno šādu c) apakšpunktu:

"c) Attiecībā uz organizācijas atbilstības ATCO.OR.C.001.A punktam sertificēšanu un uzraudzību kompetentā iestāde var piešķirt uzdevumus kvalificētajām vienībām saskaņā ar a) apakšpunktu vai jebkurai attiecīgajai iestādei, kas atbild par informācijas drošību vai kiberdrošību dalībvalstī. Uzdevumu sadalē kompetentā iestāde nodrošina, ka:

1) kvalificētā vienība vai attiecīgā iestāde koordinē un ņem vērā visus ar aviācijas drošumu saistītos aspektus;

2) kvalificētās vienības vai attiecīgās iestādes veikto sertificēšanas un uzraudzības darbību rezultāti ir iekļauti organizācijas vispārējos sertificēšanas un uzraudzības dokumentos;

3) tās informācijas drošības pārvaldības sistēma, kas izveidota saskaņā ar ATCO.AR.B.001. punkta e) apakšpunktu, aptver visus tās vārdā veiktos sertificēšanas un pastāvīgās uzraudzības uzdevumus.";

e) pielikuma ATCO.AR.C.001. punktam pievieno šādu f) apakšpunktu:

"f) Attiecībā uz organizācijas atbilstības ATCO.OR.C.001.A punktam sertificēšanu un uzraudzību kompetentā iestāde papildus a) līdz e) apakšpunkta ievērošanai pārskata visus apstiprinājumus, kas piešķirti saskaņā ar šīs regulas IS.I.OR.200. punkta e) apakšpunktu vai Deleģētās regulas (ES) 2022/1645 IS.D.OR.200. punkta e) apakšpunktu, pēc piemērojamā pārraudzības revīzijas cikla un ikreiz, kad tiek ieviestas izmaiņas organizācijas darbības jomā.";

f) aiz ATCO.AR.E.010. punkta iekļauj šādu ATCO.AR.E.010.A punktu:

"**ATCO.AR.E.010.A Informācijas drošības pārvaldības sistēmas izmaiņas**

a) Attiecībā uz izmaiņām, kas pārvaldītas un paziņotas kompetentajai iestādei saskaņā ar procedūru, kura noteikta Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta a) apakšpunktā, kompetentā iestāde iekļauj šādu izmaiņu pārbaudi savā pastāvīgajā uzraudzībā saskaņā ar ATCO.AR.C.001. punktā norādītajiem principiem. Ja tiek konstatēta neatbilstība, kompetentā iestāde informē par to organizāciju, pieprasa veikt papildu izmaiņas un rīkojas saskaņā ar ATCO.AR.C.010. punktu.

b) Attiecībā uz citām izmaiņām, kam nepieciešams apstiprināšanas pieteikums saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta b) apakšpunktu:

1) saņēmusi pieteikumu par izmaiņām, kompetentā iestāde pirms apstiprinājuma izdošanas pārbauda organizācijas atbilstību piemērojamajām prasībām;

2) kompetentā iestāde nosaka nosacījumus, saskaņā ar kuriem organizācija var darboties izmaiņu ieviešanas laikā;

3) ja kompetentā iestāde ir pārliecināta, ka organizācija atbilst piemērojamajām prasībām, tā apstiprina izmaiņas.";

2) regulas III pielikumu (ATCO.OR daļu) groza šādi:

aiz ATCO.OR.C.001. punkta iekļauj šādu ATCO.OR.C.001.A punktu:

"**ATCO.OR.C.001.A Informācijas drošības pārvaldības sistēma**

Papildus ATCO.OR.C.001. punktā noteiktajai pārvaldības sistēmai mācību organizācija izveido, īsteno un uztur informācijas drošības pārvaldības sistēmu saskaņā ar Īstenošanas regulu (ES) 2023/203, lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu."

IX PIELIKUMS

Īstenošanas regulas (ES) 2017/373 II pielikumu (*Part-ATM/ANS.AR*) un III pielikumu (*Part-ATM/ANS.OR*) groza šādi:

1) regulas II pielikumu (*Part-ATM/ANS.AR*) groza šādi:

a) ATM/ANS.AR.A.020. punktam pievieno šādu c) apakšpunktu:

"c) Dalībvalsts kompetentā iestāde pēc iespējas ātrāk sniedz Aģentūrai drošuma ziņā svarīgo informāciju, kas izriet no informācijas drošības ziņojumiem, kurus tā saņēmusi saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.230. punktu.";

b) aiz ATM/ANS.AR.A.025. punkta iekļauj šādu ATM/ANS.AR.A.025.A punktu:

"**ATM/ANS.AR.A.025.A Tūlītēja reakcija uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu**

a) Kompetentā iestāde ievieš sistēmu, kas nepieciešama, lai pienācīgi vāktu, analizētu un izplatītu organizāciju paziņoto informāciju, kura saistīta ar informācijas drošības incidentiem un ievainojamībām, kas spēj ietekmēt aviācijas drošumu. To veic, saskaņojot ar visām citām attiecīgajām iestādēm, kas ir atbildīgas par informācijas drošību vai kiberdrošību dalībvalstī, lai sekmētu ziņošanas sistēmu koordināciju un saderību.

b) Aģentūra ievieš sistēmu, kura nepieciešama, lai pienācīgi analizētu visu attiecīgo drošuma ziņā svarīgo informāciju, kas saņemta saskaņā ar ATM/ANS.AR.A.020. punkta c) apakšpunktu, un bez nepamatotas kavēšanās sniedz dalībvalstīm un Komisijai visu informāciju, tajā skaitā par ieteikumiem vai veicamajiem korektīvajiem pasākumiem, kura tām nepieciešama, lai laikus reaģētu uz informācijas drošības incidentu vai ievainojamību, kas spēj ietekmēt aviācijas drošumu, tajā skaitā saistībā ar ražojumiem, daļām, neuzstādītām ierīcēm, personām vai organizācijām, uz kurām attiecas Regula (ES) 2018/1139 un tās deleģētie un īstenošanas akti.

c) Pēc a) un b) apakšpunktā minētās informācijas saņemšanas kompetentā iestāde veic attiecīgus pasākumus, kuri nepieciešami, lai novērstu informācijas drošības incidenta vai ievainojamības iespējamo ietekmi uz aviācijas drošumu.

d) Par pasākumiem, kas veikti saskaņā ar c) apakšpunktu, nekavējoties paziņo visām personām vai organizācijām, kurām jānodrošina atbilstība šiem pasākumiem saskaņā ar Regulu (ES) 2018/1139 un tās deleģētajiem un īstenošanas aktiem. Dalībvalsts kompetentā iestāde par šiem pasākumiem informē arī Aģentūru un, ja nepieciešama kopīga rīcība, arī citu iesaistīto dalībvalstu kompetentās iestādes.";

c) pielikuma ATM/ANS.AR.B.001. punktam pievieno šādu e) apakšpunktu:

"e) Lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu, pārvaldības sistēma, ko izveido un uztur kompetentā iestāde, atbilst ne tikai a) apakšpunktā noteiktajām prasībām, bet arī Īstenošanas regulas (ES) 2023/203 I pielikumam (IS.AR daļai).";

d) pielikuma ATM/ANS.AR.B.005. punktu groza šādi:

i) virsrakstu aizstāj ar šādu:

"**ATM/ANS.AR.B.005. Uzdevumu sadale**";

ii) pievieno šādu c) apakšpunktu:

"c) Attiecībā uz organizācijas atbilstības ATM/ANS.OR.B.005.A punktam sertificēšanu un uzraudzību kompetentā iestāde var piešķirt uzdevumus kvalificētajām vienībām saskaņā ar a) apakšpunktu vai jebkurai attiecīgajai iestādei, kas atbild par informācijas drošību vai kiberdrošību dalībvalstī. Uzdevumu sadalē kompetentā iestāde nodrošina, ka:

1) kvalificētā vienība vai attiecīgā iestāde koordinē un ņem vērā visus ar aviācijas drošumu saistītos aspektus;

2) kvalificētās vienības vai attiecīgās iestādes veikto sertificēšanas un uzraudzības darbību rezultāti ir iekļauti organizācijas vispārējos sertificēšanas un uzraudzības dokumentos;

3) tās informācijas drošības pārvaldības sistēma, kas izveidota saskaņā ar ATM/ANS.AR.B.001. punkta e) apakšpunktu, aptver visus tās vārdā veiktos sertificēšanas un pastāvīgās uzraudzības uzdevumus.";

e) pielikuma ATM/ANS.AR.C.010. punktam pievieno šādu d) apakšpunktu:

"d) Attiecībā uz organizācijas atbilstības ATM/ANS.OR.B.005.A punktam sertificēšanu un uzraudzību kompetentā iestāde papildus a) līdz c) apakšpunkta ievērošanai pārskata visus apstiprinājumus, kas piešķirti saskaņā ar šīs regulas IS.I.OR.200. punkta e) apakšpunktu vai Deleģētās regulas (ES) 2022/1645 IS.D.OR.200. punkta e) apakšpunktu, pēc piemērojamā pārraudzības revīzijas cikla un ikreiz, kad tiek ieviestas izmaiņas organizācijas darbības jomā.";

f) aiz ATM/ANS.AR.C.025. punkta iekļauj šādu ATM/ANS.AR.C.025.A punktu:

"**ATM/ANS.AR.C.025.A Informācijas drošības pārvaldības sistēmas izmaiņas**

a) Attiecībā uz izmaiņām, kas pārvaldītas un paziņotas kompetentajai iestādei saskaņā ar procedūru, kura noteikta Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta a) apakšpunktā, kompetentā iestāde iekļauj šādu izmaiņu pārbaudi savā pastāvīgajā uzraudzībā saskaņā ar ATM/ANS.AR.C.010. punktā norādītajiem principiem. Ja tiek konstatēta neatbilstība, kompetentā iestāde informē par to organizāciju, pieprasa veikt papildu izmaiņas un rīkojas saskaņā ar ATM/ANS.AR.C.050. punktu.

b) Attiecībā uz citām izmaiņām, kam nepieciešams apstiprināšanas pieteikums saskaņā ar Īstenošanas regulas (ES) 2023/203 II pielikuma (IS.I.OR daļas) IS.I.OR.255. punkta b) apakšpunktu:

1) saņēmusi pieteikumu par izmaiņām, kompetentā iestāde pirms apstiprinājuma izdošanas pārbauda organizācijas atbilstību piemērojamajām prasībām;

2) kompetentā iestāde nosaka nosacījumus, saskaņā ar kuriem organizācija var darboties izmaiņu ieviešanas laikā;

3) ja kompetentā iestāde ir pārliecināta, ka organizācija atbilst piemērojamajām prasībām, tā apstiprina izmaiņas.";

2) regulas III pielikumu (*Part-ATM/ANS.OR*) groza šādi:

a) aiz ATM/ANS.OR.B.005. punkta iekļauj šādu ATM/ANS.OR.B.005.A punktu:

"**ATM/ANS.OR.B.005.A Informācijas drošības pārvaldības sistēma**

Papildus ATM/ANS.OR.B.005. punktā noteiktajai pārvaldības sistēmai pakalpojumu sniedzējs izveido, īsteno un uztur informācijas drošības pārvaldības sistēmu saskaņā ar Īstenošanas regulu (ES) 2023/203, lai nodrošinātu tādu informācijas drošības risku pienācīgu pārvaldību, kuri var ietekmēt aviācijas drošumu.";

b) pielikuma ATM/ANS.OR.D.010. punktu aizstāj ar šādu:

"**ATM/ANS.OR.D.010. Drošības pārvaldība**

a) Aeronavigācijas pakalpojumu un gaisa satiksmes plūsmas pārvaldības pakalpojumu sniedzēji un tīkla pārvaldnieks, kā paredzēts ATM/ANS.OR.B.005. punktā, kā to pārvaldības sistēmas neatņemamu daļu izveido drošības pārvaldības sistēmu, lai nodrošinātu:

1) telpu, iekārtu un personāla drošību nolūkā izvairīties no nelikumīgas iejaukšanās pakalpojumu sniegšanā;

2) to ekspluatācijas datu drošību, kurus tie saņem vai sagatavo, vai izmanto citādi, lai piekļuve datiem būtu iespējama tikai pilnvarotām personām.

b) Drošības pārvaldības sistēma nosaka:

1) procesus un procedūras attiecībā uz drošības riska novērtējumu un mazināšanu, drošības uzraudzību un uzlabošanu, drošības pārskatiem un gūtās pieredzes izplatīšanu;

2) līdzekļus, kas paredzēti, lai noteiktu, uzraudzītu un konstatētu drošības noteikumu pārkāpumus un pievērstu personāla uzmanību attiecīgajiem drošības brīdinājumiem;

3) līdzekļus, ar kuriem kontrolē drošības noteikumu pārkāpumu ietekmi un nosaka nepieciešamo rīcību situācijas labošanai un attiecīgās riska mazināšanas procedūras, lai izvairītos no situācijas atkārtošanās.

c) Aeronavigācijas pakalpojumu un gaisa satiksmes plūsmas pārvaldības pakalpojumu sniedzēji un tīkla pārvaldnieks vajadzības gadījumā nodrošina personāla drošības pārbaudes un sadarbojas ar attiecīgām civilām un militārām iestādēm, lai nodrošinātu telpu, iekārtu, personāla un datu drošību.

d) Ar informācijas drošību saistītos aspektus pārvalda saskaņā ar ATM/ANS.OR.B.005.A punktu."