II

(Ne teisėkūros procedūra priimami aktai)

REGLAMENTAI

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2023/203

2022 m. spalio 27 d.

kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2018/1139 taikymo taisyklės, susijusios su Komisijos reglamentuose (ES) Nr. 1321/2014, (ES) Nr. 965/2012, (ES) Nr. 1178/2011, (ES) 2015/340, Komisijos įgyvendinimo reglamentuose (ES) 2017/373 ir (ES) 2021/664 nurodytoms organizacijoms ir Komisijos reglamentuose (ES) Nr. 748/2012, (ES) Nr. 1321/2014, (ES) Nr. 965/2012, (ES) Nr. 1178/2011, (ES) 2015/340, Komisijos įgyvendinimo reglamentuose (ES) 2017/373, (ES) Nr. 139/2014 ir (ES) 2021/664 nurodytoms kompetentingoms institucijoms taikytinais informacijos saugumo rizikos, galinčios turėti įtakos aviacijos saugai, valdymo reikalavimais, ir kuriuo iš dalies keičiami Komisijos reglamentai (ES) Nr. 1178/2011, (ES) Nr. 748/2012, (ES) Nr. 965/2012, (ES) Nr. 139/2014, (ES) Nr. 1321/2014, (ES) 2015/340 ir Komisijos įgyvendinimo reglamentai (ES) 2017/373 ir (ES) 2021/664

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2018 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentą (ES) 2018/1139 dėl bendrųjų civilinės aviacijos taisyklių, ir kuriuo įsteigiama Europos Sąjungos aviacijos saugos agentūra, iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 2111/2005, (EB) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 ir direktyvos 2014/30/ES ir 2014/53/ES bei panaikinami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 552/2004 ir (EB) Nr. 216/2008 bei Tarybos reglamentas (EEB) Nr. 3922/91 ([1]), ypač į jo 17 straipsnio 1 dalies b punktą, 27 straipsnio 1 dalies a punktą, 31 straipsnio 1 dalies b punktą, 43 straipsnio 1 dalies b punktą, 53 straipsnio 1 dalies a punktą ir 62 straipsnio 15 dalies c punktą,

kadangi:

(1) pagal Reglamento (ES) 2018/1139 II priedo 3.1 punkto b papunktyje nustatytus esminius reikalavimus, nepertraukiamąjį tinkamumą skraidyti užtikrinančios organizacijos ir techninės priežiūros organizacijos turi taikyti ir nuolat atnaujinti saugos rizikos valdymo sistemą;

(2) be to, pagal Reglamento (ES) 2018/1139 IV priedo 3.3 punkto b papunktyje ir 5 punkto b papunktyje nustatytus esminius reikalavimus, pilotų mokymo organizacijos, keleivių salono įgulos narių mokymo organizacijos, orlaivių įguloms skirti aviacijos medicinos centrai ir imituojamo skrydžio treniruoklių naudotojai turi taikyti ir nuolat atnaujinti saugos rizikos valdymo sistemą;

(3) taip pat, pagal Reglamento (ES) 2018/1139 V priedo 8.1 punkto c papunktyje nustatytus esminius reikalavimus, oro vežėjai turi taikyti ir nuolat atnaujinti saugos rizikos valdymo sistemą;

(4) be to, pagal Reglamento (ES) 2018/1139 VIII priedo 5.1 punkto c papunktyje ir 5.4 punkto b papunktyje nustatytus esminius reikalavimus, oro eismo valdymo ir oro navigacijos paslaugų teikėjai, sistemos „U-space“ paslaugų teikėjai ir vieninteliai bendrų informacijos paslaugų teikėjai, skrydžių vadovų mokymo organizacijos ir skrydžių vadovams skirti aviacijos medicinos centrai turi taikyti ir nuolat atnaujinti saugos rizikos valdymo sistemą;

([1]) OL L 212, 2018 8 22, p. 1.

(5) tos saugos rizikos šaltiniai gali būti įvairūs, pavyzdžiui, projektavimo ir techninės priežiūros trūkumai, su žmogaus galimybėmis susiję aspektai, su aplinka ir informacijos saugumu susijusios grėsmės. Todėl Europos Sąjungos aviacijos saugos agentūros (toliau – Agentūra) ir nacionalinių kompetentingų institucijų bei organizacijų, nurodytų ankstesnėse konstatuojamosiose dalyse, taikomose valdymo sistemose turėtų būti atsižvelgiama ne tik į saugos riziką, kylančią dėl atsitiktinių įvykių, bet ir į saugos riziką, kylančią dėl grėsmių informacijos saugumui, kai esamais trūkumais gali pasinaudoti piktavališkų ketinimų turintys asmenys. Civilinės aviacijos aplinkoje ši informacijos saugumo rizika nuolat didėja, nes dabartinės informacinės sistemos tampa vis labiau tarpusavyje susijusios, be to, į jas vis dažniau taikosi piktavališki subjektai;

(6) su šiomis informacinėmis sistemomis susijusi rizika neapsiriboja galimais išpuoliais kibernetinėje erdvėje, bet apima ir grėsmes, kurios gali turėti įtakos procesams ir procedūroms, taip pat žmonių galimybėms;

(7) kad užtikrintų skaitmeninės informacijos ir duomenų saugumą, daug organizacijų jau taiko tarptautinius standartus (pavyzdžiui, ISO 27001). Tie standartai gali apimti ne visus civilinės aviacijos ypatumus; todėl tikslinga nustatyti informacijos saugumo rizikos, kuri gali turėti įtakos aviacijos saugai, valdymo reikalavimus;

(8) labai svarbu, kad tie reikalavimai apimtų visas aviacijos sritis ir jų sąsajas, nes aviacija yra iš itin glaudžiai sujungtų sistemų sudaryta sistema. Todėl jie turėtų būti taikomi visoms organizacijoms ir kompetentingoms institucijoms, kurioms taikomi Komisijos reglamentai (ES) Nr. 748/2012 ([2]), (ES) Nr. 1321/2014 ([3]), (ES) Nr. 965/2012 ([4]), (ES) Nr. 1178/2011 ([5]), (ES) 2015/340 ([6]), (ES) Nr. 139/2014 ([7]) ir Komisijos įgyvendinimo reglamentas (ES) 2021/664 ([8]), taip pat toms organizacijoms ir kompetentingoms institucijoms, kurios pagal galiojančius Sąjungos aviacijos saugos teisės aktus jau turi turėti valdymo sistemą. Tačiau kai kurios organizacijos neturėtų būti įtrauktos į šio reglamento taikymo sritį, kad būtų užtikrintas tinkamas proporcingumas mažesnei informacijos saugumo rizikai, kurią jos kelia aviacijos sistemai;

(9) šiame reglamente nustatytais reikalavimais turėtų būti užtikrinamas nuoseklus įgyvendinimas visose aviacijos srityse, kartu darant kuo mažesnį poveikį tose srityse jau taikomiems Sąjungos aviacijos saugos teisės aktams;

([2]) 2012 m. rugpjūčio 3 d. Komisijos reglamentas (ES) Nr. 748/2012, kuriuo nustatomos orlaivio tinkamumo skraidyti sertifikavimo, orlaivio ir susijusių gaminių, dalių bei prietaisų aplinkosauginio sertifikavimo, taip pat projektavimo ir gamybinių organizacijų sertifikavimo įgyvendinimo taisyklės (OL L 224, 2012 8 21, p. 1)

([3]) 2014 m. lapkričio 26 d. Komisijos Reglamentas (ES) Nr. 1321/2014 dėl orlaivių nepertraukiamojo tinkamumo skraidyti ir aviacijos produktų, dalių bei prietaisų tinkamumo naudoti ir šias užduotis atliekančių organizacijų bei darbuotojų patvirtinimo (OL L 362, 2014 12 17, p. 1).

([4]) 2012 m. spalio 5 d. Komisijos reglamentas (ES) Nr. 965/2012, kuriuo pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 216/2008 nustatomi su orlaivių naudojimu skrydžiams susiję techniniai reikalavimai ir administracinės procedūros (OL L 296, 2012 10 25, p. 1).

([5]) 2011 m. lapkričio 3 d. Komisijos reglamentas (ES) Nr. 1178/2011, kuriuo pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 216/2008 nustatomi su civilinės aviacijos orlaivių įgula susiję techniniai reikalavimai ir administracinės procedūros (OL L 311, 2011 11 25, p. 1).

([6]) 2015 m. vasario 20 d. Komisijos reglamentas (ES) 2015/340, kuriuo pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 216/2008 nustatomi su skrydžių vadovų licencijomis ir pažymėjimais susiję techniniai reikalavimai ir administracinės procedūros, iš dalies keičiamas Komisijos įgyvendinimo reglamentas (ES) Nr. 923/2012 ir panaikinamas Komisijos reglamentas (ES) Nr. 805/2011 (OL L 63, 2015 3 6, p. 1).

([7]) 2014 m. vasario 12 d. Komisijos reglamentas (ES) Nr. 139/2014, kuriuo pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 216/2008 nustatomi su aerodromais susiję reikalavimai ir administracinės procedūros (OL L 44, 2014 2 14, p. 1).

([8]) Komisijos įgyvendinimo reglamentas (ES) 2021/664 2021 m. balandžio 22 d. dėl sistemos „U-space“ reglamentavimo sistemos (OL L 139, 2021 4 23, p. 161).

(10) šiame reglamente nustatytais reikalavimais neturėtų būti daromas poveikis informacijos saugumo ir kibernetinio saugumo reikalavimams, nustatytiems Komisijos įgyvendinimo reglamento (ES) 2015/1998 ([9]) priedo 1.7 punkte ir Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 ([10]) 14 straipsnyje;

(11) Europos Parlamento ir Tarybos reglamento (ES) 2021/696 ([11]) V antraštinės dalies „Programos saugumas“ 33–43 straipsniuose nustatyti saugumo reikalavimai laikomi lygiaverčiais šiame reglamente nustatytiems reikalavimams, išskyrus šio reglamento II priedo IS.I.OR.230 punkte nustatytus reikalavimus, kurių turėtų būti laikomasi;

(12) siekiant užtikrinti teisinį tikrumą, šiame reglamente apibrėžto termino „informacijos saugumas“ aiškinimas, atspindintis jo bendrą vartoseną civilinės aviacijos srityje pasaulio mastu, turėtų būti laikomas derančiu su Direktyvos (ES) 2016/1148 4 straipsnio 2 dalyje apibrėžto termino „tinklų ir informacinių sistemų saugumas“ aiškinimu. Šiame reglamente vartojamo termino „informacijos saugumas“ apibrėžtis neturėtų būti aiškinama kaip besiskirianti nuo Direktyvoje (ES) 2016/1148 pateiktos termino „tinklų ir informacinių sistemų saugumas“ apibrėžties;

(13) siekiant išvengti teisinių reikalavimų dubliavimosi, tais atvejais, kai į šio reglamento taikymo sritį įtrauktoms organizacijoms jau taikomi (10) ir 11 konstatuojamojoje dalyje nurodytais Sąjungos aktais nustatyti saugumo reikalavimai, kurių poveikis yra lygiavertis šio reglamento nuostatoms, atitiktis tiems saugumo reikalavimams turėtų būti laikoma atitiktimi šiame reglamente nustatytiems reikalavimams;

(14) į šio reglamento taikymo sritį įtrauktos organizacijos, kurioms jau taikomi Įgyvendinimo reglamente (ES) 2015/1998 arba Reglamente (ES) 2021/696 (ar abiejuose) nustatyti saugumo reikalavimai, taip pat turėtų laikytis šio reglamento II priedo (IS.I.OR.230 dalies „Informacijos saugumo išorės pranešimų teikimo sistema“) reikalavimų, nes minėtuose reglamentuose nėra nuostatų, susijusių su išorės pranešimų apie informacijos saugumo incidentus teikimu;

(15) siekiant išsamumo, reglamentai (ES) Nr. 1178/2011, (ES) Nr. 748/2012, (ES) Nr. 965/2012, (ES) Nr. 139/2014, (ES) Nr. 1321/2014, (ES) 2015/340 ir įgyvendinimo reglamentai (ES) 2017/373 ([12]) ir (ES) 2021/664 turėtų būti iš dalies pakeisti, t. y. į juos įtraukti šiame reglamente nustatyti reikalavimai, susiję su informacijos saugumo valdymo sistema, kartu su juose nustatytomis valdymo sistemomis, ir nustatyti kompetentingoms institucijoms keliami reikalavimai, susiję su pirmiau minėtus informacijos saugumo valdymo reikalavimus vykdančių organizacijų priežiūra;

(16) siekiant organizacijoms suteikti pakankamai laiko užtikrinti atitiktį naujoms taisyklėms ir procedūroms, šis reglamentas turėtų būti pradėtas taikyti praėjus 3 metams nuo jo įsigaliojimo, išskyrus Europos geostacionarinės navigacinės tinklo sistemos (EGNOS) oro navigacijos paslaugų teikėjo, apibrėžto Įgyvendinimo reglamente (ES) 2017/373, atvejį: dėl EGNOS sistemos ir paslaugų saugumo akreditavimo, tebevykdomo pagal Reglamentą (ES) 2021/696, tokiems oro navigacijos paslaugų teikėjams reglamentas turėtų būti taikomas nuo 2026 m. sausio 1 d.;

(17) šiame reglamente nustatyti reikalavimai grindžiami Nuomone Nr. 03/2021 ([13]), kurią Agentūra paskelbė pagal Reglamento (ES) 2018/1139 75 straipsnio 2 dalies b ir c punktus ir 76 straipsnio 1 dalį;

([9]) 2015 m. lapkričio 5 d. Komisijos įgyvendinimo reglamentas (ES) 2015/1998, kuriuo nustatomos išsamios bendrųjų pagrindinių aviacijos saugumo standartų įgyvendinimo priemonės (OL L 299, 2015 11 14, p. 1).

([10]) 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1).

([11]) 2021 m. balandžio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/696, kuriuo sudaroma Sąjungos kosmoso programa, įsteigiama Europos Sąjungos kosmoso programos agentūra ir panaikinami reglamentai (ES) Nr. 912/2010, (ES) Nr. 1285/2013 bei (ES) Nr. 377/2014 ir Sprendimas Nr. 541/2014/ES (OL L 170, 2021 5 12, p. 69).

([12]) 2017 m. kovo 1 d. Komisijos įgyvendinimo reglamentas (ES) 2017/373, kuriuo nustatomi oro eismo valdymo ir oro navigacijos paslaugų teikėjų, kitų oro eismo valdymo tinklo funkcijų vykdytojų ir tų subjektų priežiūros bendrieji reikalavimai, panaikinamas Reglamentas (EB) Nr. 482/2008, įgyvendinimo reglamentai (ES) Nr. 1034/2011, (ES) Nr. 1035/2011 ir (ES) 2016/1377 ir iš dalies keičiamas Reglamentas (ES) Nr. 677/2011 (OL L 62, 2017 3 8, p. 1).

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

(18) šiame reglamente nustatyti reikalavimai atitinka pagal Reglamento (ES) 2018/1139 127 straipsnį įsteigto Bendrųjų saugos taisyklių taikymo civilinės aviacijos srityje komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Dalykas

Šiame reglamente nustatomi reikalavimai, kurių organizacijos ir kompetentingos institucijos turi laikytis tam, kad:

a) nustatytų ir valdytų informacijos saugumo riziką, galinčią daryti poveikį aviacijos saugai ir turėti įtakos civilinės aviacijos tikslais naudojamoms informacinių ir ryšių technologijų sistemoms bei duomenims,

b) aptiktų informacijos saugumo įvykius ir nustatytų įvykius, laikomus informacijos saugumo incidentais, galinčiais turėti įtakos aviacijos saugai,

c) reaguotų į tuos informacijos saugumo incidentus ir atkurtų veiklą po tokių incidentų.

2 straipsnis

Taikymo sritis

1. Šis reglamentas taikomas šioms organizacijoms:

a) į Reglamento (ES) Nr. 1321/2014 II priedo (145 dalies) A skirsnio taikymo sritį įtrauktoms techninės priežiūros organizacijoms, išskyrus tas, kurios vykdo tik orlaivių techninės priežiūros veiklą pagal Reglamento (ES) Nr. 1321/2014 Vb priedą (ML dalį);

b) į Reglamento (ES) Nr. 1321/2014 Vc priedo (CAMO dalies) A skyriaus taikymo sritį įtrauktoms nepertraukiamąjį tinkamumą skraidyti užtikrinančioms organizacijoms (CAMO), išskyrus tas, kurios vykdo tik orlaivių nepertraukiamojo tinkamumo skraidyti užtikrinimo veiklą pagal Reglamento (ES) Nr. 1321/2014 Vb priedą (ML dalį);

c) į Reglamento (ES) Nr. 965/2012 III priedo (ORO dalis) taikymo sritį įtrauktiems oro vežėjams, išskyrus tuos, kurie naudoja tik kuriuos nors iš toliau nurodytų orlaivių:

i) ELA2 orlaivį, apibrėžtą Reglamento (ES) Nr. 748/2012 1 straipsnio 2 dalies j punkte;

ii) sraigtinius vieno variklio lėktuvus, kurių didžiausia eksploatacinė keleivių krėslų konfigūracija yra ne didesnė kaip 5 ir kurie nepriskiriami prie sudėtingų varikliu varomų orlaivių, jei jie kyla ir tupia tame pačiame aerodrome ar skrydžių aikštelėje ir skrydžius vykdo pagal dienos metu vykdomų vizualiųjų skrydžių taisykles (VFR);

iii) vieno variklio sraigtasparnius, kurių didžiausia eksploatacinė keleivių krėslų konfigūracija yra ne didesnė kaip 5 ir kurie nepriskiriami prie sudėtingų varikliu varomų orlaivių, jei jie kyla ir tupia tame pačiame aerodrome ar skrydžių aikštelėje ir skrydžius vykdo pagal dienos metu vykdomų vizualiųjų skrydžių taisykles (VFR);

d) į Reglamento (ES) Nr. 1178/2011 VII priedo (ORA dalies) taikymo sritį įtrauktoms patvirtintoms mokymo organizacijoms (ATO), išskyrus tas, kurios vykdo tik su orlaiviu ELA2, apibrėžtu Reglamento (ES) Nr. 748/2012 1 straipsnio 2 dalies j punkte, susijusią mokymo veiklą arba vykdo tik teorinio mokymo veiklą;

e) į Reglamento (ES) Nr. 1178/2011 VII priedo (ORA dalies) taikymo sritį įtrauktiems orlaivių įguloms skirtiems aviacijos medicinos centrams;

f) į Reglamento (ES) Nr. 1178/2011 VII priedo (ORA dalies) taikymo sritį įtrauktiems imituojamo skrydžio treniruoklių (FSTD) naudotojams, išskyrus tuos, kurie naudoja tik su orlaiviu ELA2, apibrėžtu Reglamento (ES) Nr. 748/2012 1 straipsnio 2 dalies j punkte, susijusius FSTD;

g) į Reglamento (ES) 2015/340 III priedo (ATCO.OR dalies) taikymo sritį įtrauktoms skrydžių vadovų mokymo organizacijoms (ATCO TO) ir skrydžių vadovams skirtiems aviacijos medicinos centrams;

h) į Įgyvendinimo reglamento (ES) 2017/373 III priedo (ATM/ANS.OR dalies) taikymo sritį įtrauktoms organizacijoms, išskyrus šiuos paslaugų teikėjus:

i) oro navigacijos paslaugų teikėjus, turinčius ribotos taikymo srities pažymėjimą pagal to priedo ATM/ANS.OR.A.010 punktą;

ii) skrydžių informacijos paslaugų teikėjus, deklaruojančius savo veiklą pagal to priedo ATM/ANS.OR.A.015 dalį;

i) į Įgyvendinimo reglamento (ES) 2021/664 taikymo sritį įtrauktiems sistemos „U-space“ paslaugų teikėjams ir vieninteliams bendrų informacijos paslaugų teikėjams.

2. Šis reglamentas taikomas kompetentingoms institucijoms, įskaitant Europos Sąjungos aviacijos saugos agentūrą (toliau – Agentūra), nurodytoms šio reglamento 6 straipsnyje ir Komisijos deleguotojo reglamento (ES) 2022/1645 ([14]) 5 straipsnyje.

3. Šis reglamentas taip pat taikomas kompetentingai institucijai, atsakingai už orlaivių techninės priežiūros licencijų išdavimą, pratęsimą, keitimą, galiojimo sustabdymą arba atšaukimą pagal Reglamento (ES) Nr. 1321/2014 III priedą (66 dalį).

4. Šis reglamentas nedaro poveikio informacijos saugumo ir kibernetinio saugumo reikalavimams, nustatytiems Įgyvendinimo reglamento (ES) 2015/1998 priedo 1.7 punkte ir Direktyvos (ES) 2016/1148 14 straipsnyje.

3 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) informacijos saugumas – tinklų ir informacinių sistemų konfidencialumo, vientisumo, autentiškumo ir prieinamumo išlaikymas;

2) informacijos saugumo įvykis – nustatytas sistemos, paslaugos ar tinklo būklės įvykis, rodantis galimą informacijos saugumo politikos pažeidimą arba informacijos saugumo kontrolės triktį, arba dar nežinoma situacija, kuri gali būti svarbi informacijos saugumui;

3) incidentas – faktinį neigiamą poveikį tinklų ir informacinių sistemų saugumui turintis įvykis, apibrėžtas Direktyvos (ES) 2016/1148 4 straipsnio 7 punkte;

4) informacijos saugumo rizika – dėl informacijos saugumo įvykio galimybės kylanti rizika organizacinėms civilinės aviacijos operacijoms, turtui, asmenims ir kitoms organizacijoms. Informacijos saugumo rizika yra susijusi su galimybe, kad, kilus grėsmei, bus pasinaudota informacinio turto arba informacinių išteklių grupės pažeidžiamumu;

([14]) Komisijos deleguotasis reglamentas (ES) 2022/1645 2022 m. liepos 14 d. kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2018/1139 taikymo taisyklės, susijusios su Komisijos reglamentuose (ES) Nr. 748/2012 ir (ES) Nr. 139/2014 nurodytoms organizacijoms taikytinais informacijos saugumo rizikos, galinčios turėti įtakos aviacijos saugai, valdymo reikalavimais, ir kuriuo iš dalies keičiami Komisijos reglamentai (ES) Nr. 748/2012 ir (ES) Nr. 139/2014 (OL L 248, 2022 9 26, p. 18).

5) grėsmė – galimas informacijos saugumo pažeidimas, atsirandantis esant subjektui, aplinkybėms, veiksmui arba įvykiui, galintiems padaryti žalos;

6) pažeidžiamumas – turto, sistemos, procedūrų, projektavimo, įgyvendinimo ar informacijos saugumo priemonių trūkumas arba silpnoji vieta, kuriais būtų galima pasinaudoti ir dėl kurių būtų pažeista informacijos saugumo politika.

4 straipsnis

Organizacijoms ir kompetentingoms institucijoms taikomi reikalavimai

1. 2 straipsnio 1 dalyje nurodytos organizacijos laikosi šio reglamento II priedo (IS.I.OR dalies) reikalavimų.

2. 2 straipsnio 2 ir 3 dalyse nurodytos kompetentingos institucijos laikosi šio reglamento I priedo (IS.AR dalies) reikalavimų.

5 straipsnis

Iš kitų Sąjungos teisės aktų kylantys reikalavimai

1. Jei 2 straipsnio 1 dalyje nurodyta organizacija atitinka Direktyvos (ES) 2016/1148 14 straipsnyje nustatytus saugumo reikalavimus, kurie yra lygiaverčiai šiame reglamente nustatytiems reikalavimams, atitiktis tiems saugumo reikalavimams laikoma atitiktimi šiame reglamente nustatytiems reikalavimams.

2. Jei 2 straipsnio 1 dalyje nurodyta organizacija yra operatorius arba subjektas, nurodytas valstybių narių nacionalinėse civilinės aviacijos saugumo programose, parengtose pagal Europos Parlamento ir Tarybos reglamento (EB) Nr. 300/2008 ([15]) 10 straipsnį, Įgyvendinimo reglamento (ES) 2015/1998 priedo 1.7 punkte nustatyti kibernetinio saugumo reikalavimai laikomi lygiaverčiais šiame reglamente nustatytiems reikalavimams, išskyrus šio reglamento II priedo IS.I.OR.230 dalį, kurios turi būti laikomasi.

3. Jei 2 straipsnio 1 dalyje nurodyta organizacija yra Reglamente (ES) 2021/696 nurodytos Europos geostacionarinės navigacinės tinklo sistemos (EGNOS) oro navigacijos paslaugų teikėja, to reglamento V antraštinės dalies 33–43 straipsniuose nustatyti saugumo reikalavimai laikomi lygiaverčiais šiame reglamente nustatytiems reikalavimams, išskyrus šio reglamento II priedo IS.I.OR.230 dalyje nustatytus reikalavimus, kurių turi būti laikomasi.

4. Komisija, pasikonsultavusi su Agentūra ir Direktyvos (ES) 2016/1148 11 straipsnyje nurodyta Bendradarbiavimo grupe, gali paskelbti šiame reglamente ir Direktyvoje (ES) 2016/1148 nustatytų reikalavimų lygiavertiškumo vertinimo gaires.

6 straipsnis

Kompetentinga institucija

1. Nedarant poveikio Reglamento (ES) 2021/696 36 straipsnyje nurodytai Saugumo akreditavimo valdybai pavestoms užduotims, už atitikties šiam reglamentui patvirtinimą ir priežiūrą atsakinga institucija yra:

a) 2 straipsnio 1 dalies a punkte nurodytų organizacijų – kompetentinga institucija, paskirta pagal Reglamento (ES) Nr. 1321/2014 II priedą (145 dalį);

b) 2 straipsnio 1 dalies b punkte nurodytų organizacijų – kompetentinga institucija, paskirta pagal Reglamento (ES) Nr. 1321/2014 Vc priedą (CAMO dalį);

([15]) 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių ir panaikinantis Reglamentą (EB) Nr. 2320/2002 (OL L 97, 2008 4 9, p. 72).

c) 2 straipsnio 1 dalies c punkte nurodytų organizacijų – kompetentinga institucija, paskirta pagal Reglamento (ES) Nr. 965/2012 III priedą (ORO dalį);

d) 2 straipsnio 1 dalies d–f punktuose nurodytų organizacijų – kompetentinga institucija, paskirta pagal Reglamento (ES) Nr. 1178/2011 VII priedą (ORA dalį);

e) 2 straipsnio 1 dalies g punkte nurodytų organizacijų – kompetentinga institucija, paskirta pagal Reglamento (ES) 2015/340 6 straipsnio 2 dalį;

f) 2 straipsnio 1 dalies h punkte nurodytų organizacijų – kompetentinga institucija, paskirta pagal Įgyvendinimo reglamento (ES) 2017/373 4 straipsnio 1 dalį;

g) 2 straipsnio 1 dalies i punkte nurodytų organizacijų – kompetentinga institucija, paskirta pagal atitinkamai Įgyvendinimo reglamento (ES) 2021/664 14 straipsnio 1 arba 2 dalį.

2. Šio reglamento tikslais valstybės narės gali paskirti nepriklausomą ir savarankišką subjektą, kuris atliktų 1 dalyje nurodytoms kompetentingoms institucijoms paskirtą funkciją ir pareigas. Tokiu atveju, siekiant užtikrinti veiksmingą visų reikalavimų, kuriuos turi atitikti organizacija, priežiūrą, nustatomos to subjekto ir 1 dalyje nurodytų kompetentingų institucijų veiklos koordinavimo priemonės.

3. Agentūra, visapusiškai laikydamasi taikytinų slaptumo, asmens duomenų apsaugos ir įslaptintos informacijos apsaugos taisyklių, bendradarbiauja su Europos Sąjungos kosmoso programos agentūra (EUSPA) ir Reglamento (ES) 2021/696 36 straipsnyje nurodyta SAV, kad būtų užtikrinta veiksminga EGNOS oro navigacijos paslaugų teikėjui taikomų reikalavimų priežiūra.

7 straipsnis

Atitinkamos informacijos teikimas TIS kompetentingoms institucijoms

Kompetentingos institucijos pagal šį reglamentą nedelsdamos informuoja pagal Direktyvos (ES) 2016/1148 8 straipsnį paskirtą bendrąjį informacinį centrą apie visą svarbią informaciją, įtrauktą į pranešimus, kuriuos pagal šio reglamento II priedo IS.I.OR.230 dalį ir Deleguotojo reglamento (ES) 2022/1645 I priedo IS.D.OR.230 dalį teikia esminių paslaugų operatoriai, identifikuoti pagal Direktyvos (ES) 2016/1148 5 straipsnį.

8 straipsnis

Reglamento (ES) Nr. 1178/2011 pakeitimai

Reglamento (ES) Nr. 1178/2011 VI priedas (ARA dalis) ir VII priedas (ORA dalis) iš dalies keičiami pagal šio reglamento III priedą.

9 straipsnis

Reglamento (ES) Nr. 748/2012 pakeitimai

Reglamento (ES) Nr. 748/2012 I priedas (21 dalis) iš dalies keičiamas pagal šio reglamento IV priedą.

10 straipsnis

Reglamento (ES) Nr. 965/2012 pakeitimai

Reglamento (ES) Nr. 965/2012 II priedas (ARO dalis) ir III priedas (ORO dalis) iš dalies keičiami pagal šio reglamento V priedą.

11 straipsnis

Reglamento (ES) Nr. 139/2014 pakeitimai

Reglamento (ES) Nr. 139/2014 II priedas (ADR.AR dalis) iš dalies keičiamas pagal šio reglamento VI priedą.

12 straipsnis

Reglamento (ES) Nr. 1321/2014 pakeitimai

Reglamento (ES) Nr. 1321/2014 II priedas (145 dalis), III priedas (66 dalis) ir Vc priedas (CAMO dalis) iš dalies keičiami pagal šio reglamento VII priedą.

13 straipsnis

Reglamento (ES) 2015/340 pakeitimai

Reglamento (ES) 2015/340 II priedas (ATCO.AR dalis) ir III priedas (ATCO.OR dalis) iš dalies keičiami pagal šio reglamento VIII priedą.

14 straipsnis

Įgyvendinimo reglamento (ES) 2017/373 pakeitimai

Įgyvendinimo reglamento (ES) 2017/373 II priedas (ATM/ANS.AR dalis) ir III priedas (ATM/ANS.OR dalis) iš dalies keičiami pagal šio reglamento IX priedą.

15 straipsnis

Įgyvendinimo reglamento (ES) 2021/664 pakeitimai

Įgyvendinimo reglamentas (ES) 2021/664 iš dalies keičiamas taip:

1) 15 straipsnio 1 dalies f punktas pakeičiamas taip:

„f) taiko ir nuolat atnaujina saugumo valdymo sistemą pagal Įgyvendinimo reglamento (ES) 2017/373 III priedo D skyriaus ATM/ANS.OR.D.010 dalį ir informacijos saugumo valdymo sistemą pagal Įgyvendinimo reglamento (ES) 2023/203 II priedą (IS.I.OR dalį);“;

2) 18 straipsnis papildomas l punktu:

„l) parengia, taiko ir nuolat atnaujina informacijos saugumo valdymo sistemą pagal Įgyvendinimo reglamento (ES) 2023/203 I priedą (IS.AR dalį).“

16 straipsnis

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Jis taikomas nuo 2026 m. vasario 22 d.

Tačiau EGNOS oro navigacijos paslaugų teikėjui, kuriam taikomas Įgyvendinimo reglamentas (ES) 2017/373, jis taikomas nuo 2026 m. sausio 1 d.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2022 m. spalio 27 d.

Komisijos vardu

Pirmininkė

Ursula VON DER LEYEN

I PRIEDAS

INFORMACIJOS SAUGUMAS. INSTITUCIJOMS TAIKOMI REIKALAVIMAI

[IS.AR DALIS]

IS.AR.100. Taikymo sritis

IS.AR.200. Informacijos saugumo valdymo sistema (ISVS)

IS.AR.205. Informacijos saugumo rizikos vertinimas

IS.AR.210. Veiksmai su informacijos saugumo rizika

IS.AR.215. Informacijos saugumo incidentai. Aptikimas, reagavimas ir veiklos atkūrimas

IS.AR.220. Sutarčių dėl informacijos saugumo valdymo veiklos sudarymas

IS.AR.225. Darbuotojų reikalavimai

IS.AR.230. Įrašų saugojimas

IS.AR.235. Tęstinis tobulinimas

IS.AR.100. Taikymo sritis

Šioje dalyje nustatomi reikalavimai, kurių turi laikytis šio reglamento 2 straipsnio 2 dalyje nurodytos kompetentingos institucijos.

Reikalavimai, kuriuos turi atitikti tos kompetentingos institucijos, kad galėtų vykdyti sertifikavimo, priežiūros ir vykdymo užtikrinimo veiklą, nustatyti šio reglamento 2 straipsnio 1 dalyje ir Deleguotojo reglamento (ES) 2022/1645 2 straipsnyje nurodytuose reglamentuose.

IS.AR.200. Informacijos saugumo valdymo sistema (ISVS)

a) Siekdama 1 straipsnyje nustatytų tikslų, kompetentinga institucija sukuria, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą (ISVS), kuria užtikrinama, kad kompetentinga institucija:

1) parengtų informacijos saugumo politiką, kurioje būtų nustatyti bendrieji kompetentingos institucijos principai, susiję su galimu informacijos saugumo rizikos poveikiu aviacijos saugai;

2) pagal IS.AR.205 dalį nustatytų ir peržiūrėtų informacijos saugumo riziką;

3) pagal IS.AR.210 dalį parengtų ir įgyvendintų veiksmų su informacijos saugumo rizika priemones;

4) pagal IS.AR.215 dalį parengtų ir įgyvendintų informacijos saugumo įvykiams aptikti skirtas priemones, nustatytų įvykius, kurie laikomi incidentais, galinčiais turėti įtakos aviacijos saugai, ir imtųsi reagavimo į tuos informacijos saugumo incidentus priemonių ir atkurtų veiklą;

5) su kitomis organizacijomis sudarydama sutartis dėl bet kurios IS.AR.200 dalyje nurodytos veiklos dalies laikytųsi IS.AR.220 dalyje nustatytų reikalavimų;

6) laikytųsi IS.AR.225 dalyje nustatytų darbuotojų reikalavimų;

7) laikytųsi IS.AR.230 dalyje nustatytų įrašų saugojimo reikalavimų;

8) stebėtų, kaip jos pačios organizacija laikosi šio reglamento reikalavimų, ir IS.AR.225 dalies a punkte nurodytam asmeniui teiktų grįžtamąją informaciją apie nustatytus faktus, kad būtų užtikrintas veiksmingas taisomųjų veiksmų įgyvendinimas;

9) saugotų visos informacijos, kurią kompetentinga institucija gali turėti, susijusios su organizacijomis, kurioms taikoma jos priežiūra, ir informacijos, gautos per organizacijos išorės pranešimų teikimo sistemas, nustatytas pagal šio reglamento II priedo (IS.I.OR dalies) IS.I.OR.230 dalį ir Deleguotojo reglamento (ES) 2022/1645 priedo (IS.D.OR dalies) IS.D.OR.230 dalį, konfidencialumą;

10) praneštų Agentūrai apie pokyčius, turinčius įtakos kompetentingos institucijos gebėjimui atlikti savo užduotis ir vykdyti šiame reglamente nustatytas pareigas;

11) nustatytų ir įgyvendintų procedūras, pagal kurias, kai tinkama, praktiškai ir laiku dalijamasi aktualia informacija, siekiant padėti kitoms kompetentingoms institucijoms ir agentūroms, taip pat organizacijoms, kurioms taikomas šis reglamentas, atlikti veiksmingus su jų veikla susijusius saugumo rizikos vertinimus.

b) Siekdama nuolat atitikti 1 straipsnyje nurodytus reikalavimus, kompetentinga institucija pagal IS.AR.235 dalį įgyvendina nuolatinio tobulinimo procesą.

c) Kompetentinga institucija dokumentais įformina visus pagrindinius procesus, procedūras, funkcijas ir atsakomybę, kurių reikia, kad būtų laikomasi IS.AR.200 dalies a punkto reikalavimų, ir nustato tų dokumentų keitimo tvarką.

d) Procesai, procedūros, funkcijos ir atsakomybė, kuriuos kompetentinga institucija nustatė siekdama laikytis IS.AR.200 dalies a punkto reikalavimų, turi atitikti jos veiklos pobūdį ir sudėtingumą, atsižvelgiant į tai veiklai būdingos informacijos saugumo rizikos vertinimą, ir gali būti integruoti į kitas esamas organizacijos jau įdiegtas valdymo sistemas.

IS.AR.205. Informacijos saugumo rizikos vertinimas

a) Kompetentinga institucija nustato visus savo organizacijos elementus, kuriems gali kelti grėsmę informacijos saugumo rizika. Tai apima:

1. kompetentingos institucijos veiklą, infrastruktūrą ir išteklius, taip pat paslaugas, kurias kompetentinga institucija valdo, teikia, gauna ar prižiūri;

2. įrangą, sistemas, duomenis ir informaciją, kurie padeda užtikrinti 1 punkte išvardytų elementų veikimą.

b) Kompetentinga institucija nustato turimas savo organizacijos sąsajas su kitomis organizacijomis, dėl kurių jai ir toms organizacijoms gali kelti grėsmę informacijos saugumo rizika.

c) Kiek tai susiję su a ir b punktuose nurodytais elementais ir sąsajomis, kompetentinga institucija nustato informacijos saugumo riziką, kuri gali turėti įtakos aviacijos saugai.

Dėl kiekvienos nustatytos rizikos kompetentinga institucija:

1. nustato rizikos lygį pagal kompetentingos institucijos nustatytą iš anksto parengtą klasifikaciją;

2. kiekvieną riziką ir jos lygį susieja su atitinkamu elementu arba sąsaja, nustatytais pagal a ir b punktus.

1 punkte nurodytoje iš anksto parengtoje klasifikacijoje atsižvelgiama į galimą grėsmės scenarijaus atsiradimą ir jo pasekmių saugai sunkumą. Remdamasi ta klasifikacija ir atsižvelgdama į tai, ar yra įsidiegusi struktūrizuotą ir kartotinį veiklos rizikos valdymo procesą, kompetentinga institucija turi gebėti nustatyti, ar rizika yra priimtina, ar reikia imtis veiksmų su rizika pagal IS.AR.210 dalį.

Siekiant palengvinti abipusį rizikos vertinimų palyginimą, nustatant rizikos lygį pagal 1 punktą, atsižvelgiama į aktualią informaciją, gautą koordinuojant veiksmus su b punkte nurodytomis organizacijomis.

d) Kompetentinga institucija peržiūri ir atnaujina pagal a, b ir c punktus atliktą rizikos vertinimą bet kuriuo iš šių atvejų:

1. pasikeitus elementams, kuriems gali kelti grėsmę informacijos saugumo rizika;

2. pasikeitus kompetentingos institucijos organizacijos ir kitų organizacijų sąsajoms arba rizikai, apie kurią pranešė kitos organizacijos;

3. pasikeitus informacijai ar žinioms, naudojamoms rizikai nustatyti, analizuoti ir klasifikuoti;

4. įgijus patirties vykdant informacijos saugumo incidentų analizę.

IS.AR.210. Veiksmai su informacijos saugumo rizika

a) Kompetentinga institucija parengia pagal IS.AR.205 dalį nustatytos nepriimtinos rizikos mažinimo priemones, jas laiku įgyvendina ir nuolat tikrina jų veiksmingumą. Tos priemonės kompetentingai institucijai turi suteikti galimybę:

1. kontroliuoti aplinkybes, kurios prisideda prie faktinio grėsmės scenarijaus atsiradimo;

2. sumažinti su grėsmės scenarijaus išsipildymu susijusias pasekmes aviacijos saugai;

3. išvengti rizikos.

Tos priemonės neturi kelti jokios naujos galimos nepriimtinos rizikos aviacijos saugai.

b) IS.AR.225 dalies a punkte nurodytas asmuo ir kiti susiję kompetentingos institucijos darbuotojai informuojami apie rizikos vertinimo, atlikto pagal IS.AR.205 dalį, rezultatus, atitinkamus grėsmės scenarijus ir įgyvendintinas priemones.

Kompetentinga institucija taip pat informuoja organizacijas, su kuriomis ji turi sąsają pagal IS.AR.205 dalies b punktą, apie kompetentingai institucijai ir organizacijai bendrą riziką.

IS.AR.215. Informacijos saugumo incidentai. Aptikimas, reagavimas ir veiklos atkūrimas

a) Remdamasi pagal IS.AR.205 dalį atlikto rizikos vertinimo rezultatais ir pagal IS.AR.210 punktą atliktų veiksmų su rizika rezultatais, kompetentinga institucija įgyvendina įvykių, kurie rodo galimą nepriimtinos rizikos pasireiškimą ir kurie gali turėti įtakos aviacijos saugai, aptikimo priemones. Tos aptikimo priemonės kompetentingai institucijai turi suteikti galimybę:

1. nustatyti nuokrypius nuo iš anksto nustatytų funkcinio veiksmingumo bazinių verčių;

2. aktyvuoti įspėjimus, kad bet kokio nuokrypio atveju būtų taikomos tinkamos reagavimo priemonės.

b) Kompetentinga institucija įgyvendina priemones, kurios padeda reaguoti į bet kokias pagal a punktą nustatytas įvykio aplinkybes, kurios gali nulemti arba nulėmė informacijos saugumo incidentą. Tos reagavimo priemonės kompetentingai institucijai turi suteikti galimybę:

1. inicijuoti jos pačios organizacijos reakciją į a punkto 2 papunktyje nurodytus įspėjimus, aktyvuojant iš anksto nustatytus išteklius ir veiksmų seką;

2. sustabdyti išpuolio plitimą ir išvengti visiško grėsmės scenarijaus išsipildymo;

3. kontroliuoti IS.AR.205 dalies a punkte nustatytų paveiktų elementų veikimą trikties režimu.

c) Kompetentinga institucija įgyvendina priemones, kuriomis siekiama atkurti veiklą po informacijos saugumo incidentų, įskaitant, jei reikia, neatidėliotinas priemones. Tos veiklos atkūrimo priemonės kompetentingai institucijai turi suteikti galimybę:

1. pašalinti incidentą sukėlusią aplinkybę arba apriboti ją iki toleruotino lygio;

2. per jos pačios organizacijos iš anksto nustatytą veiklos atkūrimo laiką užtikrinti, kad paveiktų elementų, nustatytų IS.AR.205 dalies a punkte, būklė būtų saugi.

IS.AR.220. Sutarčių dėl informacijos saugumo valdymo veiklos sudarymas

Kompetentinga institucija užtikrina, kad tais atvejais, kai su kitomis organizacijomis sudaromos sutartys dėl bet kurios IS.AR.200 dalyje nurodytos veiklos dalies, veikla, dėl kurios sudaryta sutartis, atitiktų šio reglamento reikalavimus, o organizacija, su kuria sudaryta sutartis, veiktų jos prižiūrima. Kompetentinga institucija užtikrina, kad rizika, susijusi su veikla, dėl kurios sudaryta sutartis, būtų tinkamai valdoma.

IS.AR.225. Darbuotojų reikalavimai

Kompetentinga institucija:

a) turi asmenį, turintį įgaliojimus nustatyti ir prižiūrėti šiam reglamentui įgyvendinti būtinas organizacines struktūras, politiką, procesus ir procedūras.

Šis asmuo:

1. turi įgaliojimus visapusiškai naudotis ištekliais, kurių reikia, kad kompetentinga institucija galėtų atlikti visas šiame reglamente nustatytas užduotis;

2. gali perduoti galias, kurių reikia paskirtoms pareigoms atlikti;

b) turi nustatytą procesą, kuriuo užtikrinama, kad jis turėtų pakankamą skaičių darbuotojų šiame priede nurodytai veiklai vykdyti;

c) turi nustatytą procesą, kuriuo užtikrinama, kad b punkte nurodyti darbuotojai turėtų reikiamą kompetenciją savo užduotims atlikti;

d) turi nustatytą procesą, kuriuo užtikrinama, kad darbuotojai pripažintų savo pareigas, susijusias su jiems pavestomis funkcijomis ir užduotimis;

e) užtikrina, kad būtų tinkamai nustatyta darbuotojų, turinčių prieigą prie informacinių sistemų ir duomenų, kuriems taikomi šio reglamento reikalavimai, tapatybė ir patikimumas.

IS.AR.230. Įrašų saugojimas

a) Kompetentinga institucija registruoja savo informacijos saugumo valdymo veiklą.

1. Kompetentinga institucija užtikrina, kad būtų archyvuojami ir atsekami šie įrašai:

i) sutartys dėl veiklos, nurodytos IS.AR.200 dalies a punkto 5 papunktyje;

ii) įrašai apie IS.AR.200 dalies d punkte nurodytus pagrindinius procesus;

iii) įrašai apie IS.AR.205 dalyje nurodytame rizikos vertinime nustatytą riziką ir IS.AR.210 dalyje nurodytas susijusias rizikos priežiūros priemones;

iv) įrašai apie informacijos saugumo įvykius, kuriuos gali reikėti iš naujo įvertinti, kad būtų atskleisti neaptikti informacijos saugumo incidentai ar pažeidžiamumas.

2. 1 punkto i papunktyje nurodyti įrašai saugomi bent 5 metus nuo sutarties pakeitimo arba nutraukimo.

3. 1 punkto ii ir iii papunkčiuose nurodyti įrašai saugomi bent 5 metus.

4. 1 punkto iv papunktyje nurodyti įrašai saugomi tol, kol tie informacijos saugumo įvykiai bus pakartotinai įvertinti kompetentingos institucijos nustatytoje procedūroje numatytu periodiškumu.

b) Kompetentinga institucija saugo įrašus, susijusius su savo darbuotojų, vykdančių informacijos saugumo valdymo veiklą, kvalifikacija ir patirtimi.

1. Įrašai apie darbuotojų kvalifikaciją ir patirtį saugomi tol, kol asmuo dirba kompetentingoje institucijoje, ir ne trumpiau kaip 3 metus po to, kai asmuo paliko kompetentingą instituciją.

2. Jei darbuotojai paprašo, jiems suteikiama prieiga prie jų individualių įrašų. Be to, jei prieš palikdami kompetentingą instituciją jie pateikia prašymą, kompetentinga institucija jiems pateikia jų individualių įrašų kopiją.

c) Kokiu formatu saugomi įrašai, nurodoma kompetentingos institucijos tvarkoje.

d) Įrašai saugomi taip, kad būtų užtikrinta jų apsauga pažeidimo, pakeitimų ir vagystės, o informacija, kai reikia, žymima nurodant jos slaptumo žymos laipsnį. Kompetentinga institucija užtikrina, kad įrašai būtų saugomi naudojant priemones, kuriomis užtikrinamas vientisumas, autentiškumas ir leidžiama prieiga.

IS.AR.235. Tęstinis tobulinimas

a) Kompetentinga institucija įvertina, naudodama adekvačius veiklos rezultatų rodiklius, savo ISVS veiksmingumą ir išbaigtumą. Vertinimas atliekamas pagal kompetentingos institucijos iš anksto nustatytą tvarkaraštį arba po informacijos saugumo incidento.

b) Jei atlikus vertinimą pagal a punktą nustatoma trūkumų, kompetentinga institucija imasi būtinų tobulinimo priemonių, siekdama užtikrinti, kad ISVS toliau atitiktų taikomus reikalavimus ir padėtų išlaikyti priimtiną informacijos saugumo rizikos lygį. Be to, kompetentinga institucija iš naujo įvertina tuos ISVS elementus, kuriems padarė poveikį priimtos priemonės.

II PRIEDAS

INFORMACIJOS SAUGUMAS. ORGANIZACIJOMS TAIKOMI REIKALAVIMAI

[IS.I.OR DALIS]

IS.I.OR.100. Taikymo sritis

IS.I.OR.200. Informacijos saugumo valdymo sistema (ISVS)

IS.I.OR.205. Informacijos saugumo rizikos vertinimas

IS.I.OR.210. Veiksmai su informacijos saugumo rizika

IS.I.OR.215. Informacijos saugumo vidaus pranešimų teikimo sistema

IS.I.OR.220. Informacijos saugumo incidentai. Aptikimas, reagavimas ir veiklos atkūrimas

IS.I.OR.225. Reagavimas į pažeidimus, apie kuriuos pranešė kompetentinga institucija

IS.I.OR.230. Informacijos saugumo išorės pranešimų teikimo sistema

IS.I.OR.235. Sutarčių dėl informacijos saugumo valdymo veiklos sudarymas

IS.I.OR.240. Darbuotojų reikalavimai

IS.I.OR.245. Įrašų saugojimas

IS.I.OR.250. Informacijos saugumo valdymo vadovas (ISVV)

IS.I.OR.255. Informacijos saugumo valdymo sistemos pakeitimai

IS.I.OR.260. Tęstinis tobulinimas

IS.I.OR.100. Taikymo sritis

Šioje dalyje nustatomi reikalavimai, kurių turi laikytis šio reglamento 2 straipsnio 1 dalyje nurodytos organizacijos.

IS.I.OR.200. Informacijos saugumo valdymo sistema (ISVS)

a) Siekdama 1 straipsnyje nustatytų tikslų, organizacija sukuria, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą (ISVS), kuria užtikrinama, kad organizacija:

   1. parengtų informacijos saugumo politiką, kurioje būtų nustatyti bendrieji organizacijos principai, susiję su galimu informacijos saugumo rizikos poveikiu aviacijos saugai;

   2. pagal IS.I.OR.205 dalį nustatytų ir peržiūrėtų informacijos saugumo riziką;

   3. pagal IS.I.OR.210 dalį parengtų ir įgyvendintų veiksmų su informacijos saugumo rizika priemones;

   4. pagal IS.I.OR.215 dalį įdiegtų informacijos saugumo vidaus pranešimų teikimo sistemą;

   5. pagal IS.I.OR.220 dalį parengtų ir įgyvendintų informacijos saugumo įvykiams aptikti skirtas priemones, nustatytų įvykius, kurie laikomi incidentais, galinčiais turėti įtakos aviacijos saugai, išskyrus leidžiamus atvejus pagal IS.I.OR.205 dalies e punktą, imtųsi reagavimo į tuos informacijos saugumo incidentus priemonių ir atkurtų veiklą;

6. įgyvendintų neatidėliotino reagavimo į informacijos saugumo incidentą arba pažeidžiamumą, darantį poveikį aviacijos saugai, priemones, apie kurias pranešė kompetentinga institucija;

7. pagal IS.I.OR.225 dalį imtųsi tinkamų veiksmų, kad pašalintų pažeidimus, apie kuriuos pranešė kompetentinga institucija;

8. pagal IS.I.OR.230 dalį įdiegtų išorės pranešimų teikimo sistemą, kad kompetentinga institucija galėtų imtis tinkamų veiksmų;

9. su kitomis organizacijomis sudarydama sutartis dėl kurios nors IS.I.OR.200 dalyje nurodytos veiklos dalies laikytųsi IS.I.OR.235 dalyje nustatytų reikalavimų;

10. laikytųsi IS.I.OR.240 dalyje nustatytų darbuotojų reikalavimų;

11. laikytųsi IS.I.OR.245 dalyje nustatytų įrašų saugojimo reikalavimų;

12. stebėtų, kaip organizacija laikosi šio reglamento reikalavimų, ir atsakingam vadovui teiktų grįžtamąją informaciją apie nustatytus faktus, kad būtų užtikrintas veiksmingas taisomųjų veiksmų įgyvendinimas;

13. nedarydama poveikio taikytiniems pranešimo apie incidentus reikalavimams, saugotų bet kokios informacijos, kurią organizacija gavo iš kitų organizacijų, konfidencialumą, atsižvelgdama į jos slaptumo lygį.

b) Siekdama nuolat atitikti 1 straipsnyje nurodytus reikalavimus, organizacija pagal IS.I.OR.260 dalį įgyvendina nuolatinio tobulinimo procesą.

c) Organizacija pagal IS.I.OR.250 punktą dokumentais įformina visus pagrindinius procesus, procedūras, funkcijas ir atsakomybę, kurių reikia, kad būtų laikomasi IS.I.OR.200 dalies a punkto, ir nustato tų dokumentų keitimo tvarką. Tų procesų, procedūrų, funkcijų ir atsakomybės pakeitimai tvarkomi pagal IS.I.OR.255 dalį.

d) Procesai, procedūros, funkcijos ir atsakomybė, kuriuos organizacija nustatė siekdama laikytis IS.I.OR.200 dalies a punkto reikalavimų, turi atitikti jos veiklos pobūdį ir sudėtingumą, atsižvelgiant į tai veiklai būdingos informacijos saugumo rizikos vertinimą, ir gali būti integruoti į kitas esamas organizacijos jau įdiegtas valdymo sistemas.

e) Nedarydama poveikio pareigai laikytis pranešimų teikimo reikalavimų, nustatytų Reglamente (ES) Nr. 376/2014, ir IS.I.OR.200 dalies a punkto 13 papunktyje nustatytų reikalavimų, kompetentinga institucija organizacijai gali suteikti patvirtinimą nevykdyti a–d punktuose nurodytų reikalavimų ir susijusių IS.I.OR.205–IS.I.OR.260 dalyse pateiktų reikalavimų, jei ji tai institucijai priimtinu būdu įrodo, kad jos veikla, infrastruktūra ir ištekliai, taip pat jos valdomos, teikiamos, gaunamos ir prižiūrimos paslaugos nekelia jokios informacijos saugumo rizikos, galinčios turėti įtakos aviacijos saugai, nei jai pačiai, nei kitoms organizacijoms. Patvirtinimas turi būti grindžiamas dokumentais pagrįstu informacijos saugumo rizikos vertinimu, kurį organizacija arba trečioji šalis atliko pagal IS.I.OR.205 dalį, o jį peržiūrėjo ir patvirtino jos kompetentinga institucija.

Tęstinį to patvirtinimo galiojimą kompetentinga institucija peržiūrės užbaigusi taikytiną priežiūros audito ciklą ir kas kartą, kai bus atliekami organizacijos darbo apimties pakeitimai.

IS.I.OR.205. Informacijos saugumo rizikos vertinimas

a) Organizacija nustato visus savo elementus, kuriems gali kelti grėsmę informacijos saugumo rizika. Tie elementai apima:

1. organizacijos veiklą, įrenginius ir išteklius, taip pat paslaugas, kurias organizacija valdo, teikia, gauna ar prižiūri;

2. įrangą, sistemas, duomenis ir informaciją, kurie padeda užtikrinti 1 punkte išvardytų elementų veikimą.

b) Organizacija nustato su kitomis organizacijomis turimas sąsajas, dėl kurių jai ir toms organizacijoms gali kelti grėsmę informacijos saugumo rizika.

c) Kiek tai susiję su a ir b punktuose nurodytais elementais ir sąsajomis, organizacija nustato informacijos saugumo riziką, kuri gali turėti įtakos aviacijos saugai. Dėl kiekvienos nustatytos rizikos organizacija:

1. nustato rizikos lygį pagal organizacijos nustatytą iš anksto parengtą klasifikaciją;

2. kiekvieną riziką ir jos lygį susieja su atitinkamu elementu arba sąsaja, nustatytais pagal a ir b punktus.

1 punkte nurodytoje iš anksto parengtoje klasifikacijoje atsižvelgiama į galimą grėsmės scenarijaus atsiradimą ir jo pasekmių saugai sunkumą. Remdamasi ta klasifikacija ir atsižvelgdama į tai, ar yra įsidiegusi struktūrizuotą ir kartotinį veiklos rizikos valdymo procesą, organizacija turi gebėti nustatyti, ar rizika yra priimtina, arba tai, ar reikia imtis veiksmų su rizika pagal IS.I.OR.210 dalį.

Siekiant palengvinti abipusį rizikos vertinimų palyginamumą, nustatant rizikos lygį pagal 1 punktą atsižvelgiama į atitinkamą informaciją, gautą koordinuojant veiksmus su b punkte nurodytomis organizacijomis.

d) Organizacija peržiūri ir atnaujina pagal a, b ir, jei taikoma, c arba e punktą atliktą rizikos vertinimą bet kuriuo iš šių atvejų:

1. pasikeitus elementams, kuriems gali kelti grėsmę informacijos saugumo rizika;

2. pasikeitus organizacijos ir kitų organizacijų sąsajoms arba rizikai, apie kurią pranešė kitos organizacijos;

3. pasikeitus informacijai ar žinioms, naudojamoms rizikai nustatyti, analizuoti ir klasifikuoti;

4. įgijus patirties vykdant informacijos saugumo incidentų analizę.

e) Nukrypstant nuo c punkto, organizacijos, kurios turi laikytis Įgyvendinimo reglamento (ES) 2017/373 III priedo (ATM/ANS.OR dalies) C poskyrio, poveikio aviacijos saugai analizę pakeičia poveikio jų paslaugoms analize, kaip reikalaujama atliekant tinkamumo saugos atžvilgiu vertinimą, kurio reikalaujama ATM/ANS.OR.C.005 dalyje. Šis tinkamumo saugos atžvilgiu vertinimas pateikiamas oro eismo paslaugų teikėjams, kuriems organizacija teikia paslaugas, o tie oro eismo paslaugų teikėjai yra atsakingi už poveikio aviacijos saugai vertinimą.

IS.I.OR.210. Veiksmai su informacijos saugumo rizika

a) Organizacija parengia pagal IS.I.OR.205 dalį nustatytos nepriimtinos rizikos mažinimo priemones, jas laiku įgyvendina ir nuolat tikrina jų veiksmingumą. Tos priemonės organizacijai turi suteikti galimybę:

1. kontroliuoti aplinkybes, kurios prisideda prie faktinio grėsmės scenarijaus atsiradimo;

2. sumažinti su grėsmės scenarijaus išsipildymu susijusias pasekmes aviacijos saugai;

3. išvengti rizikos.

Tos priemonės neturi kelti jokios naujos galimos nepriimtinos rizikos aviacijos saugai.

b) IS.I.OR.240 dalies a ir b punktuose nurodytas asmuo ir kiti susiję organizacijos darbuotojai informuojami apie rizikos vertinimo, atlikto pagal IS.I.OR.205 dalį, rezultatus, atitinkamus grėsmės scenarijus ir įgyvendintinas priemones.

Organizacija taip pat informuoja organizacijas, su kuriomis ji turi sąsają pagal IS.I.OR.205 dalies b punktą, apie joms bendrą riziką.

IS.I.OR.215. Informacijos saugumo vidaus pranešimų teikimo sistema

a) Organizacija sukuria vidaus pranešimų teikimo sistemą, kad būtų galima rinkti informaciją apie informacijos saugumo įvykius ir vertinti tuos įvykius, įskaitant įvykius, apie kuriuos turi būti pranešama pagal IS.I.OR.230 dalį.

b) Ta sistema ir IS.I.OR.220 dalyje nurodytas procesas turi suteikti organizacijai galimybę:

1. nustatyti, kurie iš įvykių, apie kuriuos pranešta pagal a punktą, laikomi informacijos saugumo incidentais arba pažeidžiamumu, galinčiais turėti įtakos aviacijos saugai;

2. identifikuoti pagal 1 punktą nustatytų informacijos saugumo incidentų ir pažeidžiamumo priežastis ir juos lemiančius veiksnius, taip pat juos pašalinti taikant informacijos saugumo rizikos valdymo procesą pagal IS.I.OR.205 ir IS.I.OR.220 dalis;

3. užtikrinti, kad visa žinoma svarbi informacija, susijusi su informacijos saugumo incidentais ir pažeidžiamumu, nustatytais pagal 1 punktą, būtų įvertinta;

4. užtikrinti, kad prireikus būtų taikomas informacijos vidaus platinimo metodas.

c) Bet kuri organizacija, su kuria sudaroma sutartis ir dėl kurios organizacijai gali kilti informacijos saugumo rizika, galinti turėti įtakos aviacijos saugai, privalo pranešti organizacijai apie informacijos saugumo įvykius. Tie pranešimai teikiami taikant konkrečiuose sutartimi įformintuose susitarimuose nustatytas procedūras ir vertinami pagal b punktą.

d) Tyrimų srityje organizacija bendradarbiauja su kiekviena kita organizacija, kurios indėlis į jos veiklos informacijos saugumą yra reikšmingas.

e) Organizacija gali sujungti tą pranešimų teikimo sistemą su kitomis jau įsidiegtomis pranešimų teikimo sistemomis.

IS.I.OR.220. Informacijos saugumo incidentai. Aptikimas, reagavimas ir veiklos atkūrimas

a) Remdamasi pagal IS.I.OR.205 dalį atlikto rizikos vertinimo rezultatais ir pagal IS.I.OR.210 dalį atliktų veiksmų su rizika rezultatais, organizacija įgyvendina incidentų ir pažeidžiamumo, kurie rodo galimą nepriimtinos rizikos pasireiškimą ir kurie gali turėti įtakos aviacijos saugai, aptikimo priemones. Tomis aptikimo priemonėmis organizacijai suteikiama galimybė:

1. nustatyti nuokrypius nuo iš anksto nustatytų funkcinio veiksmingumo bazinių verčių;

2. aktyvuoti įspėjimus, kad bet kokio nuokrypio atveju būtų taikomos tinkamos reagavimo priemonės.

b) Organizacija įgyvendina priemones, kurios padeda reaguoti į bet kokias pagal a punktą nustatytas įvykio aplinkybes, kurios gali nulemti arba nulėmė informacijos saugumo incidentą. Tos reagavimo priemonės organizacijai turi suteikti galimybę:

1. inicijuoti reakciją į a punkto 2 papunktyje nurodytus įspėjimus, aktyvuojant iš anksto nustatytus išteklius ir veiksmų seką;

2. sustabdyti išpuolio plitimą ir išvengti visiško grėsmės scenarijaus išsipildymo;

3. kontroliuoti IS.I.OR.205 dalies a punkte nustatytų paveiktų elementų veikimą trikties režimu.

c) Organizacija įgyvendina priemones, kuriomis siekiama atkurti veiklą po informacijos saugumo incidentų, įskaitant, jei reikia, neatidėliotinas priemones. Tos veiklos atkūrimo priemonės organizacijai turi suteikti galimybę:

1. pašalinti incidentą sukėlusią aplinkybę arba apriboti ją iki toleruotino lygio;

2. per organizacijos iš anksto nustatytą veiklos atkūrimo laiką užtikrinti, kad paveiktų elementų, kurie apibrėžti IS.I.OR.205 dalies a punkte, būklė būtų saugi.

IS.I.OR.225. Reagavimas į pažeidimus, apie kuriuos pranešė kompetentinga institucija

a) Gavusi kompetentingos institucijos pranešimą apie pažeidimus, organizacija:

1. nustato pagrindinę neatitikties priežastį (-is) bei tos neatitikties veiksnius;

2. parengia taisomųjų veiksmų planą;

3. kompetentingai institucijai priimtinu būdu įrodo, kad neatitiktis yra pašalinta.

b) A punkte nurodyti veiksmai atliekami per laikotarpį, dėl kurio susitarta su kompetentinga institucija.

IS.I.OR.230. Informacijos saugumo išorės pranešimų teikimo sistema

a) Organizacija įdiegia informacijos saugumo pranešimų sistemą, atitinkančią Reglamente (ES) Nr. 376/2014 ir jo deleguotuosiuose bei įgyvendinimo aktuose, jei tas reglamentas taikomas organizacijai, nustatytus reikalavimus.

b) Nedarant poveikio Reglamente (ES) Nr. 376/2014 nustatytoms pareigoms, organizacija užtikrina, kad apie bet kokį informacijos saugumo incidentą ar pažeidžiamumą, kurie gali kelti didelę riziką aviacijos saugai, būtų pranešama jos kompetentingai institucijai. Be to:

1. jei toks incidentas ar pažeidžiamumas daro poveikį orlaiviui arba susijusiai sistemai ar komponentui, organizacija apie tai taip pat praneša projekto patvirtinimo turėtojui;

2. jei toks incidentas ar pažeidžiamumas daro poveikį organizacijos naudojamai sistemai ar sudedamajai daliai, organizacija apie tai praneša organizacijai, atsakingai už sistemos ar sudedamosios dalies projektavimą.

c) Apie b punkte nurodytas aplinkybes organizacija praneša taip:

1. pranešimas pateikiamas kompetentingai institucijai ir, jei taikoma, projekto patvirtinimo turėtojui arba organizacijai, atsakingai už sistemos ar sudedamosios dalies projektavimą, kai tik organizacija sužino apie aplinkybę;

2. pranešimas pateikiamas kompetentingai institucijai ir, jei taikoma, projekto patvirtinimo turėtojui arba už sistemos ar sudedamosios dalies projektavimą atsakingai organizacijai kuo greičiau ir ne vėliau kaip per 72 valandas nuo momento, kai organizacija sužinojo apie aplinkybę, nebent tai būtų neįmanoma dėl išskirtinių sąlygų.

   Pranešimas parengiamas kompetentingos institucijos nustatyta forma ir jame pateikiama visa svarbi informacija apie organizacijai žinomą aplinkybę;

3. kompetentingai institucijai ir, jei taikoma, projekto patvirtinimo turėtojui arba už sistemos ar sudedamosios dalies projektavimą atsakingai organizacijai pateikiama tolesnių veiksmų ataskaita, kurioje pateikiama išsami informacija apie veiksmus, kurių organizacija ėmėsi arba ketina imtis, kad atkurtų veiklą po incidento, ir apie veiksmus, kurių ji ketina imtis, kad ateityje užkirstų kelią panašiems informacijos saugumo incidentams.

   Tolesnių veiksmų ataskaita pateikiama iš karto, kai tik nustatomi tie veiksmai, ir parengiama kompetentingos institucijos nustatyta forma.

IS.I.OR.235. Sutarčių dėl informacijos saugumo valdymo veiklos sudarymas

a) Organizacija užtikrina, kad tais atvejais, kai su kitomis organizacijomis sudaromos sutartys dėl bet kurios IS.I.OR.200 dalyje nurodytos veiklos dalies, veikla, dėl kurios sudaryta sutartis, atitiktų šio reglamento reikalavimus, o organizacija, su kuria sudaryta sutartis, veiktų jos prižiūrima. Organizacija užtikrina, kad rizika, susijusi su veikla, dėl kurios sudaryta sutartis, būtų tinkamai valdoma.

b) Organizacija užtikrina, kad pateikusi prašymą kompetentinga institucija galėtų kreiptis į organizaciją, su kuria sudaryta sutartis, kad nustatytų, ar tebesilaikoma šiame reglamente nustatytų taikytinų reikalavimų.

IS.I.OR.240. Darbuotojų reikalavimai

a) Pagal reglamentus (ES) Nr. 1321/2014, (ES) Nr. 965/2012, (ES) Nr. 1178/2011, (ES) 2015/340, Įgyvendinimo reglamentą (ES) 2017/373 arba Įgyvendinimo reglamentą (ES) 2021/664, kaip nurodyta šio reglamento 2 straipsnio 1 dalyje, paskirtos organizacijos atsakingas vadovas turi turėti tarnybinius įgaliojimus užtikrinti, kad visa pagal šį reglamentą reikalaujama veikla galėtų būti finansuojama ir vykdoma. Tas asmuo:

1. užtikrina, kad būtų prieinami visi šio reglamento reikalavimams įvykdyti būtini ištekliai;

2. parengia S.I.OR.200 dalies a punkto 1 papunktyje nurodytą informacijos saugumo politiką ir skatina ją taikyti;

3. įrodo, kad yra iš esmės susipažinęs su šiuo reglamentu.

b) Atsakingas vadovas paskiria asmenį arba asmenų grupę, kurie užtikrintų, kad organizacija laikytųsi šio reglamento reikalavimų, ir nustato jų įgaliojimų apimtį. Tas asmuo ar asmenų grupė tiesiogiai atsiskaito atsakingam vadovui ir turi atitinkamų žinių, kvalifikaciją ir patirties, kad galėtų vykdyti savo pareigas. Procedūrose nustatoma, kas pavaduoja tam tikrą asmenį, jeigu jo ilgą laiką nebūtų.

c) Atsakingas vadovas paskiria asmenį arba asmenų grupę, kuriems pavedama administruoti IS.I.OR.200 dalies a punkto 12 papunktyje nurodytą atitikties stebėsenos funkciją.

d) Jeigu organizacijos informacijos saugumo organizacinės struktūros, politika, procesai ir procedūros bendrai naudojami su kitomis organizacijomis arba pačios organizacijos dalyse, kurios nėra įtrauktos į patvirtinimą ar deklaraciją, atsakingas vadovas gali pavesti savo veiklą bendram atsakingam asmeniui.

Tokiu atveju, siekiant užtikrinti tinkamą informacijos saugumo valdymo integravimą organizacijoje, tarp atsakingo organizacijos vadovo ir bendro atsakingo asmens nustatomos veiksmų koordinavimo priemonės.

e) Atsakingas vadovas arba d punkte nurodytas bendras atsakingas asmuo turi turėti tarnybinius įgaliojimus kurti ir nuolat atnaujinti IS.I.OR.200 daliai įgyvendinti būtinas organizacines struktūras, politiką, procesus ir procedūras.

f) Organizacija įdiegia procesą, kuriuo užtikrinamas pakankamas skaičius darbuotojų, galinčių vykdyti šiame priede nurodytą veiklą.

g) Organizacija įdiegia procesą, kuriuo užtikrinama, kad f punkte nurodyti darbuotojai turėtų reikiamą kompetenciją savo užduotims atlikti.

h) Organizacija įdiegia procesą, kuriuo užtikrinama, kad darbuotojai būtų informuoti apie atsakomybę, susijusią su jiems pavestomis funkcijomis ir užduotimis.

i) Organizacija užtikrina, kad būtų tinkamai nustatyta darbuotojų, turinčių prieigą prie informacinių sistemų ir duomenų, kuriems taikomi šio reglamento reikalavimai, tapatybė ir patikimumas.

IS.I.OR.245. Įrašų saugojimas

a) *Organizacija registruoja savo informacijos saugumo valdymo veiklą.*

1. Organizacija užtikrina, kad būtų archyvuojami ir atsekami šie įrašai:

i) visi gauti patvirtinimai ir visi susiję informacijos saugumo rizikos vertinimai pagal IS.I.OR.200 dalies e punktą;

ii) sutartys dėl veiklos, nurodytos IS.I.OR.200 dalies a punkto 9 papunktyje;

iii) įrašai apie IS.I.OR.200 dalies d punkte nurodytus pagrindinius procesus;

iv) įrašai apie IS.I.OR.205 dalyje nurodytame rizikos vertinime nustatytą riziką ir IS.I.OR.210 dalyje nurodytas susijusias veiksmų su rizika priemones;

v) įrašai apie informacijos saugumo incidentus ir pažeidžiamumą, apie kuriuos pranešta pagal IS.I.OR.215 ir IS.I.OR.230 dalyse nurodytas pranešimo sistemas;

vi) įrašai apie informacijos saugumo įvykius, kuriuos gali reikėti iš naujo įvertinti, kad būtų atskleisti neaptikti informacijos saugumo incidentai ar pažeidžiamumas.

2. 1 punkto i papunktyje nurodyti įrašai saugomi bent 5 metus nuo patvirtinimo galiojimo pabaigos.

3. 1 punkto ii papunktyje nurodyti įrašai saugomi bent 5 metus nuo sutarties pakeitimo arba nutraukimo.

4. 1 punkto iii, iv ir v papunkčiuose nurodyti įrašai saugomi bent 5 metus.

5. 1 punkto vi papunktyje nurodyti įrašai saugomi tol, kol tie informacijos saugumo įvykiai bus pakartotinai įvertinti organizacijos nustatytoje tvarkoje numatytu periodiškumu.

b) *Organizacija saugo įrašus, susijusius su savo darbuotojų, vykdančių informacijos saugumo valdymo veiklą, kvalifikacija ir patirtimi.*

1. Įrašai apie darbuotojų kvalifikaciją ir patirtį saugomi tol, kol asmuo dirba organizacijoje, ir ne trumpiau kaip 3 metus po to, kai asmuo paliko organizaciją.

2. Jei darbuotojai paprašo, jiems suteikiama prieiga prie jų individualių įrašų. Be to, jei prieš palikdami organizaciją jie pateikia prašymą, organizacija jiems pateikia jų individualių įrašų kopiją.

c) Kokiu formatu saugomi įrašai, nurodoma organizacijos tvarkoje.

d) Įrašai saugomi taip, kad būtų užtikrinta jų apsauga pažeidimo, pakeitimų ir vagystės, o informacija, kai reikia, žymima nurodant jos slaptumo žymos laipsnį. Organizacija užtikrina, kad įrašai būtų saugomi naudojant priemones, kuriomis užtikrinamas vientisumas, autentiškumas ir leidžiama prieiga.

IS.I.OR.250. Informacijos saugumo valdymo vadovas (ISVV)

a) Organizacija pateikia kompetentingai institucijai informacijos saugumo valdymo vadovą (ISVV) ir, kai taikoma, visus jame minimus susijusius vadovus ir procedūras; tame ISVV pateikiama:

1. atsakingo vadovo pasirašytas pareiškimas, kuriuo patvirtinama, kad organizacija visą laiką dirbs pagal šio priedo ir ISVV reikalavimus. Jei atsakingas vadovas nėra organizacijos vykdomasis direktorius (CEO), pareiškimą pasirašo vykdomasis direktorius;

2. IS.I.OR.240 dalies b ir c punktuose nurodyto asmens (-ų) vardas (-ai) ir pavardė (-ės), pareigos, atskaitomybė, atsakomybė ir įgaliojimai;

3. jei taikoma, IS.I.OR.240 dalies d punkte nurodyto bendro asmens vardas, pavardė, pareigos, atskaitomybė, atsakomybė ir įgaliojimai;

4. organizacijos informacijos saugumo politika, nurodyta IS.I.OR.200 dalies a punkto 1 papunktyje;

5. bendras turimų darbuotojų skaičiaus, jų kategorijų bei apsirūpinimo darbuotojais planavimo sistemos, reikalaujamos IS.I.OR.240 dalyje, aprašymas;

6. pagrindinių asmenų, atsakingų už IS.I.OR.200 dalies įgyvendinimą, įskaitant asmenį (-is), atsakingą (-us) už atitikties stebėsenos funkciją, nurodytą IS.I.OR.200 dalies a punkto 12 papunktyje, pareigos, atskaitomybė, atsakomybė ir įgaliojimai;

7. organizacijos struktūros schema, kurioje nurodyti susiję 2 ir 6 punktuose nurodytų asmenų atskaitomybės ir atsakomybės ryšiai;

8. vidaus pranešimų teikimo sistemos, nurodytos IS.I.OR.215 dalyje, aprašymas;

9. procedūros, kuriomis nustatoma, kaip organizacija užtikrina atitiktį šiai daliai, visų pirma:

i) IS.I.OR.200 dalies c punkte nurodyti dokumentai;

ii) procedūros, kuriomis nustatoma, kaip organizacija kontroliuoja bet kokią pagal sutartį vykdomą veiklą, nurodytą IS.I.OR.200 dalies a punkto 9 papunktyje;

iii) ISVV keitimo procedūra, nurodyta c punkte;

10. išsami informacija apie esamas patvirtintas alternatyvias atitikties užtikrinimo priemones.

b) Pirminį ISVV išdavimą patvirtina ir ISVV kopiją pasilieka kompetentinga institucija. ISVV, jeigu būtina, turi būti keičiamas siekiant užtikrinti, kad jame visa laiką būtų naujausi duomenys apie organizacijos ISVS. Visų ISVV pakeitimų kopijos pateikiamos kompetentingai institucijai.

c) ISVV pakeitimai tvarkomi organizacijos nustatyta tvarka. Visus pakeitimus, kurie nepatenka į šios procedūros taikymo sritį, ir visus pakeitimus, susijusius su IS.I.OR.255 dalies b punkte nurodytais pakeitimais, tvirtina kompetentinga institucija.

d) Organizacija gali integruoti ISVV su kitais savo turimais valdymo žinynais ar vadovais, jei yra aiški kryžminė nuoroda, kurios valdymo žinyno ar vadovo dalys atitinka įvairius šiame priede nustatytus reikalavimus.

IS.I.OR.255. Informacijos saugumo valdymo sistemos pakeitimai

a) ISVS pakeitimai gali būti administruojami ir apie juos gali būti pranešama kompetentingai institucijai pagal organizacijos parengtą procedūrą. Šią procedūrą tvirtina kompetentinga institucija.

b) Dėl ISVS pakeitimų, kuriems netaikoma a punkte nurodyta procedūra, organizacija kompetentingai institucijai turi pateikti prašymą dėl patvirtinimo ir jį gauti.

Dėl tų pakeitimų:

1. prašymas pateikiamas prieš įgyvendinant tokį pakeitimą, kad kompetentinga institucija galėtų nustatyti, ar tebesilaikoma šio reglamento, ir, jei reikia, iš dalies pakeisti organizacijos pažymėjimą ir atitinkamas prie jo pridėto patvirtinimo sąlygas.

2. organizacija pateikia kompetentingai institucijai visą informaciją, kurios ji prašo pakeitimui įvertinti;

3. pakeitimas įgyvendinamas tik gavus oficialų kompetentingos institucijos patvirtinimą;

4. tokių pakeitimų įgyvendinimo metu organizacija veikia kompetentingos institucijos nustatytomis sąlygomis.

IS.I.OR.260. Tęstinis tobulinimas

a) Organizacija, naudodama tinkamus veiklos rezultatų rodiklius, įvertina ISVS veiksmingumą ir brandumą. Tas vertinimas atliekamas pagal organizacijos iš anksto nustatytą grafiką arba po informacijos saugumo incidento.

b) Jei atlikus vertinimą pagal a punktą nustatoma trūkumų, organizacija imasi būtinų tobulinimo priemonių, siekdama užtikrinti, kad ISVS toliau atitiktų taikomus reikalavimus ir padėtų išlaikyti priimtiną informacijos saugumo rizikos lygį. Be to, organizacija iš naujo įvertina tuos ISVS elementus, kuriems padarė poveikį priimtos priemonės.

III PRIEDAS

Reglamento (ES) Nr. 1178/2011 VI priedas (ARA dalis) ir VII priedas (ORA dalis) iš dalies keičiami taip:

1) VI priedas (ARA dalis) iš dalies keičiamas taip:

a) ARA.GEN.125 dalis papildoma c punktu:

„c) Valstybės narės kompetentinga institucija Agentūrai kuo greičiau pateikia saugos požiūriu svarbią informaciją, gautą iš informacijos saugumo ataskaitų, kurias ji gavo pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.230 dalį.“;

b) po ARA.GEN.135 dalies įterpiama ARA.GEN.135A dalis:

„**ARA.GEN.135A. Neatidėliotinas reagavimas į informacijos saugumo incidentą arba pažeidžiamumą, darančius poveikį aviacijos saugai**

a) Kompetentinga institucija įgyvendina sistemą, pagal kurią būtų tinkamai renkama, analizuojama ir skleidžiama informacija, susijusi su informacijos saugumo incidentais ir pažeidžiamumu, galinčiais turėti poveikį aviacijos saugai, apie kuriuos praneša organizacijos. Tai daroma koordinuojant veiksmus su visomis kitomis atitinkamomis institucijomis, atsakingomis už informacijos saugumą ar kibernetinį saugumą valstybėje narėje, kad būtų pagerintas pranešimų teikimo sistemų koordinavimas ir suderinamumas.

b) Agentūra įgyvendina sistemą, kad tinkamai išanalizuotų visą aktualią saugos požiūriu svarbią informaciją, gautą pagal ARA.GEN.125 dalies c punktą, ir nepagrįstai nedelsdama pateiktų valstybėms narėms ir Komisijai visą informaciją, įskaitant rekomendacijas ar taisomuosius veiksmus, kurių reikia imtis, kad jos galėtų laiku reaguoti į informacijos saugumo incidentą arba pažeidžiamumą, galinčius turėti poveikį aviacijos saugai, susijusį su gaminiais, dalimis, kilnojamąja įranga, asmenimis ar organizacijomis, kuriems taikomas Reglamentas (ES) 2018/1139 ir jo deleguotieji ir įgyvendinimo aktai.

c) Gavusi a ir b punktuose nurodytos informacijos, kompetentinga institucija imasi tinkamų priemonių, kad pašalintų galimą informacijos saugumo incidento ar pažeidžiamumo poveikį aviacijos saugai.

d) Apie priemones, kurių imamasi pagal c punktą, nedelsiant pranešama visiems asmenims arba organizacijoms, kurie jas turi taikyti pagal Reglamentą (ES) 2018/1139 ir jo deleguotuosius bei įgyvendinimo aktus. Valstybės narės kompetentinga institucija apie šias priemones taip pat praneša Agentūrai ir, jei reikia imtis bendrų veiksmų, kitų susijusių valstybių narių kompetentingoms institucijoms.“;

c) ARA.GEN.200 dalis papildoma e punktu:

„e) Be a punkte nustatytų reikalavimų, kompetentingos institucijos sukurta ir prižiūrima valdymo sistema turi atitikti Įgyvendinimo reglamento (ES) 2023/203 I priedą (IS.AR dalį), kad būtų užtikrintas tinkamas informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymas.“;

d) ARA.GEN.205 dalis iš dalies keičiama taip:

i) antraštė pakeičiama taip:

„**ARA.GEN.205. Užduočių paskirstymas**“;

ii) pridedamas c punktas:

„c) Organizacijos sertifikavimo ir ORA.GEN.200A dalies reikalavimų laikymosi priežiūros užduotis kompetentinga institucija gali paskirti kompetentingiems subjektams pagal a punktą arba bet kuriai atitinkamai už informacijos saugumą ar kibernetinį saugumą valstybėje narėje atsakingai institucijai. Skirdama užduotis, kompetentinga institucija užtikrina, kad:

1) kompetentingas subjektas arba atitinkama institucija koordinuotų visus su aviacijos sauga susijusius aspektus ir į juos atsižvelgtų;

2) kompetentingo subjekto arba atitinkamos institucijos vykdomos sertifikavimo ir priežiūros veiklos rezultatai būtų įtraukti į bendras organizacijos sertifikavimo ir priežiūros bylas;

3) pagal ARA.GEN.200 dalies e punktą sukurta jos pačios informacijos saugumo valdymo sistema apimtų visas jos vardu atliekamas sertifikavimo ir nuolatinės priežiūros užduotis.“;

e) ARA.GEN.300 dalis papildoma g punktu:

„g) Vykdydama organizacijos ORA.GEN.200A dalies reikalavimų laikymosi sertifikavimą ir priežiūrą, kompetentinga institucija ne tik laikosi a–f punktų, bet ir peržiūri visus patvirtinimus, suteiktus pagal šio reglamento IS.I.OR.200 dalies e punktą arba Deleguotojo reglamento (ES) 2022/1645 IS.D.OR.200 dalies e punktą, po taikomo priežiūros audito ciklo ir visais atvejais, kai įgyvendinami organizacijos darbo apimties pakeitimai.“;

f) po ARA.GEN.330 dalies įterpiama ARA.GEN.330A dalis:

„**ARA.GEN.330A. Informacijos saugumo valdymo sistemos pakeitimai**

a) Dėl pakeitimų, kuriuos valdo kompetentinga institucija ir apie kuriuos jai pranešama pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies a punkte nustatytą procedūrą, kompetentinga institucija tokių pakeitimų peržiūrą įtraukia į savo nuolatinę priežiūrą pagal ARA.GEN.300 dalyje išdėstytus principus. Jei nustatoma kokia nors neatitiktis, kompetentinga institucija apie tai praneša organizacijai, paprašo atlikti papildomus pakeitimus ir imasi veiksmų pagal ARA.GEN.350 dalį.

b) Dėl kitų pakeitimų, dėl kurių reikia pateikti patvirtinimo paraišką pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies b punktą:

1) gavusi paraišką dėl pakeitimo, kompetentinga institucija, prieš suteikdama patvirtinimą, patikrina, ar organizacija laikosi taikomų reikalavimų;

2) kompetentinga institucija nustato sąlygas, kuriomis organizacija gali veikti įgyvendindama pakeitimą;

3) įsitikinusi, kad organizacija laikosi taikomų reikalavimų, kompetentinga institucija patvirtina pakeitimą.“;

2) VII priedas (ORA dalis) iš dalies keičiamas taip:

po ORA.GEN.200 dalies įterpiama ORA.GEN.200A dalis:

„**ORA.GEN.200A. Informacijos saugumo valdymo sistema**

Be ORA.GEN.200 dalyje nurodytos valdymo sistemos, organizacija pagal Įgyvendinimo reglamentą (ES) 2023/203 parengia, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą, kad užtikrintų tinkamą informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymą.“

IV PRIEDAS

Reglamento (ES) Nr. 748/2012 I priedas (21 dalis) iš dalies keičiamas taip:

(1) turinys iš dalies keičiamas taip:

(a) po 21.B.20 antraštės įterpiama ši antraštė:

„21.B.20A. Neatidėliotinas reagavimas į informacijos saugumo incidentą arba pažeidžiamumą, darančius poveikį aviacijos saugai“;

(b) 21.B.30 dalies antraštė pakeičiama taip:

„21.B.30. Užduočių paskirstymas“;

(c) po 21.B.240 antraštės įterpiama ši antraštė:

„21.B.240A. Informacijos saugumo valdymo sistemos pakeitimai“;

(d) po 21.B.435 antraštės įterpiama ši antraštė:

„21.B.435A. Informacijos saugumo valdymo sistemos pakeitimai“;

(2) 21.B.15 dalis papildoma c punktu:

„c) Valstybės narės kompetentinga institucija Agentūrai kuo greičiau pateikia saugos požiūriu svarbią informaciją, gautą iš informacijos saugumo ataskaitų, kurias ji gavo pagal Deleguotojo reglamento (ES) 2022/1645 priedo (IS.D.OR dalies) IS.D.OR.230 dalį.“;

(3) po 21.B.20 dalies įrašoma 21.B.20A dalis:

„21.B.20A. Neatidėliotinas reagavimas į informacijos saugumo incidentą arba pažeidžiamumą, darančius poveikį aviacijos saugai

a) Kompetentinga institucija įgyvendina sistemą, pagal kurią būtų tinkamai renkama, analizuojama ir skleidžiama informacija, susijusi su informacijos saugumo incidentais ir pažeidžiamumu, galinčiais turėti poveikį aviacijos saugai, apie kuriuos praneša organizacijos. Tai daroma koordinuojant veiksmus su visomis kitomis atitinkamomis institucijomis, atsakingomis už informacijos saugumą ar kibernetinį saugumą valstybėje narėje, kad būtų pagerintas pranešimų teikimo sistemų koordinavimas ir suderinamumas.

b) Agentūra įgyvendina sistemą, kad tinkamai išanalizuotų visą aktualią saugos požiūriu svarbią informaciją, gautą pagal 21.B.15 dalies c punktą, ir nepagrįstai nedelsdama pateiktų valstybėms narėms ir Komisijai visą informaciją, įskaitant rekomendacijas ar taisomuosius veiksmus, kurių reikia imtis, kad jos galėtų laiku reaguoti į informacijos saugumo incidentą arba pažeidžiamumą, galinčius turėti poveikį aviacijos saugai, susijusį su gaminiais, dalimis, kilnojamąja įranga, asmenimis ar organizacijomis, kuriems taikomas Reglamentas (ES) 2018/1139 ir jo deleguotieji ir įgyvendinimo aktai.

c) Gavusi a ir b punktuose nurodytos informacijos, kompetentinga institucija imasi tinkamų priemonių, kad pašalintų galimą informacijos saugumo incidento ar pažeidžiamumo poveikį aviacijos saugai.

d) Apie priemones, kurių imamasi pagal c punktą, nedelsiant pranešama visiems asmenims arba organizacijoms, kurie jas turi taikyti pagal Reglamentą (ES) 2018/1139 ir jo deleguotuosius bei įgyvendinimo aktus. Valstybės narės kompetentinga institucija apie šias priemones taip pat praneša Agentūrai ir, jei reikia imtis bendrų veiksmų, kitų susijusių valstybių narių kompetentingoms institucijoms.“;

(4) 21.B.25 dalis papildoma e punktu:

„e) Be a punkte nustatytų reikalavimų, kompetentingos institucijos sukurta ir prižiūrima valdymo sistema turi atitikti Įgyvendinimo reglamento (ES) 2023/203 I priedą (IS.AR dalį), kad būtų užtikrintas tinkamas informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugai, valdymas.“;

(5) 21.B.30 dalis iš dalies keičiama taip:

a) antraštė pakeičiama taip:

„21.B.30. Užduočių paskirstymas“;

b) pridedamas c punktas:

„c) Organizacijos sertifikavimo ir 21.A.139A ir 21.A.239A dalių reikalavimų laikymosi priežiūros užduotis kompetentinga institucija gali paskirti kompetentingiems subjektams pagal a punktą arba bet kuriai atitinkamai už informacijos saugumą ar kibernetinį saugumą valstybėje narėje atsakingai institucijai. Skirdama užduotis, kompetentinga institucija užtikrina, kad:

1) kompetentingas subjektas arba atitinkama institucija koordinuotų visus su aviacijos sauga susijusius aspektus ir į juos atsižvelgtų;

2) kompetentingo subjekto arba atitinkamos institucijos vykdomos sertifikavimo ir priežiūros veiklos rezultatai būtų įtraukti į bendras organizacijos sertifikavimo ir priežiūros bylas;

3) pagal 21.B.25 dalies e punktą sukurta jos pačios informacijos saugumo valdymo sistema apimtų visas jos vardu atliekamas sertifikavimo ir nuolatinės priežiūros užduotis.“;

(6) 21.B.221 dalis papildoma g punktu:

„g) Vykdydama organizacijos sertifikavimą ir 21.A.139A dalies reikalavimų laikymosi priežiūrą, kompetentinga institucija ne tik laikosi a–f punktų, bet ir peržiūri visus patvirtinimus, suteiktus pagal šio reglamento IS.I.OR.200 dalies e punktą arba Deleguotojo reglamento (ES) 2022/1645 IS.D.OR.200 dalies e punktą, po taikomo priežiūros audito ciklo ir visais atvejais, kai įgyvendinami organizacijos darbo apimties pakeitimai.“;

(7) po 21.B.240 dalies įrašoma 21.B.240A dalis:

„**21.B.240A. Informacijos saugumo valdymo sistemos pakeitimai**

a) Dėl pakeitimų, kuriuos valdo kompetentinga institucija ir apie kuriuos jai pranešama pagal Deleguotojo reglamento (ES) 2022/1645 priedo (IS.D.OR dalies) IS.D.OR.255 dalies a punkte nustatytą procedūrą, kompetentinga institucija tokių pakeitimų peržiūrą įtraukia į savo nuolatinę priežiūrą pagal 21.B.221 dalyje išdėstytus principus. Jei nustatoma kokia nors neatitiktis, kompetentinga institucija apie tai praneša organizacijai, paprašo atlikti papildomus pakeitimus ir imasi veiksmų pagal 21.B.225 dalį.

b) Dėl kitų pakeitimų, dėl kurių reikia pateikti patvirtinimo paraišką pagal Deleguotojo reglamento (ES) 2022/1645 priedo (IS.D.OR dalies) IS.D.OR.255 dalies b punktą:

1) gavusi paraišką dėl pakeitimo, kompetentinga institucija, prieš suteikdama patvirtinimą, patikrina, ar organizacija laikosi taikomų reikalavimų;

2) kompetentinga institucija nustato sąlygas, kuriomis organizacija gali veikti įgyvendindama pakeitimą;

3) įsitikinusi, kad organizacija laikosi taikomų reikalavimų, kompetentinga institucija patvirtina pakeitimą.“;

(8) 21.B.431 dalis papildoma d punktu:

„d) Sertifikuodama organizaciją ir prižiūrėdama, kaip ji laikosi 21.A.239A dalies reikalavimų, kompetentinga institucija laikosi ne tik a–c punktų, bet ir šių principų:

1) kompetentinga institucija peržiūri sąsajas ir susijusią riziką, kurią pagal Deleguotojo reglamento (ES) 2022/1645 priedo (IS.D.OR dalies) IS.D.OR.205 dalies b punktą nustatė kiekviena organizacija, kuriai taikoma jos priežiūra;

2) jei nustatoma tarpusavio sąsajų ir skirtingų organizacijų nustatytos susijusios rizikos neatitikimų, kompetentinga institucija juos peržiūri su paveiktomis organizacijomis ir, jei reikia, praneša atitinkamus pažeidimus, kad būtų užtikrintas taisomųjų veiksmų įgyvendinimas;

3) jei pagal 2 punktą peržiūrėti dokumentai rodo, kad esama didelės rizikos dėl sąsajų su organizacijomis, kurių priežiūrą vykdo kita tos pačios valstybės narės kompetentinga institucija, ši informacija pranešama atitinkamai kompetentingai institucijai.“;

(9) po 21.B.435 dalies įrašoma 21.B.435A dalis:

„**21.B.435A. Informacijos saugumo valdymo sistemos pakeitimai**

a) Dėl pakeitimų, kuriuos valdo kompetentinga institucija ir apie kuriuos jai pranešama pagal Deleguotojo reglamento (ES) 2022/1645 priedo (IS.D.OR dalies) IS.D.OR.255 dalies a punkte nustatytą procedūrą, kompetentinga institucija tokių pakeitimų peržiūrą įtraukia į savo nuolatinę priežiūrą pagal 21.B.431 dalyje išdėstytus principus. Jei nustatoma kokia nors neatitiktis, kompetentinga institucija apie tai praneša organizacijai, paprašo atlikti papildomus pakeitimus ir imasi veiksmų pagal 21.B.433 dalį.

b) Dėl kitų pakeitimų, dėl kurių reikia pateikti patvirtinimo paraišką pagal Deleguotojo reglamento (ES) 2022/1645 priedo (IS.D.OR dalies) IS.D.OR.255 dalies b punktą:

1) gavusi paraišką dėl pakeitimo, kompetentinga institucija, prieš suteikdama patvirtinimą, patikrina, ar organizacija laikosi taikomų reikalavimų;

2) kompetentinga institucija nustato sąlygas, kuriomis organizacija gali veikti įgyvendindama pakeitimą;

3) įsitikinusi, kad organizacija laikosi taikomų reikalavimų, kompetentinga institucija patvirtina pakeitimą.“

V PRIEDAS

Reglamento (ES) Nr. 965/2012 II priedas (ARO dalis) ir III priedas (ORO dalis) iš dalies keičiami taip:

(1) II priedas (ARO dalis) iš dalies keičiamas taip:

a) ARO.GEN.125 dalis papildoma c punktu:

„c) Valstybės narės kompetentinga institucija Agentūrai kuo greičiau pateikia saugos požiūriu svarbią informaciją, gautą iš informacijos saugumo ataskaitų, kurias ji gavo pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.230 dalį.“;

b) po ARO.GEN.135 dalies įterpiama ARO.GEN.135A dalis:

„**ARO.GEN.135A. Neatidėliotinas reagavimas į informacijos saugumo incidentą arba pažeidžiamumą, darančius poveikį aviacijos saugai**

a) Kompetentinga institucija įgyvendina sistemą, pagal kurią būtų tinkamai renkama, analizuojama ir skleidžiama informacija, susijusi su informacijos saugumo incidentais ir pažeidžiamumu, galinčiais turėti poveikį aviacijos saugai, apie kuriuos praneša organizacijos. Tai daroma koordinuojant veiksmus su visomis kitomis atitinkamomis institucijomis, atsakingomis už informacijos saugumą ar kibernetinį saugumą valstybėje narėje, kad būtų pagerintas pranešimų teikimo sistemų koordinavimas ir suderinamumas.

b) Agentūra įgyvendina sistemą, kad tinkamai išanalizuotų visą aktualią saugos požiūriu svarbią informaciją, gautą pagal ARO.GEN.125 dalies c punktą, ir nepagrįstai nedelsdama pateiktų valstybėms narėms ir Komisijai visą informaciją, įskaitant rekomendacijas ar taisomuosius veiksmus, kurių reikia imtis, kad jos galėtų laiku reaguoti į informacijos saugumo incidentą arba pažeidžiamumą, galinčius turėti poveikį aviacijos saugai, susijusį su gaminiais, dalimis, kilnojamąja įranga, asmenimis ar organizacijomis, kuriems taikomas Reglamentas (ES) 2018/1139 ir jo deleguotieji ir įgyvendinimo aktai.

c) Gavusi a ir b punktuose nurodytos informacijos, kompetentinga institucija imasi tinkamų priemonių, kad pašalintų galimą informacijos saugumo incidento ar pažeidžiamumo poveikį aviacijos saugai.

d) Apie priemones, kurių imamasi pagal c punktą, nedelsiant pranešama visiems asmenims arba organizacijoms, kurie jas turi taikyti pagal Reglamentą (ES) 2018/1139 ir jo deleguotuosius bei įgyvendinimo aktus. Valstybės narės kompetentinga institucija apie šias priemones taip pat praneša Agentūrai ir, jei reikia imtis bendrų veiksmų, kitų susijusių valstybių narių kompetentingoms institucijoms.“;

c) ARO.GEN.200 dalis papildoma e punktu:

„e) Be a punkte nustatytų reikalavimų, kompetentingos institucijos sukurta ir prižiūrima valdymo sistema turi atitikti Įgyvendinimo reglamento (ES) 2023/203 I priedą (IS.AR dalį), kad būtų užtikrintas tinkamas informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymas.“;

d) ARO.GEN.205 dalis iš dalies keičiama taip:

i) antraštė pakeičiama taip:

„**ARO.GEN.205. Užduočių paskirstymas**“;

ii) pridedamas c punktas:

„c) Organizacijos sertifikavimo ir ORO.GEN.200A dalies reikalavimų laikymosi priežiūros užduotis kompetentinga institucija gali paskirti kompetentingiems subjektams pagal a punktą arba bet kuriai atitinkamai už informacijos saugumą ar kibernetinį saugumą valstybėje narėje atsakingai institucijai. Skirdama užduotis, kompetentinga institucija užtikrina, kad:

1) kompetentingas subjektas arba atitinkama institucija koordinuotų visus su aviacijos sauga susijusius aspektus ir į juos atsižvelgtų;

2) kompetentingo subjekto arba atitinkamos institucijos vykdomos sertifikavimo ir priežiūros veiklos rezultatai būtų įtraukti į bendras organizacijos sertifikavimo ir priežiūros bylas;

3) pagal ARO.GEN.200 dalies e punktą sukurta jos pačios informacijos saugumo valdymo sistema apimtų visas jos vardu atliekamas sertifikavimo ir nuolatinės priežiūros užduotis.“;

e) ARO.GEN.300 dalis papildoma g punktu:

„g) Vykdydama organizacijos ORO.GEN.200A dalies reikalavimų laikymosi sertifikavimą ir priežiūrą, kompetentinga institucija ne tik laikosi a–f punktų, bet ir peržiūri visus patvirtinimus, suteiktus pagal šio reglamento IS.I.OR.200 dalies e punktą arba Deleguotojo reglamento (ES) 2022/1645 IS.D.OR.200 dalies e punktą, po taikomo priežiūros audito ciklo ir visais atvejais, kai įgyvendinami organizacijos darbo apimties pakeitimai.“;

f) po ARO.GEN.330 dalies įterpiama ARO.GEN.330A dalis:

„**ARO.GEN.330A. Informacijos saugumo valdymo sistemos pakeitimai**

a) Dėl pakeitimų, kuriuos valdo kompetentinga institucija ir apie kuriuos jai pranešama pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies a punkte nustatytą procedūrą, kompetentinga institucija tokių pakeitimų peržiūrą įtraukia į savo nuolatinę priežiūrą pagal ARO.GEN.300 dalyje išdėstytus principus. Jei nustatoma kokia nors neatitiktis, kompetentinga institucija apie tai praneša organizacijai, paprašo atlikti papildomus pakeitimus ir imasi veiksmų pagal ARO.GEN.350 dalį.

b) Dėl kitų pakeitimų, dėl kurių reikia pateikti patvirtinimo paraišką pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies b punktą:

1) gavusi paraišką dėl pakeitimo, kompetentinga institucija, prieš suteikdama patvirtinimą, patikrina, ar organizacija laikosi taikomų reikalavimų;

2) kompetentinga institucija nustato sąlygas, kuriomis organizacija gali veikti įgyvendindama pakeitimą;

3) įsitikinusi, kad organizacija laikosi taikomų reikalavimų, kompetentinga institucija patvirtina pakeitimą.“;

(2) III priedas (ORO dalis) iš dalies keičiamas taip:

po ORO.GEN.200 dalies įterpiama ORO.GEN.200A dalis:

„**ORO.GEN.200A. Informacijos saugumo valdymo sistema**

Be ORO.GEN.200 dalyje nurodytos valdymo sistemos, veiklos vykdytojas pagal Įgyvendinimo reglamentą (ES) 2023/203 parengia, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą, kad užtikrintų tinkamą informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymą.“

VI PRIEDAS

Reglamento (ES) Nr. 139/2014 II priedas (ADR.AR dalis) iš dalies keičiamas taip:

(1) ADR.AR.A.025 dalis papildoma c punktu:

„c) Valstybės narės kompetentinga institucija Agentūrai kuo greičiau pateikia saugos požiūriu svarbią informaciją, gautą iš informacijos saugumo ataskaitų, kurias ji gavo pagal Deleguotojo reglamento (ES) 2022/1645 priedo (IS.D.OR dalies) IS.D.OR.230 dalį.“;

(2) po ADR.AR.A.030 dalies įterpiama ADR.AR.A.030A dalis:

„**ADR.AR.A.030A. Neatidėliotinas reagavimas į informacijos saugumo incidentą arba pažeidžiamumą, darančius poveikį aviacijos saugai**

a) Kompetentinga institucija įgyvendina sistemą, pagal kurią būtų tinkamai renkama, analizuojama ir skleidžiama informacija, susijusi su informacijos saugumo incidentais ir pažeidžiamumu, galinčiais turėti poveikį aviacijos saugai, apie kuriuos praneša organizacijos. Tai daroma koordinuojant veiksmus su visomis kitomis atitinkamomis institucijomis, atsakingomis už informacijos saugumą ar kibernetinį saugumą valstybėje narėje, kad būtų pagerintas pranešimų teikimo sistemų koordinavimas ir suderinamumas.

b) Agentūra įgyvendina sistemą, kad tinkamai išanalizuotų visą aktualią saugos požiūriu svarbią informaciją, gautą pagal ADR.AR.A.025 dalies c punktą, ir nepagrįstai nedelsdama pateiktų valstybėms narėms ir Komisijai visą informaciją, įskaitant rekomendacijas ar taisomuosius veiksmus, kurių reikia imtis, kad jos galėtų laiku reaguoti į informacijos saugumo incidentą arba pažeidžiamumą, galinčius turėti poveikį aviacijos saugai, susijusį su gaminiais, dalimis, kilnojamąja įranga, asmenimis ar organizacijomis, kuriems taikomas Reglamentas (ES) 2018/1139 ir jo deleguotieji ir įgyvendinimo aktai.

c) Gavusi a ir b punktuose nurodytos informacijos, kompetentinga institucija imasi tinkamų priemonių, kad pašalintų galimą informacijos saugumo incidento ar pažeidžiamumo poveikį aviacijos saugai.

d) Apie priemones, kurių imamasi pagal c punktą, nedelsiant pranešama visiems asmenims arba organizacijoms, kurie jas turi taikyti pagal Reglamentą (ES) 2018/1139 ir jo deleguotuosius bei įgyvendinimo aktus. Valstybės narės kompetentinga institucija apie šias priemones taip pat praneša Agentūrai ir, jei reikia imtis bendrų veiksmų, kitų susijusių valstybių narių kompetentingoms institucijoms.“;

(3) ADR.AR.B.005 dalis papildoma d punktu:

„d) Be a punkte nustatytų reikalavimų, kompetentingos institucijos sukurta ir prižiūrima valdymo sistema turi atitikti Įgyvendinimo reglamento (ES) 2023/203 I priedą (IS.AR dalį), kad būtų užtikrintas tinkamas informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymas.“;

(4) ADR.AR.B.010 dalis iš dalies keičiama taip:

i) antraštė pakeičiama taip:

„**ADR.AR.B.010. Užduočių paskirstymas**“;

ii) pridedamas c punktas:

„c) Organizacijos sertifikavimo ir ADR.OR.D.005A dalies reikalavimų laikymosi priežiūros užduotis kompetentinga institucija gali paskirti kompetentingiems subjektams pagal a punktą arba bet kuriai atitinkamai už informacijos saugumą ar kibernetinį saugumą valstybėje narėje atsakingai institucijai. Skirdama užduotis, kompetentinga institucija užtikrina, kad:

1. kompetentingas subjektas arba atitinkama institucija koordinuotų visus su aviacijos sauga susijusius aspektus ir į juos atsižvelgtų;

2. kompetentingo subjekto arba atitinkamos institucijos vykdomos sertifikavimo ir priežiūros veiklos rezultatai būtų įtraukti į bendras organizacijos sertifikavimo ir priežiūros bylas;

3. pagal ADR.AR.B.005 dalies e punktą sukurta jos pačios informacijos saugumo valdymo sistema apimtų visas jos vardu atliekamas sertifikavimo ir nuolatinės priežiūros užduotis.“;

(5) ADR.AR.C.005 dalis papildoma f punktu:

„f) Vykdydama organizacijos ADR.OR.D.005A dalies reikalavimų laikymosi sertifikavimą ir priežiūrą, kompetentinga institucija ne tik laikosi a–e punktų, bet ir peržiūri visus patvirtinimus, suteiktus pagal šio reglamento IS.I.OR.200 dalies e punktą arba Deleguotojo reglamento (ES) 2022/1645 IS.D.OR.200 dalies e punktą, po taikomo priežiūros audito ciklo ir visais atvejais, kai įgyvendinami organizacijos darbo apimties pakeitimai.“;

(6) po ADR.AR.C.040 dalies įterpiama ADR.AR.C.040A dalis:

„**ADR.AR.C.040A. Informacijos saugumo valdymo sistemos pakeitimai**

a) Dėl pakeitimų, kurie administruojami ir apie kuriuos kompetentingai institucijai pranešama pagal Deleguotojo reglamento (ES) 2022/1645 priedo (IS.D.OR dalies) IS.D.OR.255 dalies a punkte nustatytą procedūrą, kompetentinga institucija tokių pakeitimų peržiūrą įtraukia į savo nuolatinę priežiūrą pagal ADR.AR.C.005 dalyje išdėstytus principus. Jei nustatoma kokia nors neatitiktis, kompetentinga institucija apie tai praneša organizacijai, paprašo atlikti papildomus pakeitimus ir imasi veiksmų pagal ADR.AR.C.055 dalį.

b) Dėl kitų pakeitimų, dėl kurių reikia pateikti patvirtinimo paraišką pagal Deleguotojo reglamento (ES) 2022/1645 priedo (IS.D.OR dalies) IS.D.OR.255 dalies b punktą:

1) gavusi paraišką dėl pakeitimo, kompetentinga institucija, prieš suteikdama patvirtinimą, patikrina, ar organizacija laikosi taikomų reikalavimų;

2) kompetentinga institucija nustato sąlygas, kuriomis organizacija gali veikti įgyvendindama pakeitimą;

3) įsitikinusi, kad organizacija laikosi taikomų reikalavimų, kompetentinga institucija patvirtina pakeitimą.“

VII PRIEDAS

Reglamento (ES) Nr. 1321/2014 II priedas (145 dalis), III priedas (66 dalis) ir Vc priedas (CAMO dalis) iš dalies keičiami taip:

(1) II priedas (145 dalis) iš dalies keičiamas taip:

a) turinys iš dalies keičiamas taip:

i) po 145.A.200 antraštės įterpiama ši antraštė:

„145.A.200A. Informacijos saugumo valdymo sistema“;

ii) po 145.B.135 antraštės įterpiama ši antraštė:

„145.B.135A. Neatidėliotinas reagavimas į informacijos saugumo incidentą arba pažeidžiamumą, darančius poveikį aviacijos saugai“;

iii) 145.B.205 dalies antraštė pakeičiama taip:

„145.B.205. Užduočių paskirstymas“;

iv) po 145.B.330 antraštės įterpiama ši antraštė:

„145.B.330A. Informacijos saugumo valdymo sistemos pakeitimai“;

b) po 145.A.200 dalies įrašoma 145.A.200A dalis:

„145.A.200A. **Informacijos saugumo valdymo sistema**

Be 145.A.200 dalyje nurodytos valdymo sistemos, techninės priežiūros organizacija pagal Įgyvendinimo reglamentą (ES) 2023/203 parengia, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą, kad užtikrintų tinkamą informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugai, valdymą.“;

c) 145.B.125 dalis papildoma c punktu:

„c) Valstybės narės kompetentinga institucija Agentūrai kuo greičiau pateikia saugos požiūriu svarbią informaciją, gautą iš informacijos saugumo ataskaitų, kurias ji gavo pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.230 dalį.“;

d) po 145.B.135 dalies įrašoma 145.B.135A dalis:

„145.B.135A. **Neatidėliotinas reagavimas į informacijos saugumo incidentą arba pažeidžiamumą, darančius poveikį aviacijos saugai**

a) Kompetentinga institucija įgyvendina sistemą, pagal kurią būtų tinkamai renkama, analizuojama ir skleidžiama informacija, susijusi su informacijos saugumo incidentais ir pažeidžiamumu, galinčiais turėti poveikį aviacijos saugai, apie kuriuos praneša organizacijos. Tai daroma koordinuojant veiksmus su visomis kitomis atitinkamomis institucijomis, atsakingomis už informacijos saugumą ar kibernetinį saugumą valstybėje narėje, kad būtų pagerintas pranešimų teikimo sistemų koordinavimas ir suderinamumas.

b) Agentūra įgyvendina sistemą, kad tinkamai išanalizuotų visą aktualią saugos požiūriu svarbią informaciją, gautą pagal 145.B.125 dalies c punktą, ir nepagrįstai nedelsdama pateiktų valstybėms narėms ir Komisijai visą informaciją, įskaitant rekomendacijas ar taisomuosius veiksmus, kurių reikia imtis, kad jos galėtų laiku reaguoti į informacijos saugumo incidentą arba pažeidžiamumą, galinčius turėti poveikį aviacijos saugai, susijusį su gaminiais, dalimis, kilnojamąja įranga, asmenimis ar organizacijomis, kuriems taikomas Reglamentas (ES) 2018/1139 ir jo deleguotieji ir įgyvendinimo aktai.

c) Gavusi a ir b punktuose nurodytos informacijos, kompetentinga institucija imasi tinkamų priemonių, kad pašalintų galimą informacijos saugumo incidento ar pažeidžiamumo poveikį aviacijos saugai.

d) Apie priemones, kurių imamasi pagal c punktą, nedelsiant pranešama visiems asmenims arba organizacijoms, kurie jas turi taikyti pagal Reglamentą (ES) 2018/1139 ir jo deleguotuosius bei įgyvendinimo aktus. Valstybės narės kompetentinga institucija apie šias priemones taip pat praneša Agentūrai ir, jei reikia imtis bendrų veiksmų, kitų susijusių valstybių narių kompetentingoms institucijoms.“;

e) 145.B.200 dalis papildoma e punktu:

„e) Be a punkte nustatytų reikalavimų, kompetentingos institucijos sukurta ir prižiūrima valdymo sistema turi atitikti Įgyvendinimo reglamento (ES) 2023/203 I priedą (IS.AR dalį), kad būtų užtikrintas tinkamas informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugai, valdymas.“;

(f) 145.B.205 dalis iš dalies keičiama taip:

i) antraštė pakeičiama taip:

„145.B.205. **Užduočių paskirstymas**“;

ii) pridedamas c punktas:

„c) Organizacijos sertifikavimo ir 145.A.200A dalies reikalavimų laikymosi priežiūros užduotis kompetentinga institucija gali paskirti kompetentingiems subjektams pagal a punktą arba bet kuriai atitinkamai už informacijos saugumą ar kibernetinį saugumą valstybėje narėje atsakingai institucijai. Skirdama užduotis, kompetentinga institucija užtikrina, kad:

1) kompetentingas subjektas arba atitinkama institucija koordinuotų visus su aviacijos sauga susijusius aspektus ir į juos atsižvelgtų;

2) kompetentingo subjekto arba atitinkamos institucijos vykdomos sertifikavimo ir priežiūros veiklos rezultatai būtų įtraukti į bendras organizacijos sertifikavimo ir priežiūros bylas;

3) pagal 145.B.200 dalies e punktą sukurta jos pačios informacijos saugumo valdymo sistema apimtų visas jos vardu atliekamas sertifikavimo ir nuolatinės priežiūros užduotis.“;

g) 145.B.300 dalis papildoma g punktu:

„g) Vykdydama organizacijos sertifikavimą ir 145.A.200A dalies reikalavimų laikymosi priežiūrą, kompetentinga institucija ne tik laikosi a–f punktų, bet ir peržiūri visus patvirtinimus, suteiktus pagal šio reglamento IS.I.OR.200 dalies e punktą arba Deleguotojo reglamento (ES) 2022/1645 IS.D.OR.200 dalies e punktą, po taikomo priežiūros audito ciklo ir visais atvejais, kai įgyvendinami organizacijos darbo apimties pakeitimai.“;

h) po 145.B.330 dalies įrašoma 145.B.330A dalis:

„145.B.330A. **Informacijos saugumo valdymo sistemos pakeitimai**

a) Dėl pakeitimų, kuriuos valdo kompetentinga institucija ir apie kuriuos jai pranešama pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies a punkte nustatytą procedūrą, kompetentinga institucija tokių pakeitimų peržiūrą įtraukia į savo nuolatinę priežiūrą pagal 145.B.300 dalyje išdėstytus principus. Jei nustatoma kokia nors neatitiktis, kompetentinga institucija apie tai praneša organizacijai, paprašo atlikti papildomus pakeitimus ir imasi veiksmų pagal 145.B.350 dalį.

b) Dėl kitų pakeitimų, dėl kurių reikia pateikti patvirtinimo paraišką pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies b punktą:

1) gavusi paraišką dėl pakeitimo, kompetentinga institucija, prieš suteikdama patvirtinimą, patikrina, ar organizacija laikosi taikomų reikalavimų;

2) kompetentinga institucija nustato sąlygas, kuriomis organizacija gali veikti įgyvendindama pakeitimą;

3) įsitikinusi, kad organizacija laikosi taikomų reikalavimų, kompetentinga institucija patvirtina pakeitimą.“

(2) III priedas (66 dalis) iš dalies keičiamas taip:

a) turinyje po 66.B.10 antraštės įterpiama ši antraštė:

„66.B.15. Informacijos saugumo valdymo sistema“;

b) po 66.B.10 dalies įterpiama 66.B.15 dalis:

„66.B.15. **Informacijos saugumo valdymo sistema**

Kompetentinga institucija sukuria, įdiegia ir prižiūri informacijos saugumo valdymo sistemą pagal Įgyvendinimo reglamento (ES) 2023/203 I priedą (IS.AR dalį), kad užtikrintų tinkamą informacijos saugumo rizikos, kuri gali turėti įtakos aviacijos saugai, valdymą.“;

(3) Vc priedas (CAMO dalis) iš dalies keičiamas taip:

a) turinys iš dalies keičiamas taip:

i) po CAMO.A.200 antraštės įterpiama ši antraštė:

„CAMO.A.200A Informacijos saugumo valdymo sistema“;

ii) po CAMO.B.135 antraštės įterpiama ši antraštė:

„CAMO.B.135A. Neatidėliotinas reagavimas į informacijos saugumo incidentą arba pažeidžiamumą, darančius poveikį aviacijos saugai“;

iii) CAMO.B.205 dalies antraštė pakeičiama taip:

„CAMO.B.205. Užduočių paskirstymas“;

iv) po CAMO.B.330 antraštės įterpiama ši antraštė:

„CAMO.B.330A. Informacijos saugumo valdymo sistemos pakeitimai“;

b) po CAMO.A.200 dalies įterpiama CAMO.A.200A dalis:

„CAMO.A.200A. **Informacijos saugumo valdymo sistema**

Be CAMO.A.200 dalyje nurodytos valdymo sistemos, organizacija pagal Įgyvendinimo reglamentą (ES) 2023/203 parengia, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą, kad užtikrintų tinkamą informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymą.“;

c) CAMO.B.125 dalis papildoma c punktu:

„c) Valstybės narės kompetentinga institucija Agentūrai kuo greičiau pateikia saugos požiūriu svarbią informaciją, gautą iš informacijos saugumo ataskaitų, kurias ji gavo pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.230 dalį.“;

d) po CAMO.B.135 dalies įterpiama CAMO.B.135A dalis:

„CAMO.B.135A. **Neatidėliotinas reagavimas į informacijos saugumo incidentą arba pažeidžiamumą, darančius poveikį aviacijos saugai**

a) Kompetentinga institucija įgyvendina sistemą, pagal kurią būtų tinkamai renkama, analizuojama ir skleidžiama informacija, susijusi su informacijos saugumo incidentais ir pažeidžiamumu, galinčiais turėti poveikį aviacijos saugai, apie kuriuos praneša organizacijos. Tai daroma koordinuojant veiksmus su visomis kitomis atitinkamomis institucijomis, atsakingomis už informacijos saugumą ar kibernetinį saugumą valstybėje narėje, kad būtų pagerintas pranešimų teikimo sistemų koordinavimas ir suderinamumas.

b) Agentūra įgyvendina sistemą, kad tinkamai išanalizuotų visą aktualią saugos požiūriu svarbią informaciją, gautą pagal CAMO.B.125 dalies c punktą, ir nepagrįstai nedelsdama pateiktų valstybėms narėms ir Komisijai visą informaciją, įskaitant rekomendacijas ar taisomuosius veiksmus, kurių reikia imtis, kad jos galėtų laiku reaguoti į informacijos saugumo incidentą arba pažeidžiamumą, galinčius turėti poveikį aviacijos saugai, susijusį su gaminiais, dalimis, kilnojamąja įranga, asmenimis ar organizacijomis, kuriems taikomas Reglamentas (ES) 2018/1139 ir jo deleguotieji ir įgyvendinimo aktai.

c) Gavusi a ir b punktuose nurodytos informacijos, kompetentinga institucija imasi tinkamų priemonių, kad pašalintų galimą informacijos saugumo incidento ar pažeidžiamumo poveikį aviacijos saugai.

d) Apie priemones, kurių imamasi pagal c punktą, nedelsiant pranešama visiems asmenims arba organizacijoms, kurie jas turi taikyti pagal Reglamentą (ES) 2018/1139 ir jo deleguotuosius bei įgyvendinimo aktus. Valstybės narės kompetentinga institucija apie šias priemones taip pat praneša Agentūrai ir, jei reikia imtis bendrų veiksmų, kitų susijusių valstybių narių kompetentingoms institucijoms.“;

e) CAMO.B.200 dalis papildoma e punktu:

„e) Be a punkte nustatytų reikalavimų, kompetentingos institucijos sukurta ir prižiūrima valdymo sistema turi atitikti Įgyvendinimo reglamento (ES) 2023/203 I priedą (IS.AR dalį), kad būtų užtikrintas tinkamas informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymas.“;

f) CAMO.B.205 dalis iš dalies keičiama taip:

i) antraštė pakeičiama taip:

„CAMO.B.205. **Užduočių paskirstymas**“;

ii) pridedamas c punktas:

„c) Organizacijos sertifikavimo ir CAMO.A.200A dalies reikalavimų laikymosi priežiūros užduotis kompetentinga institucija gali paskirti kompetentingiems subjektams pagal a punktą arba bet kuriai atitinkamai už informacijos saugumą ar kibernetinį saugumą valstybėje narėje atsakingai institucijai. Skirdama užduotis, kompetentinga institucija užtikrina, kad:

1) kompetentingas subjektas arba atitinkama institucija koordinuotų visus su aviacijos sauga susijusius aspektus ir į juos atsižvelgtų;

2) kompetentingo subjekto arba atitinkamos institucijos vykdomos sertifikavimo ir priežiūros veiklos rezultatai būtų įtraukti į bendras organizacijos sertifikavimo ir priežiūros bylas;

3) pagal CAMO.B.200 dalies e punktą sukurta jos pačios informacijos saugumo valdymo sistema apimtų visas jos vardu atliekamas sertifikavimo ir nuolatinės priežiūros užduotis.“;

g) CAMO.B.300 dalis papildoma g punktu:

„g) Vykdydama organizacijos CAMO.A.200A dalies reikalavimų laikymosi sertifikavimą ir priežiūrą, kompetentinga institucija ne tik laikosi a–f punktų, bet ir peržiūri visus patvirtinimus, suteiktus pagal šio reglamento IS.I.OR.200 dalies e punktą arba Deleguotojo reglamento (ES) 2022/1645 IS.D.OR.200 dalies e punktą, po taikomo priežiūros audito ciklo ir visais atvejais, kai įgyvendinami organizacijos darbo apimties pakeitimai.“;

h) po CAMO.B.330 dalies įterpiama CAMO.B.330A dalis:

„CAMO.B.330A. **Informacijos saugumo valdymo sistemos pakeitimai**

a) Dėl pakeitimų, kuriuos valdo kompetentinga institucija ir apie kuriuos jai pranešama pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies a punkte nustatytą procedūrą, kompetentinga institucija tokių pakeitimų peržiūrą įtraukia į savo nuolatinę priežiūrą pagal CAMO.B.300 dalyje išdėstytus principus. Jei nustatoma kokia nors neatitiktis, kompetentinga institucija apie tai praneša organizacijai, paprašo atlikti papildomus pakeitimus ir imasi veiksmų pagal CAMO.B.350 dalį.

b) Dėl kitų pakeitimų, dėl kurių reikia pateikti patvirtinimo paraišką pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies b punktą:

1) gavusi paraišką dėl pakeitimo, kompetentinga institucija, prieš suteikdama patvirtinimą, patikrina, ar organizacija laikosi taikomų reikalavimų;

2) kompetentinga institucija nustato sąlygas, kuriomis organizacija gali veikti įgyvendindama pakeitimą;

3) įsitikinusi, kad organizacija laikosi taikomų reikalavimų, kompetentinga institucija patvirtina pakeitimą.“

VIII PRIEDAS

Reglamento (ES) 2015/340 II priedas (ATCO.AR dalis) ir III priedas (ATCO.OR dalis) iš dalies keičiami taip:

(1) II priedas (ATCO.AR dalis) iš dalies keičiamas taip:

a) ATCO.AR.A.020 dalis papildoma c punktu:

„c) Valstybės narės kompetentinga institucija Agentūrai kuo greičiau pateikia saugos požiūriu svarbią informaciją, gautą iš informacijos saugumo ataskaitų, kurias ji gavo pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.230 dalį.“;

b) po ATCO.AR.A.025 dalies įterpiama ATCO.AR.A.025A dalis:

„**ATCO.AR.A.025A. Neatidėliotinas reagavimas į informacijos saugumo incidentą arba pažeidžiamumą, darančius poveikį aviacijos saugai**

a) Kompetentinga institucija įgyvendina sistemą, pagal kurią būtų tinkamai renkama, analizuojama ir skleidžiama informacija, susijusi su informacijos saugumo incidentais ir pažeidžiamumu, galinčiais turėti poveikį aviacijos saugai, apie kuriuos praneša organizacijos. Tai daroma koordinuojant veiksmus su visomis kitomis atitinkamomis institucijomis, atsakingomis už informacijos saugumą ar kibernetinį saugumą valstybėje narėje, kad būtų pagerintas pranešimų teikimo sistemų koordinavimas ir suderinamumas.

b) Agentūra įgyvendina sistemą, kad tinkamai išanalizuotų visą aktualią saugos požiūriu svarbią informaciją, gautą pagal ATCO.AR.A.020 dalį, ir nepagrįstai nedelsdama pateiktų valstybėms narėms ir Komisijai visą informaciją, įskaitant rekomendacijas ar taisomuosius veiksmus, kurių reikia imtis, kad jos galėtų laiku reaguoti į informacijos saugumo incidentą arba pažeidžiamumą, galinčius turėti poveikį aviacijos saugai, susijusį su gaminiais, dalimis, kilnojamąja įranga, asmenimis ar organizacijomis, kuriems taikomas Reglamentas (ES) 2018/1139 ir jo deleguotieji ir įgyvendinimo aktai.

c) Gavusi a ir b punktuose nurodytos informacijos, kompetentinga institucija imasi tinkamų priemonių, kad pašalintų galimą informacijos saugumo incidento ar pažeidžiamumo poveikį aviacijos saugai.

d) Apie priemones, kurių imamasi pagal c punktą, nedelsiant pranešama visiems asmenims arba organizacijoms, kurie jas turi taikyti pagal Reglamentą (ES) 2018/1139 ir jo deleguotuosius bei įgyvendinimo aktus. Valstybės narės kompetentinga institucija apie šias priemones taip pat praneša Agentūrai ir, jei reikia imtis bendrų veiksmų, kitų susijusių valstybių narių kompetentingoms institucijoms.“;

c) ATCO.AR.B.001 dalis papildoma e punktu:

„e) Be a punkte nustatytų reikalavimų, kompetentingos institucijos sukurta ir prižiūrima valdymo sistema turi atitikti Įgyvendinimo reglamento (ES) 2023/203 I priedą (IS.AR dalį), kad būtų užtikrintas tinkamas informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymas.“;

d) ATCO.AR.B.005 dalis iš dalies keičiama taip:

i) antraštė pakeičiama taip:

„**ATCO.AR.B.005. Užduočių paskirstymas**“;

ii) pridedamas c punktas:

„c) Organizacijos sertifikavimo ir ATCO.OR.C.001A dalies reikalavimų laikymosi priežiūros užduotis kompetentinga institucija gali paskirti kompetentingiems subjektams pagal a punktą arba bet kuriai atitinkamai už informacijos saugumą ar kibernetinį saugumą valstybėje narėje atsakingai institucijai. Skirdama užduotis, kompetentinga institucija užtikrina, kad:

1) kompetentingas subjektas arba atitinkama institucija koordinuotų visus su aviacijos sauga susijusius aspektus ir į juos atsižvelgtų;

2) kompetentingo subjekto arba atitinkamos institucijos vykdomos sertifikavimo ir priežiūros veiklos rezultatai būtų įtraukti į bendras organizacijos sertifikavimo ir priežiūros bylas;

3) pagal ATCO.AR.B.001 dalies e punktą sukurta jos pačios informacijos saugumo valdymo sistema apimtų visas jos vardu atliekamas sertifikavimo ir nuolatinės priežiūros užduotis.“;

e) ATCO.AR.C.001 dalis papildoma f punktu:

„f) Vykdydama organizacijos ATCO.OR.C.001A dalies reikalavimų laikymosi sertifikavimą ir priežiūrą, kompetentinga institucija ne tik laikosi a–e punktų, bet ir peržiūri visus patvirtinimus, suteiktus pagal šio reglamento IS.I.OR.200 dalies e punktą arba Deleguotojo reglamento (ES) 2022/1645 IS.D.OR.200 dalies e punktą, po taikomo priežiūros audito ciklo ir visais atvejais, kai įgyvendinami organizacijos darbo apimties pakeitimai.“;

f) po ATCO.AR.E.010 dalies įterpiama ATCO.AR.E.010A dalis:

„**ATCO.AR.E.010A. Informacijos saugumo valdymo sistemos pakeitimai**

a) Dėl pakeitimų, kuriuos valdo kompetentinga institucija ir apie kuriuos jai pranešama pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies a punkte nustatytą procedūrą, kompetentinga institucija tokių pakeitimų peržiūrą įtraukia į savo nuolatinę priežiūrą pagal ATCO.AR.C.001 dalyje išdėstytus principus. Jei nustatoma kokia nors neatitiktis, kompetentinga institucija apie tai praneša organizacijai, paprašo atlikti papildomus pakeitimus ir imasi veiksmų pagal ATCO.AR.C.010 dalį.

b) Dėl kitų pakeitimų, dėl kurių reikia pateikti patvirtinimo paraišką pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies b punktą:

1) gavusi paraišką dėl pakeitimo, kompetentinga institucija, prieš suteikdama patvirtinimą, patikrina, ar organizacija laikosi taikomų reikalavimų;

2) kompetentinga institucija nustato sąlygas, kuriomis organizacija gali veikti įgyvendindama pakeitimą;

3) įsitikinusi, kad organizacija laikosi taikomų reikalavimų, kompetentinga institucija patvirtina pakeitimą.“;

(2) III priedas (ATCO.OR dalis) iš dalies keičiamas taip:

po ATCO.OR.C.001 dalies įterpiama ATCO.OR.C.001A dalis:

„**ATCO.OR.C.001A. Informacijos saugumo valdymo sistema**

Be ATCO.OR.C.001 dalyje nurodytos valdymo sistemos, mokymo organizacija pagal Įgyvendinimo reglamentą (ES) 2023/203 parengia, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą, kad užtikrintų tinkamą informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymą.“

IX PRIEDAS

Įgyvendinimo reglamento (ES) 2017/373 II priedas (ATM/ANS.AR dalis) ir III priedas (ATM/ANS.OR dalis) iš dalies keičiami taip:

(1) II priedas (ATM/ANS.AR dalis) iš dalies keičiamas taip:

a) ATM/ANS.AR.A.020 dalis papildoma c punktu:

„c) Valstybės narės kompetentinga institucija Agentūrai kuo greičiau pateikia saugos požiūriu svarbią informaciją, gautą iš informacijos saugumo ataskaitų, kurias ji gavo pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.230 dalį.“;

b) po ATM/ANS.AR.A.025 dalies įterpiama ATM/ANS.AR.A.025A dalis:

„**ATM/ANS.AR.A.025A. Neatidėliotinas reagavimas į informacijos saugumo incidentą arba pažeidžiamumą, darančius poveikį aviacijos saugai**

a) Kompetentinga institucija įgyvendina sistemą, pagal kurią būtų tinkamai renkama, analizuojama ir skleidžiama informacija, susijusi su informacijos saugumo incidentais ir pažeidžiamumu, galinčiais turėti poveikį aviacijos saugai, apie kuriuos praneša organizacijos. Tai daroma koordinuojant veiksmus su visomis kitomis atitinkamomis institucijomis, atsakingomis už informacijos saugumą ar kibernetinį saugumą valstybėje narėje, kad būtų pagerintas pranešimų teikimo sistemų koordinavimas ir suderinamumas.

b) Agentūra įgyvendina sistemą, kad tinkamai išanalizuotų visą aktualią saugos požiūriu svarbią informaciją, gautą pagal ATM/ANS.AR.A.020 dalies c punktą, ir nepagrįstai nedelsdama pateiktų valstybėms narėms ir Komisijai visą informaciją, įskaitant rekomendacijas ar taisomuosius veiksmus, kurių reikia imtis, kad jos galėtų laiku reaguoti į informacijos saugumo incidentą arba pažeidžiamumą, galinčius turėti poveikį aviacijos saugai, susijusį su gaminiais, dalimis, kilnojamąja įranga, asmenimis ar organizacijomis, kuriems taikomas Reglamentas (ES) 2018/1139 ir jo deleguotieji ir įgyvendinimo aktai.

c) Gavusi a ir b punktuose nurodytos informacijos, kompetentinga institucija imasi tinkamų priemonių, kad pašalintų galimą informacijos saugumo incidento ar pažeidžiamumo poveikį aviacijos saugai.

d) Apie priemones, kurių imamasi pagal c punktą, nedelsiant pranešama visiems asmenims arba organizacijoms, kurie jas turi taikyti pagal Reglamentą (ES) 2018/1139 ir jo deleguotuosius bei įgyvendinimo aktus. Valstybės narės kompetentinga institucija apie šias priemones taip pat praneša Agentūrai ir, jei reikia imtis bendrų veiksmų, kitų susijusių valstybių narių kompetentingoms institucijoms.“;

c) ATM/ANS.AR.B.001 dalis papildoma e punktu:

„e) Be a punkte nustatytų reikalavimų, kompetentingos institucijos sukurta ir prižiūrima valdymo sistema turi atitikti Įgyvendinimo reglamento (ES) 2023/203 I priedą (IS.AR dalį), kad būtų užtikrintas tinkamas informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymas.“;

d) ATM/ANS.AR.B.005 dalis iš dalies keičiama taip:

i) antraštė pakeičiama taip:

„**ATM/ANS.AR.B.005. Užduočių paskirstymas**“;

ii) pridedamas c punktas:

„c) Organizacijos sertifikavimo ir ATM/ANS.OR.B.005A dalies reikalavimų laikymosi priežiūros užduotis kompetentinga institucija gali paskirti kompetentingiems subjektams pagal a punktą arba bet kuriai atitinkamai už informacijos saugumą ar kibernetinį saugumą valstybėje narėje atsakingai institucijai. Skirdama užduotis, kompetentinga institucija užtikrina, kad:

1) kompetentingas subjektas arba atitinkama institucija koordinuotų visus su aviacijos sauga susijusius aspektus ir į juos atsižvelgtų;

2) kompetentingo subjekto arba atitinkamos institucijos vykdomos sertifikavimo ir priežiūros veiklos rezultatai būtų įtraukti į bendras organizacijos sertifikavimo ir priežiūros bylas;

3) pagal ATM/ANS.AR.B.001 dalies e punktą sukurta jos pačios informacijos saugumo valdymo sistema apimtų visas jos vardu atliekamas sertifikavimo ir nuolatinės priežiūros užduotis.“;

e) ATM/ANS.AR.C.010 dalis papildoma d punktu:

„d) Vykdydama organizacijos ATM/ANS.OR.B.005A dalies reikalavimų laikymosi sertifikavimą ir priežiūrą, kompetentinga institucija ne tik laikosi a–c punktų, bet ir peržiūri visus patvirtinimus, suteiktus pagal šio reglamento IS.I.OR.200 dalies e punktą arba Deleguotojo reglamento (ES) 2022/1645 IS.D.OR.200 dalies e punktą, po taikomo priežiūros audito ciklo ir visais atvejais, kai įgyvendinami organizacijos darbo apimties pakeitimai.“;

f) po ATM/ANS.AR.C.025 dalies įterpiama ATM/ANS.AR.C.025A dalis:

„**ATM/ANS.AR.C.025A. Informacijos saugumo valdymo sistemos pakeitimai**

a) Dėl pakeitimų, kuriuos valdo kompetentinga institucija ir apie kuriuos jai pranešama pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies a punkte nustatytą procedūrą, kompetentinga institucija tokių pakeitimų peržiūrą įtraukia į savo nuolatinę priežiūrą pagal ATM/ANS.AR.C.010 dalyje išdėstytus principus. Jei nustatoma kokia nors neatitiktis, kompetentinga institucija apie tai praneša organizacijai, paprašo atlikti papildomus pakeitimus ir imasi veiksmų pagal ATM/ANS.AR.C.050 dalį.

b) Dėl kitų pakeitimų, dėl kurių reikia pateikti patvirtinimo paraišką pagal Įgyvendinimo reglamento (ES) 2023/203 II priedo (IS.I.OR dalies) IS.I.OR.255 dalies b punktą:

1) gavusi paraišką dėl pakeitimo, kompetentinga institucija, prieš suteikdama patvirtinimą, patikrina, ar organizacija laikosi taikomų reikalavimų;

2) kompetentinga institucija nustato sąlygas, kuriomis organizacija gali veikti įgyvendindama pakeitimą;

3) įsitikinusi, kad organizacija laikosi taikomų reikalavimų, kompetentinga institucija patvirtina pakeitimą.“;

(2) III priedas (ATM/ANS.OR dalis) iš dalies keičiamas taip:

a) po ATM/ANS.OR.B.005 dalies įterpiama ATM/ANS.OR.B.005A dalis:

„**ATM/ANS.OR.B.005A. Informacijos saugumo valdymo sistema**

Be ATM/ANS.OR.B.005 dalyje nurodytos valdymo sistemos, paslaugų teikėjas pagal Įgyvendinimo reglamentą (ES) 2023/203 parengia, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą, kad užtikrintų tinkamą informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymą.“;

b) ATM/ANS.OR.D.010 dalis pakeičiama taip:

„**ATM/ANS.OR.D.010. Saugumo valdymas**

a) Oro navigacijos paslaugų ir oro eismo srautų valdymo paslaugų teikėjai ir tinklo valdytojas parengia saugumo valdymo sistemą, kuri yra neatsiejama pagal ATM/ANS.OR.B.005 taisyklę būtinos valdymo sistemos dalis, kad užtikrintų:

1) savo priemonių ir darbuotojų saugumą siekiant neleisti neteisėtai įsikišti į paslaugų teikimą;

2) gaunamų arba sukuriamų ar kitaip naudojamų veiklos duomenų saugumą, kad jie būtų prieinami tik atitinkamai įgaliotiems asmenims.

b) Saugumo valdymo sistemoje apibrėžiama:

1) procesas ir procedūros, susiję su saugumo rizikos vertinimu ir mažinimu, saugumo stebėjimu ir gerinimu, saugumo patikrinimais ir patirties sklaida;

2) priemonės, kurias naudojant identifikuojami, stebimi ir aptinkami saugumo pažeidimai ir atitinkamais saugumo signalais perspėjami darbuotojai;

3) saugumo pažeidimų poveikio valdymo ir taisomųjų veiksmų bei mažinimo procedūrų nustatymo priemonės, taikomos siekiant išvengti pažeidimų pasikartojimo.

c) Jei reikia, oro navigacijos paslaugų ir oro eismo srautų valdymo paslaugų teikėjai ir tinklo valdytojas užtikrina savo darbuotojų patikimumo kontrolę ir, siekdami užtikrinti savo priemonių, darbuotojų ir duomenų saugumą, koordinuoja šią veiklą su atitinkamomis civilinėmis ir karinėmis institucijomis.

d) Su informacijos saugumu susiję aspektai tvarkomi pagal ATM/ANS.OR.B.005A dalį.“