II

(Muud kui seadusandlikud aktid)

MÄÄRUSED

KOMISJONI RAKENDUSMÄÄRUS (EL) 2023/203,

27. oktoober 2022,

millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139 rakendamise eeskirjad nõuete osas, mis on seotud selliste infoturvariskide juhtimisega, mis võivad mõjutada lennuohutust ning mida kohaldatakse komisjoni määrustega (EL) nr 1321/2014, (EL) nr 965/2012, (EL) nr 1178/2011, (EL) 2015/340 ning komisjoni rakendusmäärustega (EL) 2017/373 ja (EL) 2021/664 hõlmatud organisatsioonide ning komisjoni määrustega (EL) nr 748/2012, (EL) nr 1321/2014, (EL) nr 965/2012, (EL) nr 1178/2011, (EL) 2015/340 ja (EL) nr 139/2014, komisjoni rakendusmäärustega (EL) 2017/373 ja (EL) 2021/664 hõlmatud pädevate asutuste suhtes, ning muudetakse komisjoni määrusi (EL) nr 1178/2011, (EL) nr 748/2012, (EL) nr 965/2012, (EL) nr 139/2014, (EL) nr 1321/2014, (EL) 2015/340 ning komisjoni rakendusmäärusi (EL) 2017/373 ja (EL) 2021/664

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 4. juuli 2018. aasta määrust (EL) 2018/1139, mis käsitleb tsiviillennunduse valdkonna ühisnorme ja millega luuakse Euroopa Liidu Lennundusohutusamet ning millega muudetakse Euroopa Parlamendi ja nõukogu määrusi (EÜ) nr 2111/2005, (EÜ) nr 1008/2008, (EL) nr 996/2010, (EL) nr 376/2014 ja Euroopa Parlamendi ja nõukogu direktiive 2014/30/EL ning 2014/53/EL ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 552/2004 ja (EÜ) nr 216/2008 ning nõukogu määrus (EMÜ) nr 3922/91, ([1]) eriti selle artikli 17 lõike 1 punkti b, artikli 27 lõike 1 punkti a, artikli 31 lõike 1 punkti b, artikli 43 lõike 1 punkti b, artikli 53 lõike 1 punkti a ning artikli 62 lõike 15 punkti c,

ning arvestades järgmist:

(1) Kooskõlas määruse (EL) 2018/1139 II lisa punkti 3.1 alapunktis b sätestatud oluliste nõuetega peavad õhusõidukite jätkuva lennukõlblikkusega tegelevad ja hooldusorganisatsioonid rakendama ohutusriskide juhtimise süsteemi ja hoidma seda töös.

(2) Lisaks peavad pilootide koolitusorganisatsioonid, salongitöötajate koolitusorganisatsioonid, õhusõidukimeeskondade lennundusmeditsiinikeskused ja lennutreeningseadmete käitajad vastavalt määruse (EL) 2018/1139 IV lisa punkti 3.3 alapunktis b ja punkti 5 alapunktis b sätestatud olulistele nõuetele rakendama ohutusriskide juhtimise süsteemi ja seda töös hoidma.

(3) Peale selle peavad õhusõidukite käitajad kooskõlas määruse (EL) 2018/1139 V lisa punkti 8.1 alapunktis c sätestatud oluliste nõuetega rakendama ohutusriskide juhtimise süsteemi ja seda töös hoidma.

(4) Samuti peavad lennuliikluse korraldamise ja aeronavigatsiooniteenuste osutajad, U-space'i teenuseosutajad ja ühtse ühise teabeteenuse osutajad ning lennujuhtide koolitusorganisatsioonid ja lennundusmeditsiinikeskused vastavalt määruse (EL) 2018/1139 VIII lisa punkti 5.1 alapunktis c ja punkti 5.4 alapunktis b sätestatud olulistele nõuetele rakendama ohutusriskide juhtimise süsteemi ja seda töös hoidma.

([1]) ELT L 212, 22.8.2018, lk 1.

(5) Sellised ohutusriskid võivad tuleneda eri asjaoludest, näiteks konstruktsiooni- ja hooldusvigadest, inimtegevusega seotud aspektidest ning keskkonna- ja infoturbeohtudest. Seepärast tuleks Euroopa Liidu Lennundusohutusameti (edaspidi „amet“) ning eespool põhjendustes osutatud riiklike pädevate asutuste ja organisatsioonide poolt rakendatavate juhtimissüsteemide puhul lisaks juhuslikest sündmustest tulenevatele ohutusriskidele arvesse võtta ka infoturbeohtudest tulenevaid ohutusriske, kui kuritahtlike kavatsustega isikud võivad olemasolevaid puudusi omakasupüüdlikult ära kasutada. Need infoturvariskid on tsiviillennundussektoris pidevalt suurenenud, kuna praegused infosüsteemid on omavahel üha tihedamalt seotud ja langevad üha sagedamini kuritahtlike rünnakute ohvriks.

(6) Nende infosüsteemidega seotud riskid ei piirdu küberruumi vastu suunatud võimalike rünnakutega, vaid hõlmavad ka ohte, mis võivad mõjutada protsesse ja menetlusi ning inimeste käitumist.

(7) Paljud organisatsioonid juba kasutavad digiteabe ja -andmete turvalisuse tagamiseks rahvusvahelisi standardeid, näiteks standardit ISO 27001. Need standardid ei pruugi täielikult hõlmata tsiviillennunduse kogu eripära. Seetõttu on asjakohane kehtestada nõuded selliste infoturvariskide juhtimiseks, mis võivad mõjutada lennuohutust.

(8) On oluline, et need nõuded hõlmaksid kõiki lennundusvaldkondi ja nende liideseid, kuna lennundus koosneb omavahel tihedalt seotud süsteemidest. Seepärast tuleks neid kohaldada kõikide komisjoni määrustega (EL) nr 748/2012, ([2]) (EL) nr 1321/2014, ([3]) (EL) nr 965/2012, ([4]) (EL) nr 1178/2011, ([5]) (EL) 2015/340, ([6]) (EL) nr 139/2014 ([7]) ja komisjoni rakendusmäärusega (EL) 2021/664 ([8]) hõlmatud organisatsioonide ja pädevate asutuste suhtes, samuti nende organisatsioonide ja pädevate asutuste suhtes, kellelt juba nõutakse juhtimissüsteemi rakendamist vastavalt kehtivatele liidu lennuohutusalastele õigusaktidele. Samas tuleks mõned organisatsioonid, kelle puhul lennundussüsteemi ohustavad infoturvariskid on väiksemad, asjakohase proportsionaalsuse tagamiseks käesoleva määruse kohaldamisalast välja jätta.

(9) Käesolevas määruses sätestatud nõuetega tuleks tagada nende järjepidev rakendamine kõigis lennundusvaldkondades viisil, mis mõjutaksid võimalikult vähe selliseid liidu lennuohutusalaseid õigusakte, mida asjaomaste valdkondade suhtes juba kohaldatakse.

([2]) Komisjoni 3. augusti 2012. aasta määrus (EL) nr 748/2012, millega nähakse ette õhusõidukite ja nendega seotud toodete, osade ja seadmete lennukõlblikkuse ja keskkonnaohutuse sertifitseerimise ning projekteerimis- ja tootjaorganisatsioonide sertifitseerimise rakenduseeskirjad (ELT L 224, 21.8.2012, lk 1).

([3]) Komisjoni 26. novembri 2014. aasta määrus (EL) nr 1321/2014 õhusõidukite ja lennundustoodete ning nende osade ja seadmete jätkuva lennukõlblikkuse ning sellega tegelevate organisatsioonide ja isikute sertifitseerimise kohta (ELT L 362, 17.12.2014, lk 1).

([4]) Komisjoni 5. oktoobri 2012. aasta määrus (EL) nr 965/2012, millega kehtestatakse lennutegevusega seotud tehnilised nõuded ja haldusmenetlused vastavalt Euroopa Parlamendi ja nõukogu määrusele (EÜ) nr 216/2008 (ELT L 296, 25.10.2012, lk 1).

([5]) Komisjoni 3. novembri 2011. aasta määrus (EL) nr 1178/2011, millega kehtestatakse tsiviillennunduses kasutatavate õhusõidukite meeskonnaga seotud tehnilised nõuded ja haldusmenetlused vastavalt Euroopa Parlamendi ja nõukogu määrusele (EÜ) nr 216/2008 (ELT L 311, 25.11.2011, lk 1).

([6]) Komisjoni 20. veebruari 2015. aasta määrus (EL) 2015/340, millega kehtestatakse lennujuhtide lubade ning Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 216/2008 kohaste sertifikaatidega seotud tehnilised nõuded ja haldusmenetlused, muudetakse komisjoni rakendusmäärust (EL) nr 923/2012 ja tunnistatakse kehtetuks komisjoni määrus (EL) nr 805/2011 (ELT L 63, 6.3.2015, lk 1).

([7]) Komisjoni 12. veebruari 2014. aasta määrus (EL) nr 139/2014, millega kehtestatakse lennuväljadega seotud nõuded ja haldusmenetlused vastavalt Euroopa Parlamendi ja nõukogu määrusele (EÜ) nr 216/2008 (ELT L 44, 14.2.2014, lk 1).

([8]) Komisjoni 22. aprilli 2021.aasta rakendusmäärus (EL) 2021/664, U-space'i õigusraamistiku kohta (ELT L 139, 23.4.2021, lk 161).

(10) Käesolevas määruses sätestatud nõuded ei tohiks mõjutada komisjoni rakendusmääruse (EL) 2015/1998 ([9]) lisa punktis 1.7 ega Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 ([10]) artiklis 14 sätestatud infoturbe- ja küberturbenõuete kohaldamist.

(11) Euroopa Parlamendi ja nõukogu määruse (EL) 2021/696 ([11]) V jaotise (Kosmoseprogrammi turvalisus) artiklites 33–43 sätestatud turbenõuded loetakse samaväärseks käesolevas määruses sätestatud nõuetega, välja arvatud käesoleva määruse II lisa punkt IS.I.OR.230, mille nõuded peavad olema täidetud.

(12) Õiguskindluse tagamiseks tuleks käesolevas määruses määratletud mõiste „infoturve“ tõlgendust, mis kajastab selle üldlevinud ülemaailmset kasutamist tsiviillennunduse valdkonnas, pidada kooskõlas olevaks mõistega „võrgu- ja infosüsteemide turvalisus“, nagu on määratletud direktiivi (EL) 2016/1148 artikli 4 lõikes 2. Käesolevas määruses kasutatud infoturbemääratluse tõlgendamisel ei tohiks see erineda direktiivis (EL) 2016/1148 sätestatud võrgu- ja infosüsteemide turvalisuse määratlusest.

(13) Selleks et vältida õiguslike nõuete dubleerimist, tuleks juhul, kui käesoleva määrusega hõlmatud organisatsioonide suhtes juba kohaldatakse põhjendustes (10) ja 11 osutatud liidu õigusaktidest tulenevaid turbenõudeid, mis on oma toimelt samaväärsed käesoleva määruse sätetega, pidada kõnealuste turbenõuete järgimist käesolevas määruses sätestatud nõuetele vastavaks.

(14) Käesoleva määrusega hõlmatud organisatsioonid, kelle suhtes juba kohaldatakse rakendusmäärusest (EL) 2015/1998 või määrusest (EL) 2021/696 või mõlemast määrusest tulenevaid turbenõudeid, peaksid täitma ka käesoleva määruse II lisa (osa IS.I.OR.230 „Infoturbealane välisaruandluskava“) nõudeid, kuna kumbki määrus ei sisalda sätteid infoturvaintsidentidest asutusevälise teavitamise kohta.

(15) Täielikkuse huvides tuleks määrusi (EL) nr 1178/2011, (EL) nr 748/2012, (EL) nr 965/2012, (EL) nr 139/2014, (EL) nr 1321/2014, (EL) 2015/340 ja rakendusmäärusi (EL) 2017/373 ([12]) ja (EL) 2021/664 muuta, et kehtestada käesoleva määrusega ette nähtud infoturbe halduse süsteemi nõuded koos selles sätestatud haldussüsteemidega, ning sätestada pädevate asutuste nõuded järelevalve teostamiseks organisatsioonide üle, mis rakendavad eespool nimetatud infoturbe halduse nõudeid.

(16) Selleks et anda organisatsioonidele piisavalt aega, et tagada uute eeskirjade ja menetluste täitmine, tuleks käesolevat määrust hakata kohaldama kolm aastat pärast selle jõustumist, välja arvatud rakendusmääruses (EL) 2017/373 määratletud Euroopa Geostatsionaarse Navigatsioonilisasüsteemi (EGNOS) aeronavigatsiooniteenuse osutaja suhtes, kelle puhul EGNOSe süsteemi ja teenuste turvalisuse jätkuva akrediteerimise tõttu kooskõlas määrusega (EL) 2021/696 tuleks käesolevat määrust kohaldama hakata alates 1. jaanuarist 2026.

(17) Käesolevas määruses sätestatud nõuded põhinevad arvamusel nr 03/2021, ([13]) mille amet on esitanud kooskõlas määruse (EL) 2018/1139 artikli 75 lõike 2 punktidega b ja c ning artikli 76 lõikega 1.

([9]) Komisjoni 5. novembri 2015. aasta rakendusmäärus (EL) 2015/1998, millega nähakse ette lennundusjulgestuse ühiste põhistandardite rakendamise üksikasjalikud meetmed (ELT L 299, 14.11.2015, lk 1).

([10]) Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

([11]) Euroopa Parlamendi ja nõukogu 28. aprilli 2021. aasta määrus (EL) 2021/696, millega luuakse liidu kosmoseprogramm ja Euroopa Liidu Kosmoseprogrammi Amet ning tunnistatakse kehtetuks määrused (EL) nr 912/2010, (EL) nr 1285/2013 ja (EL) nr 377/2014 ning otsus nr 541/2014/EL (ELT L 170, 12.5.2021, lk 69).

([12]) Komisjoni 1. märtsi 2017. aasta rakendusmäärus (EL) 2017/373, millega sätestatakse lennuliikluse korraldamise teenuste ja aeronavigatsiooniteenuste osutajate ning muude lennuliikluse korraldamise võrgustiku funktsioonide suhtes ja kõigi nende järelevalve suhtes kohaldatavad ühisnõuded ning millega tunnistatakse kehtetuks määrus (EÜ) nr 482/2008, rakendusmäärused (EL) nr 1034/2011, (EL) nr 1035/2011 ja (EL) 2016/1377 ning muudetakse määrust (EL) nr 677/2011 (ELT L 62, 8.3.2017, lk 1).

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

(18) Käesolevas määruses sätestatud nõuded on kooskõlas määruse (EL) 2018/1139 artikli 127 kohaselt loodud tsiviillennunduse valdkonna ühiste ohutuseeskirjade kohaldamise komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Reguleerimisese

Käesolevas määruses on sätestatud nõuded, mida organisatsioonid ja pädevad asutused peavad täitma, et:

a) teha kindlaks ja juhtida infoturvariske, millel võib olla mõju lennundusohutusele ja mis võivad mõjutada tsiviillennunduses kasutatavaid info- ja kommunikatsioonitehnoloogia süsteeme ja andmeid;

b) avastada infoturvasündmusi ja teha kindlaks need, mida peetakse infoturvaintsidentideks ja mis võivad mõjutada lennundusohutust;

c) reageerida nendele infoturvaintsidentidele ja neist taastuda.

Artikkel 2

Kohaldamisala

1. Käesolevat määrust kohaldatakse järgmiste organisatsioonide suhtes:

a) hooldusorganisatsioonid, kelle suhtes kohaldatakse määruse (EL) nr 1321/2014 II lisa (osa 145) A jagu, välja arvatud organisatsioonid, mis tegelevad üksnes õhusõidukite hooldusega vastavalt määruse (EL) nr 1321/2014 Vb lisale (osa ML);

b) õhusõidukite jätkuva lennukõlblikkusega tegelevad organisatsioonid, kelle suhtes kohaldatakse määruse (EL) nr 1321/2014 Vc lisa (osa CAMO) A jagu, välja arvatud organisatsioonid, mis tegelevad üksnes õhusõidukite jätkuva lennukõlblikkusega vastavalt määruse (EL) nr 1321/2014 Vb lisale (osa ML);

c) lennuettevõtjad, kelle suhtes kohaldatakse määruse (EL) nr 965/2012 III lisa (osa ORO), välja arvatud need, kes käitavad üksnes järgmisi õhusõidukeid:

i) määruse (EL) nr 748/2012 artikli 1 lõike 2 punktis j määratletud ELA 2 õhusõiduk;

ii) ühe mootoriga propellerlennukid, mille suurim lubatud reisijakohtade arv on kuni viis ja mis ei ole liigitatud keerukateks mootorõhusõidukiteks, kui need stardivad ja maanduvad samal lennuväljal või samas käitamiskohas ning lendavad päeva ajal visuaallennureeglite (VFR) kohaselt;

iii) ühe mootoriga kopterid, mille suurim lubatud reisijakohtade arv on kuni viis ja mis ei ole liigitatud keerukateks mootorõhusõidukiteks, kui need stardivad ja maanduvad samal lennuväljal või samas käitamiskohas ning lendavad päeva ajal VFRi kohaselt;

d) sertifitseeritud koolitusorganisatsioonid, kelle suhtes kohaldatakse määruse (EL) nr 1178/2011 VII lisa (osa ORA), välja arvatud need, kes tegelevad üksnes määruse (EL) nr 748/2012 artikli 1 lõike 2 punktis j määratletud ELA2 õhusõidukeid hõlmava koolitustegevusega või kes tegelevad üksnes teoreetilise koolitusega;

e) õhusõidukite meeskondade lennundusmeditsiinikeskused, mille suhtes kohaldatakse määruse (EL) nr 1178/2011 VII lisa (osa ORA);

f) lennutreeningseadmete käitajad, kelle suhtes kohaldatakse määruse (EL) nr 1178/2011 VII lisa (osa ORA), välja arvatud need, kes tegelevad üksnes määruse (EL) nr 748/2012 artikli 1 lõike 2 punktis j määratletud ELA2 õhusõidukite lennutreeningseadmete käitamisega;

g) lennujuhtide koolitusorganisatsioonid ja lennujuhtide lennundusmeditsiinikeskused, mille suhtes kohaldatakse määruse (EL) 2015/340 III lisa (osa ATCO.OR);

h) organisatsioonid, kelle suhtes kohaldatakse rakendusmääruse (EL) 2017/373 III lisa (osa ATM/ANS.OR), välja arvatud järgmised teenuseosutajad:

i) aeronavigatsiooniteenuse osutajad, kellel on kõnealuse lisa punkti ATM/ANS.OR.A.010 kohane piiratud sertifikaat;

ii) lennuinfoteenuse osutajad, kes esitavad deklaratsioone kõnealuse lisa punkti ATM/ANS.OR.A.015 kohaselt;

i) U-space'i teenuseosutajad ja ühtse ühise teabeteenuse osutajad, kelle suhtes kohaldatakse rakendusmäärust (EL) 2021/664.

2. Käesolevat määrust kohaldatakse pädevate asutuste, sealhulgas Euroopa Liidu Lennundusohutusameti (edaspidi „amet") suhtes, kellele on osutatud käesoleva määruse artiklis 6 ja komisjoni delegeeritud määruse (EL) 2022/1645 ([14]) artiklis 5.

3. Käesolevat määrust kohaldatakse ka pädeva asutuse suhtes, kes vastutab lennundustehnilise töötaja lubade väljaandmise, pikendamise, muutmise, peatamise või kehtetuks tunnistamise eest vastavalt määruse (EL) nr 1321/2014 III lisale (osa 66).

4. Käesolev määrus ei piira rakendusmääruse (EL) 2015/1998 lisa punktis 1.7 ega direktiivi (EL) 2016/1148 artiklis 14 sätestatud info- ja küberturbenõuete kohaldamist.

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „infoturve" – võrgu- ja infosüsteemide konfidentsiaalsuse, tervikluse, autentsuse ja kättesaadavuse säilitamine;

2) „infoturvasündmus" – süsteemi, teenuse või võrgu puhul kindlaks tehtud ilming, mis osutab infoturbepoliitika võimalikule rikkumisele või infoturbekontrolli puudustele või seni tundmatule olukorrale, mis võib olla infoturbe seisukohast oluline;

3) „intsident" – sündmus, mis tegelikult kahjustab direktiivi (EL) 2016/1148 artikli 4 punktis 7 määratletud võrgu- ja infosüsteemide turvalisust;

4) „infoturvarisk" – infoturvasündmuse toimumise võimalusest tulenev risk organisatsiooni tsiviillennundustegevusele, varale, isikutele ja teistele organisatsioonidele. Infoturvariskid on seotud võimalusega, et potentsiaalsed ohuallikad kasutavad ära teabevara või teabevarade rühma turvaauke;

([14]) Komisjoni 14. juuli 2022. aasta delegeeritud määrus (EL) 2022/1645, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139 rakendamise eeskirjad nõuete osas, mis on seotud selliste infoturvariskide juhtimisega, mis võivad mõjutada komisjoni määrustega (EL) nr 748/2012 ja (EL) nr 139/2014 hõlmatud organisatsioonide lennuohutust, ning muudetakse komisjoni määrusi (EL) nr 748/2012 ja (EL) nr 139/2014 (ELT L 248, 26.9.2022, lk 18).

5) „ohuallikas“ – võimalik infoturbealane rikkumine, mis esineb kahju põhjustada võiva üksuse olemasolu või asjaolu, tegevuse või sündmuse esinemise korral;

6) „turvaauk“ – vara või süsteemi, menetluse, projekti, rakendamise või infoturbemeetmete viga või puudus, mida saab ära kasutada ja mille tulemuseks on vastuolu infoturbepoliitika nõuetega või nende rikkumine.

Artikkel 4

Organisatsioonidele ja pädevatele asutustele esitatavad nõuded

1. Artikli 2 lõikes 1 osutatud organisatsioonid täidavad käesoleva määruse II lisa (osa IS.I.OR) nõudeid.

2. Artikli 2 lõigetes 2 ja 3 osutatud pädevad asutused täidavad käesoleva määruse I lisa (osa IS.AR) nõudeid.

Artikkel 5

Muudest liidu õigusaktidest tulenevad nõuded

1. Kui artikli 2 lõikes 1 osutatud organisatsioon vastab direktiivi (EL) 2016/1148 artiklis 14 sätestatud turvanõuetele, mis on samaväärsed käesolevas määruses sätestatud nõuetega, loetakse nende turvanõuete täitmine käesolevas määruses sätestatud nõuetele vastavaks.

2. Kui artikli 2 lõikes 1 osutatud organisatsioon on käitaja või üksus, millele on osutatud liikmesriikide riiklikes tsiviillennundusjulgestuse programmides, mis on kehtestatud kooskõlas Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 300/2008 ([15]) artikliga 10, loetakse rakendusmääruse (EL) 2015/1998 lisa punktis 1.7 esitatud küberturbenõuded samaväärseks käesolevas määruses sätestatud nõuetega, välja arvatud käesoleva määruse II lisa punkti IS.I.OR.230 osas, mida täidetakse sõna-sõnaliselt.

3. Kui artikli 2 lõikes 1 osutatud organisatsiooniks on määruses (EL) 2021/696 osutatud Euroopa Geostatsionaarse Navigatsioonilisasüsteemi (EGNOS) aeronavigatsiooniteenuse osutaja, käsitatakse kõnealuse määruse V jaotise artiklites 33–43 sisalduvaid turvalisusega seotud nõudeid samaväärsetena käesolevas määruses sätestatud nõuetega, välja arvatud käesoleva määruse II lisa punkti IS.I.OR.230 osas, mida täidetakse sõna-sõnaliselt.

4. Komisjon võib pärast ameti ja direktiivi (EL) 2016/1148 artiklis 11 osutatud koostöörühmaga konsulteerimist anda välja suunised käesolevas määruses ja direktiivis (EL) 2016/1148 sätestatud nõuete samaväärsuse hindamiseks.

Artikkel 6

Pädev asutus

1. Ilma et see piiraks määruse (EL) 2021/696 artiklis 36 osutatud turvalisuse akrediteerimise nõukogule usaldatud ülesandeid, on asutus, kes vastutab käesolevas määruses sertifitseerimise ja järelevalve suhtes kehtestatud nõuete täitmise eest, järgmine:

a) artikli 2 lõike 1 punktis a osutatud organisatsioonide puhul määruse (EL) nr 1321/2014 II lisa (osa 145) kohaselt määratud pädev asutus;

b) artikli 2 lõike 1 punktis b osutatud organisatsioonide puhul määruse (EL) nr 1321/2014 Vc lisa (osa CAMO) kohaselt määratud pädev asutus;

([15]) Euroopa Parlamendi ja nõukogu 11. märtsi 2008. aasta määrus (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002 (ELT L 97, 9.4.2008, lk 72).

c) artikli 2 lõike 1 punktis c osutatud organisatsioonide puhul määruse (EL) nr 965/2012 III lisa (osa ORO) kohaselt määratud pädev asutus;

d) artikli 2 lõike 1 punktides d–f osutatud organisatsioonide puhul määruse (EL) nr 1178/2011 VII lisa (osa ORA) kohaselt määratud pädev asutus;

e) artikli 2 lõike 1 punktis g osutatud organisatsioonide puhul määruse (EL) 2015/340 artikli 6 lõike 2 kohaselt määratud pädev asutus;

f) artikli 2 lõike 1 punktis h osutatud organisatsioonide puhul rakendusmääruse (EL) 2017/373 artikli 4 lõike 1 kohaselt määratud pädev asutus;

g) artikli 2 lõike 1 punktis i osutatud organisatsioonide puhul vastavalt kas rakendusmääruse (EL) 2021/664 artikli 14 lõike 1 või lõike 2 kohaselt määratud pädev asutus.

2. Liikmesriigid võivad käesoleva määruse kohaldamisel määrata sõltumatu ja eraldiseisva üksuse, kes täidab lõikes 1 osutatud pädevate asutuste ülesandeid ja kohustusi. Sel juhul lepitakse kõnealuse üksuse ja lõikes 1 osutatud pädevate asutuste vahel kokku koordineerimismeetmed, et tagada tõhus järelevalve kõigi nõuete üle, mida asjaomane organisatsioon peab täitma.

3. Amet teeb täielikus kooskõlas kohaldatavate konfidentsiaalsuse, isikuandmete ja salastatud teabe kaitse eeskirjadega koostööd Euroopa Liidu Kosmoseprogrammi Ametiga (EUSPA) ja määruse (EL) 2021/696 artiklis 36 osutatud turvalisuse akrediteerimise nõukoguga, et tagada tõhus järelevalve EGNOSe aeronavigatsiooniteenuse osutaja suhtes kohaldatavate nõuete üle.

Artikkel 7

Asjakohase teabe esitamine võrgu- ja infoturbe valdkonna pädevatele asutustele

Käesolevas määruses sätestatud pädevad asutused teavitavad vastavalt direktiivi (EL) 2016/1148 artiklile 8 määratud ühtset kontaktpunkti põhjendamatu viivituseta kogu asjakohasest teabest, mis sisaldub teadetes, mille direktiivi (EL) 2016/1148 artikli 5 kohaselt identifitseeritud oluliste teenuste operaatorid on esitanud vastavalt käesoleva määruse II lisa punktile IS.I.OR.230 ja delegeeritud määruse (EL) 2022/1645 I lisa punktile IS.D.OR.230.

Artikkel 8

Määruse (EL) nr 1178/2011 muutmine

Määruse (EL) nr 1178/2011 VI lisa (osa ARA) ja VII lisa (osa ORA) muudetakse vastavalt käesoleva määruse III lisale.

Artikkel 9

Määruse (EL) nr 748/2012 muutmine

Määruse (EL) nr 748/2012 I lisa (osa 21) muudetakse vastavalt käesoleva määruse IV lisale.

Artikkel 10

Määruse (EL) nr 965/2012 muutmine

Määruse (EL) nr 965/2012 II lisa (osa ARO) ja III lisa (osa ORO) muudetakse vastavalt käesoleva määruse V lisale.

Artikkel 11

Määruse (EL) nr 139/2014 muutmine

Määruse (EL) nr 139/2014 II lisa (osa ADR.AR) muudetakse vastavalt käesoleva määruse VI lisale.

Artikkel 12

Määruse (EL) nr 1321/2014 muutmine

Määruse (EL) nr 1321/2014 II lisa (osa 145), III lisa (osa 66) ja Vc lisa (osa CAMO) muudetakse vastavalt käesoleva määruse VII lisale.

Artikkel 13

Määruse (EL) 2015/340 muutmine

Määruse (EL) 2015/340 II lisa (osa ATCO.AR) ja III lisa (osa ATCO.OR) muudetakse vastavalt käesoleva määruse VIII lisale.

Artikkel 14

Rakendusmääruse (EL) 2017/373 muutmine

Rakendusmääruse (EL) 2017/373 II lisa (osa ATM/ANS.AR) ja III lisa (osa ATM/ANS.OR) muudetakse vastavalt käesoleva määruse IX lisale.

Artikkel 15

Rakendusmääruse (EL) 2021/664 muutmine

Rakendusmäärust (EL) 2021/664 muudetakse järgmiselt.

1) Artikli 15 lõike 1 punkt f asendatakse järgmisega:

„f) rakendavad ja haldavad rakendusmääruse (EL) 2017/373 III lisa D alajao punkti ATM/ANS.OR.D.010 kohast julgestusalase juhtimise süsteemi ning delegeeritud määruse (EL) 2023/203 II lisa (osa IS.I.OR) kohast infoturbe halduse süsteemi;“

2) artiklisse 18 lisatakse punkt l:

„l) kehtestavad kooskõlas delegeeritud määruse (EL) 2023/203 I lisaga (osa IS.AR) infoturbe halduse süsteemi, rakendavad ja haldavad seda.“

Artikkel 16

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Seda kohaldatakse alates 22. veebruarist 2026.

EGNOSe aeronavigatsiooniteenuse osutaja puhul, kelle suhtes kohaldatakse rakendusmäärust (EL) 2017/373, kohaldatakse rakendusmäärust siiski alates 1. jaanuarist 2026.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 27. oktoober 2022

Komisjoni nimel
president
Ursula VON DER LEYEN

I LISA

INFOTURVE – ASUTUSELE ESITATAVAD NÕUDED

[OSA IS.AR]

IS.AR.100 Kohaldamisala

Käesoleva osaga kehtestatakse haldusele esitatavad nõuded, mida käesoleva määruse artikli 2 lõikes 2 osutatud pädevad asutused peavad täitma.

Nõuded, mida kõnealused pädevad asutused peavad täitma oma sertifitseerimis-, järelevalve- ja nõuete täitmise tagamise toimingute tegemisel, sisalduvad käesoleva määruse artikli 2 lõikes 1 ja delegeeritud määruse (EL) 2022/1645 artiklis 2 osutatud määrustes.

IS.AR.200 Infoturbe halduse süsteem

a) Pädev asutus kehtestab artiklis 1 sätestatud eesmärkide täitmiseks infoturbe halduse süsteemi ning rakendab ja hoiab seda töös, tagamaks, et pädev asutus:

   1) kehtestab infoturbepoliitika, milles sätestatakse pädeva asutuse üldpõhimõtted seoses infoturvariskide võimaliku mõjuga lennuohutusele;

   2) teeb kindlaks ja vaatab läbi infoturvariskid kooskõlas punktiga IS.AR.205;

   3) määrab kindlaks infoturvariski käsitlemise meetmed ja rakendab neid kooskõlas punktiga IS.AR.210;

   4) kooskõlas punktiga IS.AR.215 määrab kindlaks meetmed, mida on vaja infoturvasündmuste avastamiseks, ja rakendab neid meetmeid, teeb kindlaks juhtumid, mida käsitatakse intsidentidena, mis võivad mõjutada lennuohutust, ning reageerib nendele infoturvaintsidentidele ja võtab meetmeid neist taastumiseks;

   5) järgib punkti IS.AR.220 nõudeid, kui sõlmib punktis IS.AR.200 kirjeldatud tegevuse mis tahes osa kohta allhankelepingu mõne muu organisatsiooniga;

   6) järgib punktis IS.AR.225 esitatud nõudeid töötajatele;

   7) järgib punktis IS.AR.230 esitatud arvestuse pidamise nõudeid;

   8) jälgib oma organisatsiooni vastavust käesoleva määruse nõuetele ja annab puuduste kohta tagasisidet punkti IS.AR.225 alapunktis a osutatud isikule, et tagada parandusmeetmete tõhus rakendamine;

9) kaitseb konfidentsiaalsust teabe puhul, mida pädev asutus võib omada tema järelevalve alla kuuluvate organisatsioonide kohta, ja teabe puhul, mis on saadud käesoleva määruse II lisa (osa IS.I.OR) punkti IS.I.OR.230 ja delegeeritud määruse (EL) 2022/1645 lisa (osa IS.I.OR) punkti IS.I.OR.230 kohaselt loodud organisatsioonivälise aruandlusskeemide kaudu;

10) teavitab ametit muudatustest, mis mõjutavad pädeva asutuse suutlikkust täita käesolevas määruses määratletud ülesandeid ja kohustusi;

11) määrab kindlaks menetlused asjakohase teabe jagamiseks vastavalt vajadusele ning praktilisel ja õigeaegsel viisil, et abistada teisi pädevaid asutusi ja ameteid ning organisatsioone, kelle suhtes käesolevat määrust kohaldatakse, nende tegevusega seotud julgeolekuriskide tõhusal hindamisel, ja rakendab neid menetlusi.

b) Artiklis 1 osutatud nõuete pidevaks täitmiseks peab pädev asutus rakendama pidevat täiustamisprotsessi kooskõlas punktiga IS.AR.235.

c) Pädev asutus dokumenteerib kõik olulised protsessid, menetlused, rollid ja kohustused, mida on vaja punkti IS.AR.200 alapunkti a järgimiseks, ning kehtestab korra asjaomaste dokumentide muutmiseks.

d) Pädeva asutuse poolt punkti IS.AR.200 alapunkti a täitmiseks kehtestatud protsessid, menetlused, rollid ja kohustused peavad vastama tema tegevuse laadile ja keerukusele, lähtudes selle tegevusega kaasnevate infoturvariskide hindamisest, ning need võib integreerida muudesse olemasolevatesse juhtimissüsteemidesse, mida pädev asutus juba rakendab.

IS.AR.205 Infoturvariski hindamine

a) Pädev asutus teeb kindlaks kõik oma asutuse elemendid, mida võivad ähvardada infoturvariskid. See hõlmab järgmist:

1) toimingud, mida pädev asutus teostab, rajatised, mida ta pakub, ressursid, mis talle eraldatakse ja teenused, mida ta osutab;

2) seadmed, süsteemid, andmed ja teave, mis aitavad kaasa alapunktis 1 osutatud elementide toimimisele.

b) Pädev asutus teeb kindlaks liidesed, mis tema organisatsioonil on teiste organisatsioonidega ja mis võivad vastastikku põhjustada infoturvariske.

c) Alapunktides a ja b osutatud elementide ja liideste puhul teeb pädev asutus kindlaks infoturvariskid, mis võivad mõjutada lennuohutust.

Pädev asutus teeb iga kindlakstehtud riski puhul järgmist:

1) määrab riskitaseme vastavalt pädeva asutuse kehtestatud ja eelnevalt kindlaks määratud liigitusele;

2) seostab iga riski ja selle taseme alapunktide a ja b kohaselt kindlaks määratud asjakohase elemendi või liidesega.

Alapunktis 1 osutatud eelnevalt kindlaksmääratud liigituse puhul võetakse arvesse ohustsenaariumi esinemise võimalust ja selle ohutusalaste tagajärgede raskusastet. Selle liigituse kaudu ja võttes arvesse, kas pädeval asutusel on toimingute jaoks struktureeritud ning korratav riskijuhtimisprotsess, peab pädev asutus suutma kindlaks teha, kas risk on vastuvõetav või tuleb seda käsitleda kooskõlas punktiga IS.AR.210.

Selleks et riskihindamisi oleks vastastikku hõlpsam võrrelda, võetakse alapunkti 1 kohasel riskitaseme määramisel arvesse asjakohast teavet, mis on kogutud koostöös alapunktis b osutatud organisatsioonidega.

d) Pädev asutus vaatab alapunktide a, b ja c kohaselt tehtud riskihindamise läbi ning ajakohastab seda kõikidel järgmistel juhtudel:

1) infoturvariskiga seotud elemendid on muutunud;

2) pädeva asutuse ja teiste organisatsioonide vahelised liidesed või teiste organisatsioonide teatatud riskid on muutunud;

3) riskide kindlakstegemiseks, analüüsimiseks ja liigitamiseks kasutatud teave või teadmised on muutunud;

4) infoturvaintsidente analüüsides on saadud uusi teadmisi.

IS.AR.210 Infoturvariski käsitlemine

a) Pädev asutus töötab välja punkti IS.AR.205 kohaselt kindlaks tehtud vastuvõetamatute riskide käsitlemise meetmed, rakendab neid õigel ajal ja kontrollib nende jätkuvat tõhusust. Need meetmed võimaldavad pädeval asutusel teha järgmist:

1) kontrollida asjaolusid, mis aitavad kaasa ohustsenaariumi tegelikule esinemisele;

2) vähendada ohustsenaariumi realiseerumisest tulenevaid tagajärgi lennuohutusele;

3) vältida riske.

Kõnealuste meetmetega ei kaasne uusi võimalikke vastuvõetamatuid riske lennuohutusele.

b) Punkti IS.AR.225 alapunktis a osutatud isikut ja pädeva asutuse teisi asjassepuutuvaid töötajaid teavitatakse punkti IS.AR.205 kohaselt tehtud riskihindamise tulemustest, asjaomastest ohustsenaariumidest ja rakendatavatest meetmetest.

Pädev asutus teavitab ka selliseid organisatsioone, kellega tal on punkti IS.AR.205 alapunkti b kohane liides, mis tahes riskidest, mida pädev asutus ja organisatsioon jagavad.

IS.AR.215 Infoturvaintsidendid – nende avastamine, nendele reageerimine ja nendest taastumine

a) Pädev asutus rakendab punkti IS.AR.205 kohaselt tehtud riskihindamise tulemuste ja punkti IS.AR.210 kohaselt tehtud riskikäsitluse tulemuste põhjal meetmeid, et teha kindlaks sellised sündmused, mille puhul võivad realiseeruda vastuvõetamatud riskid ja mis võivad mõjutada lennuohutust. Kõnealused avastamismeetmed võimaldavad pädeval asutusel teha järgmist:

1) avastada kõrvalekalded eelnevalt kindlaks määratud funktsionaalse tulemuslikkuse lähtetasemetest;

2) anda hoiatus, et kõrvalekalde korral aktiveerida nõuetekohased reageerimismeetmed.

b) Pädev asutus rakendab meetmeid, et reageerida alapunkti a kohaselt kindlaks tehtud sündmusele, mis võib muutuda või olla muutunud infoturvaintsidendiks. Need reageerimismeetmed võimaldavad pädeval asutusel teha järgmist:

1) panna oma organisatsioon reageerima alapunkti a alapunktis 2 osutatud hoiatustele, aktiveerides eelnevalt kindlaks määratud vahendid ja tegevussuunad;

2) piirata rünnaku levikut ja vältida ohustsenaariumi täielikku realiseerumist;

3) kontrollida punkti IS.AR.205 alapunktis a kindlaks määratud asjaomaste elementide tõrkeolekut.

c) Pädev asutus rakendab infoturvaintsidentidest taastumiseks meetmeid, sealhulgas vajaduse korral erakorralisi meetmeid. Need taastumiseks kasutatavad meetmed võimaldavad pädeval asutusel teha järgmist:

1) kõrvaldada intsidendi põhjustanud olukorra või muuta intsidendi ohutase vastuvõetavaks;

2) taastada punkti IS.AR.205 alapunktis a kindlaks määratud asjaomaste elementide ohutus ajavahemiku jooksul, mille pädev asutus on taastumiseks eelnevalt kindlaks määranud.

IS.AR.220 Allhankelepingu sõlmimine infoturbe haldamiseks

Kui pädev asutus sõlmib punktis IS.AR.200 osutatud tegevuse mis tahes osa teostamiseks allhankelepingu mõne muu organisatsiooniga, peab ta tagama, et lepinguga hõlmatud tegevus vastab käesoleva määruse nõuetele ja et lepingupartner töötab tema järelevalve all. Pädev asutus tagab, et allhanketegevusega seotud riske juhitakse nõuetekohaselt.

IS.AR.225 Töötajatele esitatavad nõuded

Pädev asutus peab:

a) kindlaks määrama isiku, kes on volitatud kehtestama ja haldama käesoleva määruse rakendamiseks vajalikke organisatsioonilisi struktuure, põhimõtteid, protsesse ja menetlusi.

See isik peab:

1) omama täielikku juurdepääsuõigust ressurssidele, mida pädev asutus vajab kõigi käesoleva määrusega nõutavate ülesannete täitmiseks;

2) omama talle määratud ülesannete täitmiseks vajalikke volitusi;

b) olema kehtestanud korra, millega tagatakse, et käesoleva lisaga hõlmatud toiminguteks on piisavalt töötajaid;

c) olema kehtestanud korra, millega tagatakse, et alapunktis b osutatud töötajatel on oma ülesannete täitmiseks vajalik pädevus;

d) olema kehtestanud korra, millega tagatakse, et töötajad on teadlikud neile määratud rollide ja ülesannetega seotud kohustustest;

e) tagama selliste töötajate identiteedi ja usaldusväärsuse nõuetekohase kontrolli, kellel on juurdepääs infosüsteemidele ja andmetele, mille suhtes kohaldatakse käesoleva määruse nõudeid.

IS.AR.230 Arvestuse pidamine

a) Pädev asutus peab arvestust oma infoturbe halduse toimingute üle.

1) Pädev asutus tagab järgmiste dokumentide arhiveerimise ja jälgitavuse:

i) punkti IS.AR.200 alapunkti a alapunktis 5 osutatud allhankelepingud;

ii) teave punkti IS.AR.200 alapunktis d osutatud oluliste protsesside kohta;

iii) teave punktis IS.AR.205 osutatud riskihindamise käigus kindlaks tehtud riskide kohta koos punktis IS.AR.210 osutatud asjakohaste riskikäsitlusmeetmetega;

iv) teave infoturvasündmuste kohta, mida võib avastamata infoturvaintsidentide või turvaaukude kindlakstegemiseks olla vaja uuesti hinnata.

2) Alapunkti 1 alapunktis i osutatud teavet säilitatakse vähemalt viis aastat pärast allhankelepingu muutmist või lõpetamist.

3) Alapunkti 1 alapunktides ii ja iii osutatud teavet säilitatakse vähemalt viis aastat.

4) Alapunkti 1 alapunktis iv osutatud teavet säilitatakse seni, kuni asjaomased infoturvasündmused on pädeva asutuse kehtestatud perioodilisusega ümber hinnatud.

b) Pädev asutus registreerib infoturbehaldustöötajate kvalifikatsiooni ja kogemused.

1) Töötajate kvalifikatsiooni ja kogemusi käsitlevat teavet säilitatakse seni, kuni isik töötab pädeva asutuse heaks, ja vähemalt kolm aastat pärast seda, kui asjaomane isik on pädevast asutusest lahkunud.

2) Töötajate taotlusel tagatakse neile juurdepääs oma isiklikele dokumentidele. Lisaks esitab pädev asutus lahkuvatele töötajatele nende taotlusel koopia isiklikest dokumentidest.

c) Dokumentide vorming sätestatakse pädeva asutuse tegevuskorras.

d) Dokumente säilitatakse nii, et need oleksid kaitstud rikkumise, muutmise ja varguse eest, ning vajaduse korral määratakse kindlaks teabe salastatusaste. Pädev asutus kasutab asjakohaseid vahendeid dokumentide tervikluse ja autentsuse säilitamiseks ning tagab, et neile pääsevad juurde ainult selleks volitatud isikud.

IS.AR.235 Pidev täiustamine

a) Pädev asutus hindab asjakohaste tulemusnäitajate abil oma infoturbe halduse süsteemi tulemuslikkust ja küpsust. Hindamine viiakse läbi pädeva asutuse poolt eelnevalt kindlaks määratud ajakava alusel või pärast infoturvaintsidenti.

b) Kui alapunkti a kohase hindamise käigus leitakse puudusi, võtab pädev asutus vajalikud parandusmeetmed selle tagamiseks, et infoturbe halduse süsteem vastaks jätkuvalt kohaldatavatele nõuetele ja et infoturvariskide tase oleks jätkuvalt vastuvõetav. Lisaks hindab pädev asutus uuesti infoturbe halduse süsteemi neid elemente, mida vastuvõetud meetmed mõjutavad.

II LISA

INFOTURVE – ORGANISATSIOONIDELE ESITATAVAD NÕUDED

[OSA IS.I.OR]

IS.I.OR.100 Kohaldamisala

Käesoleva osaga kehtestatakse nõuded, mida käesoleva määruse artikli 2 lõikes 1 osutatud organisatsioonid peavad täitma.

IS.I.OR.200 Infoturbe halduse süsteem

a) Organisatsioon kehtestab artiklis 1 sätestatud eesmärkide täitmiseks infoturbe halduse süsteemi ning rakendab ja hoiab seda töös, tagamaks, et organisatsioon:

   1) kehtestab infoturbepoliitika, milles sätestatakse organisatsiooni üldpõhimõtted seoses infoturvariskide võimaliku mõjuga lennuohutusele;

   2) teeb kindlaks ja vaatab läbi infoturvariskid kooskõlas punktiga IS.I.OR.205;

   3) määrab kindlaks infoturvariski käsitlemise meetmed ja rakendab neid kooskõlas punktiga IS.I.OR.210;

   4) rakendab infoturbealast sisearuandluskava kooskõlas punktiga IS.I.OR.215;

   5) kooskõlas punktiga IS.I.OR.220 määrab kindlaks meetmed, mida on vaja infoturvasündmuste avastamiseks, ja rakendab neid meetmeid, teeb kindlaks juhtumid, mida käsitatakse intsidentidena, mis võivad mõjutada lennuohutust, välja arvatud punkti IS.I.OR.205 alapunkti e kohaselt lubatud juhud, ning reageerib nendele infoturvaintsidentidele ja võtab meetmeid neist taastumiseks;

6) rakendab meetmeid, millest pädev asutus on teatanud kui viivitamatust reageeringust lennuohutust mõjutavale infoturvaintsidendile või turvaaugule;

7) võtab kooskõlas punktiga IS.I.OR.225 asjakohaseid meetmeid pädeva asutuse teatatud puuduste kõrvaldamiseks;

8) rakendab punkti IS.I.OR.230 kohast välisaruandluskava, et pädev asutus saaks võtta asjakohaseid meetmeid;

9) järgib punkti IS.I.OR.235 nõudeid, kui sõlmib punktis IS.I.OR.200 osutatud tegevuse mis tahes osa kohta allhankelepingu mõne muu organisatsiooniga;

10) järgib punkti IS.I.OR.240 kohaseid nõudeid töötajatele;

11) järgib punkti IS.I.OR.245 kohaseid arvestuse pidamise nõudeid;

12) jälgib organisatsiooni vastavust käesoleva määruse nõuetele ja annab puuduste kohta tagasisidet vastutavale juhatajale, et tagada parandusmeetmete tõhus rakendamine;

13) kaitseb kogu sellise teabe konfidentsiaalsust, mida organisatsioon võib olla saanud teistelt organisatsioonidelt, vastavalt teabe tundlikkustasemele, ilma et see piiraks intsidentidest teatamise suhtes kohaldatavate nõuete järgimist.

b) Artiklis 1 osutatud nõuete pidevaks täitmiseks peab organisatsioon rakendama pidevat täiustamisprotsessi kooskõlas punktiga IS.I.OR.260.

c) Organisatsioon dokumenteerib kooskõlas punktiga IS.I.OR.250 kõik olulised protsessid, menetlused, rollid ja kohustused, mida on vaja punkti IS.I.OR.200 alapunkti a järgimiseks, ning kehtestab korra asjaomaste dokumentide muutmiseks. Kõnealuste protsesside, menetluste, rollide ja kohustustega seotud muudatusi hallatakse kooskõlas punktiga IS.I.OR.255.

d) Organisatsiooni poolt punkti IS.I.OR.200 alapunkti a täitmiseks kehtestatud protsessid, menetlused, rollid ja kohustused peavad vastama organisatsiooni tegevuse laadile ja keerukusele, lähtudes selle tegevusega kaasnevate infoturvariskide hindamisest, ning need võib integreerida muudesse olemasolevatesse juhtimissüsteemidesse, mida organisatsioon juba rakendab.

e) Ilma et see piiraks kohustust täita määruses (EL) nr 376/2014 sätestatud aruandlusnõudeid ja punkti IS.I.OR.200 alapunkti a alapunktis 13 sätestatud nõudeid, võib pädev asutus anda organisatsioonile loa mitte rakendada alapunktides a–d osutatud nõudeid ja punktides IS.I.OR.205–IS.I.OR.260 osutatud asjakohaseid nõudeid, kui organisatsioon tõendab asjaomast pädevat asutust rahuldaval viisil, et toimingud, mida ta teostab, rajatised, mida ta pakub, ressursid, mis talle eraldatakse ja teenused, mida ta osutab, ei põhjusta ei talle endale ega teistele organisatsioonidele infoturvariske, mis võivad mõjutada lennuohutust. See luba põhineb infoturvariskide dokumenteeritud hindamisel, mille teostab organisatsioon või kolmas isik kooskõlas punktiga IS.I.OR.205 ning mille on läbi vaadanud ja heaks kiitnud pädev asutus.

Pädev asutus vaatab kõnealuse loa kehtivuse üle pärast kohaldatavat järelevalveauditi tsüklit ja iga kord, kui organisatsiooni töös tehakse muudatusi.

IS.I.OR.205 Infoturvariski hindamine

a) Organisatsioon teeb kindlaks kõik oma elemendid, mida võivad ähvardada infoturvariskid. Need hõlmavad järgmist:

1) toimingud, mida organisatsioon teostab, rajatised, mida ta pakub, ressursid, mis talle eraldatakse ja teenused, mida ta osutab;

2) seadmed, süsteemid, andmed ja teave, mis aitavad kaasa alapunktis 1 loetletud elementide toimimisele.

b) Organisatsioon teeb kindlaks liidesed, mis tal on teiste organisatsioonidega ja mis võivad vastastikku põhjustada infoturvariske.

c) Alapunktides a ja b osutatud elementide ja liideste puhul teeb organisatsioon kindlaks infoturvariskid, mis võivad mõjutada lennuohutust. Organisatsioon teeb iga kindlakstehtud riski puhul järgmist:

1) määrab riskitaseme vastavalt organisatsiooni kehtestatud ja eelnevalt kindlaks määratud liigitusele;

2) seostab iga riski ja selle taseme alapunktide a ja b kohaselt kindlaks määratud asjakohase elemendi või liidesega.

Alapunktis 1 osutatud eelnevalt kindlaksmääratud liigituse puhul võetakse arvesse ohustsenaariumi esinemise võimalust ja selle ohutusalaste tagajärgede raskusastet. Sellele liigitusele tuginedes ja võttes arvesse, kas organisatsioonil on toimingute jaoks struktureeritud ning korratav riskijuhtimisprotsess, peab organisatsioon suutma kindlaks teha, kas risk on vastuvõetav või tuleb seda käsitleda kooskõlas punktiga IS.I.OR.210.

Selleks et riskihindamisi oleks vastastikku hõlpsam võrrelda, võetakse alapunkti 1 kohasel riskitaseme määramisel arvesse asjakohast teavet, mis on kogutud koostöös alapunktis b osutatud organisatsioonidega.

d) Organisatsioon vaatab alapunktide a ja b ning vajaduse korral c ja e kohaselt tehtud riskihindamise läbi ja ajakohastab seda kõikidel järgmistel juhtudel:

1) infoturvariskiga seotud elemendid on muutunud;

2) organisatsiooni ja teiste organisatsioonide vahelised liidesed või teiste organisatsioonide teatatud riskid on muutunud;

3) riskide kindlakstegemiseks, analüüsimiseks ja liigitamiseks kasutatud teave või teadmised on muutunud;

4) infoturvaintsidente analüüsides on saadud uusi teadmisi.

e) Erandina punktist c asendavad organisatsioonid, kes peavad täitma rakendusmääruse (EL) 2017/373 III lisa (osa ATM/ANS.OR) C-alajao nõudeid, lennuohutusele avalduva mõju analüüsi oma teenustele avalduva mõju analüüsiga, mis on ette nähtud punktis ATM/ANS.OR.C.005 nõutud hinnanguga ohutuse tagamise kohta. Hinnang ohutuse tagamise kohta tehakse kättesaadavaks lennuliiklusteenuse osutajatele, kellele nad teenuseid osutavad, ja kes vastutavad lennuohutusele avalduva mõju hindamise eest.

IS.I.OR.210 Infoturvariski käsitlemine

a) Organisatsioon töötab välja meetmed punkti IS.I.OR.205 kohaselt kindlaks tehtud vastuvõetamatute riskide käsitlemiseks, rakendab neid õigel ajal ja kontrollib nende jätkuvat tõhusust. Need meetmed võimaldavad organisatsioonil teha järgmist:

1) kontrollida asjaolusid, mis aitavad kaasa ohustsenaariumi tegelikule esinemisele;

2) vähendada ohustsenaariumi realiseerumisest tulenevaid tagajärgi lennuohutusele;

3) vältida riske.

Kõnealuste meetmetega ei kaasne uusi võimalikke vastuvõetamatuid riske lennuohutusele.

b) Punkti IS.I.OR.240 alapunktides a ja b osutatud isikut ja organisatsiooni teisi mõjutatud töötajaid teavitatakse punkti IS.I.OR.205 kohaselt tehtud riskihindamise tulemustest, asjaomastest ohustsenaariumidest ja rakendatavatest meetmetest.

Organisatsioon teavitab ka selliseid organisatsioone, kellega tal on punkti IS.I.OR.205 alapunkti b kohane liides, mis tahes riskidest, mida kumbki organisatsioon teisega jagab.

IS.I.OR.215 Infoturbealane sisearuandluskava

a) Organisatsioon kehtestab asutusesisese aruandluskava, mis võimaldab talletada ja hinnata infoturvasündmusi, sealhulgas neid, millest tuleb teatada vastavalt punktile IS.I.OR.230.

b) Kõnealune kava ja punktis IS.I.OR.220 osutatud protsess peavad võimaldama organisatsioonil teha järgmist:

1) välja selgitada, milliseid alapunkti a kohaselt teatatud juhtumeid peetakse infoturvaintsidentideks või turvaaukudeks, mis võivad mõjutada lennuohutust;

2) teha kindlaks alapunkti 1 kohaselt avastatud infoturvaintsidentide ja turvaaukude põhjused ning neid mõjutavad tegurid ning käsitleda neid infoturvariskide juhtimise protsessi osana kooskõlas punktidega IS.I.OR.205 ja IS.I.OR.220;

3) tagada, et hinnatakse kogu teadaolevat asjakohast teavet, mis on seotud alapunkti 1 kohaselt kindlaks tehtud infoturvaintsidentide ja turvaaukudega;

4) vajaduse korral tagada, et rakendatakse meetodit teabe asutusesiseseks levitamiseks.

c) Kõik allhankelepingu alusel tegutsevad organisatsioonid, kes põhjustavad asjaomasele organisatsioonile infoturvariske, mis võivad mõjutada lennuohutust, peavad teavitama organisatsiooni infoturvasündmustest. Kõnealune teave esitatakse konkreetsetes allhankelepingutes kehtestatud korras ja seda hinnatakse vastavalt alapunktile b.

d) Organisatsioon teeb uurimise käigus koostööd kõigi teiste organisatsioonidega, kes on märkimisväärselt panustanud oma tegevusega seotud infoturbesse.

e) Organisatsioon võib selle aruandlussüsteemi integreerida muude aruandlussüsteemidega, mida ta on juba rakendanud.

IS.I.OR.220 Infoturvaintsidendid – nende avastamine, nendele reageerimine ja nendest taastumine

a) Organisatsioon rakendab punkti IS.I.OR.205 kohaselt tehtud riskihindamise tulemuste ja punkti IS.I.OR.210 kohaselt tehtud riskikäsitluse tulemuste põhjal meetmeid, et teha kindlaks sellised intsidendid ja turvaaugud, mille puhul võivad realiseeruda vastuvõetamatud riskid ja mis võivad mõjutada lennuohutust. Kõnealused avastamismeetmed võimaldavad organisatsioonil teha järgmist:

1) avastada kõrvalekalded eelnevalt kindlaks määratud funktsionaalse tulemuslikkuse lähtetasemetest;

2) anda hoiatus, et kõrvalekalde korral aktiveerida nõuetekohased reageerimismeetmed.

b) Organisatsioon rakendab meetmeid, et reageerida alapunkti a kohaselt kindlaks tehtud sündmusele, mis võib muutuda või olla muutunud infoturvaintsidendiks. Kõnealused reageerimismeetmed võimaldavad organisatsioonil teha järgmist:

1) reageerida alapunkti a alapunktis 2 osutatud hoiatustele, aktiveerides eelnevalt kindlaks määratud vahendid ja tegevussuunad;

2) piirata rünnaku levikut ja vältida ohustsenaariumi täielikku realiseerumist;

3) kontrollida punkti IS.I.OR.205 alapunktis a kindlaks määratud asjaomaste elementide tõrkeolekut.

c) Organisatsioon rakendab infoturvaintsidentidest taastumiseks meetmeid, sealhulgas vajaduse korral erakorralisi meetmeid. Kõnealused taastumismeetmed võimaldavad organisatsioonil:

1) kõrvaldada intsidendi põhjustanud olukorra või muuta intsidendi ohutase vastuvõetavaks;

2) saavutada punkti IS.I.OR.205 alapunktis a kindlaks määratud asjaomaste elementide ohutus ajavahemiku jooksul, mille organisatsioon on taastumiseks eelnevalt kindlaks määranud.

IS.I.OR.225 Reageerimine pädeva asutuse teatatud puudustele

a) Kui pädevalt asutuselt saadakse teade puuduse kohta, teeb organisatsioon järgmist:

1) selgitab välja nõuetele mittevastavuse algpõhjuse või -põhjused ja nõuetele mittevastavust soodustavad tegurid;

2) töötab välja parandusmeetmete kava;

3) tõendab pädevat asutust rahuldaval viisil, et nõuetele mittevastavus on kõrvaldatud.

b) Alapunktis a osutatud meetmed võetakse pädeva asutusega kokkulepitud aja jooksul.

IS.I.OR.230 Infoturbealane välisaruandluskava

a) Organisatsioon rakendab infoturbealast aruandlussüsteemi, mis vastab määruses (EL) nr 376/2014 ning selle alusel vastu võetud delegeeritud õigusaktides ja rakendusaktides sätestatud nõuetele, kui kõnealust määrust organisatsiooni suhtes kohaldatakse.

b) Ilma et see piiraks määruses (EL) nr 376/2014 sätestatud kohustusi, tagab organisatsioon, et ta teavitab oma pädevat asutust kõigist infoturvaintsidentidest või turvaaukudest, mis võivad kujutada endast märkimisväärset riski lennuohutusele. Lisaks kohaldatakse järgmist:

1) kui selline intsident või turvaauk mõjutab õhusõidukit või sellega seotud süsteemi või komponenti, teatab organisatsioon sellest ka projekti kinnituse omanikule;

2) kui selline intsident või turvaauk mõjutab organisatsioonis kasutatavat süsteemi või komponenti, teatab organisatsioon sellest süsteemi või komponendi konstrueerimise eest vastutavale organisatsioonile.

c) Organisatsioon edastab alapunktis b osutatud olukordade kohta teavet järgmiselt:

1) pädevat asutust ja vajaduse korral projekti kinnituse omanikku või süsteemi või komponendi projekteerimise eest vastutavat organisatsiooni teavitatakse kohe, kui organisatsioon asjaomasest olukorrast teada saab;

2) pädevat asutust ja vajaduse korral projekti kinnituse omanikku või süsteemi või komponendi projekteerimise eest vastutavat organisatsiooni teavitatakse nii kiiresti kui võimalik, kuid mitte hiljem kui 72 tundi pärast seda, kui organisatsioon asjaomasest olukorrast teada saab, välja arvatud erakorraliste takistavate asjaolude korral.

Teade koostatakse pädeva asutuse määratud vormis ja see peab sisaldama kogu asjakohast teavet, mida organisatsioon on olukorra kohta kogunud;

3) pädevale asutusele ja vajaduse korral projekti kinnituse omanikule või süsteemi või komponendi projekteerimise eest vastutavale organisatsioonile esitatakse järelaruanne, milles on üksikasjalikult kirjeldatud meetmeid, mida organisatsioon on intsidendist taastumiseks võtnud või kavatseb võtta, ning meetmeid, mida ta kavatseb võtta samasuguste infoturvaintsidentide vältimiseks tulevikus.

Järelaruanne esitatakse kohe, kui need meetmed on kindlaks määratud, ja see koostatakse pädeva asutuse määratud vormis.

IS.I.OR.235 Allhankelepingu sõlmimine infoturbe haldamiseks

a) Kui organisatsioon sõlmib punktis IS.I.OR.200 osutatud tegevuse mis tahes osa teostamiseks allhankelepingu mõne muu organisatsiooniga, peab ta tagama, et lepinguga hõlmatud tegevus vastab käesoleva määruse nõuetele ja et lepingupartner töötab tema järelevalve all. Organisatsioon tagab, et allhanketegevusega seotud riske juhitakse nõuetekohaselt.

b) Organisatsioon tagab, et pädeval asutusel on taotluse korral juurdepääs allhankelepingu alusel tegutsevale organisatsioonile, et teha kindlaks käesolevas määruses sätestatud kohaldatavate nõuete jätkuv järgimine.

IS.I.OR.240 Töötajatele esitatavad nõuded

a) Organisatsiooni vastutav juhataja, kes on määratud määruste (EL) nr 1321/2014, (EL) nr 965/2012, (EL) nr 1178/2011, (EL) 2015/340, rakendusmääruse (EL) 2017/373 või rakendusmääruse (EL) 2021/664 kohaselt, nagu on osutatud käesoleva määruse artikli 2 lõikes 1, vastutab organisatsiooni esindajana selle eest, et organisatsioonis on kõiki käesoleva määrusega nõutavaid toiminguid võimalik rahastada ja ellu viia. See isik peab tegema järgmist:

1) tagama, et käesoleva määruse nõuete täitmiseks on olemas kõik vajalikud vahendid;

2) kehtestama punkti IS.I.OR.200 alapunkti a alapunktis 1 osutatud infoturvapoliitika ja seda edendama;

3) tõendama, et tal on olemas põhiteadmised käesoleva määruse kohta.

b) Vastutav juhataja määrab isiku või isikute rühma, et tagada organisatsiooni vastavus käesoleva määruse nõuetele, ning määrab kindlaks nende volituste ulatuse. Kõnealune isik või isikute rühm allub otse vastutavale juhatajale ning tal peavad olema oma kohustuste täitmiseks vajalikud teadmised, taust ja kogemused. Menetlustes tuleb kindlaks määrata, kes asendab konkreetset isikut tema pikemal äraolekul.

c) Vastutav juhataja määrab isiku või isikute rühma, kes vastutab punkti IS.I.OR.200 alapunkti a alapunktis 12 osutatud vastavuskontrolli eest.

d) Kui organisatsioon kasutab organisatsioonilisi infoturbestruktuure, -põhimõtteid, -protsesse ja -menetlusi koos teiste organisatsioonidega või oma organisatsiooni selliste valdkondadega, mille puhul kinnitust või deklaratsiooni ei nõuta, võib vastutav juhataja delegeerida oma ülesanded ühisele vastutavale isikule.

Sel juhul lepivad organisatsiooni vastutav juhataja ja ühine vastutav isik kokku koordineerimismeetmed, et tagada infoturbehalduse nõuetekohane integreerimine organisatsiooni.

e) Vastutav juhataja või alapunktis d osutatud ühine vastutav isik vastutab organisatsiooni esindajana punkti IS.I.OR.200 rakendamiseks vajalike organisatsiooniliste struktuuride, põhimõtete, protsesside ja menetluste ning nende haldamise eest organisatsioonis.

f) Organisatsioonis kehtestatakse kord, millega tagatakse, et käesoleva lisaga hõlmatud toiminguteks on piisavalt töötajaid.

g) Organisatsioonis kehtestatakse kord, millega tagatakse, et alapunktis f osutatud töötajatel on oma ülesannete täitmiseks vajalik pädevus.

h) Organisatsioonis kehtestatakse kord, millega tagatakse, et töötajad on teadlikud neile määratud rollide ja ülesannetega seotud kohustustest.

i) Organisatsioon peab tagama, selliste töötajate identiteedi ja usaldusväärsuse nõuetekohase kontrolli, kellel on juurdepääs infosüsteemidele ja andmetele, mille suhtes kohaldatakse käesoleva määruse nõudeid.

IS.I.OR.245 Arvestuse pidamine

a) *Organisatsioon peab arvestust oma infoturbe halduse toimingute üle.*

1) Organisatsioon tagab järgmiste dokumentide arhiveerimise ja jälgitavuse:

i) kõik punkti IS.I.OR.200 alapunkti e kohaselt saadud load ja nendega seotud turvariskihindamised;

ii) punkti IS.I.OR.200 alapunkti a alapunktis 9 osutatud allhankelepingud;

iii) teave punkti IS.I.OR.200 alapunktis d osutatud oluliste protsesside kohta;

iv) teave punktis IS.I.OR.205 osutatud riskihindamise käigus kindlaks tehtud riskide kohta koos punktis IS.I.OR.210 osutatud asjakohaste riskikäsitlusmeetmetega;

v) andmed punktides IS.I.OR.215 ja IS.I.OR.230 osutatud aruandluskavade kohaselt teatatud infoturvaintsidentide ja turvaaukude kohta;

vi) teave selliste infoturvasündmuste kohta, mida võib avastamata infoturvaintsidentide või turvaaukude kindlakstegemiseks olla vaja uuesti hinnata.

2) Alapunkti 1 alapunktis i osutatud teavet säilitatakse vähemalt viis aastat pärast asjaomase loa kehtivuse lõppemist.

3) Alapunkti 1 alapunktis ii osutatud teavet säilitatakse vähemalt viis aastat pärast allhankelepingu muutmist või lõpetamist.

4) Alapunkti 1 alapunktides iii, iv ja v osutatud teavet säilitatakse vähemalt viis aastat.

5) Alapunkti 1 alapunktis vi osutatud teavet säilitatakse seni, kuni asjaomased infoturvasündmused on organisatsiooni kehtestatud perioodilisusega ümber hinnatud.

b) *Organisatsioon registreerib infoturbehaldustöötajate kvalifikatsiooni ja kogemused.*

1) Töötajate kvalifikatsiooni ja kogemusi käsitlevat teavet säilitatakse seni, kuni isik töötab organisatsiooni heaks, ja vähemalt kolm aastat pärast seda, kui asjaomane isik on organisatsioonist lahkunud.

2) Töötajate taotlusel tagatakse neile juurdepääs oma isiklikele dokumentidele. Lisaks esitab organisatsioon lahkuvatele töötajatele nende taotlusel koopia isiklikest dokumentidest.

c) Dokumentide vorming sätestatakse organisatsiooni tegevuskorras.

d) Dokumente säilitatakse nii, et need oleksid kaitstud rikkumise, muutmise ja varguse eest, ning vajaduse korral määratakse kindlaks teabe salastatusaste. Organisatsioon kasutab asjakohaseid vahendeid dokumentide tervikluse ja autentsuse säilitamiseks ning tagab, et neile pääsevad juurde ainult selleks volitatud isikud.

IS.I.OR.250 Infoturbehalduse käsiraamat

a) Organisatsioon teeb pädevale asutusele kättesaadavaks infoturbehalduse käsiraamatu ning vajaduse korral kõik selles viidatud käsiraamatud ja menetlused, mis sisaldavad järgmist teavet:

1) vastutava juhataja allkirjastatud kinnitus selle kohta, et organisatsioon tegutseb pidevalt kooskõlas käesoleva lisa ja infoturbehalduse käsiraamatuga. Kui vastutav juhataja ei ole organisatsiooni tegevjuht, kaasallkirjastab avalduse tegevjuht;

2) punkti IS.I.OR.240 alapunktides b ja c kindlaks määratud isiku(te) ametinimetus(ed), nimi (nimed), kohustused, vastutus, ülesanded ja volitused;

3) vajaduse korral punkti IS.I.OR.240 alapunktis d määratletud ühise vastutava isiku ametinimetus, nimi, kohustused, vastutus, ülesanded ja volitused;

4) organisatsiooni infoturvapoliitika, millele on osutatud punkti IS.I.OR.200 alapunkti a alapunktis 1;

5) töötajate arvu ja kategooriate ning töötajate olemasolu planeerimiseks kasutatava süsteemi üldine kirjeldus vastavalt punkti IS.I.OR.240 nõuetele;

6) punkti IS.I.OR.200 rakendamise eest vastutavate võtmeisikute, sealhulgas punkti IS.I.OR.200 alapunkti a alapunktis 12 osutatud vastavuskontrolli funktsiooni eest vastutava(te) isiku(te) ametinimetus(ed), kohustused, vastutus, ülesanded ja volitused;

7) organisatsiooni skeem, milles on näidatud alapunktides 2 ja 6 osutatud isikute aruandlus- ja vastutusahelad;

8) punktis IS.I.OR.215 osutatud sisearuandluskava kirjeldus;

9) menetlused, milles täpsustatakse, kuidas organisatsioon tagab käesoleva osa nõuete täitmise, ning eelkõige:

i) punkti IS.I.OR.200 alapunktis c osutatud dokumenteerimistoimingud;

ii) menetlused, millega määratakse kindlaks, kuidas organisatsioon kontrollib punkti IS.I.OR.200 alapunkti a alapunktis 9 osutatud lepingulist tegevust;

iii) alapunktis c osutatud menetlus infoturbehalduse käsiraamatu muutmiseks;

10) loetelu nõuete täitmise alternatiivsetest meetoditest, mis on praegu heaks kiidetud.

b) Infoturbehalduse käsiraamatu esimene väljaanne kiidetakse heaks ja pädev asutus säilitab selle koopia. Infoturbehalduse käsiraamatut muudetakse vastavalt vajadusele, et tagada organisatsiooni infoturbe halduse süsteemi kirjelduse ajakohasus. Pädevale asutusele esitatakse koopia kõigist infoturbehalduse käsiraamatu muudatustest.

c) Infoturbehalduse käsiraamatu muudatusi hallatakse organisatsiooni kehtestatud korras. Pädev asutus peab heaks kiitma kõik muudatused, mille suhtes asjaomast korda ei kohaldata, ja muudatused, mis on seotud punkti IS.I. OR.255 alapunktis b osutatud muudatustega.

d) Organisatsioon võib infoturbehalduse käsiraamatu integreerida muude olemasolevate juhtkonna näidismaterjalide või käsiraamatutega, kui on olemas selged ristviited, mis näitavad, millised juhtkonna näidismaterjali või käsiraamatu osad vastavad käesolevas lisas esitatud eri nõuetele.

IS.I.OR.255 Infoturbe halduse süsteemi muudatused

a) Infoturbe halduse süsteemi muudatusi võib hallata ja neist võib pädevat asutust teavitada organisatsiooni väljatöötatud korras. Selle korra peab heaks kiitma pädev asutus.

b) Kui asjaomase infoturbe halduse süsteemi muudatuste suhtes ei kohaldata alapunktis a osutatud korda, peab organisatsioon esitama need pädevale asutusele heakskiidu taotlemiseks ning selle saamiseks.

Kõnealuste muudatuste suhtes kohaldatakse järgmist:

1) taotlus tuleb esitada enne muudatuse tegemist, et pädeval asutusel oleks võimalik kontrollida, kas organisatsioon vastab jätkuvalt käesolevas määruses sätestatud nõuetele, ning vajaduse korral muuta organisatsiooni sertifikaati ja sellele lisatud sertifitseerimistingimusi;

2) organisatsioon teeb pädevale asutusele kättesaadavaks kogu teabe, mida nõutakse muudatuse hindamiseks;

3) muudatust rakendatakse alles siis, kui pädevalt asutuselt on selle kohta saadud ametlik heakskiit;

4) organisatsioon peab selliste muudatuste rakendamise ajal tegutsema pädeva asutuse ettenähtud tingimustel.

IS.I.OR.260 Pidev täiustamine

a) Organisatsioon hindab asjakohaste tulemusnäitajate abil infoturbe halduse süsteemi tulemuslikkust ja küpsust. Hindamine toimub organisatsiooni poolt eelnevalt kindlaks määratud ajakava alusel või pärast infoturvaintsidenti.

b) Kui alapunkti a kohase hindamise käigus leitakse puudusi, võtab organisatsioon vajalikud parandusmeetmed selle tagamiseks, et infoturbe halduse süsteem vastaks jätkuvalt kohaldatavatele nõuetele ja et infoturvariskide tase oleks jätkuvalt vastuvõetav. Lisaks hindab organisatsioon uuesti infoturbe halduse süsteemi neid elemente, mida vastuvõetud meetmed mõjutavad.

III LISA

Määruse (EL) nr 1178/2011 VI lisa (osa ARA) ja VII lisa (osa ORA) muudetakse järgmiselt.

1) VI lisa (osa ARA) muudetakse järgmiselt:

a) punktile ARA.GEN.125 lisatakse alapunkt c:

„c) Liikmesriigi pädev asutus esitab ametile viivitamata ohutuse seisukohast olulise teabe, mis on pärit infoturbearuannetest, mis asutus on saanud vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punktile IS.I.OR.230.“;

b) punkti ARA.GEN.135 järele lisatakse punkt ARA.GEN.135A:

„**ARA.GEN.135A Viivitamatu reageering lennuohutust mõjutavale infoturvaintsidendile või turvaaugule**

a) Pädev asutus rakendab süsteemi, et nõuetekohaselt koguda, analüüsida ja levitada teavet, mis on seotud lennuohutust mõjutada võivate infoturvaintsidentide ja turvaaukudega, millest organisatsioonid teatavad. Seda tehakse kooskõlastatult kõigi teiste asjaomaste asutustega, kes vastutavad liikmesriigis info- või küberturbe eest, et suurendada aruandluskavade kooskõlastatust ja ühilduvust.

b) Amet rakendab süsteemi, et nõuetekohaselt analüüsida kogu punkti ARA.GEN.125 alapunkti c kohaselt saadud asjakohast ohutusalast teavet, ning esitab põhjendamatu viivituseta liikmesriikidele ja komisjonile kogu teabe, sealhulgas soovitused või parandusmeetmed, mis on vaja võtta selleks, et nad saaksid õigeaegselt reageerida infoturvaintsidendile või turvaaugule, mis võib mõjutada lennuohutust seoses toodete, osade, teisaldatava varustuse, isikute või organisatsioonidega, kelle suhtes kohaldatakse määrust (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusakte ja rakendusakte.

c) Alapunktides a ja b osutatud teabe saamisel võtab pädev asutus asjakohased meetmed, et käsitleda infoturvaintsidendi või turvaaugu võimalikku mõju lennuohutusele.

d) Alapunkti c kohaselt võetavad meetmed tehakse viivitamata teatavaks kõikidele isikutele ja organisatsioonidele, kes vastavalt määrusele (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusaktidele ja rakendusaktidele neid meetmeid kohaldavad. Liikmesriigi pädev asutus teeb meetmed teatavaks ka ametile ning ühise tegutsemise vajaduse tekkimise korral teiste asjaomaste liikmesriikide pädevatele asutustele.“;

c) punktile ARA.GEN.200 lisatakse alapunkt e:

„e) Lisaks alapunktis a esitatud nõuetele vastab pädeva asutuse poolt kehtestatud ja töös hoitav juhtimissüsteem rakendusmääruse (EL) 2023/203 I lisa (osa IS.AR) nõuetele, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust.“;

d) punkti ARA.GEN.205 muudetakse järgmiselt:

i) pealkiri asendatakse järgmisega:

„**ARA.GEN.205 Ülesannete jaotus**“;

ii) lisatakse alapunkt c:

„c) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti ORA.GEN.200A nõudeid, võib pädev asutus jaotada ülesandeid kvalifitseeritud üksustele kooskõlas alapunktiga a või mis tahes asjaomasele asutusele, kes vastutab liikmesriigis info- või küberturbe eest. Ülesannete jaotamisel tagab pädev asutus, et:

1) pädev üksus või asjaomane asutus koordineerib ja võtab arvesse kõiki lennuohutusega seotud aspekte;

2) pädeva üksuse või asjaomase asutuse sertifitseerimis- ja järelevalvetoimingute tulemused integreeritakse organisatsiooni üldistesse sertifitseerimis- ja järelevalvetoimikutesse;

3) tema poolt punkti ARA.GEN.200 alapunkti e kohaselt kehtestatud infoturbe halduse süsteem hõlmab kõiki tema nimel täidetavaid sertifitseerimise ja pideva järelevalvega seotud ülesandeid.“;

e) punktile ARA.GEN.300 lisatakse alapunkt g:

„g) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti ORA.GEN.200A nõudeid, kontrollib pädev asutus alapunktide a–f järgimist ja vaatab läbi kõik käesoleva määruse punkti IS.I.OR.200 alapunkti e või delegeeritud määruse (EL) 2022/1645 punkti IS.D.OR.200 alapunkti e kohaselt antud sertifikaadid pärast kohaldatavat järelevalveauditi tsüklit ja iga kord, kui organisatsiooni töös tehakse muudatusi.“

f) punkti ARA.GEN.330 järele lisatakse punkt ARA.GEN.330A:

„**ARA.GEN.330A Infoturbe halduse süsteemi muudatused**

a) Muudatuste puhul, mida hallatakse ja millest teavitatakse pädevat asutust vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktis a sätestatud menetlusele, lisab pädev asutus selliste muudatuste läbivaatamise oma pidevasse järelevalvesse kooskõlas punktis ARA.GEN.300 sätestatud põhimõtetega. Nõuetele mittevastavuse korral teavitab pädev asutus sellest organisatsiooni, nõuab täiendavaid muudatusi ja tegutseb vastavalt punktile ARA.GEN.350.

b) Teiste muudatuste puhul, mis nõuavad heakskiidu taotlemist vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktile b, kohaldatakse järgmist:

1) muudatuse taotluse saamisel kontrollib pädev asutus enne heakskiidu andmist organisatsiooni vastavust kohaldatavatele nõuetele;

2) pädev asutus kehtestab tingimused, mille alusel organisatsioon võib muudatuse rakendamise ajal tegutseda;

3) kui pädev asutus on veendunud, et organisatsioon vastab kohaldatavatele nõuetele, kiidab pädev asutus muudatuse heaks.“;

2) VII lisa (osa ORA) muudetakse järgmiselt:

punkti ORA.GEN.200 järele lisatakse punkt ORA.GEN.200A:

„**ORA.GEN.200A Infoturbe halduse süsteem**

Lisaks punktis ORA.GEN.200 osutatud juhtimissüsteemile kehtestab organisatsioon kooskõlas rakendusmäärusega (EL) 2023/203 infoturbe halduse süsteemi, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust, ning rakendab süsteemi ja hoiab seda töös.“

IV LISA

Määruse (EL) nr 748/2012 I lisa (osa 21) muudetakse järgmiselt:

1) sisukorda muudetakse järgmiselt.

a) pealkirja 21.B.20 järele lisatakse järgmine pealkiri:

„21.B.20A Viivitamatu reageering lennuohutust mõjutavale infoturvaintsidendile või turvaaugule“;

b) punkti 21.B.30 pealkiri asendatakse järgmisega:

„21.B.30 Ülesannete jaotus“;

c) pealkirja 21.B.240 järele lisatakse järgmine pealkiri:

„21.B.240A Infoturbe halduse süsteemi muudatused“;

d) pealkirja 21.B.435 järele lisatakse järgmine pealkiri:

„21.B.435A Infoturbe halduse süsteemi muudatused“;

2) punktile 21.B.15 lisatakse alapunkt c:

„c) Liikmesriigi pädev asutus esitab ametile viivitamata ohutuse seisukohast olulise teabe, mis on pärit infoturbearuannetest, mis asutus on saanud vastavalt delegeeritud määruse (EL) 2022/1645 lisa (osa IS.D.OR) punktile IS.D.OR.230.“;

3) punkti 21.B.20 järele lisatakse punkt 21.B.20A:

„21.B.20A Viivitamatu reageering lennuohutust mõjutavale infoturvaintsidendile või turvaaugule

a) Pädev asutus rakendab süsteemi, et nõuetekohaselt koguda, analüüsida ja levitada teavet, mis on seotud lennuohutust mõjutada võivate infoturvaintsidentide ja turvaaukudega, millest organisatsioonid teatavad. Seda tehakse kooskõlastatult kõigi teiste asjaomaste asutustega, kes vastutavad liikmesriigis info- või küberturbe eest, et suurendada aruandluskavade kooskõlastatust ja ühilduvust.

b) Amet rakendab süsteemi, et nõuetekohaselt analüüsida kogu punkti 21.B.15 alapunkti c kohaselt saadud asjakohast ohutusalast teavet, ning esitab põhjendamatu viivituseta liikmesriikidele ja komisjonile kogu teabe, sealhulgas soovitused või parandusmeetmed, mis on vaja võtta selleks, et nad saaksid õigeaegselt reageerida infoturvaintsidendile või turvaaugule, mis võib mõjutada lennuohutust seoses toodete, osade, teisaldatava varustuse, isikute või organisatsioonidega, kelle suhtes kohaldatakse määrust (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusakte ja rakendusakte.

c) Alapunktides a ja b osutatud teabe saamisel võtab pädev asutus asjakohased meetmed, et käsitleda infoturvaintsidendi või turvaaugu võimalikku mõju lennuohutusele.

d) Alapunkti c kohaselt võetavad meetmed tehakse viivitamata teatavaks kõikidele isikutele ja organisatsioonidele, kes vastavalt määrusele (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusaktidele ja rakendusaktidele neid meetmeid kohaldavad. Liikmesriigi pädev asutus teeb meetmed teatavaks ka ametile ning ühise tegutsemise vajaduse tekkimise korral teiste asjaomaste liikmesriikide pädevatele asutustele.“;

4) punktile 21.B.25 lisatakse alapunkt e:

„e) Lisaks alapunktis a esitatud nõuetele vastab pädeva asutuse poolt kehtestatud ja töös hoitav juhtimissüsteem rakendusmääruse (EL) 2023/203 I lisa (osa IS.AR) nõuetele, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust.“;

5) punkti 21.B.30 muudetakse järgmiselt:

a) pealkiri asendatakse järgmisega:

„21.B.30 Ülesannete jaotus“;

b) lisatakse alapunkt c:

„c) Sertifitseerimisel ja järelevalve teostamisel selle üle, kas organisatsioon täidab punktide 21.A.139A ja 21.A.239A nõudeid, võib pädev asutus jaotada ülesandeid kvalifitseeritud üksustele kooskõlas alapunktiga a või mis tahes asjaomasele asutusele, kes vastutab liikmesriigis info- või küberturbe eest. Ülesannete jaotamisel tagab pädev asutus, et:

1) pädev üksus või asjaomane asutus koordineerib ja võtab arvesse kõiki lennuohutusega seotud aspekte;

2) pädeva üksuse või asjaomase asutuse sertifitseerimis- ja järelevalvetoimingute tulemused integreeritakse organisatsiooni üldistesse sertifitseerimis- ja järelevalvetoimikutesse;

3) tema poolt punkti 21.B.25 alapunkti e kohaselt kehtestatud infoturbe halduse süsteem hõlmab kõiki tema nimel täidetavaid sertifitseerimise ja pideva järelevalvega seotud ülesandeid.“;

6) punktile 21.B.221 lisatakse alapunkt g:

„g) Seoses sertifitseerimisega ja järelevalvega selle üle, kas organisatsioon täidab punkti 21.A.139A nõudeid, kontrollib pädev asutus alapunktide a–f järgimist ja vaatab läbi kõik käesoleva määruse punkti IS.I.OR.200 alapunkti e või delegeeritud määruse (EL) 2022/1645 punkti IS.D.OR.200 alapunkti e kohaselt antud sertifikaadid pärast kohaldatavat järelevalveauditi tsüklit ja iga kord, kui organisatsiooni töös tehakse muudatusi.“;

7) punkti 21.B.240 järele lisatakse punkt 21.B.240A:

„**21.B.240A Infoturbe halduse süsteemi muudatused**

a) Muudatuste puhul, mida hallatakse ja millest teavitatakse pädevat asutust vastavalt delegeeritud määruse (EL) 2022/1645 lisa (osa IS.D.OR) punkti IS.D.OR.255 alapunktis a sätestatud menetlusele, lisab pädev asutus selliste muudatuste läbivaatamise oma pidevasse järelevalvesse kooskõlas punktis 21.B.221 sätestatud põhimõtetega. Nõuetele mittevastavuse korral teavitab pädev asutus sellest organisatsiooni, nõuab täiendavaid muudatusi ja tegutseb vastavalt punktile 21.B.225.

b) Teiste muudatuste puhul, mis nõuavad heakskiidu taotlemist vastavalt delegeeritud määruse (EL) 2022/1645 lisa (osa IS.D.OR) punkti IS.D.OR.255 alapunktile b, kohaldatakse järgmist:

1) muudatuse taotluse saamisel kontrollib pädev asutus enne heakskiidu andmist organisatsiooni vastavust kohaldatavatele nõuetele;

2) pädev asutus kehtestab tingimused, mille alusel organisatsioon võib muudatuse rakendamise ajal tegutseda;

3) kui pädev asutus on veendunud, et organisatsioon vastab kohaldatavatele nõuetele, kiidab pädev asutus muudatuse heaks.“;

8) punktile 21.B.431 lisatakse alapunkt d:

„d) Sertifitseerimisel ja järelevalve teostamisel selle üle, kas organisatsioon täidab punkti 21.A.239A nõudeid, kohaldab pädev asutus lisaks alapunktide a–c nõuetele järgmisi põhimõtteid:

1) pädev asutus vaatab läbi liidesed ja nendega seotud riskid, mis on kindlaks tehtud vastavalt delegeeritud määruse (EL) 2022/1645 lisa (osa IS.D.OR) punkti IS.D.OR.205 alapunktile b iga tema järelevalve alla kuuluva organisatsiooni poolt;

2) kui eri organisatsioonid avastavad vastastikes liidetes lahknevusi ja teevad kindlaks sellega seotud riskid, vaatab pädev asutus need koos asjaomaste organisatsioonidega läbi ja teeb vajaduse korral asjakohased järeldused, et tagada parandusmeetmete rakendamine;

3) kui alapunkti 2 kohaselt läbivaadatud dokumentidest ilmneb märkimisväärseid riske, mis on seotud selliste organisatsioonide poolt kasutatavate liidestega, mille üle teostab järelevalvet sama liikmesriigi muu pädev asutus, edastatakse see teave vastavale pädevale asutusele.“;

9) punkti 21.B.435 järele lisatakse punkt 21.B.435A:

„**21.B.435A Infoturbe halduse süsteemi muudatused**

a) Muudatuste puhul, mida hallatakse ja millest teavitatakse pädevat asutust vastavalt delegeeritud määruse (EL) 2022/1645 lisa (osa IS.D.OR) punkti IS.D.OR.255 alapunktis a sätestatud menetlusele, lisab pädev asutus selliste muudatuste läbivaatamise oma pidevasse järelevalvesse kooskõlas punktis 21.B.431 sätestatud põhimõtetega. Nõuetele mittevastavuse korral teavitab pädev asutus sellest organisatsiooni, nõuab täiendavaid muudatusi ja tegutseb vastavalt punktile 21.B.433.

b) Teiste muudatuste puhul, mis nõuavad heakskiidu taotlemist vastavalt delegeeritud määruse (EL) 2022/1645 lisa (osa IS.D.OR) punkti IS.D.OR.255 alapunktile b, kohaldatakse järgmist:

1) muudatuse taotluse saamisel kontrollib pädev asutus enne heakskiidu andmist organisatsiooni vastavust kohaldatavatele nõuetele;

2) pädev asutus kehtestab tingimused, mille alusel organisatsioon võib muudatuse rakendamise ajal tegutseda;

3) kui pädev asutus on veendunud, et organisatsioon täidab kohaldatavaid nõudeid, kiidab pädev asutus muudatuse heaks“.

V LISA

Määruse (EL) nr 965/2012 II lisa (osa ARO) ja III lisa (osa ORO) muudetakse järgmiselt.

1) II lisa (osa ARO) muudetakse järgmiselt:

a) punktile ARO.GEN.125 lisatakse alapunkt c:

„c) Liikmesriigi pädev asutus esitab ametile viivitamata ohutuse seisukohast olulise teabe, mis on pärit infoturbearuannetest, mis asutus on saanud vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punktile IS.I.OR.230.“;

b) punkti ARO.GEN.135 järele lisatakse punkt ARO.GEN.135A:

„**ARO.GEN.135A Viivitamatu reageering lennuohutust mõjutavale infoturvaintsidendile või turvaaugule**

a) Pädev asutus rakendab süsteemi, et nõuetekohaselt koguda, analüüsida ja levitada teavet, mis on seotud lennuohutust mõjutada võivate infoturvaintsidentide ja turvaaukudega, millest organisatsioonid teatavad. Seda tehakse kooskõlastatult kõigi teiste asjaomaste asutustega, kes vastutavad liikmesriigis info- või küberturbe eest, et suurendada aruandluskavade kooskõlastatust ja ühilduvust.

b) Amet rakendab süsteemi, et nõuetekohaselt analüüsida kogu punkti ARO.GEN.125 alapunkti c kohaselt saadud asjakohast ohutusalast teavet, ning esitab põhjendamatu viivituseta liikmesriikidele ja komisjonile kogu teabe, sealhulgas soovitused või parandusmeetmed, mis on vaja võtta selleks, et nad saaksid õigeaegselt reageerida infoturvaintsidendile või turvaaugule, mis võib mõjutada lennuohutust seoses toodete, osade, teisaldatava varustuse, isikute või organisatsioonidega, kelle suhtes kohaldatakse määrust (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusakte ja rakendusakte.

c) Alapunktides a ja b osutatud teabe saamisel võtab pädev asutus asjakohased meetmed, et käsitleda infoturvaintsidendi või turvaaugu võimalikku mõju lennuohutusele.

d) Alapunkti c kohaselt võetavad meetmed tehakse viivitamata teatavaks kõikidele isikutele ja organisatsioonidele, kes vastavalt määrusele (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusaktidele ja rakendusaktidele neid meetmeid kohaldavad. Liikmesriigi pädev asutus teeb meetmed teatavaks ka ametile ning ühise tegutsemise vajaduse tekkimise korral teiste asjaomaste liikmesriikide pädevatele asutustele.“;

c) punktile ARO.GEN.200 lisatakse alapunkt e:

„e) Lisaks alapunktis a esitatud nõuetele vastab pädeva asutuse poolt kehtestatud ja töös hoitav juhtimissüsteem rakendusmääruse (EL) 2023/203 I lisa (osa IS.AR) nõuetele, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust.“;

d) punkti ARO.GEN.205 muudetakse järgmiselt:

i) pealkiri asendatakse järgmisega:

„**ARO.GEN.205 Ülesannete jaotus**“;

ii) lisatakse alapunkt c:

„c) Sertifitseerimisel ja järelevalve teostamisel selle üle, kas organisatsioon täidab punkti ORO.GEN.200A nõudeid, võib pädev asutus jaotada ülesandeid kvalifitseeritud üksustele kooskõlas alapunktiga a või mis tahes asjaomasele asutusele, kes vastutab liikmesriigis info- või küberturbe eest. Ülesannete jaotamisel tagab pädev asutus, et:

1) pädev üksus või asjaomane asutus koordineerib ja võtab arvesse kõiki lennuohutusega seotud aspekte;

2) pädeva üksuse või asjaomase asutuse sertifitseerimis- ja järelevalvetoimingute tulemused integreeritakse organisatsiooni üldistesse sertifitseerimis- ja järelevalvetoimikutesse;

3) tema poolt punkti ARO.GEN.200 alapunkti e kohaselt kehtestatud infoturbe halduse süsteem hõlmab kõiki tema nimel täidetavaid sertifitseerimise ja pideva järelevalvega seotud ülesandeid.“;

e) punktile ARO.GEN.300 lisatakse alapunkt g:

„g) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti ORO.GEN.200A nõudeid, kontrollib pädev asutus alapunktide a–f järgimist ja vaatab läbi kõik käesoleva määruse punkti IS.I.OR.200 alapunkti e või delegeeritud määruse (EL) 2022/1645 punkti IS.D.OR.200 alapunkti e kohaselt antud sertifikaadid pärast kohaldatavat järelevalveauditi tsüklit ja iga kord, kui organisatsiooni töös tehakse muudatusi.“

f) punkti ARO.GEN.330 järele lisatakse punkt ARO.GEN.330A:

„**ARO.GEN.330A Infoturbe halduse süsteemi muudatused**

a) Muudatusteks, mida hallatakse ja millest teavitatakse pädevat asutust vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktis a sätestatud menetlusele, lisab pädev asutus selliste muudatuste läbivaatamise oma pidevasse järelevalvesse kooskõlas punktis ARO.GEN.300 sätestatud põhimõtetega. Nõuetele mittevastavuse korral teavitab pädev asutus sellest organisatsiooni, nõuab täiendavaid muudatusi ja tegutseb vastavalt punktile ARO.GEN.350.

b) Teiste muudatuste puhul, mis nõuavad heakskiidu taotlemist vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktile b, kohaldatakse järgmist:

1) muudatuse taotluse saamisel kontrollib pädev asutus enne heakskiidu andmist organisatsiooni vastavust kohaldatavatele nõuetele;

2) pädev asutus kehtestab tingimused, mille alusel organisatsioon võib muudatuse rakendamise ajal tegutseda;

3) kui pädev asutus on veendunud, et organisatsioon vastab kohaldatavatele nõuetele, kiidab pädev asutus muudatuse heaks.“;

2) III lisa (osa ORO) muudetakse järgmiselt:

punkti ORO.GEN.200 järele lisatakse punkt ORO.GEN.200A:

„**ORO.GEN.200A Infoturbe halduse süsteem**

Lisaks punktis ORO.GEN.200 osutatud juhtimissüsteemile kehtestab käitaja kooskõlas rakendusmäärusega (EL) 2023/203 infoturbe halduse süsteemi, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust, ning rakendab süsteemi ja hoiab seda töös.“

VI LISA

Määruse (EL) nr 139/2014 II lisa (osa ADR.AR) muudetakse järgmiselt:

1) punktile ADR.AR.A.025 lisatakse alapunkt c:

„c) Liikmesriigi pädev asutus esitab ametile viivitamata ohutuse seisukohast olulise teabe, mis on pärit infoturbearuannetest, mis asutus on saanud vastavalt delegeeritud määruse (EL) 2022/1645 lisa (osa IS.D.OR) punktile IS.D.OR.230.“;

2) punkti ADR.AR.A.030 järele lisatakse punkt ADR.AR.A.030A:

„**ADR.AR.A.030A Viivitamatu reageering lennuohutust mõjutavale infoturvaintsidendile või turvaaugule**

a) Pädev asutus rakendab süsteemi, et nõuetekohaselt koguda, analüüsida ja levitada teavet, mis on seotud lennuohutust mõjutada võivate infoturvaintsidentide ja turvaaukudega, millest organisatsioonid teatavad. Seda tehakse kooskõlastatult kõigi teiste asjaomaste asutustega, kes vastutavad liikmesriigis info- või küberturbe eest, et suurendada aruandluskavade kooskõlastatust ja ühilduvust.

b) Amet rakendab süsteemi, et nõuetekohaselt analüüsida kogu punkti ADR.AR.A.025 alapunkti c kohaselt saadud asjakohast ohutusalast teavet, ning esitab põhjendamatu viivituseta liikmesriikidele ja komisjonile kogu teabe, sealhulgas soovitused või parandusmeetmed, mis on vaja võtta selleks, et nad saaksid õigeaegselt reageerida infoturvaintsidendile või turvaaugule, mis võib mõjutada lennuohutust seoses toodete, osade, teisaldatava varustuse, isikute või organisatsioonidega, kelle suhtes kohaldatakse määrust (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusakte ja rakendusakte.

c) Alapunktides a ja b osutatud teabe saamisel võtab pädev asutus asjakohased meetmed, et käsitleda infoturvaintsidendi või turvaaugu võimalikku mõju lennuohutusele.

d) Alapunkti c kohaselt võetavad meetmed tehakse viivitamata teatavaks kõikidele isikutele ja organisatsioonidele, kes vastavalt määrusele (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusaktidele ja rakendusaktidele neid meetmeid kohaldavad. Liikmesriigi pädev asutus teeb meetmed teatavaks ka ametile ning ühise tegutsemise vajaduse tekkimise korral teiste asjaomaste liikmesriikide pädevatele asutustele.“;

3) punktile ADR.AR.B.005 lisatakse alapunkt d:

„d) Lisaks alapunktis a esitatud nõuetele vastab pädeva asutuse poolt kehtestatud ja töös hoitav juhtimissüsteem rakendusmääruse (EL) 2023/203 I lisa (osa IS.AR) nõuetele, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust.“;

4) punkti ADR.AR.B.010 muudetakse järgmiselt:

i) pealkiri asendatakse järgmisega:

„**ADR.AR.B.010 Ülesannete jaotus**“;

ii) lisatakse alapunkt c:

„c) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti ADR.OR.D.005A nõudeid, võib pädev asutus jaotada ülesandeid kvalifitseeritud üksustele kooskõlas alapunktiga a või mis tahes asjaomasele asutusele, kes vastutab liikmesriigis info- või küberturbe eest. Ülesannete jaotamisel tagab pädev asutus, et:

1) pädev üksus või asjaomane asutus koordineerib ja võtab arvesse kõiki lennuohutusega seotud aspekte;

2) pädeva üksuse või asjaomase asutuse sertifitseerimis- ja järelevalvetoimingute tulemused integreeritakse organisatsiooni üldistesse sertifitseerimis- ja järelevalvetoimikutesse;

3) tema poolt punkti ADR.AR.B.005 alapunkti e kohaselt kehtestatud infoturbe halduse süsteem hõlmab kõiki tema nimel täidetavaid sertifitseerimise ja pideva järelevalvega seotud ülesandeid.“;

5) punktile ADR.AR.C.005 lisatakse alapunkt f:

„f) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti ADR.OR.D.005A nõudeid, kontrollib pädev asutus alapunktide a–e järgimist ja vaatab läbi kõik käesoleva määruse punkti IS.I.OR.200 alapunkti e või delegeeritud määruse (EL) 2022/1645 punkti IS.D.OR.200 alapunkti e kohaselt antud sertifikaadid pärast kohaldatavat järelevalveauditi tsüklit ja iga kord, kui organisatsiooni töös tehakse muudatusi.“

6) punkti ADR.AR.C.040 järele lisatakse punkt ADR.AR.C.040A:

„**ADR.AR.C.040A Infoturbe halduse süsteemi muudatused**

a) Seoses muudatustega, mida hallatakse ja millest teavitatakse pädevat asutust vastavalt delegeeritud määruse (EL) 2022/1645 lisa (osa IS.D.OR) punkti IS.D.OR.255 alapunktis a sätestatud menetlusele, lisab pädev asutus selliste muudatuste läbivaatamise oma pidevasse järelevalvesse kooskõlas punktis ADR.AR.C.005 sätestatud põhimõtetega. Nõuetele mittevastavuse korral teavitab pädev asutus sellest organisatsiooni, nõuab täiendavaid muudatusi ja tegutseb vastavalt punktile ADR.AR.C.055.

b) Seoses teiste muudatustega, mis nõuavad heakskiidu taotlemist vastavalt delegeeritud määruse (EL) 2022/1645 lisa (osa IS.D.OR) punkti IS.D.OR.255 alapunktile b, kohaldatakse järgmist:

1) muudatuse taotluse saamisel kontrollib pädev asutus enne heakskiidu andmist organisatsiooni vastavust kohaldatavatele nõuetele;

2) pädev asutus kehtestab tingimused, mille alusel organisatsioon võib muudatuse rakendamise ajal tegutseda;

3) kui pädev asutus on veendunud, et organisatsioon täidab kohaldatavaid nõudeid, kiidab pädev asutus muudatuse heaks.“

VII LISA

Määruse (EL) nr 1321/2014 II lisa (osa 145), III lisa (osa 66) ja Vc lisa (osa CAMO) muudetakse järgmiselt.

1) II lisa (osa 145) muudetakse järgmiselt:

a) sisukorda muudetakse järgmiselt.

i) pealkirja 145.A.200 järele lisatakse järgmine pealkiri:

„145.A.200A Infoturbe halduse süsteem“;

ii) pealkirja 145.B.135 järele lisatakse järgmine pealkiri:

„145.B.135A Viivitamatu reageering lennuohutust mõjutavale infoturvaintsidendile või turvaaugule“;

iii) punkti 145.B.205 pealkiri asendatakse järgmisega:

„145.B.205 Ülesannete jaotus“;

iv) pealkirja 145.B.330 järele lisatakse järgmine pealkiri:

„145.B.330A Infoturbe halduse süsteemi muudatused“;

b) punkti 145.A.200 järele lisatakse punkt 145.A.200A:

„145.A.200A **Infoturbe halduse süsteem**

Lisaks punktis 145.A.200 osutatud juhtimissüsteemile kehtestab hooldusorganisatsioon kooskõlas rakendusmäärusega (EL) 2023/203 infoturbe halduse süsteemi, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust, ning rakendab süsteemi ja hoiab seda töös.“;

c) punktile 145.B.125 lisatakse alapunkt c:

„c) Liikmesriigi pädev asutus esitab ametile viivitamata ohutuse seisukohast olulise teabe, mis on pärit infoturbearuannetest, mis asutus on saanud vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punktile IS.I.OR.230.“;

d) punkti 145.B.135 järele lisatakse punkt 145.B.135A:

„145.B.135A **Viivitamatu reageering lennuohutust mõjutavale infoturvaintsidendile või turvaaugule**

a) Pädev asutus rakendab süsteemi, et nõuetekohaselt koguda, analüüsida ja levitada teavet, mis on seotud lennuohutust mõjutada võivate infoturvaintsidentide ja turvaaukudega, millest organisatsioonid teatavad. Seda tehakse kooskõlastatult kõigi teiste asjaomaste asutustega, kes vastutavad liikmesriigis info- või küberturbe eest, et suurendada aruandluskavade kooskõlastatust ja ühilduvust.

b) Amet rakendab süsteemi, et nõuetekohaselt analüüsida kogu punkti 145.B.125 alapunkti c kohaselt saadud asjakohast ohutusalast teavet, ning esitab põhjendamatu viivituseta liikmesriikidele ja komisjonile kogu teabe, sealhulgas soovitused või parandusmeetmed, mis on vaja võtta selleks, et nad saaksid õigeaegselt reageerida infoturvaintsidendile või turvaaugule, mis võib mõjutada lennuohutust seoses toodete, osade, teisaldatava varustuse, isikute või organisatsioonidega, kelle suhtes kohaldatakse määrust (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusakte ja rakendusakte.

c) Alapunktides a ja b osutatud teabe saamisel võtab pädev asutus asjakohased meetmed, et käsitleda infoturvaintsidendi või turvaaugu võimalikku mõju lennuohutusele.

d) Alapunkti c kohaselt võetavad meetmed tehakse viivitamata teatavaks kõikidele isikutele ja organisatsioonidele, kes vastavalt määrusele (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusaktidele ja rakendusaktidele neid meetmeid kohaldavad. Liikmesriigi pädev asutus teeb meetmed teatavaks ka ametile ning ühise tegutsemise vajaduse tekkimise korral teiste asjaomaste liikmesriikide pädevatele asutustele.“;

e) punktile 145.B.200 lisatakse alapunkt e:

„e) Lisaks alapunktis a esitatud nõuetele vastab pädeva asutuse poolt kehtestatud ja töös hoitav juhtimissüsteem rakendusmääruse (EL) 2023/203 I lisa (osa IS.AR) nõuetele, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust.“;

f) punkti 145.B.205 muudetakse järgmiselt:

i) pealkiri asendatakse järgmisega:

„145.B.205 **Ülesannete jaotus**“;

ii) lisatakse alapunkt c:

„c) Sertifitseerimisel ja järelevalve teostamisel selle üle, kas organisatsioon täidab punkti 145.A.200A nõudeid, võib pädev asutus jaotada ülesandeid kvalifitseeritud üksustele kooskõlas alapunktiga a või mis tahes asjaomasele asutusele, kes vastutab liikmesriigis info- või küberturbe eest. Ülesannete jaotamisel tagab pädev asutus, et:

1) pädev üksus või asjaomane asutus koordineerib ja võtab arvesse kõiki lennuohutusega seotud aspekte;

2) pädeva üksuse või asjaomase asutuse sertifitseerimis- ja järelevalvetoimingute tulemused integreeritakse organisatsiooni üldistesse sertifitseerimis- ja järelevalvetoimikutesse;

3) tema poolt punkti 145.B.200 alapunkti e kohaselt kehtestatud infoturbe halduse süsteem hõlmab kõiki tema nimel täidetavaid sertifitseerimise ja pideva järelevalvega seotud ülesandeid.“;

g) punktile 145.B.300 lisatakse alapunkt g:

„g) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti 145.A.200A nõudeid, kontrollib pädev asutus alapunktide a–f järgimist ja vaatab läbi kõik käesoleva määruse punkti IS.I.OR.200 alapunkti e või delegeeritud määruse (EL) 2022/1645 punkti IS.D.OR.200 alapunkti e kohaselt antud sertifikaadid pärast kohaldatavat järelevalveauditi tsüklit ja iga kord, kui organisatsiooni töös tehakse muudatusi.“;

h) punkti 145.B.330 järele lisatakse punkt 145.B.330A:

„145.B.330A **Infoturbe halduse süsteemi muudatused**

a) Muudatuste puhul, mida hallatakse ja millest teavitatakse pädevat asutust vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktis a sätestatud menetlusele, lisab pädev asutus selliste muudatuste läbivaatamise oma pidevasse järelevalvesse kooskõlas punktis 145.B.300 sätestatud põhimõtetega. Nõuetele mittevastavuse korral teavitab pädev asutus sellest organisatsiooni, nõuab täiendavaid muudatusi ja tegutseb vastavalt punktile 145.B.350.

b) Teiste muudatuste puhul, mis nõuavad heakskiidu taotlemist vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktile b, kohaldatakse järgmist:

1) muudatuse taotluse saamisel kontrollib pädev asutus enne heakskiidu andmist organisatsiooni vastavust kohaldatavatele nõuetele;

2) pädev asutus kehtestab tingimused, mille alusel organisatsioon võib muudatuse rakendamise ajal tegutseda;

3) kui pädev asutus on veendunud, et organisatsioon täidab kohaldatavaid nõudeid, kiidab pädev asutus muudatuse heaks.“

2) III lisa (osa 66) muudetakse järgmiselt:

a) sisukorda lisatakse pealkirja 66.B.10 järele järgmine pealkiri:

„66.B.15 Infoturbe halduse süsteem“;

b) punkti 66.B.10 järele lisatakse punkt 66.B.15:

„66.B.15 **Infoturbe halduse süsteem**

Pädev asutus kehtestab kooskõlas rakendusmääruse (EL) 2023/203 I lisaga (osa IS.AR) infoturbe halduse süsteemi, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust, ning rakendab süsteemi ja hoiab seda töös.“;

3) Vc lisa (osa CAMO) muudetakse järgmiselt:

a) sisukorda muudetakse järgmiselt:

i) pealkirja CAMO.A.200 järele lisatakse järgmine pealkiri:

„CAMO.A.200A Infoturbe halduse süsteem“;

ii) pealkirja CAMO.B.135 järele lisatakse järgmine pealkiri:

„CAMO.B.135A Viivitamatu reageering lennuohutust mõjutavale infoturvaintsidendile või turvaaugule“;

iii) punkti CAMO.B.205 pealkiri asendatakse järgmisega:

„CAMO.B.205 Ülesannete jaotus“;

iv) pealkirja CAMO.B.330 järele lisatakse järgmine pealkiri:

„CAMO.B.330A Infoturbe halduse süsteemi muudatused“;

b) punkti CAMO.A.200 järele lisatakse punkt CAMO.A.200A:

„CAMO.A.200A **Infoturbe halduse süsteem**

Lisaks punktis CAMO.A.200 osutatud juhtimissüsteemile kehtestab organisatsioon kooskõlas rakendusmäärusega (EL) 2023/203 infoturbe halduse süsteemi, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust, ning rakendab süsteemi ja hoiab seda töös.“;

c) punktile CAMO.B.125 lisatakse alapunkt c:

„c) Liikmesriigi pädev asutus esitab ametile viivitamata ohutuse seisukohast olulise teabe, mis on pärit infoturbearuannetest, mis asutus on saanud vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punktile IS.I.OR.230.“;

d) punkti CAMO.B.135 järele lisatakse punkt CAMO.B.135A:

„CAMO.B.135A **Viivitamatu reageering lennuohutust mõjutavale infoturvaintsidendile või turvaaugule**

a) Pädev asutus rakendab süsteemi, et nõuetekohaselt koguda, analüüsida ja levitada teavet, mis on seotud lennuohutust mõjutada võivate infoturvaintsidentide ja turvaaukudega, millest organisatsioonid teatavad. Seda tehakse kooskõlastatult kõigi teiste asjaomaste asutustega, kes vastutavad liikmesriigis info- või küberturbe eest, et suurendada aruandluskavade kooskõlastatust ja ühilduvust.

b) Amet rakendab süsteemi, et nõuetekohaselt analüüsida kogu punkti CAMO.B.125 alapunkti c kohaselt saadud asjakohast ohutusalast teavet, ning esitab põhjendamatu viivituseta liikmesriikidele ja komisjonile kogu teabe, sealhulgas soovitused või parandusmeetmed, mis on vaja võtta selleks, et nad saaksid õigeaegselt reageerida infoturvaintsidendile või turvaaugule, mis võib mõjutada lennuohutust seoses toodete, osade, teisaldatava varustuse, isikute või organisatsioonidega, kelle suhtes kohaldatakse määrust (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusakte ja rakendusakte.

c) Alapunktides a ja b osutatud teabe saamisel võtab pädev asutus asjakohased meetmed, et käsitleda infoturvaintsidendi või turvaaugu võimalikku mõju lennuohutusele.

d) Alapunkti c kohaselt võetavad meetmed tehakse viivitamata teatavaks kõikidele isikutele ja organisatsioonidele, kes vastavalt määrusele (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusaktidele ja rakendusaktidele neid meetmeid kohaldavad. Liikmesriigi pädev asutus teeb meetmed teatavaks ka ametile ning ühise tegutsemise vajaduse tekkimise korral teiste asjaomaste liikmesriikide pädevatele asutustele.“;

e) punktile CAMO.B.200 lisatakse alapunkt e:

„e) Lisaks alapunktis a esitatud nõuetele vastab pädeva asutuse poolt kehtestatud ja töös hoitav juhtimissüsteem rakendusmääruse (EL) 2023/203 I lisa (osa IS.AR) nõuetele, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust.“;

f) punkti CAMO.B.205 muudetakse järgmiselt:

i) pealkiri asendatakse järgmisega:

„CAMO.B.205 **Ülesannete jaotus**“;

ii) lisatakse alapunkt c:

„c) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti CAMO.A.200A nõudeid, võib pädev asutus jaotada ülesandeid kvalifitseeritud üksustele kooskõlas punktiga a või mis tahes asjaomasele asutusele, kes vastutab liikmesriigis info- või küberturbe eest. Ülesannete jaotamisel tagab pädev asutus, et:

1) pädev üksus või asjaomane asutus koordineerib ja võtab arvesse kõiki lennuohutusega seotud aspekte;

2) pädeva üksuse või asjaomase asutuse sertifitseerimis- ja järelevalvetoimingute tulemused integreeritakse organisatsiooni üldistesse sertifitseerimis- ja järelevalvetoimikutesse;

3) tema poolt punkti CAMO.B.200 alapunkti e kohaselt kehtestatud infoturbe halduse süsteem hõlmab kõiki tema nimel täidetavaid sertifitseerimise ja pideva järelevalvega seotud ülesandeid.“;

g) punktile CAMO.B.300 lisatakse alapunkt g:

„g) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti CAMO.A.200A nõudeid, kontrollib pädev asutus alapunktide a–f järgimist ja vaatab läbi kõik käesoleva määruse punkti IS.I.OR.200 alapunkti e või delegeeritud määruse (EL) 2022/1645 punkti IS.D.OR.200 alapunkti e kohaselt antud sertifikaadid pärast kohaldatavat järelevalveauditi tsüklit ja iga kord, kui organisatsiooni töös tehakse muudatusi.“

h) punkti CAMO.B.330 järele lisatakse punkt CAMO.B.330A:

„CAMO.B.330A **Infoturbe halduse süsteemi muudatused**

a) Muudatusteks, mida hallatakse ja millest teavitatakse pädevat asutust vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktis a sätestatud menetlusele, lisab pädev asutus selliste muudatuste läbivaatamise oma pidevasse järelevalvesse kooskõlas punktis CAMO.B.300 sätestatud põhimõtetega. Nõuetele mittevastavuse korral teavitab pädev asutus sellest organisatsiooni, nõuab täiendavaid muudatusi ja tegutseb vastavalt punktile CAMO.B.350.

b) Teiste muudatuste puhul, mis nõuavad heakskiidu taotlemist vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktile b, kohaldatakse järgmist:

1) muudatuse taotluse saamisel kontrollib pädev asutus enne heakskiidu andmist organisatsiooni vastavust kohaldatavatele nõuetele;

2) pädev asutus kehtestab tingimused, mille alusel organisatsioon võib muudatuse rakendamise ajal tegutseda;

3) kui pädev asutus on veendunud, et organisatsioon täidab kohaldatavaid nõudeid, kiidab pädev asutus muudatuse heaks.“

VIII LISA

Määruse (EL) 2015/340 II lisa (osa ATCO.AR) ja III lisa (osa ATCO.OR) muudetakse järgmiselt.

1) II lisa (osa ATCO.AR) muudetakse järgmiselt:

a) punktile ATCO.AR.A.020 lisatakse alapunkt c:

„c) Liikmesriigi pädev asutus esitab ametile viivitamata ohutuse seisukohast olulise teabe, mis on pärit infoturbearuannetest, mis asutus on saanud vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punktile IS.I.OR.230.“;

b) punkti ATCO.AR.A.025 järele lisatakse punkt ATCO.AR.A.025A:

„**ATCO.AR.A.025A Viivitamatu reageering lennuohutust mõjutavale infoturvaintsidendile või turvaaugule**

a) Pädev asutus rakendab süsteemi, et nõuetekohaselt koguda, analüüsida ja levitada teavet, mis on seotud lennuohutust mõjutada võivate infoturvaintsidentide ja turvaaukudega, millest organisatsioonid teatavad. Seda tehakse kooskõlastatult kõigi teiste asjaomaste asutustega, kes vastutavad liikmesriigis info- või küberturbe eest, et suurendada aruandluskavade kooskõlastatust ja ühilduvust.

b) Amet rakendab süsteemi, et nõuetekohaselt analüüsida kogu punkti ATCO.AR.A.020 kohaselt saadud asjakohast ohutusalast teavet, ning esitab põhjendamatu viivituseta liikmesriikidele ja komisjonile kogu teabe, sealhulgas soovitused või parandusmeetmed, mis on vaja võtta selleks, et nad saaksid õigeaegselt reageerida infoturvaintsidendile või turvaaugule, mis võib mõjutada lennuohutust seoses toodete, osade, teisaldatava varustuse, isikute või organisatsioonidega, kelle suhtes kohaldatakse määrust (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusakte ja rakendusakte.

c) Alapunktides a ja b osutatud teabe saamisel võtab pädev asutus asjakohased meetmed, et käsitleda infoturvaintsidendi või turvaaugu võimalikku mõju lennuohutusele.

d) Alapunkti c kohaselt võetavad meetmed tehakse viivitamata teatavaks kõikidele isikutele ja organisatsioonidele, kes vastavalt määrusele (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusaktidele ja rakendusaktidele neid meetmeid kohaldavad. Liikmesriigi pädev asutus teeb meetmed teatavaks ka ametile ning ühise tegutsemise vajaduse tekkimise korral teiste asjaomaste liikmesriikide pädevatele asutustele.“;

c) punktile ATCO.AR.B.001 lisatakse alapunkt e:

„e) Lisaks alapunktis a esitatud nõuetele vastab pädeva asutuse poolt kehtestatud ja töös hoitav juhtimissüsteem rakendusmääruse (EL) 2023/203 I lisa (osa IS.AR) nõuetele, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust.“;

d) punkti ATCO.AR.B.005 muudetakse järgmiselt:

i) pealkiri asendatakse järgmisega:

„**ATCO.AR.B.005 Ülesannete jaotus**“;

ii) lisatakse alapunkt c:

„c) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti ATCO.OR.C.001A nõudeid, võib pädev asutus jaotada ülesandeid kvalifitseeritud üksustele kooskõlas alapunktiga a või mis tahes asjaomasele asutusele, kes vastutab liikmesriigis info- või küberturbe eest. Ülesannete jaotamisel tagab pädev asutus, et:

1) pädev üksus või asjaomane asutus koordineerib ja võtab arvesse kõiki lennuohutusega seotud aspekte;

2) pädeva üksuse või asjaomase asutuse sertifitseerimis- ja järelevalvetoimingute tulemused integreeritakse organisatsiooni üldistesse sertifitseerimis- ja järelevalvetoimikutesse;

3) tema poolt punkti ATCO.AR.B.001 alapunkti e kohaselt kehtestatud infoturbe halduse süsteem hõlmab kõiki tema nimel täidetavaid sertifitseerimise ja pideva järelevalvega seotud ülesandeid.“;

e) punktile ATCO.AR.C.001 lisatakse alapunkt f:

„f) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti ATCO.OR.C.001A nõudeid, kontrollib pädev asutus alapunktide a–e järgimist ja vaatab läbi kõik käesoleva määruse punkti IS.I.OR.200 alapunkti e või delegeeritud määruse (EL) 2022/1645 punkti IS.D.OR.200 alapunkti e kohaselt antud sertifikaadid pärast kohaldatavat järelevalveauditi tsüklit ja iga kord, kui organisatsiooni töös tehakse muudatusi.“

f) punkti ATCO.AR.E.010 järele lisatakse punkt ATCO.AR.E.010A:

„**ATCO.AR.E.010A Infoturbe halduse süsteemi muudatused**

a) Muudatuste puhul, mida hallatakse ja millest teavitatakse pädevat asutust vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktis a sätestatud menetlusele, lisab pädev asutus selliste muudatuste läbivaatamise oma pidevasse järelevalvesse kooskõlas punktis ATCO.AR.C.001 sätestatud põhimõtetega. Nõuetele mittevastavuse korral teavitab pädev asutus sellest organisatsiooni, nõuab täiendavaid muudatusi ja tegutseb vastavalt punktile ATCO.AR.C.010.

b) Teiste muudatuste puhul, mis nõuavad heakskiidu taotlemist vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktile b, kohaldatakse järgmist:

1) muudatuse taotluse saamisel kontrollib pädev asutus enne heakskiidu andmist organisatsiooni vastavust kohaldatavatele nõuetele;

2) pädev asutus kehtestab tingimused, mille alusel organisatsioon võib muudatuse rakendamise ajal tegutseda;

3) kui pädev asutus on veendunud, et organisatsioon vastab kohaldatavatele nõuetele, kiidab pädev asutus muudatuse heaks.“;

2) III lisa (osa ATCO.OR) muudetakse järgmiselt:

punkti ATCO.OR.C.001 järele lisatakse punkt ATCO.OR.C.001A:

„**ATCO.OR.C.001A Infoturbe halduse süsteem**

Lisaks punktis ATCO.OR.C.001 osutatud juhtimissüsteemile kehtestab koolitusorganisatsioon kooskõlas rakendusmäärusega (EL) 2023/203 infoturbe halduse süsteemi, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust, ning rakendab süsteemi ja hoiab seda töös.“

IX LISA

Rakendusmääruse (EL) 2017/373 II lisa (osa ATM/ANS.AR) ja III lisa (osa ATM/ANS.OR) muudetakse järgmiselt.

1) II lisa (osa ATM/ANS.AR) muudetakse järgmiselt:

a) punktile ATM/ANS.AR.A.020 lisatakse alapunkt c:

„c) Liikmesriigi pädev asutus esitab ametile viivitamata ohutuse seisukohast olulise teabe, mis on pärit infoturbearuannetest, mis asutus on saanud vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punktile IS.I.OR.230.“;

b) punkti ATM/ANS.AR.A.025 järele lisatakse punkt ATM/ANS.AR.A.025A:

„**ATM/ANS.AR.A.025A Viivitamatu reageering lennuohutust mõjutavale infoturvaintsidendile või turvaaugule**

a) Pädev asutus rakendab süsteemi, et nõuetekohaselt koguda, analüüsida ja levitada teavet, mis on seotud lennuohutust mõjutada võivate infoturvaintsidentide ja turvaaukudega, millest organisatsioonid teatavad. Seda tehakse kooskõlastatult kõigi teiste asjaomaste asutustega, kes vastutavad liikmesriigis info- või küberturbe eest, et suurendada aruandluskavade kooskõlastatust ja ühilduvust.

b) Amet rakendab süsteemi, et nõuetekohaselt analüüsida kogu punkti ATM/ANS.AR.A.020 alapunkti c kohaselt saadud asjakohast ohutusalast teavet, ning esitab põhjendamatu viivituseta liikmesriikidele ja komisjonile kogu teabe, sealhulgas soovitused või parandusmeetmed, mis on vaja võtta selleks, et nad saaksid õigeaegselt reageerida infoturvaintsidendile või turvaaugule mis võib mõjutada lennuohutust seoses toodete, osade, teisaldatava varustuse, isikute või organisatsioonidega, kelle suhtes kohaldatakse määrust (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusakte ja rakendusakte.

c) Alapunktides a ja b osutatud teabe saamisel võtab pädev asutus asjakohased meetmed, et käsitleda infoturvaintsidendi või turvaaugu võimalikku mõju lennuohutusele.

d) Alapunkti c kohaselt võetavad meetmed tehakse viivitamata teatavaks kõikidele isikutele ja organisatsioonidele, kes vastavalt määrusele (EL) 2018/1139 ning selle alusel vastu võetud delegeeritud õigusaktidele ja rakendusaktidele neid meetmeid kohaldavad. Liikmesriigi pädev asutus teeb meetmed teatavaks ka ametile ning ühise tegutsemise vajaduse tekkimise korral teiste asjaomaste liikmesriikide pädevatele asutustele.“;

c) punktile ATM/ANS.AR.B.001 lisatakse alapunkt e:

„e) Lisaks alapunktis a esitatud nõuetele vastab pädeva asutuse poolt kehtestatud ja töös hoitav juhtimissüsteem rakendusmääruse (EL) 2023/203 I lisa (osa IS.AR) nõuetele, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust.“;

d) punkti ATM/ANS.AR.B.005 muudetakse järgmiselt:

i) pealkiri asendatakse järgmisega:

„**ATM/ANS.AR.B.005 Ülesannete jaotamine**“;

ii) lisatakse alapunkt c:

„c) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti ATM/ANS.OR.B.005A nõudeid, võib pädev asutus jaotada ülesandeid kvalifitseeritud üksustele kooskõlas alapunktiga a või mis tahes asjaomasele asutusele, kes vastutab liikmesriigis info- või küberturbe eest. Ülesannete jaotamisel tagab pädev asutus, et:

1) pädev üksus või asjaomane asutus koordineerib ja võtab arvesse kõiki lennuohutusega seotud aspekte;

2) pädeva üksuse või asjaomase asutuse sertifitseerimis- ja järelevalvetoimingute tulemused integreeritakse organisatsiooni üldistesse sertifitseerimis- ja järelevalvetoimikutesse;

3) tema poolt punkti ATM/ANS.AR.B.001 alapunkti e kohaselt kehtestatud infoturbe halduse süsteem hõlmab kõiki tema nimel täidetavaid sertifitseerimise ja pideva järelevalvega seotud ülesandeid.“;

e) punktile ATM/ANS.AR.C.010 lisatakse alapunkt d:

„d) Seoses sertifitseerimise ja järelevalvega selle üle, kas organisatsioon täidab punkti ATM/ANS.OR.B.005A nõudeid, kontrollib pädev asutus alapunktide a–c järgimist ja vaatab läbi kõik käesoleva määruse punkti IS.I.OR.200 alapunkti e või delegeeritud määruse (EL) 2022/1645 punkti IS.D.OR.200 alapunkti e kohaselt antud sertifikaadid pärast kohaldatavat järelevalveauditi tsüklit ja iga kord, kui organisatsiooni töös tehakse muudatusi.“

f) punkti ATM/ANS.AR.C.025 järele lisatakse punkt ATM/ANS.AR.C.025A:

„**ATM/ANS.AR.C.025A Infoturbe halduse süsteemi muudatused**

a) Muudatusteks, mida hallatakse ja millest teavitatakse pädevat asutust vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktis a sätestatud menetlusele, lisab pädev asutus selliste muudatuste läbivaatamise oma pidevasse järelevalvesse kooskõlas punktis ATM/ANS.AR.C.010 sätestatud põhimõtetega. Nõuetele mittevastavuse korral teavitab pädev asutus sellest organisatsiooni, nõuab täiendavaid muudatusi ja tegutseb vastavalt punktile ATM/ANS.AR.C.050.

b) Teiste muudatuste puhul, mis nõuavad heakskiidu taotlemist vastavalt rakendusmääruse (EL) 2023/203 II lisa (osa IS.I.OR) punkti IS.I.OR.255 alapunktile b, kohaldatakse järgmist:

1) muudatuse taotluse saamisel kontrollib pädev asutus enne heakskiidu andmist organisatsiooni vastavust kohaldatavatele nõuetele;

2) pädev asutus kehtestab tingimused, mille alusel organisatsioon võib muudatuse rakendamise ajal tegutseda;

3) kui pädev asutus on veendunud, et organisatsioon vastab kohaldatavatele nõuetele, kiidab pädev asutus muudatuse heaks.“;

2) III lisa (osa ATM/ANS.OR) muudetakse järgmiselt:

a) punkti ATM/ANS.OR.B.005 järele lisatakse punkt ATM/ANS.OR.B.005A:

„**ATM/ANS.OR.B.005A Infoturbe halduse süsteem**

Lisaks punktis ATM/ANS.OR.B.005 osutatud juhtimissüsteemile kehtestab teenuseosutaja kooskõlas rakendusmäärusega (EL) 2023/203 infoturbe halduse süsteemi, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust, ning rakendab süsteemi ja hoiab seda töös.“;

b) punkt ATM/ANS.OR.D.010 asendatakse järgmisega:

„**ATM/ANS.OR.D.010 Julgestusalane juhtimine**

a) Aeronavigatsiooniteenuste ja lennuliiklusvoogude juhtimisteenuste osutajad ning võrgustiku haldaja peavad juhtimissüsteemi lahutamatu osana kehtestama vastavalt punktile ATM/ANS.OR.B.005 julgestusalase juhtimissüsteemi, et tagada:

1) oma ruumide ja töötajate julgeolek, et vältida teenuste osutamist mõjutavaid õigusvastaseid tegusid;

2) teenuseosutajale edastatud, tema poolt kogutud või muul viisil kasutatavate operatiivandmete turvalisus, tehes need kättesaadavaks üksnes volitatud isikutele.

b) Julgestusalase juhtimise süsteemis määratakse kindlaks järgmine:

1) protsess ja menetlused, mis on seotud julgestusriski hindamise ja leevendamisega, julgestuse jälgimise ja parandamisega, julgestuse ümberhindamise ja kogemuste levitamisega;

2) vahendid, mis on kavandatud julgestusega seotud puuduste kindlaksmääramiseks, seireks ja avastamiseks ning töötajate teavitamiseks asjakohastest hoiatustest;

3) vahendid julgestusega seotud puuduste kontrollimiseks ning parandusmeetmete ja leevendusmenetluste kindlaksmääramiseks, et vältida puuduste taastekkimist.

c) Aeronavigatsiooniteenuste ja lennuliiklusvoogude juhtimisteenuste osutajad ning võrgustiku haldaja korraldavad oma töötajate julgestuskontrolli ning vajaduse korral teevad koostööd asjaomaste tsiviil- ja militaarasutustega oma ruumide, töötajate ja andmete kaitsmiseks.

d) Infoturbeaspekte hallatakse vastavalt punktile ATM/ANS.OR.B.005A.“