II

(Nezakonodavni akti)

UREDBE

PROVEDBENA UREDBA KOMISIJE (EU) 2023/203

od 27. listopada 2022.

o utvrđivanju pravila za primjenu Uredbe (EU) 2018/1139 Europskog parlamenta i Vijeća u pogledu zahtjeva za upravljanje rizicima za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa za organizacije obuhvaćene uredbama Komisije (EU) br. 1321/2014, (EU) br. 965/2012, (EU) br. 1178/2011, (EU) 2015/340, provedbenim uredbama Komisije (EU) 2017/373 i (EU) 2021/664 i za nadležna tijela obuhvaćena uredbama Komisije (EU) br. 748/2012, (EU) br. 1321/2014, (EU) br. 965/2012, (EU) br. 1178/2011, (EU) 2015/340 i (EU) br. 139/2014, provedbenim uredbama Komisije (EU) 2017/373 i (EU) 2021/664 te o izmjeni uredbi Komisije (EU) br. 1178/2011, (EU) br. 748/2012, (EU) br. 965/2012, (EU) br. 139/2014, (EU) br. 1321/2014, (EU) 2015/340 i provedbenih uredbi Komisije (EU) 2017/373 i (EU) 2021/664

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2018/1139 Europskog parlamenta i Vijeća od 4. srpnja 2018. o zajedničkim pravilima u području civilnog zrakoplovstva i osnivanju Agencije Europske unije za sigurnost zračnog prometa i izmjeni uredbi (EZ) br. 2111/2005, (EZ) br. 1008/2008, (EU) br. 996/2010, (EU) br. 376/2014 i direktiva 2014/30/EU i 2014/53/EU Europskog parlamenta i Vijeća te stavljanju izvan snage uredbi (EZ) br. 552/2004 i (EZ) br. 216/2008 Europskog parlamenta i Vijeća i Uredbe Vijeća (EEZ) br. 3922/91 ([1]), a posebno njezin članak 17. stavak 1. točku (b), članak 27. stavak 1. točku (a), članak 31. stavak 1. točku (b), članak 43. stavak 1. točku (b), članak 53. stavak 1. točku (a) i članak 62. stavak 15. točku (c),

budući da:

(1) U skladu s bitnim zahtjevima iz točke 3.1. podtočke (b) Priloga II. Uredbi (EU) 2018/1139 organizacije za upravljanje kontinuiranom plovidbenošću i organizacije za održavanje moraju uspostaviti i održavati sustav upravljanja radi upravljanja sigurnosnim rizicima.

(2) Osim toga, u skladu s bitnim zahtjevima iz točke 3.3. podtočke (b) i točke 5. podtočke (b) Priloga IV. Uredbi (EU) 2018/1139 organizacije za osposobljavanje pilota, organizacije za osposobljavanje kabinske posade, zrakoplovno-medicinski centri za posadu zrakoplova i operatori uređaja za osposobljavanje koji simuliraju let moraju uspostaviti i održavati sustav upravljanja radi upravljanja sigurnosnim rizicima i održavati takav sustav.

(3) Usto, u skladu s bitnim zahtjevima iz točke 8.1. podtočke (c) Priloga V. Uredbi (EU) 2018/1139 operatori zrakoplova moraju uspostaviti i održavati sustav upravljanja radi upravljanja sigurnosnim rizicima.

(4) Nadalje, u skladu s bitnim zahtjevima iz točke 5.1. podtočke (c) i točke 5.4. podtočke (b) Priloga VIII. Uredbi (EU) 2018/1139 pružatelji usluga upravljanja zračnim prometom i usluga u zračnoj plovidbi, pružatelji U-space usluga i jedinstveni pružatelji zajedničkih usluga informiranja, organizacije za osposobljavanje i zrakoplovno-medicinski centri za kontrolore zračnog prometa moraju uspostaviti i održavati sustav upravljanja radi upravljanja sigurnosnim rizicima.

([1]) SL L 212, 22.8.2018., str. 1.

(5) Ti sigurnosni rizici mogu proizlaziti iz raznih izvora, kao što su nedostaci u projektiranju i održavanju, aspekti ljudske učinkovitosti, prijetnje okolišu i prijetnje za informacijsku sigurnost. Stoga bi u sustavima upravljanja koje primjenjuju Agencija Europske unije za sigurnost zračnog prometa („Agencija”) te nacionalna nadležna tijela i organizacije navedene u prethodnim uvodnim izjavama trebalo uzeti u obzir sigurnosne rizike koji proizlaze iz slučajnih događaja, ali i sigurnosne rizike koji proizlaze iz prijetnji za informacijsku sigurnost kad postojeće nedostatke mogu iskorištavati pojedinci u zlonamjerne svrhe. Ti rizici za informacijsku sigurnost stalno se povećavaju u okruženju civilnog zrakoplovstva kako postojeći informacijski sustavi postaju sve povezaniji, a sve češće i meta zlonamjernih aktera.

(6) Rizici povezani s tim informacijskim sustavima nisu ograničeni na moguće napade na kiberprostor, nego obuhvaćaju i prijetnje koje mogu utjecati na procese i postupke te ljudsku učinkovitost.

(7) Niz organizacija već upotrebljava međunarodne norme, kao npr. ISO 27001, radi rješavanja pitanja sigurnosti digitalnih informacija i podataka. Te norme možda ne mogu u potpunosti obuhvatiti sve posebnosti civilnog zrakoplovstva. Stoga je primjereno utvrditi zahtjeve za upravljanje rizicima za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa.

(8) Ključno je da se tim zahtjevima obuhvate sva područja zrakoplovstva i njihova sučelja jer je zrakoplovstvo sustav međusobno vrlo povezanih sustava. Stoga bi se oni trebali primjenjivati na sve organizacije i nadležna tijela obuhvaćene uredbama Komisije (EU) br. 748/2012 ([2]), (EU) br. 1321/2014 ([3]), (EU) br. 965/2012 ([4]), (EU) br. 1178/2011 ([5]), (EU) 2015/340 ([6]), (EU) br. 139/2014 ([7]) i Provedbenom uredbom Komisije (EU) 2021/664 ([8]), uključujući one koji već moraju imati sustav upravljanja u skladu s postojećim zakonodavstvom Unije o sigurnosti zračnog prometa. Međutim, neke bi organizacije trebalo izuzeti iz područja primjene ove Uredbe kako bi se osigurala odgovarajuća proporcionalnost manjoj razini rizika za informacijsku sigurnost zrakoplovnog sustava.

(9) Zahtjevima utvrđenima u ovoj Uredbi trebala bi se osigurati dosljedna primjena u svim područjima zrakoplovstva, pritom stvarajući minimalan učinak na zakonodavstvo Unije o sigurnosti zračnog prometa koje se već primjenjuje na ta područja.

([2]) Uredba Komisije (EU) br. 748/2012 od 3. kolovoza 2012. o utvrđivanju provedbenih pravila za certifikaciju plovidbenosti i ekološku certifikaciju zrakoplova i s njima povezanih proizvoda, dijelova i uređaja te za certifikaciju projektnih i proizvodnih organizacija (SL L 224, 21.8.2012., str. 1.).

([3]) Uredba Komisije (EU) br. 1321/2014 od 26. studenoga 2014. o kontinuiranoj plovidbenosti zrakoplova i aeronautičkih proizvoda, dijelova i uređaja, te o odobravanju organizacija i osoblja uključenih u te poslove (Preinaka) (SL L 362, 17.12.2014., str. 1.).

([4]) Uredba Komisije (EU) br. 965/2012 od 5. listopada 2012. o utvrđivanju tehničkih zahtjeva i upravnih postupaka u vezi s letačkim operacijama u skladu s Uredbom (EZ) br. 216/2008 Europskog parlamenta i Vijeća (SL L 296, 25.10.2012., str. 1.).

([5]) Uredba Komisije (EU) br. 1178/2011 od 3. studenoga 2011. o utvrđivanju tehničkih zahtjeva i administrativnih postupaka vezano za članove posade zrakoplova u civilnom zrakoplovstvu u skladu s Uredbom (EZ) br. 216/2008 Europskog parlamenta i Vijeća (SL L 311, 25.11.2011., str. 1.).

([6]) Uredba Komisije (EU) 2015/340 od 20. veljače 2015. o utvrđivanju tehničkih zahtjeva i administrativnih postupaka koji se odnose na dozvole i certifikate kontrolora zračnog prometa u skladu s Uredbom (EZ) br. 216/2008 Europskog parlamenta i Vijeća, o izmjeni Provedbene uredbe Komisije (EU) br. 923/2012 i o stavljanju izvan snage Uredbe Komisije (EU) br. 805/2011 (SL L 63, 6.3.2015., str. 1.).

([7]) Uredba Komisije (EU) br. 139/2014 od 12. veljače 2014. o utvrđivanju zahtjeva i upravnih postupaka u vezi s aerodromima u skladu s Uredbom (EZ) br. 216/2008 Europskog parlamenta i Vijeća (SL L 44, 14.2.2014., str. 1.).

([8]) Provedbena uredba Komisije (EU) 2021/664 od 22. travnja 2021. o regulatornom okviru za U-space (SL L 139, 23.4.2021., str. 161.).

(10) Zahtjevima utvrđenima u ovoj Uredbi ne bi se trebali dovoditi u pitanje zahtjevi u pogledu informacijske sigurnosti i kibersigurnosti utvrđeni u točki 1.7. Priloga Provedbenoj uredbi Komisije (EU) 2015/1998 ([9]) i članku 14. Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća ([10]).

(11) Sigurnosni zahtjevi utvrđeni u člancima od 33. do 43. glave V. „Sigurnost Programa" Uredbe (EU) 2021/696 Europskog parlamenta i Vijeća ([11]) smatraju se istovrijednima zahtjevima utvrđenima u ovoj Uredbi, osim u pogledu točke IS.I.OR.230 Priloga II. ovoj Uredbi, koja bi se trebala poštovati.

(12) Radi pravne sigurnosti tumačenje pojma „informacijska sigurnost", kako je definiran u ovoj Uredbi u skladu s uobičajenom upotrebom u civilnom zračnom prometu u svijetu, trebalo bi se smatrati dosljednim s tumačenjem pojma „sigurnost mrežnih i informacijskih sustava" kako je definiran u članku 4. točki 2. Direktive (EU) 2016/1148. Definiciju informacijske sigurnosti koja se upotrebljava za potrebe ove Uredbe ne bi trebalo tumačiti kao da se razlikuje od definicije sigurnosti mrežnih i informacijskih sustava utvrđene u Direktivi (EU) 2016/1148.

(13) Kako bi se izbjeglo udvostručavanje pravnih zahtjeva, ako organizacije obuhvaćene ovom Uredbom već podliježu sigurnosnim zahtjevima koji proizlaze iz akata Unije iz uvodnih izjava 10. i 11., a koji su po svojem učinku istovrijedni odredbama utvrđenima u ovoj Uredbi, usklađenost s tim sigurnosnim zahtjevima trebala bi se smatrati usklađenošću sa zahtjevima utvrđenima u ovoj Uredbi.

(14) Organizacije obuhvaćene ovom Uredbom koje već podliježu sigurnosnim zahtjevima koji proizlaze iz Provedbene uredbe (EU) 2015/1998 ili Uredbe (EU) 2021/696 ili obje te uredbe trebale bi ispunjavati i zahtjeve iz Priloga II. (točka IS.I.OR.230 „Sustav vanjskog izvješćivanja o informacijskoj sigurnosti") ovoj Uredbi jer nijedna od tih uredbi ne sadržava odredbe o vanjskom izvješćivanju o incidentima povezanima s informacijskom sigurnošću.

(15) Radi cjelovitosti trebalo bi izmijeniti uredbe (EU) br. 1178/2011, (EU) br. 748/2012, (EU) br. 965/2012, (EU) br. 139/2014, (EU) br. 1321/2014, (EU) 2015/340 te provedbene uredbe (EU) 2017/373 ([12]) i (EU) 2021/664 kako bi se uveli zahtjevi za sustav upravljanja informacijskom sigurnošću propisani ovom Uredbom zajedno sa sustavima upravljanja koji su u njoj utvrđeni te kako bi se utvrdili zahtjevi za nadležna tijela povezani s nadzorom organizacija koje provode prethodno navedene zahtjeve za upravljanje informacijskom sigurnošću.

(16) Kako bi se organizacijama dalo dovoljno vremena da se usklade s novim pravilima i postupcima, ova bi se Uredba trebala početi primjenjivati tri godine nakon datuma stupanja na snagu, osim na pružatelja usluga u zračnoj plovidbi Europskoga geostacionarnog navigacijskog sustava (EGNOS) definiranog u Provedbenoj uredbi (EU) 2017/373, na kojeg bi se zbog tekuće sigurnosne akreditacije sustava i usluga EGNOS u skladu Uredbom (EU) 2021/696 trebala početi primjenjivati 1. siječnja 2026.

(17) Zahtjevi utvrđeni u ovoj Uredbi temelje se na Mišljenju br. 03/2021 ([13]), koje je izdala Agencija u skladu s člankom 75. stavkom 2. točkama (b) i (c) i člankom 76. stavkom 1. Uredbe (EU) 2018/1139.

([9]) Provedbena uredba Komisije (EU) 2015/1998 od 5. studenoga 2015. o utvrđivanju detaljnih mjera za provedbu zajedničkih osnovnih standarda iz područja zaštite zračnog prometa (SL L 299, 14.11.2015., str. 1.).

([10]) Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

([11]) Uredba (EU) 2021/696 Europskog parlamenta i Vijeća od 28. travnja 2021. o uspostavi Svemirskog programa Unije i osnivanju Agencije Europske unije za svemirski program te o stavljanju izvan snage uredaba (EU) br. 912/2010, (EU) br. 1285/2013 i (EU) br. 377/2014 i Odluke br. 541/2014/EU (SL L 170, 12.5.2021., str. 69.).

([12]) Provedbena uredba Komisije (EU) 2017/373 od 1. ožujka 2017. o utvrđivanju zajedničkih zahtjeva za pružatelje usluga upravljanja zračnim prometom/pružatelje usluga u zračnoj plovidbi i drugih mrežnih funkcija za upravljanje zračnim prometom i za njihov nadzor, o stavljanju izvan snage Uredbe (EZ) br. 482/2008 i provedbenih uredbi (EU) br. 1034/2011, (EU) br. 1035/2011 i (EU) 2016/1377 te o izmjeni Uredbe (EU) br. 677/2011 (SL L 62, 8.3.2017., str. 1.).

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

(18) Zahtjevi utvrđeni u ovoj Uredbi u skladu su s mišljenjem Odbora za primjenu zajedničkih sigurnosnih pravila u području civilnog zrakoplovstva osnovanog člankom 127. Uredbe (EU) 2018/1139,

DONIJELA JE OVU UREDBU:

Članak 1.

Predmet

Ovom se Uredbom utvrđuju zahtjevi koje organizacije i nadležna tijela moraju ispuniti:

(a) kako bi identificirali i upravljali rizicima za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa, što bi moglo utjecati na sustave informacijske i komunikacijske tehnologije i podatke koji se upotrebljavaju u civilnom zrakoplovstvu;

(b) kako bi se otkrili događaji povezani s informacijskom sigurnošću i identificirali oni koji se smatraju incidentima povezanima s informacijskom sigurnošću koji bi mogli utjecati na sigurnost zračnog prometa;

(c) radi odgovora na te incidente i oporavka od njih.

Članak 2.

Područje primjene

1. Ova Uredba primjenjuje se na sljedeće organizacije:

(a) organizacije za održavanje podložne odjeljku A Priloga II. (dio 145.) Uredbi (EU) br. 1321/2014, osim onih koje su isključivo uključene u održavanje zrakoplova u skladu s Prilogom V.b (dio ML) Uredbi (EU) br. 1321/2014;

(b) organizacije za upravljanje kontinuiranom plovidbenošću (CAMO-ovi) podložne odjeljku A Priloga V.c (dio CAMO) Uredbi (EU) br. 1321/2014, osim onih koje su isključivo uključene u upravljanje kontinuiranom plovidbenošću zrakoplova u skladu s Prilogom V.b (dio ML) Uredbi (EU) br. 1321/2014;

(c) operatore zrakoplova podložne Prilogu III. (dio ORO) Uredbi (EU) br. 965/2012, osim onih koji su isključivo uključeni u rad bilo koje od sljedećih vrsta zrakoplova:

i. zrakoplova ELA 2 kako je definiran u članku 1. stavku 2. točki (j) Uredbe (EU) br. 748/2012;

ii. aviona uzgonjenih jednim elisnim motorom s konfiguracijom najvećeg operativnog broja putničkih sjedala od pet ili manje koji nisu klasificirani kao složeni zrakoplovi na motorni pogon, koji polijeću i slijeću na isti aerodrom ili operativnu površinu i kojima se upravlja po danu prema pravilima vizualnog letenja (VFR);

iii. jednomotornih helikoptera s konfiguracijom najvećeg operativnog broja putničkih sjedala od pet ili manje koji nisu klasificirani kao složeni zrakoplovi na motorni pogon, koji polijeću i slijeću na isti aerodrom ili operativnu površinu i kojima se upravlja po danu prema VFR-u;

(d) odobrene organizacije za osposobljavanje (ATO-ovi) podložne Prilogu VII. (dio ORA) Uredbi (EU) br. 1178/2011, osim onih koje su isključivo uključene u osposobljavanje za zrakoplove ELA 2 kako su definirani u članku 1. stavku 2. točki (j) Uredbe (EU) br. 748/2012 ili koje su isključivo uključene u teorijsko osposobljavanje;

(e) zrakoplovno-medicinske centre za posadu zrakoplova podložne Prilogu VII. (dio ORA) Uredbi (EU) br. 1178/2011;

(f) operatore uređaja za osposobljavanje koji simuliraju let (FSTD-i) podložne Prilogu VII. (dio ORA) Uredbi (EU) br. 1178/2011, osim onih koji su isključivo uključeni u rad FSTD-a za zrakoplove ELA 2 kako je definirano u članku 1. stavku 2. točki (j) Uredbe (EU) br. 748/2012;

(g) organizacije za osposobljavanje kontrolora zračnog prometa (ATCO TO-ovi) i zrakoplovno-medicinske centre za kontrolore zračnog prometa podložne Prilogu III. (dio ATCO.OR) Uredbi (EU) 2015/340;

(h) organizacije podložne Prilogu III. (dio ATM/ANS.OR) Provedbenoj uredbi (EU) 2017/373, osim sljedećih pružatelja usluga:

i. pružatelja usluga u zračnoj plovidbi koji imaju ograničenu svjedodžbu u skladu s točkom ATM/ANS.OR.A.010 tog priloga;

ii. pružatelja usluga letnih informacija koji daju izjavu o svojim aktivnostima u skladu s točkom ATM/ANS.OR. A.015 tog priloga;

(i) pružatelje U-space usluga i jedinstvene pružatelje zajedničkih usluga informiranja podložne Provedbenoj uredbi (EU) 2021/664.

2. Ova se Uredba primjenjuje na nadležna tijela, među ostalim na Agenciju Europske unije za sigurnost zračnog prometa („Agencija”), navedena u članku 6. ove Uredbe i članku 5. Delegirane uredbe Komisije (EU) 2022/1645 ([14]).

3. Ova se Uredba primjenjuje i na nadležno tijelo odgovorno za izdavanje, produljivanje, mijenjanje, privremeno ili trajno oduzimanje dozvola za održavanje zrakoplova u skladu s Prilogom III. (dio 66.) Uredbi (EU) br. 1321/2014.

4. Ovom se Uredbom ne dovode u pitanje zahtjevi u pogledu informacijske sigurnosti i kibersigurnosti utvrđeni u točki 1.7. Priloga Provedbenoj uredbi (EU) 2015/1998 i članku 14. Direktive (EU) 2016/1148.

Članak 3.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

(1) „informacijska sigurnost” znači očuvanje povjerljivosti, integriteta, autentičnosti i dostupnosti mrežnih i informacijskih sustava;

(2) „događaj povezan s informacijskom sigurnošću” znači identificirani događaj u stanju sustava, usluge ili mreže koji ukazuje na moguće narušavanje politike informacijske sigurnosti ili zakazivanje kontrola informacijske sigurnosti ili prethodno nepoznatu situaciju koja može biti relevantna za informacijsku sigurnost;

(3) „incident” znači svaki događaj koji ima stvaran negativni učinak na sigurnost mrežnih i informacijskih sustava, kako je definiran u članku 4. točki 7. Direktive (EU) 2016/1148;

(4) „rizik za informacijsku sigurnost” znači rizik za organizacijske operacije civilnog zrakoplovstva, imovinu, pojedince te druge organizacije zbog mogućeg događaja povezanog s informacijskom sigurnošću. Rizici za informacijsku sigurnost povezani su s mogućnošću prijetnje iskorištavanja ranjivosti informacijske imovine ili skupine informacijske imovine;

([14]) Delegirana uredba Komisije (EU) 2022/1645 od 14. srpnja 2022. o utvrđivanju pravila za primjenu Uredbe (EU) 2018/1139 Europskog parlamenta i Vijeća u pogledu zahtjeva za upravljanje rizicima za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa za organizacije obuhvaćene uredbama Komisije (EU) br. 748/2012 i (EU) br. 139/2014 i o izmjeni uredbi Komisije (EU) br. 748/2012 i (EU) br. 139/2014 (SL L 248, 26.9.2022., str. 18.).

(5) „prijetnja” znači mogućnost povrede informacijske sigurnosti koja postoji kad postoji subjekt, okolnost, radnja ili događaj koji bi mogli prouzročiti štetu;

(6) „ranjivost” znači nedostatak ili slaba točka u imovini ili sustavu, postupcima, dizajnu, provedbi ili mjerama informacijske sigurnosti koja bi se mogla iskoristiti i koja dovede do kršenja politike informacijske sigurnosti.

Članak 4.

Zahtjevi za organizacije i nadležna tijela

1. Organizacije iz članka 2. stavka 1. moraju ispunjavati zahtjeve iz Priloga II. (dio IS.I.OR) ovoj Uredbi.

2. Nadležna tijela iz članka 2. stavaka 2. i 3. moraju ispunjavati zahtjeve iz Priloga I. (dio IS.AR) ovoj Uredbi.

Članak 5.

Zahtjevi koji proizlaze iz drugih akata Unije

1. Ako organizacija iz članka 2. stavka 1. ispunjava sigurnosne zahtjeve utvrđene u skladu s člankom 14. Direktive (EU) 2016/1148 koji su istovrijedni zahtjevima utvrđenima u ovoj Uredbi, usklađenost s tim sigurnosnim zahtjevima smatra se usklađenošću sa zahtjevima utvrđenima u ovoj Uredbi.

2. Ako je organizacija iz članka 2. stavka 1. operator ili subjekt iz nacionalnih programa zaštite civilnog zračnog prometa država članica utvrđenih u skladu s člankom 10. Uredbe (EZ) br. 300/2008 Europskog parlamenta i Vijeća ([15]), kibersigurnosni zahtjevi iz točke 1.7. Priloga Provedbenoj uredbi (EU) 2015/1998 smatraju se istovrijednima zahtjevima utvrđenima u ovoj Uredbi, osim u pogledu točke IS.I.OR.230 Priloga II. ovoj Uredbi, koja se mora poštovati.

3. Ako je organizacija iz članka 2. stavka 1. pružatelj usluga u zračnoj plovidbi Europskoga geostacionarnog navigacijskog sustava (EGNOS) iz Uredbe (EU) 2021/696, sigurnosni zahtjevi iz članaka od 33. do 43. glave V. te uredbe smatraju se istovrijednima zahtjevima utvrđenima u ovoj Uredbi, osim u pogledu točke IS.I.OR.230 Priloga II. ovoj Uredbi, koja se mora poštovati.

4. Nakon savjetovanja s Agencijom i skupinom za suradnju iz članka 11. Direktive (EU) 2016/1148 Komisija može izdati smjernice za procjenu istovrijednosti zahtjeva utvrđenih u ovoj Uredbi i Direktivi (EU) 2016/1148.

Članak 6.

Nadležno tijelo

1. Ne dovodeći u pitanje zadaće povjerene Odboru za sigurnosnu akreditaciju iz članka 36. Uredbe (EU) 2021/696, tijelo nadležno za potvrđivanje i nadzor usklađenosti s ovom Uredbom je:

(a) za organizacije iz članka 2. stavka 1. točke (a), nadležno tijelo imenovano u skladu s Prilogom II. (dio 145.) Uredbi (EU) br. 1321/2014;

(b) za organizacije iz članka 2. stavka 1. točke (b), nadležno tijelo imenovano u skladu s Prilogom V.c (dio CAMO) Uredbi (EU) br. 1321/2014;

([15]) Uredba (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (SL L 97, 9.4.2008., str. 72.).

(c) za organizacije iz članka 2. stavka 1. točke (c), nadležno tijelo imenovano u skladu s Prilogom III. (dio ORO) Uredbi (EU) br. 965/2012;

(d) za organizacije iz članka 2. stavka 1. točaka od (d) do (f), nadležno tijelo imenovano u skladu s Prilogom VII. (dio ORA) Uredbi (EU) br. 1178/2011;

(e) za organizacije iz članka 2. stavka 1. točke (g), nadležno tijelo imenovano u skladu s člankom 6. stavkom 2. Uredbe (EU) 2015/340;

(f) za organizacije iz članka 2. stavka 1. točke (h), nadležno tijelo imenovano u skladu s člankom 4. stavkom 1. Provedbene uredbe (EU) 2017/373;

(g) za organizacije iz članka 2. stavka 1. točke (i), nadležno tijelo imenovano u skladu s člankom 14. stavkom 1. ili 2., kako je primjenjivo, Provedbene uredbe (EU) 2021/664.

2. Države članice mogu za potrebe ove Uredbe imenovati neovisan i autonoman subjekt za izvršavanje dodijeljene uloge i odgovornosti nadležnih tijela iz stavka 1. U tom slučaju uspostavljaju se mjere koordinacije između tog subjekta i nadležnih tijela, kako su navedena u stavku 1., kako bi se osigurao djelotvoran nadzor nad svim zahtjevima koje organizacija mora ispuniti.

3. Agencija mora u potpunosti u skladu s primjenjivim pravilima o tajnosti, zaštiti osobnih podataka i zaštiti povjerljivih informacija surađivati s Agencijom Europske unije za svemirski program (EUSPA) i Odborom za sigurnosnu akreditaciju iz članka 36. Uredbe (EU) 2021/696 kako bi se osigurao djelotvoran nadzor nad zahtjevima primjenjivima na pružatelja usluga u zračnoj plovidbi EGNOS-a.

Članak 7.

Dostavljanje relevantnih informacija tijelima nadležnima za sigurnost mreža i informacija

Nadležna tijela na temelju ove Uredbe bez neopravdane odgode obavješćuju jedinstvenu kontaktnu točku određenu u skladu s člankom 8. Direktive (EU) 2016/1148 o svim relevantnim informacijama koje su uključene u obavijesti koje operatori ključnih usluga iz članka 5. Direktive (EU) 2016/1148 dostavljaju u skladu s točkom IS.I.OR.230 Priloga II. ovoj Uredbi i točkom IS.D.OR.230 Priloga I. Provedbenoj uredbi (EU) 2022/1645.

Članak 8.

Izmjena Uredbe (EU) br. 1178/2011

Prilozi VI. (dio ARA) i VII. (dio ORA) Uredbi (EU) br. 1178/2011 mijenjaju se u skladu s Prilogom III. ovoj Uredbi.

Članak 9.

Izmjena Uredbe (EU) br. 748/2012

Prilog I. (dio 21.) Uredbi (EU) br. 748/2012 mijenja se u skladu s Prilogom IV. ovoj Uredbi.

Članak 10.

Izmjena Uredbe (EU) br. 965/2012

Prilozi II. (dio ARO) i III. (dio ORO) Uredbi (EU) br. 965/2012 mijenjaju se u skladu s Prilogom V. ovoj Uredbi.

Članak 11.

Izmjena Uredbe (EU) br. 139/2014

Prilog II. (dio ADR.AR) Uredbi (EU) br. 139/2014 mijenja se u skladu s Prilogom VI. ovoj Uredbi.

Članak 12.

Izmjena Uredbe (EU) br. 1321/2014

Prilozi II. (dio 145.), III. (dio 66.) i V.c (dio CAMO) Uredbi (EU) br. 1321/2014 mijenjaju se u skladu s Prilogom VII. ovoj Uredbi.

Članak 13.

Izmjena Uredbe (EU) 2015/340

Prilozi II. (dio ATCO.AR) i III. (dio ATCO.OR) Uredbi (EU) 2015/340 mijenjaju se u skladu s Prilogom VIII. ovoj Uredbi.

Članak 14.

Izmjena Provedbene uredbe (EU) 2017/373

Prilozi II. (dio ATM/ANS.AR) i III. (dio ATM/ANS.OR) Provedbenoj uredbi (EU) 2017/373 mijenjaju se u skladu s Prilogom IX. ovoj Uredbi.

Članak 15.

Izmjena Provedbene uredbe (EU) 2021/664

Provedbena uredba (EU) 2021/664 mijenja se kako slijedi:

(1) u članku 15. stavku 1. točka (f) zamjenjuje se sljedećim:

„(f) provode i održavaju sustav upravljanja zaštitom u skladu s točkom ATM/ANS.OR.D.010 u poddijelu D Priloga III. Provedbenoj uredbi (EU) 2017/373 i sustav upravljanja informacijskom sigurnošću u skladu s Prilogom II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203.”;

(2) u članku 18. dodaje se sljedeća točka (l):

„(l) uspostavljaju, provode i održavaju sustav upravljanja informacijskom sigurnošću u skladu s Prilogom I. (dio IS.AR) Provedbenoj uredbi (EU) 2023/203.”

Članak 16.

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Primjenjuje se od 22. veljače 2026.

Međutim, na pružatelja usluga u zračnoj plovidbi EGNOS-a podložnog Provedbenoj uredbi (EU) 2017/373 ona se primjenjuje od 1. siječnja 2026.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 27. listopada 2022.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

PRILOG I.

INFORMACIJSKA SIGURNOST – ZAHTJEVI U VEZI S TIJELIMA

[DIO IS.AR]

IS.AR.100 Područje primjene

IS.AR.200 Sustav upravljanja informacijskom sigurnošću (ISMS)

IS.AR.205 Procjena rizika za informacijsku sigurnost

IS.AR.210 Postupanje s rizicima za informacijsku sigurnost

IS.AR.215 Incidenti povezani s informacijskom sigurnošću – otkrivanje, odgovor i oporavak

IS.AR.220 Ugovaranje aktivnosti upravljanja informacijskom sigurnošću

IS.AR.225 Zahtjevi u vezi s osobljem

IS.AR.230 Vođenje evidencije

IS.AR.235 Kontinuirano poboljšavanje

IS.AR.100 Područje primjene

U ovom se dijelu utvrđuju zahtjevi za upravljanje koje moraju ispuniti nadležna tijela iz članka 2. stavka 2. ove Uredbe.

Zahtjevi koje ta nadležna tijela moraju ispuniti pri obavljanju aktivnosti certifikacije, nadzora i osiguravanja provedbe propisa navedeni su u uredbama iz članka 2. stavka 1. ove Uredbe i članka 2. Delegirane uredbe (EU) 2022/1645.

IS.AR.200 Sustav upravljanja informacijskom sigurnošću (ISMS)

(a) Kako bi se ostvarili ciljevi utvrđeni u članku 1., nadležno tijelo uspostavlja, provodi i održava sustav upravljanja informacijskom sigurnošću (ISMS) kojim se osigurava da nadležno tijelo:

(1) uspostavlja politiku informacijske sigurnosti kojom se utvrđuju opća načela nadležnog tijela u pogledu mogućeg utjecaja rizika za informacijsku sigurnost na sigurnost zračnog prometa;

(2) identificira i preispituje rizike za informacijsku sigurnost u skladu s točkom IS.AR.205;

(3) definira i provodi mjere postupanja s rizicima za informacijsku sigurnost u skladu s točkom IS.AR.210;

(4) u skladu s točkom IS.AR.215 definira i provodi mjere potrebne za otkrivanje događaja povezanih s informacijskom sigurnošću, identificira one koji se smatraju incidentima koji mogu utjecati na sigurnost zračnog prometa, odgovara na te incidente i oporavlja se od njih;

(5) ispunjava zahtjeve iz točke IS.AR.220 pri ugovaranju bilo kojeg dijela aktivnosti iz točke IS.AR.200 s drugim organizacijama;

(6) ispunjava zahtjeve u vezi s osobljem iz točke IS.AR.225;

(7) ispunjava zahtjeve u vezi s vođenjem evidencije iz točke IS.AR.230;

(8) prati usklađenost vlastite organizacije sa zahtjevima ove Uredbe i pruža povratne informacije o nalazima osobi iz točke IS.AR.225 podtočke (a) kako bi se osigurala djelotvorna provedba korektivnih mjera;

(9) štiti povjerljivost svih informacija koje nadležno tijelo posjeduje o organizacijama koje nadzire i informacija koje je primilo putem sustava vanjskog izvješćivanja organizacija uspostavljenih u skladu s točkom IS.I.OR.230 Priloga II. (dio IS.I.OR) ovoj Uredbi i točkom IS.D.OR.230 Priloga (dio IS.D.OR) Delegiranoj uredbi (EU) 2022/1645;

(10) obavješćuje Agenciju o promjenama koje utječu na sposobnost nadležnog tijela da obavlja svoje zadaće i izvršava svoje odgovornosti kako je definirano u ovoj Uredbi;

(11) definira i provodi postupke za primjereno, praktično i pravodobno dijeljenje relevantnih informacija kako bi drugim nadležnim tijelima i agencijama te organizacijama koje podliježu ovoj Uredbi pomoglo u provođenju djelotvornih procjena rizika za sigurnost povezanih s njihovim aktivnostima.

(b) Kako bi kontinuirano ispunjavalo zahtjeve iz članka 1., nadležno tijelo provodi postupak kontinuiranog poboljšavanja u skladu s točkom IS.AR.235.

(c) Nadležno tijelo dokumentira sve ključne procese, postupke, uloge i odgovornosti potrebne za usklađivanje s točkom IS.AR.200 podtočkom (a) i uspostavlja postupak za izmjenu te dokumentacije.

(d) Procesi, postupci, uloge i odgovornosti koje je nadležno tijelo uspostavilo radi usklađenosti s točkom IS.AR.200 podtočkom (a) odgovaraju prirodi i složenosti njegovih aktivnosti, na temelju procjene rizika za informacijsku sigurnost svojstvenih tim aktivnostima, i mogu se integrirati u druge postojeće sustave upravljanja koje nadležno tijelo već primjenjuje.

IS.AR.205 Procjena rizika za informacijsku sigurnost

(a) Nadležno tijelo dužno je identificirati sve elemente svoje vlastite organizacije koji bi mogli biti izloženi rizicima za informacijsku sigurnost. To uključuje:

(1) aktivnosti, objekte i resurse nadležnog tijela, kao i usluge koje nadležno tijelo pruža, prima ili održava;

(2) opremu, sustave, podatke i informacije koji pridonose funkcioniranju elemenata iz podpodtočke 1.

(b) Nadležno tijelo mora identificirati sučelja koja njegova vlastita organizacija ima s drugim organizacijama i koja bi mogla dovesti do međusobne izloženosti rizicima za informacijsku sigurnost.

(c) Za elemente i sučelja iz podtočaka (a) i (b) nadležno tijelo mora identificirati rizike za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa.

Za svaki identificirani rizik nadležno tijelo dužno je:

(1) odrediti razinu rizika u skladu s unaprijed definiranom klasifikacijom koju je utvrdilo nadležno tijelo;

(2) povezati svaki rizik i njegovu razinu s odgovarajućim elementom ili sučeljem utvrđenim u skladu s podtočkama (a) i (b).

U unaprijed definiranoj klasifikaciji iz podpodtočke 1. uzimaju se u obzir mogućnost pojave scenarija prijetnje i ozbiljnost njegovih posljedica za sigurnost. S pomoću te klasifikacije i uzimajući u obzir ima li nadležno tijelo strukturiran i ponovljiv postupak upravljanja rizicima za operacije, nadležno tijelo može utvrditi je li rizik prihvatljiv ili je s njim potrebno postupati u skladu s točkom IS.AR.210.

Kako bi se olakšala međusobna usporedivost procjena rizika, pri određivanju razine rizika u skladu s podpodtočkom 1. uzimaju se u obzir relevantne informacije prikupljene u koordinaciji s organizacijama iz podtočke (b).

(d) Nadležno tijelo pregledava i ažurira procjenu rizika provedenu u skladu s podtočkama (a), (b) i (c) u bilo kojem od sljedećih slučajeva:

(1) došlo je do promjene elemenata koji su izloženi rizicima za informacijsku sigurnost;

(2) došlo je do promjene u sučeljima između organizacije nadležnog tijela i drugih organizacija ili u rizicima koje su priopćile druge organizacije;

(3) došlo je do promjene informacija ili znanja koji se upotrebljavaju za identifikaciju, analizu i klasifikaciju rizika;

(4) izvučene su pouke na temelju analize incidenata povezanih s informacijskom sigurnošću.

IS.AR.210 Postupanje s rizicima za informacijsku sigurnost

(a) Nadležno tijelo osmišljava mjere za otklanjanje neprihvatljivih rizika identificiranih u skladu s točkom IS.AR.205, pravodobno ih provodi i provjerava njihovu kontinuiranu djelotvornost. Te mjere omogućuju da nadležno tijelo:

(1) kontrolira okolnosti koje pridonose stvarnoj pojavi scenarija prijetnje;

(2) ublaži posljedice za sigurnost zračnog prometa povezane s nastankom scenarija prijetnje;

(3) izbjegava rizike.

Te mjere ne smiju uvesti nove neprihvatljive rizike za sigurnost zračnog prometa.

(b) Osoba iz točke IS.AR.225 podtočke (a) i drugo uključeno osoblje nadležnog tijela obavješćuju se o ishodu procjene rizika provedene u skladu s točkom IS.AR.205, odgovarajućim scenarijima prijetnji i mjerama koje treba provesti.

Nadležno tijelo obavješćuje i organizacije s kojima ima sučelje u skladu s točkom IS.AR.205 podtočkom (b) o svim rizicima koji su zajednički nadležnom tijelu i organizaciji.

IS.AR.215 Incidenti povezani s informacijskom sigurnošću – otkrivanje, odgovor i oporavak

(a) Na temelju rezultata procjene rizika provedene u skladu s točkom IS.AR.205 i ishoda postupanja s rizicima provedenog u skladu s točkom IS.AR.210, nadležno tijelo provodi mjere za otkrivanje događaja koji ukazuju na moguću pojavu neprihvatljivih rizika i koji bi mogli utjecati na sigurnost zračnog prometa. Te mjere otkrivanja omogućuju da nadležno tijelo:

(1) identificira odstupanja od unaprijed utvrđenih osnovnih vrijednosti funkcionalne učinkovitosti;

(2) aktivira upozorenja za primjenu odgovarajućih mjera odgovora u slučaju bilo kakvog odstupanja.

(b) Nadležno tijelo provodi mjere odgovora na sve uvjete događaja identificiranih u podtočki (a) koji mogu postati ili su postali incident povezan s informacijskom sigurnošću. Te mjere odgovora omogućuju da nadležno tijelo:

(1) pokrene reakciju vlastite organizacije na upozorenja iz podtočke (a) podpodtočke 2. aktiviranjem unaprijed definiranih resursa i načina postupanja;

(2) ograniči širenje napada i izbjegne potpuno ostvarenje scenarija prijetnje;

(3) kontrolira zakazivanje zahvaćenih elemenata definiranih u točki IS.AR.205 podtočki (a).

(c) Nadležno tijelo provodi mjere čiji je cilj oporavak od incidenata povezanih s informacijskom sigurnošću, uključujući hitne mjere, prema potrebi. Te mjere oporavka omogućuju da nadležno tijelo:

(1) ukloni ili ograniči na prihvatljivu razinu uvjete koji su uzrokovali incident;

(2) ponovno uspostavi sigurno stanje zahvaćenih elemenata definiranih u točki IS.AR.205 podtočki (a) unutar vremena oporavka koje je prethodno odredila njegova vlastita organizacija.

IS.AR.220 Ugovaranje aktivnosti upravljanja informacijskom sigurnošću

Nadležno tijelo osigurava da su pri ugovaranju bilo kojeg dijela aktivnosti iz točke IS.AR.200 s drugim organizacijama ugovorene aktivnosti u skladu sa zahtjevima ove Uredbe i da organizacija s kojom je sklopljen ugovor radi pod njegovim nadzorom. Nadležno tijelo osigurava da se rizicima povezanima s ugovorenim aktivnostima upravlja na odgovarajući način.

IS.AR.225 Zahtjevi u vezi s osobljem

Nadležno tijelo:

(a) mora imati osobu koja ima ovlast uspostaviti i održavati organizacijske strukture, politike, procese i postupke potrebne za provedbu ove Uredbe.

Ta osoba:

(1) mora imati ovlast za potpun pristup resursima koji su nadležnom tijelu potrebni za obavljanje svih zadaća u skladu s ovom Uredbom;

(2) mora imati delegiranu ovlast potrebnu za izvršavanje dodijeljenih dužnosti;

(b) mora imati uspostavljen postupak kojim se osigurava da ima dovoljno osoblja za obavljanje aktivnosti obuhvaćenih ovim Prilogom;

(c) mora imati uspostavljen postupak kojim se osigurava da osoblje iz podtočke (b) ima potrebnu stručnost za obavljanje zadaća;

(d) mora imati uspostavljen postupak kojim se osigurava da je osoblje upoznato s odgovornostima povezanima s dodijeljenim ulogama i zadaćama;

(e) osigurava da su identitet i pouzdanost osoblja koje ima pristup informacijskim sustavima i podacima podložno zahtjevima ove Uredbe primjereno utvrđeni.

IS.AR.230 Vođenje evidencije

(a) Nadležno tijelo vodi evidenciju o svojim aktivnostima upravljanja informacijskom sigurnošću.

(1) Nadležno tijelo osigurava arhiviranje i sljedivost sljedeće evidencije:

i. ugovora za aktivnosti iz točke IS.AR.200 podtočke (a) podpodtočke 5.;

ii. evidencije ključnih procesa iz točke IS.AR.200 podtočke (d);

iii. evidencije o rizicima utvrđenima u procjeni rizika iz točke IS.AR.205 i povezanim mjerama postupanja s rizicima iz točke IS.AR.210;

iv. evidencije o događajima povezanima s informacijskom sigurnošću koje će možda trebati ponovno procijeniti kako bi se otkrili neotkriveni incidenti ili ranjivosti povezani s informacijskom sigurnošću.

(2) Evidencija iz podpodtočke 1. podpodpodtočke i. čuva se najmanje pet godina nakon izmjene ili raskida ugovora.

(3) Evidencija iz podpodtočke 1. podpodpodtočaka ii. i iii. čuva se najmanje pet godina.

(4) Evidencija iz podpodtočke 1. podpodpodtočke iv. čuva se dok se ti događaji povezani s informacijskom sigurnošću ponovno ne procijene u skladu s učestalošću utvrđenom u postupku koji je utvrdilo nadležno tijelo.

(b) Nadležno tijelo vodi evidenciju o kvalifikacijama i iskustvu vlastitog osoblja uključenog u aktivnosti upravljanja informacijskom sigurnošću.

(1) Evidencija o kvalifikacijama i iskustvu osoblja čuva se sve dok osoba radi za nadležno tijelo i najmanje tri godine nakon što je osoba napustila nadležno tijelo.

(2) Članovima osoblja na njihov se zahtjev daje pristup njihovim pojedinačnim evidencijama. Osim toga, nadležno tijelo im na zahtjev po napuštanju nadležnog tijela dostavlja presliku njihove pojedinačne evidencije.

(c) Format evidencije mora biti određen u postupcima nadležnog tijela.

(d) Evidencija se čuva na način kojim se osigurava zaštita od oštećenja, preinake i krađe, a informacije se prema potrebi identificira u skladu s njihovim stupnjem tajnosti. Nadležno tijelo osigurava da se evidencija čuva na način kojim se osiguravaju integritet, autentičnost i odobren pristup.

IS.AR.235 Kontinuirano poboljšavanje

(a) Nadležno tijelo procjenjuje, koristeći odgovarajuće pokazatelje uspješnosti, djelotvornost i zrelost vlastitog ISMS-a. Ta se procjena provodi na temelju unaprijed određenog kalendara koji je definiralo nadležno tijelo ili nakon incidenta povezanog s informacijskom sigurnošću.

(b) Ako se nakon procjene provedene u skladu s podtočkom (a) utvrde nedostaci, nadležno tijelo poduzima potrebne mjere za poboljšanje kako bi osiguralo da ISMS i dalje ispunjava primjenjive zahtjeve i održava rizike za informacijsku sigurnost na prihvatljivoj razini. Osim toga, nadležno tijelo ponovno procjenjuje one elemente ISMS-a na koje utječu donesene mjere.

PRILOG II.

INFORMACIJSKA SIGURNOST – ZAHTJEVI U VEZI S ORGANIZACIJAMA

[DIO IS.I.OR]

IS.I.OR.100 Područje primjene

IS.I.OR.200 Sustav upravljanja informacijskom sigurnošću (ISMS)

IS.I.OR.205 Procjena rizika za informacijsku sigurnost

IS.I.OR.210 Postupanje s rizicima za informacijsku sigurnost

IS.I.OR.215 Sustav unutarnjeg izvješćivanja o informacijskoj sigurnosti

IS.I.OR.220 Incidenti povezani s informacijskom sigurnošću – otkrivanje, odgovor i oporavak

IS.I.OR.225 Odgovor na nalaze koje je prijavilo nadležno tijelo

IS.I.OR.230 Sustav vanjskog izvješćivanja o informacijskoj sigurnosti

IS.I.OR.235 Ugovaranje aktivnosti upravljanja informacijskom sigurnošću

IS.I.OR.240 Zahtjevi u vezi s osobljem

IS.I.OR.245 Vođenje evidencije

IS.I.OR.250 Priručnik za upravljanje informacijskom sigurnošću (ISMM)

IS.I.OR.255 Promjene sustava upravljanja informacijskom sigurnošću

IS.I.OR.260 Kontinuirano poboljšavanje

IS.I.OR.100 Područje primjene

U ovom se dijelu utvrđuju zahtjevi koje moraju ispuniti organizacije iz članka 2. stavka 1. ove Uredbe.

IS.I.OR.200 Sustav upravljanja informacijskom sigurnošću (ISMS)

(a) Kako bi se ostvarili ciljevi utvrđeni u članku 1., organizacija uspostavlja, provodi i održava sustav upravljanja informacijskom sigurnošću (ISMS) kojim se osigurava da organizacija:

(1) uspostavlja politiku informacijske sigurnosti kojom se utvrđuju opća načela organizacije u pogledu mogućeg utjecaja rizika za informacijsku sigurnost na sigurnost zračnog prometa;

(2) identificira i preispituje rizike za informacijsku sigurnost u skladu s točkom IS.I.OR.205;

(3) definira i provodi mjere postupanja s rizicima za informacijsku sigurnost u skladu s točkom IS.I.OR.210;

(4) primjenjuje sustav unutarnjeg izvješćivanja o informacijskoj sigurnosti u skladu s točkom IS.I.OR.215;

(5) u skladu s točkom IS.I.OR.220 definira i provodi mjere potrebne za otkrivanje događaja povezanih s informacijskom sigurnošću, identificira događaje koji se smatraju incidentima koji mogu utjecati na sigurnost zračnog prometa, osim u slučajevima koji su dopušteni točkom IS.I.OR.205 podtočkom (e), odgovara na te incidente i oporavlja se od njih;

(6) provodi mjere koje je nadležno tijelo prijavilo kao neposrednu reakciju na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa;

(7) poduzima odgovarajuće mjere u skladu s točkom IS.I.OR.225 kako bi postupilo u skladu s nalazima koje je prijavilo nadležno tijelo;

(8) provodi sustav vanjskog izvješćivanja u skladu s točkom IS.I.OR.230 kako bi se nadležnom tijelu omogućilo poduzimanje odgovarajućih mjera;

(9) ispunjava zahtjeve iz točke IS.I.OR.235 pri ugovaranju bilo kojeg dijela aktivnosti iz točke IS.I.OR.200 s drugim organizacijama;

(10) ispunjava zahtjeve u vezi s osobljem utvrđene u točki IS.I.OR.240;

(11) ispunjava zahtjeve u vezi s vođenjem evidencije utvrđene u točki IS.I.OR.245;

(12) prati usklađenost organizacije sa zahtjevima ove Uredbe i pruža povratne informacije o nalazima odgovornom rukovoditelju kako bi se osigurala djelotvorna provedba korektivnih mjera;

(13) ne dovodeći u pitanje primjenjive zahtjeve za izvješćivanje o incidentima, štiti povjerljivost svih informacija koje je organizacija primila od drugih organizacija, u skladu s njihovom razinom osjetljivosti.

(b) Kako bi kontinuirano ispunjavala zahtjeve iz članka 1., organizacija provodi postupak kontinuiranog poboljšavanja u skladu s točkom IS.I.OR.260.

(c) Organizacija u skladu s točkom IS.I.OR.250 dokumentira sve ključne procese, postupke, uloge i odgovornosti potrebne za usklađivanje s točkom IS.I.OR.200 podtočkom (a) i uspostavlja postupak za izmjenu te dokumentacije. Promjenama tih procesa, postupaka, uloga i odgovornosti upravlja se u skladu s točkom IS.I.OR.255.

(d) Procesi, postupci, uloge i odgovornosti koje je organizacija uspostavila radi usklađenosti s točkom IS.I.OR.200 podtočkom (a) odgovaraju prirodi i složenosti njezinih aktivnosti, na temelju procjene rizika za informacijsku sigurnost svojstvenih tim aktivnostima, i mogu se integrirati u druge postojeće sustave upravljanja koje organizacija već primjenjuje.

(e) Ne dovodeći u pitanje obvezu ispunjavanja zahtjeva za izvješćivanje utvrđenih u Uredbi (EU) br. 376/2014 i zahtjeve utvrđene u točki IS.I.OR.200 podtočki (a) podpodtočki 13., nadležno tijelo može organizaciji odobriti neprimjenjivanje zahtjeva iz podtočaka od (a) do (d) i povezanih zahtjeva iz točaka od IS.I.OR.205 do IS.I.OR.260 ako na zadovoljavajući način dokaže tom tijelu da njezine aktivnosti, objekti i resursi, kao i usluge koje pruža, prima i održava, njoj samoj ni drugim organizacijama ne predstavljaju nikakve rizike za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa. Odobrenje se temelji na dokumentiranoj procjeni rizika za informacijsku sigurnost koju je provela organizacija ili treća strana u skladu s točkom IS.I.OR.205 i pregledalo i odobrilo nadležno tijelo.

Nadležno tijelo preispitat će kontinuiranu valjanost tog odobrenja nakon primjenjivog ciklusa nadzora sigurnosti i kad god se provedu promjene u opsegu rada organizacije.

IS.I.OR.205 Procjena rizika za informacijsku sigurnost

(a) Organizacija je dužna identificirati sve svoje elemente koji bi mogli biti izloženi rizicima za informacijsku sigurnost. To uključuje:

(1) aktivnosti, objekte i resurse organizacije, kao i usluge koje organizacija pruža, prima ili održava;

(2) opremu, sustave, podatke i informacije koji pridonose funkcioniranju elemenata navedenih u podpodtočki 1.

(b) Organizacija mora identificirati sučelja koja ima s drugim organizacijama i koja bi mogla dovesti do međusobne izloženosti rizicima za informacijsku sigurnost.

(c) U pogledu elemenata i sučelja iz podtočaka (a) i (b), organizacija mora identificirati rizike za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa. Za svaki identificirani rizik organizacija je dužna:

(1) odrediti razinu rizika u skladu s unaprijed definiranom klasifikacijom koju je utvrdila organizacija;

(2) povezati svaki rizik i njegovu razinu s odgovarajućim elementom ili sučeljem utvrđenim u skladu s podtočkama (a) i (b).

U unaprijed definiranoj klasifikaciji iz podpodtočke 1. uzimaju se u obzir mogućnost pojave scenarija prijetnje i ozbiljnost njegovih posljedica za sigurnost. Na temelju te klasifikacije i uzimajući u obzir ima li organizacija strukturiran i ponovljiv postupak upravljanja rizicima za operacije, organizacija može utvrditi je li rizik prihvatljiv ili je s njim potrebno postupati u skladu s točkom IS.I.OR.210.

Kako bi se olakšala međusobna usporedivost procjena rizika, pri određivanju razine rizika u skladu s podpodtočkom 1. uzimaju se u obzir relevantne informacije prikupljene u koordinaciji s organizacijama iz podtočke (b).

(d) Organizacija pregledava i ažurira procjenu rizika provedenu u skladu s podtočkama (a) i (b) te prema potrebi podtočkom (c) ili (e) u bilo kojoj od sljedećih situacija:

(1) došlo je do promjene elemenata koji su izloženi rizicima za informacijsku sigurnost;

(2) došlo je do promjene u sučeljima između organizacije i drugih organizacija ili u rizicima koje su priopćile druge organizacije;

(3) došlo je do promjene informacija ili znanja koji se upotrebljavaju za identifikaciju, analizu i klasifikaciju rizika;

(4) izvučene su pouke na temelju analize incidenata povezanih s informacijskom sigurnošću.

(e) Odstupajući od podtočke (c), organizacije koje moraju biti usklađene s poddijelom C Priloga III. (dio ATM/ANS.OR) Provedbenoj uredbi (EU) 2017/373 zamjenjuju analizu utjecaja na sigurnost zračnog prometa analizom utjecaja na vlastite usluge u skladu s ocjenjivanjem sigurnosne podrške koje se zahtijeva točkom ATM/ANS.OR.C.005. To ocjenjivanje sigurnosne podrške stavlja se na raspolaganje pružateljima usluga zračnog prometa kojima one pružaju usluge i ti pružatelji usluga zračnog prometa odgovorni su za evaluaciju utjecaja na sigurnost zračnog prometa.

IS.I.OR.210 Postupanje s rizicima za informacijsku sigurnost

(a) Organizacija osmišljava mjere za otklanjanje neprihvatljivih rizika identificiranih u skladu s točkom IS.I.OR.205, pravodobno ih provodi i provjerava njihovu kontinuiranu djelotvornost. Te mjere omogućuju da organizacija:

(1) kontrolira okolnosti koje pridonose stvarnoj pojavi scenarija prijetnje;

(2) ublaži posljedice za sigurnost zračnog prometa povezane s nastankom scenarija prijetnje;

(3) izbjegava rizike.

Te mjere ne smiju uvesti nove neprihvatljive rizike za sigurnost zračnog prometa.

(b) Osoba iz točke IS.I.OR.240 podtočaka (a) i (b) i drugo uključeno osoblje organizacije obavješćuju se o ishodu procjene rizika provedene u skladu s točkom IS.I.OR.205, odgovarajućim scenarijima prijetnji i mjerama koje treba provesti.

Organizacija obavješćuje i organizacije s kojima ima sučelje u skladu s točkom IS.I.OR.205 podtočkom (b) o svim rizicima koji su zajednički objema organizacijama.

IS.I.OR.215 Sustav unutarnjeg izvješćivanja o informacijskoj sigurnosti

(a) Organizacija uspostavlja sustav unutarnjeg izvješćivanja radi prikupljanja i procjene događaja povezanih s informacijskom sigurnošću, uključujući one o kojima treba izvješćivati u skladu s točkom IS.I.OR.230.

(b) Taj sustav i postupak iz točke IS.I.OR.220 omogućuju da organizacija:

(1) identificira događaje prijavljene u skladu s podtočkom (a) koji se smatraju incidentima ili ranjivostima povezanima s informacijskom sigurnošću koji mogu utjecati na sigurnost zračnog prometa;

(2) identificira uzroke incidenata i ranjivosti povezanih s informacijskom sigurnošću utvrđenih u skladu s podpodtočkom 1. i čimbenike koji im doprinose i rješava ih u okviru procesa upravljanja rizicima za informacijsku sigurnost u skladu s točkama IS.I.OR.205 i IS.I.OR.220;

(3) osigura procjenu svih poznatih i relevantnih informacija koje se odnose na incidente i ranjivosti povezane s informacijskom sigurnošću i identificirane u skladu s podpodtočkom 1.;

(4) osigura primjenu metode za internu distribuciju informacija prema potrebi.

(c) Svaka ugovorna organizacija koja organizaciju može izložiti rizicima za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa mora organizaciju izvijestiti o događajima povezanima s informacijskom sigurnošću. Ta se izvješća podnose primjenom postupaka utvrđenih u posebnim ugovornim aranžmanima i ocjenjuju se u skladu s podtočkom (b).

(d) Organizacija surađuje u istragama sa svakom drugom organizacijom koja znatno pridonosi informacijskoj sigurnosti vlastitih aktivnosti.

(e) Organizacija može integrirati taj sustav izvješćivanja s drugim sustavima izvješćivanja koje je već uvela.

IS.I.OR.220 Incidenti povezani s informacijskom sigurnošću – otkrivanje, odgovor i oporavak

(a) Na temelju rezultata procjene rizika provedene u skladu s točkom IS.I.OR.205 i ishoda postupanja s rizicima provedenog u skladu s točkom IS.I.OR.210, organizacija provodi mjere za otkrivanje incidenata i ranjivosti koje ukazuju na moguću pojavu neprihvatljivih rizika i koje bi mogle utjecati na sigurnost zračnog prometa. Te mjere otkrivanja omogućuju da organizacija:

(1) identificira odstupanja od unaprijed utvrđenih osnovnih vrijednosti funkcionalne učinkovitosti;

(2) aktivira upozorenja za primjenu odgovarajućih mjera odgovora u slučaju bilo kakvog odstupanja.

(b) Organizacija provodi mjere odgovora na sve uvjete događaja identificiranih u podtočki (a) koji mogu postati ili su postali incident povezan s informacijskom sigurnošću. Te mjere odgovora omogućuju da organizacija:

(1) pokrene reakciju na upozorenja iz podtočke (a) podpodtočke 2. aktiviranjem unaprijed definiranih resursa i načina postupanja;

(2) ograniči širenje napada i izbjegne potpuno ostvarenje scenarija prijetnje;

(3) kontrolira zakazivanje zahvaćenih elemenata definiranih u točki IS.I.OR.205 podtočki (a).

(c) Organizacija provodi mjere čiji je cilj oporavak od incidenata povezanih s informacijskom sigurnošću, uključujući hitne mjere, prema potrebi. Te mjere oporavka omogućuju da organizacija:

(1) ukloni ili ograniči na prihvatljivu razinu uvjete koji su uzrokovali incident;

(2) ostvari sigurno stanje zahvaćenih elemenata definiranih u točki IS.I.OR.205 podtočki (a) unutar vremena oporavka koje je prethodno odredila organizacija.

IS.I.OR.225 Odgovor na nalaze koje je prijavilo nadležno tijelo

(a) Nakon primitka obavijesti o nalazima koju je dostavilo nadležno tijelo, organizacija:

(1) utvrđuje temeljni uzrok ili temeljne uzroke neusklađenosti i čimbenike koji tomu doprinose;

(2) utvrđuje plan korektivnih mjera;

(3) dokazuje korekciju neusklađenosti na način prihvatljiv nadležnom tijelu.

(b) Mjere iz podtočke (a) provode se u razdoblju dogovorenom s nadležnim tijelom.

IS.I.OR.230 Sustav vanjskog izvješćivanja o informacijskoj sigurnosti

(a) Organizacija primjenjuje sustav izvješćivanja o informacijskoj sigurnosti koji je u skladu sa zahtjevima utvrđenima u Uredbi (EU) br. 376/2014 i njezinim delegiranim i provedbenim aktima ako se ta uredba primjenjuje na nju.

(b) Ne dovodeći u pitanje obveze iz Uredbe (EU) br. 376/2014, organizacija osigurava da se nadležnom tijelu prijavljuje svaki incident ili ranjivost povezana s informacijskom sigurnošću koji mogu predstavljati znatan rizik za sigurnost zračnog prometa. Nadalje:

(1) ako takav incident ili ranjivost utječe na zrakoplov ili povezani sustav ili sastavni dio, organizacija o tome također izvješćuje nositelja odobrenja projekta;

(2) ako takav incident ili ranjivost utječe na sustav ili sastavni dio koji upotrebljava organizacija, ona o tome izvješćuje organizaciju odgovornu za projektiranje sustava ili sastavnog dijela.

(c) Organizacija izvješćuje o stanju iz podtočke (b) kako slijedi:

(1) obavijest se dostavlja nadležnom tijelu i, ako je primjenjivo, nositelju odobrenja projekta ili organizaciji odgovornoj za projektiranje sustava ili sastavnog dijela čim organizacija bude upoznata s tim stanjem;

(2) izvješće se dostavlja nadležnom tijelu i, ako je primjenjivo, nositelju odobrenja projekta ili organizaciji odgovornoj za projektiranje sustava ili sastavnog dijela što prije, ali najkasnije 72 sata od trenutka kad je organizacija upoznata s tim stanjem, osim ako to spriječe izvanredne okolnosti.

Izvješće se sastavlja u obliku koji određuje nadležno tijelo i sadržava sve relevantne informacije o stanju koje je poznato organizaciji;

(3) izvješće o daljnjim mjerama podnosi se nadležnom tijelu i, ako je primjenjivo, nositelju odobrenja projekta ili organizaciji odgovornoj za projektiranje sustava ili sastavnog dijela te sadržava pojedinosti o mjerama koje je organizacija poduzela ili koje namjerava poduzeti kako bi se oporavila od incidenta i mjerama koje namjerava poduzeti kako bi spriječila slične incidente povezane s informacijskom sigurnošću u budućnosti.

Izvješće o daljnjim mjerama podnosi se čim se utvrde te mjere i sastavlja se u obliku koji odredi nadležno tijelo.

IS.I.OR.235 Ugovaranje aktivnosti upravljanja informacijskom sigurnošću

(a) Organizacija osigurava da su pri ugovaranju bilo kojeg dijela aktivnosti iz točke IS.I.OR.200 s drugim organizacijama ugovorene aktivnosti u skladu sa zahtjevima ove Uredbe i da organizacija s kojom je sklopljen ugovor radi pod njezinim nadzorom. Organizacija osigurava da se rizicima povezanima s ugovorenim aktivnostima upravlja na odgovarajući način.

(b) Organizacija osigurava da nadležno tijelo na zahtjev može imati pristup organizaciji s kojom je sklopljen ugovor kako bi se utvrdila kontinuirana usklađenost s primjenjivim zahtjevima utvrđenima u ovoj Uredbi.

IS.I.OR.240 Zahtjevi u vezi s osobljem

(a) Odgovorni rukovoditelj organizacije imenovan u skladu s uredbama (EU) br. 1321/2014, (EU) br. 965/2012, (EU) br. 1178/2011, (EU) 2015/340, Provedbenom uredbom (EU) 2017/373 ili Provedbenom uredbom (EU) 2021/664, kako je primjenjivo u skladu s člankom 2. stavkom 1. ove Uredbe, ima statutarnu ovlast osigurati financiranja i provedbe svih aktivnosti koje se zahtijevaju ovom Uredbom. Ta osoba mora:

(1) osigurati dostupnost svih potrebnih sredstava za ispunjavanje zahtjeva ove Uredbe;

(2) uspostaviti i promicati politiku informacijske sigurnosti iz točke IS.I.OR.200 podtočke (a) podpodtočke 1.;

(3) pokazati osnovno razumijevanje ove Uredbe.

(b) Odgovorni rukovoditelj imenuje osobu ili skupinu osoba za osiguravanje da organizacija ispunjava zahtjeve ove Uredbe i određuje opseg njihovih ovlasti. Ta osoba ili skupina osoba izravno odgovara odgovornom rukovoditelju i mora imati odgovarajuće znanje, obrazovanje i iskustvo za izvršavanje svojih odgovornosti. U postupcima se određuje tko zamjenjuje određenu osobu u slučaju njezine dugotrajne odsutnosti.

(c) Odgovorni rukovoditelj imenuje osobu ili skupinu osoba za upravljanje funkcijom praćenja usklađenosti iz točke IS.I.OR.200 podtočke (a) podpodtočke 12.

(d) Ako organizacija dijeli organizacijske strukture, politike, procese i postupke povezane s informacijskom sigurnošću s drugim organizacijama ili područjima aktivnosti u vlastitoj organizaciji koja nisu dio odobrenja ili izjave, odgovorni rukovoditelj može povjeriti te aktivnosti zajedničkoj odgovornoj osobi.

U tom slučaju uspostavljaju se mjere koordinacije između odgovornog rukovoditelja organizacije i zajedničke odgovorne osobe kako bi se osigurala odgovarajuća integracija upravljanja informacijskom sigurnošću unutar organizacije.

(e) Odgovorni rukovoditelj ili zajednička odgovorna osoba iz podtočke (d) ima statutarnu ovlast uspostaviti i održavati organizacijske strukture, politike, procese i postupke potrebne za primjenu točke IS.I.OR.200.

(f) Organizacija mora imati uspostavljen postupak kojim se osigurava da ima dovoljno osoblja za obavljanje aktivnosti obuhvaćenih ovim Prilogom.

(g) Organizacija mora imati uspostavljen postupak kojim se osigurava da osoblje iz podtočke (f) ima potrebnu stručnost za obavljanje zadaća.

(h) Organizacija mora imati uspostavljen postupak kojim se osigurava da je osoblje upoznato s odgovornostima povezanima s dodijeljenim ulogama i zadaćama.

(i) Organizacija osigurava da su identitet i pouzdanost osoblja koje ima pristup informacijskim sustavima i podacima podložno zahtjevima ove Uredbe primjereno utvrđeni.

IS.I.OR.245 Vođenje evidencije

(a) *Organizacija vodi evidenciju o svojim aktivnostima upravljanja informacijskom sigurnošću.*

(1) Organizacija osigurava arhiviranje i sljedivost sljedeće evidencije:

i. svih primljenih odobrenja i svih povezanih procjena rizika za informacijsku sigurnost u skladu s točkom IS.I.OR.200 podtočkom (e);

ii. ugovora za aktivnosti iz točke IS.I.OR.200 podtočke (a) podpodtočke 9.;

iii. evidencije ključnih procesa iz točke IS.I.OR.200 podtočke (d);

iv. evidencije o rizicima utvrđenima u procjeni rizika iz točke IS.I.OR.205 i povezanim mjerama postupanja s rizicima iz točke IS.I.OR.210;

v. evidencije o incidentima i ranjivostima povezanima s informacijskom sigurnošću prijavljenima u skladu sa sustavima izvješćivanja iz točaka IS.I.OR.215 i IS.I.OR.230;

vi. evidencije o događajima povezanima s informacijskom sigurnošću koje će možda trebati ponovno procijeniti kako bi se otkrili neotkriveni incidenti ili ranjivosti povezani s informacijskom sigurnošću.

(2) Evidencija iz podpodtočke 1. podpodpodtočke i. čuva se najmanje pet godina nakon što odobrenje prestane važiti.

(3) Evidencija iz podpodtočke 1. podpodpodtočke ii. čuva se najmanje pet godina nakon izmjene ili raskida ugovora.

(4) Evidencija iz podpodtočke 1. podpodpodtočaka iii., iv. i v. čuva se najmanje pet godina.

(5) Evidencija iz podpodtočke 1. podpodpodtočke vi. čuva se dok se ti događaji povezani s informacijskom sigurnošću ponovno ne procijene u skladu s učestalošću utvrđenom u postupku koji je utvrdila organizacija.

(b) *Organizacija vodi evidenciju o kvalifikacijama i iskustvu vlastitog osoblja uključenog u aktivnosti upravljanja informacijskom sigurnošću.*

(1) Evidencija o kvalifikacijama i iskustvu osoblja čuva se sve dok osoba radi za organizaciju i najmanje tri godine nakon što je osoba napustila organizaciju.

(2) Članovima osoblja na njihov se zahtjev daje pristup njihovim pojedinačnim evidencijama. Osim toga, organizacija im na zahtjev po napuštanju organizacije dostavlja presliku njihove pojedinačne evidencije.

(c) Format evidencije mora biti određen u postupcima organizacije.

(d) Evidencija se čuva na način kojim se osigurava zaštita od oštećenja, preinake i krađe, a informacije se prema potrebi identificira u skladu s njihovim stupnjem tajnosti. Organizacija osigurava da se evidencija čuva na način kojim se osiguravaju integritet, autentičnost i odobren pristup.

IS.I.OR.250 Priručnik za upravljanje informacijskom sigurnošću (ISMM)

(a) Organizacija nadležnom tijelu stavlja na raspolaganje priručnik za upravljanje informacijskom sigurnošću (ISMM) i, ako je primjenjivo, sve povezane priručnike i postupke na koje se upućuje, koji sadržavaju:

(1) izjavu koju je potpisao odgovorni rukovoditelj kojom se potvrđuje da će organizacija uvijek raditi u skladu s ovim Prilogom i ISMM-om. Ako odgovorni rukovoditelj nije glavni izvršni direktor (CEO) organizacije, glavni izvršni direktor supotpisuje izjavu;

(2) titule, imena, dužnosti, odgovornosti i ovlasti osobe ili osoba iz točke IS.I.OR.240 podtočaka (b) i (c);

(3) titulu, ime, dužnosti, odgovornosti i ovlasti zajedničke odgovorne osobe iz točke IS.I.OR.240 podtočke (d), ako je primjenjivo;

(4) politiku informacijske sigurnosti organizacije iz točke IS.I.OR.200 podtočke (a) podpodtočke 1.;

(5) opći opis broja i kategorija osoblja i uspostavljenog sustava za planiranje raspoloživosti osoblja kako je propisano točkom IS.I.OR.240;

(6) titule, imena, dužnosti, odgovornosti i ovlasti ključnih osoba odgovornih za primjenu točke IS.I.OR.200, uključujući osobu ili osobe odgovorne za funkciju praćenja usklađenosti iz točke IS.I.OR.200 podtočke (a) podpodtočke 12.;

(7) organigram koji prikazuje povezane lance odgovornosti za osobe iz podpodtočaka 2. i 6.;

(8) opis sustava unutarnjeg izvješćivanja iz točke IS.I.OR.215;

(9) postupke kojima se utvrđuje kako organizacija osigurava usklađenost s ovim dijelom, a posebno:

i. dokumentaciju iz točke IS.I.OR.200 podtočke (c);

ii. postupke kojima se definira kako organizacija kontrolira sve ugovorene aktivnosti iz točke IS.I.OR.200 podtočke (a) podpodtočke 9.;

iii. postupak izmjene ISMM-a iz podtočke (c);

(10) popis trenutačno odobrenih alternativnih načina usklađivanja.

(b) Prvo izdanje ISMM-a odobrava se, a jedan primjerak zadržava nadležno tijelo. ISMM se izmjenjuje prema potrebi kako bi kontinuirano bio ažurni opis ISMS-a organizacije. Primjerak svih izmjena ISMM-a dostavlja se nadležnom tijelu.

(c) Izmjenama ISMM-a upravlja se u skladu s postupkom koji utvrđuje organizacija. Sve izmjene koje nisu obuhvaćene ovim postupkom te izmjene povezane s promjenama navedenima u točki IS.I.OR.255 podtočki (b) odobrava nadležno tijelo.

(d) Organizacija može integrirati ISMM s drugim priručnicima za upravljanje ili priručnicima koje pohranjuje, pod uvjetom da postoji jasno unakrsno upućivanje koje pokazuje koji dijelovi priručnika za upravljanje odgovaraju različitim zahtjevima sadržanima u ovom Prilogu.

IS.I.OR.255 Promjene sustava upravljanja informacijskom sigurnošću

(a) Promjenama ISMS-a može se upravljati i o njima obavijestiti nadležno tijelo provedbom postupka koji je razvila organizacija. Taj postupak odobrava nadležno tijelo.

(b) Kad je riječ o promjenama ISMS-a koje nisu obuhvaćene postupkom iz podtočke (a), organizacija podnosi zahtjev i dobiva odobrenje koje izdaje nadležno tijelo.

U vezi s tim promjenama:

(1) zahtjev se podnosi prije uvođenja bilo kakve takve promjene, kako bi nadležno tijelo moglo utvrditi kontinuiranu usklađenost s ovom Uredbom i, prema potrebi, izmijeniti certifikat organizacije i povezane uvjete odobrenja koji su mu priloženi;

(2) organizacija nadležnom tijelu stavlja na raspolaganje sve informacije koje zatraži radi ocjene promjene;

(3) promjena se provodi tek nakon primitka službenog odobrenja nadležnog tijela;

(4) organizacija mora postupati u skladu s uvjetima koje je propisalo nadležno tijelo tijekom provedbe takvih promjena.

IS.I.OR.260 Kontinuirano poboljšavanje

(a) Organizacija procjenjuje, koristeći odgovarajuće pokazatelje uspješnosti, djelotvornost i zrelost ISMS-a. Ta se procjena provodi na temelju kalendara koji je unaprijed odredila organizacija ili nakon incidenta povezanog s informacijskom sigurnošću.

(b) Ako se nakon procjene provedene u skladu s podtočkom (a) utvrde nedostaci, organizacija poduzima potrebne mjere za poboljšanje kako bi osigurala da ISMS i dalje ispunjava primjenjive zahtjeve i održava rizike za informacijsku sigurnost na prihvatljivoj razini. Osim toga, organizacija ponovno procjenjuje one elemente ISMS-a na koje utječu donesene mjere.

PRILOG III.

Prilozi VI. (dio-ARA) i VII. (dio-ORA) Uredbi (EU) br. 1178/2011 mijenjaju se kako slijedi:

(1) Prilog VI. (dio-ARA) mijenja se kako slijedi:

(a) u točki ARA.GEN.125 dodaje se sljedeća podtočka (c):

„(c) Nadležno tijelo države članice što prije obavještava Agenciju o informacijama važnima za sigurnost koje proizlaze iz izvješća o informacijskoj sigurnosti koje je zaprimilo u skladu s točkom IS.I.OR.230 Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203.";

(b) iza točke ARA.GEN.135 umeće se sljedeća točka ARA.GEN.135A:

„**ARA.GEN.135A Neposredna reakcija na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa**

(a) Nadležno tijelo uspostavlja sustav za primjereno prikupljanje, analizu i širenje informacija o incidentima i ranjivostima povezanima s informacijskom sigurnošću koji bi mogli utjecati na sigurnost zračnog prometa i o kojima izvješćuju organizacije. To se provodi u koordinaciji s drugim relevantnim tijelima koja su odgovorna za informacijsku sigurnost ili kibersigurnost u državi članici kako bi se poboljšale koordinacija i usklađenost sustava izvješćivanja.

(b) Agencija uspostavlja sustav za primjerenu analizu svih relevantnih informacija važnih za sigurnost koje zaprimi u skladu s točkom ARA.GEN.125 podtočkom (c) i bez nepotrebne odgode dostavlja državama članicama i Komisiji sve informacije, uključujući preporuke ili korektivne mjere koje se trebaju poduzeti, potrebne za pravodobnu reakciju na incident ili ranjivost povezanu s informacijskom sigurnošću koja bi mogla utjecati na sigurnost zračnog prometa i koja uključuje proizvode, dijelove, neugrađenu opremu, osobe ili organizacije podložne Uredbi (EU) 2018/1139 i njezinim delegiranim i provedbenim aktima.

(c) Nakon što zaprimi informacije iz podtočaka (a) i (b), nadležno tijelo poduzima prikladne mjere kako bi ispravno pristupilo mogućem utjecaju incidenta ili ranjivosti povezane s informacijskom sigurnošću na sigurnost zračnog prometa.

(d) O mjerama poduzetima u skladu s podtočkom (c) odmah se obavješćuju sve osobe ili organizacije koje moraju postupiti u skladu s tim mjerama na temelju Uredbe (EU) 2018/1139 i njezinih delegiranih i provedbenih akata. Nadležno tijelo države članice o tim mjerama također obavješćuje Agenciju i, ako je potrebno zajedničko djelovanje, nadležna tijela drugih predmetnih država članica.";

(c) u točki ARA.GEN.200 dodaje se sljedeća podtočka (e):

„(e) Uz zahtjeve iz podtočke (a) sustav upravljanja koji uspostavlja i održava nadležno tijelo mora biti usklađen s Prilogom I. (dio IS.AR) Provedbenoj uredbi (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.";

(d) točka ARA.GEN.205 mijenja se kako slijedi:

i. naslov se zamjenjuje sljedećim:

„**ARA.GEN.205 Dodjeljivanje zadataka**";

ii. dodaje se sljedeća podtočka (c):

„(c) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom ORA.GEN.200A nadležno tijelo može dodijeliti zadatke kvalificiranim subjektima u skladu s podtočkom (a) ili bilo kojem relevantnom tijelu koje je odgovorno za informacijsku sigurnost ili kibersigurnost u državi članici. Pri dodjeljivanju zadataka nadležno tijelo osigurava:

(1) da kvalificirani subjekt ili relevantno tijelo koordinira i uzima u obzir sve aspekte povezane sa sigurnosti zračnog prometa;

(2) da su rezultati aktivnosti certifikacije i nadzora koje obavlja kvalificirani subjekt ili relevantno tijelo uključeni u opće spise organizacije o certifikaciji i nadzoru;

(3) da njegov vlastiti sustav upravljanja informacijskom sigurnošću uspostavljen u skladu s točkom ARA.GEN.200 podtočkom (e) obuhvaća sve zadatke certifikacije i kontinuiranog nadzora koji se obavljaju u njegovo ime.";

(e) u točki ARA.GEN.300 dodaje se sljedeća podtočka (g):

„(g) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom ORA.GEN.200A nadležno tijelo, uz usklađivanje s točkama od (a) do (f), preispituje sva odobrenja izdana na temelju točke IS.I.OR.200 podtočke (e) ove Uredbe ili točke IS.D.OR.200 podtočke (e) Delegirane uredbe (EU) 2022/1645 nakon primjenjivog ciklusa nadzora sigurnosti i kad god se provedu promjene u opsegu rada organizacije.";

(f) iza točke ARA.GEN.330 umeće se sljedeća točka ARA.GEN.330A:

„**ARA.GEN.330A Promjene sustava upravljanja informacijskom sigurnošću**

(a) U vezi s promjenama kojima se upravlja i o kojima se obavješćuje nadležno tijelo u skladu s postupkom iz točke IS.I.OR.255 podtočke (a) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203 nadležno tijelo uključuje preispitivanje tih promjena u svoj kontinuirani nadzor u skladu s načelima utvrđenima u točki ARA.GEN.300. Ako se utvrdi bilo kakva neusklađenost, nadležno tijelo o tome obavješćuje organizaciju, zahtijeva daljnje promjene i postupa u skladu s točkom ARA.GEN.350.

(b) U vezi s drugim promjenama za koje je potreban zahtjev za odobrenje u skladu s točkom IS.I.OR.255 podtočkom (b) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203:

(1) nakon što zaprimi zahtjev za promjenu, nadležno tijelo provjerava usklađenost organizacije s primjenjivim zahtjevima prije izdavanja odobrenja;

(2) nadležno tijelo utvrđuje uvjete pod kojima organizacija može raditi tijekom provedbe promjene;

(3) ako utvrdi da organizacija ispunjava primjenjive zahtjeve, nadležno tijelo odobrava promjenu.";

(2) Prilog VII. (dio-ORA) mijenja se kako slijedi:

iza točke ORA.GEN.200 umeće se sljedeća točka ORA.GEN.200A:

„**ORA.GEN.200A Sustav upravljanja informacijskom sigurnošću**

Uz sustav upravljanja iz točke ORA.GEN.200 organizacija uspostavlja, provodi i održava sustav upravljanja informacijskom sigurnošću u skladu s Provedbenom uredbom (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.".

PRILOG IV.

Prilog I. (Part 21.) Uredbi (EU) br. 748/2012 mijenja se kako slijedi:

(1) sadržaj se mijenja kako slijedi:

(a) iza naslova 21.B.20 umeće se sljedeći naslov:

„21.B.20A Neposredna reakcija na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa”;

(b) naslov točke 21.B.30 zamjenjuje se sljedećim:

„21.B.30 Dodjeljivanje zadataka”;

(c) iza naslova 21.B.240 umeće se sljedeći naslov:

„21.B.240A Promjene sustava upravljanja informacijskom sigurnošću”;

(d) iza naslova 21.B.435 umeće se sljedeći naslov:

„21.B.435A Promjene sustava upravljanja informacijskom sigurnošću”;

(2) u točki 21.B.15 dodaje se sljedeća podtočka (c):

„(c) Nadležno tijelo države članice što prije obavještava Agenciju o informacijama važnima za sigurnost koje proizlaze iz izvješća o informacijskoj sigurnosti koje je zaprimilo u skladu s točkom IS.D.OR.230 Priloga (dio IS.D.OR) Delegiranoj uredbi (EU) 2022/1645”;

(3) iza točke 21.B.20 umeće se sljedeća točka 21.B.20A:

„21.B.20A Neposredna reakcija na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa

(a) Nadležno tijelo uspostavlja sustav za primjereno prikupljanje, analizu i širenje informacija o incidentima i ranjivostima povezanima s informacijskom sigurnošću koji bi mogli utjecati na sigurnost zračnog prometa i o kojima izvješćuju organizacije. To se provodi u koordinaciji s drugim relevantnim tijelima koja su odgovorna za informacijsku sigurnost ili kibersigurnost u državi članici kako bi se poboljšale koordinacija i usklađenost sustava izvješćivanja.

(b) Agencija uspostavlja sustav za primjerenu analizu svih relevantnih informacija važnih za sigurnost koje zaprimi u skladu s točkom 21.B.15 podtočkom (c) i bez nepotrebne odgode dostavlja državama članicama i Komisiji sve informacije, uključujući preporuke ili korektivne mjere koje se trebaju poduzeti, potrebne za pravodobnu reakciju na incident ili ranjivost povezanu s informacijskom sigurnošću koja bi mogla utjecati na sigurnost zračnog prometa i koja uključuje proizvode, dijelove, neugrađenu opremu, osobe ili organizacije podložne Uredbi (EU) 2018/1139 i njezinim delegiranim i provedbenim aktima.

(c) Nakon što zaprimi informacije iz podtočaka (a) i (b), nadležno tijelo poduzima prikladne mjere kako bi ispravno pristupilo mogućem utjecaju incidenta ili ranjivosti povezane s informacijskom sigurnošću na sigurnost zračnog prometa.

(d) O mjerama poduzetima u skladu s podtočkom (c) odmah se obavješćuju sve osobe ili organizacije koje moraju postupiti u skladu s tim mjerama na temelju Uredbe (EU) 2018/1139 i njezinih delegiranih i provedbenih akata. Nadležno tijelo države članice o tim mjerama također obavješćuje Agenciju i, ako je potrebno zajedničko djelovanje, nadležna tijela drugih predmetnih država članica.”;

(4) u točki 21.B.25 dodaje se sljedeća podtočka (e):

„(e) Uz zahtjeve iz podtočke (a) sustav upravljanja koji uspostavlja i održava nadležno tijelo mora biti usklađen s Prilogom I. (dio IS.AR) Provedbenoj uredbi (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.”;

(5) točka 21.B.30 mijenja se kako slijedi:

(a) naslov se zamjenjuje sljedećim:

„21.B.30 Dodjeljivanje zadataka”;

(b) dodaje se sljedeća podtočka (c):

„(c) Za certifikaciju i nadzor usklađenosti organizacije s točkama 21.A.139A i 21.A.239A nadležno tijelo može dodijeliti zadatke kvalificiranim subjektima u skladu s podtočkom (a) ili bilo kojem relevantnom tijelu koje je odgovorno za informacijsku sigurnost ili kibersigurnost u državi članici. Pri dodjeljivanju zadataka nadležno tijelo osigurava:

1. da kvalificirani subjekt ili relevantno tijelo koordinira i uzima u obzir sve aspekte povezane sa sigurnosti zračnog prometa;

2. da su rezultati aktivnosti certifikacije i nadzora koje obavlja kvalificirani subjekt ili relevantno tijelo uključeni u opće spise organizacije o certifikaciji i nadzoru;

3. da njegov vlastiti sustav upravljanja informacijskom sigurnošću uspostavljen u skladu s točkom 21.B.25 podtočkom (e) obuhvaća sve zadatke certifikacije i kontinuiranog nadzora koji se obavljaju u njegovo ime.”;

(6) u točki 21.B.221 dodaje se sljedeća podtočka (g):

„(g) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom 21.A.139A nadležno tijelo, uz usklađivanje s točkama od (a) do (f), preispituje sva odobrenja izdana na temelju točke IS.I.OR.200 podtočke (e) ove Uredbe ili točke IS.D.OR.200 podtočke (e) Delegirane uredbe (EU) 2022/1645 nakon primjenjivog ciklusa nadzora sigurnosti i kad god se provedu promjene u opsegu rada organizacije.”;

(7) iza točke 21.B.240 umeće se sljedeća točka 21.B.240A:

„**21.B.240A Promjene sustava upravljanja informacijskom sigurnošću**

(a) Za promjene kojima se upravlja i o kojima se obavješćuje nadležno tijelo u skladu s postupkom iz točke IS.D.OR.255 podtočke (a) Priloga (dio IS.D.OR) Delegiranoj uredbi (EU) 2022/1645 nadležno tijelo uključuje preispitivanje tih promjena u svoj kontinuirani nadzor u skladu s načelima utvrđenima u točki 21.B.221. Ako se utvrdi bilo kakva neusklađenost, nadležno tijelo o tome obavješćuje organizaciju, zahtijeva daljnje promjene i postupa u skladu s točkom 21.B.225.

(b) Za druge promjene za koje je potreban zahtjev za odobrenje u skladu s točkom IS.D.OR.255 podtočkom (b) Priloga (dio IS.D.OR) Delegiranoj uredbi (EU) 2022/1645:

1. nakon što zaprimi zahtjev za promjenu, nadležno tijelo provjerava usklađenost organizacije s primjenjivim zahtjevima prije izdavanja odobrenja;

2. nadležno tijelo utvrđuje uvjete pod kojima organizacija može raditi tijekom provedbe promjene;

3. ako utvrdi da organizacija ispunjava primjenjive zahtjeve, nadležno tijelo odobrava promjenu.”;

(8) u točki 21.B.431 dodaje se sljedeća podtočka (d):

„(d) Za certifikaciju i nadzor usklađenosti organizacije s točkom 21.A.239A nadležno tijelo, uz usklađivanje s točkama od (a) do (c), mora biti usklađeno sa sljedećim načelima:

1. nadležno tijelo mora preispitati sučelja i povezane rizike koje je u skladu s točkom IS.D.OR.205 podtočkom (b) Priloga (dio IS.D.OR) Delegiranoj uredbi (EU) 2022/1645 identificirala svaka organizacija koja je podložna njegovu nadzoru;

2. ako se utvrde odstupanja u zajedničkim sučeljima i povezanim rizicima koje su identificirale različite organizacije, nadležno tijelo mora ih preispitati s predmetnim organizacijama i prema potrebi iznijeti odgovarajuće nalaze kako bi se osigurala provedba korektivnih mjera;

3. ako se u dokumentaciji koja se preispituje u skladu s podpodtočkom 2. otkriju znatni rizici povezani sa sučeljima s organizacijama koje su podložne nadzoru drugog nadležnog tijela u istoj državi članici, o tome se mora obavijestiti odgovarajuće nadležno tijelo.”;

(9) iza točke 21.B.435 umeće se sljedeća točka 21.B.435A:

„21.B.435A Promjene sustava upravljanja informacijskom sigurnošću

(a) Za promjene kojima se upravlja i o kojima se obavješćuje nadležno tijelo u skladu s postupkom iz točke IS.D.OR.255 podtočke (a) Priloga (dio IS.D.OR) Delegiranoj uredbi (EU) 2022/1645 nadležno tijelo uključuje preispitivanje tih promjena u svoj kontinuirani nadzor u skladu s načelima utvrđenima u točki 21.B.431. Ako se utvrdi bilo kakva neusklađenost, nadležno tijelo o tome obavješćuje organizaciju, zahtijeva daljnje promjene i postupa u skladu s točkom 21.B.433.

(b) Za druge promjene za koje je potreban zahtjev za odobrenje u skladu s točkom IS.D.OR.255 podtočkom (b) Priloga (dio IS.D.OR) Delegiranoj uredbi (EU) 2022/1645:

1. nakon što zaprimi zahtjev za promjenu, nadležno tijelo provjerava usklađenost organizacije s primjenjivim zahtjevima prije izdavanja odobrenja;

2. nadležno tijelo utvrđuje uvjete pod kojima organizacija može raditi tijekom provedbe promjene;

3. ako utvrdi da organizacija ispunjava primjenjive zahtjeve, nadležno tijelo odobrava promjenu.”.

PRILOG V.

Prilozi II. (dio ARO) i III. (dio ORO) Uredbi (EU) br. 965/2012 mijenjaju se kako slijedi:

(1) Prilog II. (dio-ARO) mijenja se kako slijedi:

(a) u točki ARO.GEN.125 dodaje se sljedeća podtočka (c):

„(c) Nadležno tijelo države članice što prije obavještava Agenciju o informacijama važnima za sigurnost koje proizlaze iz izvješća o informacijskoj sigurnosti koje je zaprimilo u skladu s točkom IS.I.OR.230 Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203.";

(b) iza točke ARO.GEN.135 umeće se sljedeća točka ARO.GEN.135A:

„**ARO.GEN.135A Neposredna reakcija na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa**

(a) Nadležno tijelo uspostavlja sustav za primjereno prikupljanje, analizu i širenje informacija o incidentima i ranjivostima povezanima s informacijskom sigurnošću koji bi mogli utjecati na sigurnost zračnog prometa i o kojima izvješćuju organizacije. To se provodi u koordinaciji s drugim relevantnim tijelima koja su odgovorna za informacijsku sigurnost ili kibersigurnost u državi članici kako bi se poboljšale koordinacija i usklađenost sustava izvješćivanja.

(b) Agencija uspostavlja sustav za primjerenu analizu svih relevantnih informacija važnih za sigurnost koje zaprimi u skladu s točkom ARO.GEN.125 podtočkom (c) i bez nepotrebne odgode dostavlja državama članicama i Komisiji sve informacije, uključujući preporuke ili korektivne mjere koje se trebaju poduzeti, potrebne za pravodobnu reakciju na incident ili ranjivost povezanu s informacijskom sigurnošću koja bi mogla utjecati na sigurnost zračnog prometa i koja uključuje proizvode, dijelove, neugrađenu opremu, osobe ili organizacije podložne Uredbi (EU) 2018/1139 i njezinim delegiranim i provedbenim aktima.

(c) Nakon što zaprimi informacije iz podtočaka (a) i (b), nadležno tijelo poduzima prikladne mjere kako bi ispravno pristupilo mogućem utjecaju incidenta ili ranjivosti povezane s informacijskom sigurnošću na sigurnost zračnog prometa.

(d) O mjerama poduzetima u skladu s podtočkom (c) odmah se obavješćuju sve osobe ili organizacije koje moraju postupiti u skladu s tim mjerama na temelju Uredbe (EU) 2018/1139 i njezinih delegiranih i provedbenih akata. Nadležno tijelo države članice o tim mjerama također obavješćuje Agenciju i, ako je potrebno zajedničko djelovanje, nadležna tijela drugih predmetnih država članica.";

(c) u točki ARO.GEN.200 dodaje se sljedeća podtočka (e):

„(e) Uz zahtjeve iz podtočke (a) sustav upravljanja koji uspostavlja i održava nadležno tijelo mora biti usklađen s Prilogom I. (dio IS.AR) Provedbenoj uredbi (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.";

(d) točka ARO.GEN.205 mijenja se kako slijedi:

i. naslov se zamjenjuje sljedećim:

„**ARO.GEN.205 Dodjeljivanje zadataka**";

ii. dodaje se sljedeća podtočka (c):

„(c) Za certifikaciju i nadzor usklađenosti organizacije s točkom ORO.GEN.200A nadležno tijelo može dodijeliti zadatke kvalificiranim subjektima u skladu s podtočkom (a) ili bilo kojem relevantnom tijelu koje je odgovorno za informacijsku sigurnost ili kibersigurnost u državi članici. Pri dodjeljivanju zadataka nadležno tijelo osigurava:

(1) da kvalificirani subjekt ili relevantno tijelo koordinira i uzima u obzir sve aspekte povezane sa sigurnosti zračnog prometa;

(2) da su rezultati aktivnosti certifikacije i nadzora koje obavlja kvalificirani subjekt ili relevantno tijelo uključeni u opće spise organizacije o certifikaciji i nadzoru;

(3) da njegov vlastiti sustav upravljanja informacijskom sigurnošću uspostavljen u skladu s točkom ARO.GEN.200 podtočkom (e) obuhvaća sve zadatke certifikacije i kontinuiranog nadzora koji se obavljaju u njegovo ime.”;

(e) u točki ARO.GEN.300 dodaje se sljedeća podtočka (g):

„(g) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom ORO.GEN.200A nadležno tijelo, uz usklađivanje s točkama od (a) do (f), preispituje sva odobrenja izdana na temelju točke IS.I.OR.200 podtočke (e) ove Uredbe ili točke IS.D.OR.200 podtočke (e) Delegirane uredbe (EU) 2022/1645 nakon primjenjivog ciklusa nadzora sigurnosti i kad god se provedu promjene u opsegu rada organizacije.”;

(f) iza točke ARO.GEN.330 umeće se sljedeća točka ARO.GEN.330A:

„**ARO.GEN.330A Promjene sustava upravljanja informacijskom sigurnošću**

(a) Za promjene kojima se upravlja i o kojima se obavješćuje nadležno tijelo u skladu s postupkom iz točke IS.I.OR.255 podtočke (a) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203 nadležno tijelo uključuje preispitivanje tih promjena u svoj kontinuirani nadzor u skladu s načelima utvrđenima u točki ARO.GEN.300. Ako se utvrdi bilo kakva neusklađenost, nadležno tijelo o tome obavješćuje organizaciju, zahtijeva daljnje promjene i postupa u skladu s točkom ARO.GEN.350.

(b) Za druge promjene za koje je potreban zahtjev za odobrenje u skladu s točkom IS.I.OR.255 podtočkom (b) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203:

(1) nakon što zaprimi zahtjev za promjenu, nadležno tijelo provjerava usklađenost organizacije s primjenjivim zahtjevima prije izdavanja odobrenja;

(2) nadležno tijelo utvrđuje uvjete pod kojima organizacija može raditi tijekom provedbe promjene;

(3) ako utvrdi da organizacija ispunjava primjenjive zahtjeve, nadležno tijelo odobrava promjenu.”;

(2) Prilog III. (dio-ORO) mijenja se kako slijedi:

iza točke ORO.GEN.200 umeće se sljedeća točka ORO.GEN.200A:

„**ORO.GEN.200A Sustav upravljanja informacijskom sigurnošću**

Uz sustav upravljanja iz točke ORO.GEN.200 operator uspostavlja, provodi i održava sustav upravljanja informacijskom sigurnošću u skladu s Provedbenom uredbom (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.”.

PRILOG VI.

Prilog II. (Part ADR.AR) Uredbi (EU) br. 139/2014 mijenja se kako slijedi:

(1) u točki ADR.AR.A.025 dodaje se sljedeća podtočka (c):

„(c) Nadležno tijelo države članice što prije obavještava Agenciju o informacijama važnima za sigurnost koje proizlaze iz izvješća o informacijskoj sigurnosti koje je zaprimilo u skladu s točkom IS.D.OR.230 Priloga (dio IS.D.OR) Delegiranoj uredbi (EU) 2022/1645”;

(2) iza točke ADR.AR.A.030 umeće se sljedeća točka ADR.AR.A.030A:

„**ADR.AR.A.030A Neposredna reakcija na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa**

(a) Nadležno tijelo uspostavlja sustav za primjereno prikupljanje, analizu i širenje informacija o incidentima i ranjivostima povezanima s informacijskom sigurnošću koji bi mogli utjecati na sigurnost zračnog prometa i o kojima izvješćuju organizacije. To se provodi u koordinaciji s drugim relevantnim tijelima koja su odgovorna za informacijsku sigurnost ili kibersigurnost u državi članici kako bi se poboljšale koordinacija i usklađenost sustava izvješćivanja.

(b) Agencija uspostavlja sustav za primjerenu analizu svih relevantnih informacija važnih za sigurnost koje zaprimi u skladu s točkom ADR.AR.A.025 podtočkom (c) i bez nepotrebne odgode dostavlja državama članicama i Komisiji sve informacije, uključujući preporuke ili korektivne mjere koje se trebaju poduzeti, potrebne za pravodobnu reakciju na incident ili ranjivost povezanu s informacijskom sigurnošću koja bi mogla utjecati na sigurnost zračnog prometa i koja uključuje proizvode, dijelove, neugrađenu opremu, osobe ili organizacije podložne Uredbi (EU) 2018/1139 i njezinim delegiranim i provedbenim aktima.

(c) Nakon što zaprimi informacije iz podtočaka (a) i (b), nadležno tijelo poduzima prikladne mjere kako bi ispravno pristupilo mogućem utjecaju incidenta ili ranjivosti povezane s informacijskom sigurnošću na sigurnost zračnog prometa.

(d) O mjerama poduzetima u skladu s podtočkom (c) odmah se obavješćuju sve osobe ili organizacije koje moraju postupiti u skladu s tim mjerama na temelju Uredbe (EU) 2018/1139 i njezinih delegiranih i provedbenih akata. Nadležno tijelo države članice o tim mjerama također obavješćuje Agenciju i, ako je potrebno zajedničko djelovanje, nadležna tijela drugih predmetnih država članica.”;

(3) u točki ADR.AR.B.005 dodaje se sljedeća podtočka (d):

„(d) Uz zahtjeve iz podtočke (a) sustav upravljanja koji uspostavlja i održava nadležno tijelo mora biti usklađen s Prilogom I. (dio IS.AR) Provedbenoj uredbi (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.”;

(4) točka ADR.AR.B.010 mijenja se kako slijedi:

i. naslov se zamjenjuje sljedećim:

„**ADR.AR.B.010 Dodjeljivanje zadataka**”;

ii. dodaje se sljedeća podtočka (c):

„(c) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom ADR.OR.D.005A nadležno tijelo može dodijeliti zadatke kvalificiranim subjektima u skladu s podtočkom (a) ili bilo kojem relevantnom tijelu koje je odgovorno za informacijsku sigurnost ili kibersigurnost u državi članici. Pri dodjeljivanju zadataka nadležno tijelo osigurava:

(1) da kvalificirani subjekt ili relevantno tijelo koordinira i uzima u obzir sve aspekte povezane sa sigurnosti zračnog prometa;

(2) da su rezultati aktivnosti certifikacije i nadzora koje obavlja kvalificirani subjekt ili relevantno tijelo uključeni u opće spise organizacije o certifikaciji i nadzoru;

(3) da njegov vlastiti sustav upravljanja informacijskom sigurnošću uspostavljen u skladu s točkom ADR.AR.B.005 podtočkom (e) obuhvaća sve zadatke certifikacije i kontinuiranog nadzora koji se obavljaju u njegovo ime.”;

(5) u točki ADR.AR.C.005 dodaje se sljedeća podtočka (f):

„(f) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom ADR.OR.D.005A nadležno tijelo, uz usklađivanje s točkama od (a) do (e), preispituje sva odobrenja izdana na temelju točke IS.I.OR.200 podtočke (e) ove Uredbe ili točke IS.D.OR.200 podtočke (e) Delegirane uredbe (EU) 2022/1645 nakon primjenjivog ciklusa nadzora sigurnosti i kad god se provedu promjene u opsegu rada organizacije.”;

(6) iza točke ADR.AR.C.040 umeće se sljedeća točka ADR.AR.C.040A:

„**ADR.AR.C.040A Promjene sustava upravljanja informacijskom sigurnošću**

(a) Za promjene kojima se upravlja i o kojima se obavješćuje nadležno tijelo u skladu s postupkom iz točke IS.D.OR.255 podtočke (a) Priloga (dio IS.D.OR) Delegiranoj uredbi (EU) 2022/1645 nadležno tijelo uključuje preispitivanje tih promjena u svoj kontinuirani nadzor u skladu s načelima utvrđenima u točki ADR.AR.C.005. Ako se utvrdi bilo kakva neusklađenost, nadležno tijelo o tome obavješćuje organizaciju, zahtijeva daljnje promjene i postupa u skladu s točkom ADR.AR.C.055.

(b) U vezi s drugim promjenama za koje je potreban zahtjev za odobrenje u skladu s točkom IS.D.OR.255 podtočkom (b) Priloga (dio IS.D.OR) Delegiranoj uredbi (EU) 2022/1645:

1. nakon što zaprimi zahtjev za promjenu, nadležno tijelo provjerava usklađenost organizacije s primjenjivim zahtjevima prije izdavanja odobrenja;

2. nadležno tijelo utvrđuje uvjete pod kojima organizacija može raditi tijekom provedbe promjene;

3. ako utvrdi da organizacija ispunjava primjenjive zahtjeve, nadležno tijelo odobrava promjenu.”.

PRILOG VII.

Prilozi II. (dio 145.), III. (dio 66.) i V.c (dio CAMO) Uredbi (EU) br. 1321/2014 mijenjaju se kako slijedi:

(1) Prilog II. (dio 145.) mijenja se kako slijedi:

(a) sadržaj se mijenja kako slijedi:

i. iza naslova 145.A.200 umeće se sljedeći naslov:

„145.A.200A Sustav upravljanja informacijskom sigurnošću”;

ii. iza naslova 145.B.135 umeće se sljedeći naslov:

„145.B.135A Neposredna reakcija na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa”;

iii. naslov točke 145.B.205 zamjenjuje se sljedećim:

„145.B.205 Dodjeljivanje zadataka”;

iv. iza naslova 145.B.330 umeće se sljedeći naslov:

„145.B.330A Promjene sustava upravljanja informacijskom sigurnošću”;

(b) iza točke 145.A.200 umeće se sljedeća točka 145.A.200A:

„145.A.200A **Sustav upravljanja informacijskom sigurnošću**

Uz sustav upravljanja iz točke 145.A.200 organizacija za održavanje uspostavlja, provodi i održava sustav upravljanja informacijskom sigurnošću u skladu s Provedbenom uredbom (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.”;

(c) u točki 145.B.125 dodaje se sljedeća podtočka (c):

„(c) Nadležno tijelo države članice što prije obavještava Agenciju o informacijama važnima za sigurnost koje proizlaze iz izvješća o informacijskoj sigurnosti koje je zaprimilo u skladu s točkom IS.I.OR.230 Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203.”;

(d) iza točke 145.B.135 umeće se sljedeća točka 145.B.135A:

„145.B.135A **Neposredna reakcija na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa**

(a) Nadležno tijelo uspostavlja sustav za primjereno prikupljanje, analizu i širenje informacija o incidentima i ranjivostima povezanima s informacijskom sigurnošću koji bi mogli utjecati na sigurnost zračnog prometa i o kojima izvješćuju organizacije. To se provodi u koordinaciji s drugim relevantnim tijelima koja su odgovorna za informacijsku sigurnost ili kibersigurnost u državi članici kako bi se poboljšale koordinacija i usklađenost sustava izvješćivanja.

(b) Agencija uspostavlja sustav za primjerenu analizu svih relevantnih informacija važnih za sigurnost koje zaprimi u skladu s točkom 145.B.125 podtočkom (c) i bez nepotrebne odgode dostavlja državama članicama i Komisiji sve informacije, uključujući preporuke ili korektivne mjere koje se trebaju poduzeti, potrebne za pravodobnu reakciju na incident ili ranjivost povezanu s informacijskom sigurnošću koja bi mogla utjecati na sigurnost zračnog prometa i koja uključuje proizvode, dijelove, neugrađenu opremu, osobe ili organizacije podložne Uredbi (EU) 2018/1139 i njezinim delegiranim i provedbenim aktima.

(c) Nakon što zaprimi informacije iz podtočaka (a) i (b), nadležno tijelo poduzima prikladne mjere kako bi ispravno pristupilo mogućem utjecaju incidenta ili ranjivosti povezane s informacijskom sigurnošću na sigurnost zračnog prometa.

(d) O mjerama poduzetima u skladu s podtočkom (c) odmah se obavješćuju sve osobe ili organizacije koje moraju postupiti u skladu s tim mjerama na temelju Uredbe (EU) 2018/1139 i njezinih delegiranih i provedbenih akata. Nadležno tijelo države članice o tim mjerama također obavješćuje Agenciju i, ako je potrebno zajedničko djelovanje, nadležna tijela drugih predmetnih država članica.";

(e) u točki 145.B.200 dodaje se sljedeća podtočka (e):

„(e) Uz zahtjeve iz podtočke (a) sustav upravljanja koji uspostavlja i održava nadležno tijelo mora biti usklađen s Prilogom I. (dio IS.AR) Provedbenoj uredbi (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.";

(f) točka 145.B.205 mijenja se kako slijedi:

i. naslov se zamjenjuje sljedećim:

„145.B.205 **Dodjeljivanje zadataka**";

ii. dodaje se sljedeća podtočka (c):

„(c) Za certifikaciju i nadzor usklađenosti organizacije s točkom 145.A.200A nadležno tijelo može dodijeliti zadatke kvalificiranim subjektima u skladu s podtočkom (a) ili bilo kojem relevantnom tijelu koje je odgovorno za informacijsku sigurnost ili kibersigurnost u državi članici. Pri dodjeljivanju zadataka nadležno tijelo osigurava:

1. da kvalificirani subjekt ili relevantno tijelo koordinira i uzima u obzir sve aspekte povezane sa sigurnosti zračnog prometa;

2. da su rezultati aktivnosti certifikacije i nadzora koje obavlja kvalificirani subjekt ili relevantno tijelo uključeni u opće spise organizacije o certifikaciji i nadzoru;

3. da njegov vlastiti sustav upravljanja informacijskom sigurnošću uspostavljen u skladu s točkom 145.B.200 podtočkom (e) obuhvaća sve zadatke certifikacije i kontinuiranog nadzora koji se obavljaju u njegovo ime.";

(g) u točki 145.B.300 dodaje se sljedeća podtočka (g):

„(g) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom 145.A.200A nadležno tijelo, uz usklađivanje s točkama od (a) do (f), preispituje sva odobrenja izdana na temelju točke IS.I.OR.200 podtočke (e) ove Uredbe ili točke IS.D.OR.200 podtočke (e) Delegirane uredbe (EU) 2022/1645 nakon primjenjivog ciklusa nadzora sigurnosti i kad god se provedu promjene u opsegu rada organizacije.";

(h) iza točke 145.B.330 umeće se sljedeća točka 145.B.330A:

„145.B.330A **Promjene sustava upravljanja informacijskom sigurnošću**

(a) Za promjene kojima se upravlja i o kojima se obavješćuje nadležno tijelo u skladu s postupkom iz točke IS.I.OR.255 podtočke (a) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203 nadležno tijelo uključuje preispitivanje tih promjena u svoj kontinuirani nadzor u skladu s načelima utvrđenima u točki 145.B.300. Ako se utvrdi bilo kakva neusklađenost, nadležno tijelo o tome obavješćuje organizaciju, zahtijeva daljnje promjene i postupa u skladu s točkom 145.B.350.

(b) Za druge promjene za koje je potreban zahtjev za odobrenje u skladu s točkom IS.I.OR.255 podtočkom (b) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203:

1. nakon što zaprimi zahtjev za promjenu, nadležno tijelo provjerava usklađenost organizacije s primjenjivim zahtjevima prije izdavanja odobrenja;

2. nadležno tijelo utvrđuje uvjete pod kojima organizacija može raditi tijekom provedbe promjene;

3. ako utvrdi da organizacija ispunjava primjenjive zahtjeve, nadležno tijelo odobrava promjenu.";

(2) Prilog III. (dio 66.) mijenja se kako slijedi:

(a) iza naslova 66.B.10 u sadržaju umeće se sljedeći naslov:

„66.B.15 Sustav upravljanja informacijskom sigurnošću";

(b) iza točke 66.B.10 umeće se sljedeća točka 66.B.15:

„66.B.15 **Sustav upravljanja informacijskom sigurnošću**

Nadležno tijelo uspostavlja, provodi i održava sustav upravljanja informacijskom sigurnošću u skladu s Prilogom I. (dio IS.AR) Provedbenoj uredbi (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.";

(3) Prilog V.c (dio CAMO) mijenja se kako slijedi:

(a) sadržaj se mijenja kako slijedi:

i. iza naslova CAMO.A.200 umeće se sljedeći naslov:

„CAMO.A.200A Sustav upravljanja informacijskom sigurnošću";

ii. iza naslova CAMO.B.135 umeće se sljedeći naslov:

„CAMO.B.135A Neposredna reakcija na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa";

iii. naslov točke CAMO.B.205 zamjenjuje se sljedećim:

„CAMO.B.205 Dodjeljivanje zadataka";

iv. iza naslova CAMO.B.330 umeće se sljedeći naslov:

„CAMO.B.330A Promjene sustava upravljanja informacijskom sigurnošću";

(b) iza točke CAMO.A.200 umeće se sljedeća točka CAMO.A.200A:

„CAMO.A.200A **Sustav upravljanja informacijskom sigurnošću**

Uz sustav upravljanja iz točke CAMO.A.200 organizacija uspostavlja, provodi i održava sustav upravljanja informacijskom sigurnošću u skladu s Provedbenom uredbom (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.";

(c) u točki CAMO.B.125 dodaje se sljedeća podtočka (c):

„(c) Nadležno tijelo države članice što prije obavještava Agenciju o informacijama važnima za sigurnost koje proizlaze iz izvješća o informacijskoj sigurnosti koje je zaprimilo u skladu s točkom IS.I.OR.230 Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203.”;

(d) iza točke CAMO.B.135 umeće se točka CAMO.B.135A:

„CAMO.B.135A **Neposredna reakcija na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa**

(a) Nadležno tijelo uspostavlja sustav za primjereno prikupljanje, analizu i širenje informacija o incidentima i ranjivostima povezanima s informacijskom sigurnošću koji bi mogli utjecati na sigurnost zračnog prometa i o kojima izvješćuju organizacije. To se provodi u koordinaciji s drugim relevantnim tijelima koja su odgovorna za informacijsku sigurnost ili kibersigurnost u državi članici kako bi se poboljšale koordinacija i usklađenost sustava izvješćivanja.

(b) Agencija uspostavlja sustav za primjerenu analizu svih relevantnih informacija važnih za sigurnost koje zaprimi u skladu s točkom CAMO.B.125 podtočkom (c) i bez nepotrebne odgode dostavlja državama članicama i Komisiji sve informacije, uključujući preporuke ili korektivne mjere koje se trebaju poduzeti, potrebne za pravodobnu reakciju na incident ili ranjivost povezanu s informacijskom sigurnošću koja bi mogla utjecati na sigurnost zračnog prometa i koja uključuje proizvode, dijelove, neugrađenu opremu, osobe ili organizacije podložne Uredbi (EU) 2018/1139 i njezinim delegiranim i provedbenim aktima.

(c) Nakon što zaprimi informacije iz podtočaka (a) i (b), nadležno tijelo poduzima prikladne mjere kako bi ispravno pristupilo mogućem utjecaju incidenta ili ranjivosti povezane s informacijskom sigurnošću na sigurnost zračnog prometa.

(d) O mjerama poduzetima u skladu s podtočkom (c) odmah se obavješćuju sve osobe ili organizacije koje moraju postupiti u skladu s tim mjerama na temelju Uredbe (EU) 2018/1139 i njezinih delegiranih i provedbenih akata. Nadležno tijelo države članice o tim mjerama također obavješćuje Agenciju i, ako je potrebno zajedničko djelovanje, nadležna tijela drugih predmetnih država članica.”;

(e) u točki CAMO.B.200 dodaje se sljedeća podtočka (e):

„(e) Uz zahtjeve iz podtočke (a) sustav upravljanja koji uspostavlja i održava nadležno tijelo mora biti usklađen s Prilogom I. (dio IS.AR) Provedbenoj uredbi (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.”;

(f) točka CAMO.B.205 mijenja se kako slijedi:

i. naslov se zamjenjuje sljedećim:

„CAMO.B.205 **Dodjeljivanje zadataka**”;

ii. dodaje se sljedeća podtočka (c):

„(c) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom CAMO.A.200A nadležno tijelo može dodijeliti zadatke kvalificiranim subjektima u skladu s podtočkom (a) ili bilo kojem relevantnom tijelu koje je odgovorno za informacijsku sigurnost ili kibersigurnost u državi članici. Pri dodjeljivanju zadataka nadležno tijelo osigurava:

(1) da kvalificirani subjekt ili relevantno tijelo koordinira i uzima u obzir sve aspekte povezane sa sigurnosti zračnog prometa;

(2) da su rezultati aktivnosti certifikacije i nadzora koje obavlja kvalificirani subjekt ili relevantno tijelo uključeni u opće spise organizacije o certifikaciji i nadzoru;

(3) da njegov vlastiti sustav upravljanja informacijskom sigurnošću uspostavljen u skladu s točkom - CAMO.B.200 podtočkom (e) obuhvaća sve zadatke certifikacije i kontinuiranog nadzora koji se obavljaju u njegovo ime.";

(g) u točki CAMO.B.300 dodaje se sljedeća podtočka (g):

„(g) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom CAMO.A.200A nadležno tijelo, uz usklađivanje s točkama od (a) do (f), preispituje sva odobrenja izdana na temelju točke IS.I.OR.200 podtočke (e) ove Uredbe ili točke IS.D.OR.200 podtočke (e) Delegirane uredbe (EU) 2022/1645 nakon primjenjivog ciklusa nadzora sigurnosti i kad god se provedu promjene u opsegu rada organizacije.";

(h) iza točke CAMO.B.330 umeće se sljedeća točka CAMO.B.330A:

„CAMO.B.330A **Promjene sustava upravljanja informacijskom sigurnošću**

(a) Za promjene kojima se upravlja i o kojima se obavješćuje nadležno tijelo u skladu s postupkom iz točke IS.I.OR.255 podtočke (a) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203 nadležno tijelo uključuje preispitivanje tih promjena u svoj kontinuirani nadzor u skladu s načelima utvrđenima u točki CAMO.B.300. Ako se utvrdi bilo kakva neusklađenost, nadležno tijelo o tome obavješćuje organizaciju, zahtijeva daljnje promjene i postupa u skladu s točkom CAMO.B.350.

(b) Za druge promjene za koje je potreban zahtjev za odobrenje u skladu s točkom IS.I.OR.255 podtočkom (b) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203:

(1) nakon što zaprimi zahtjev za promjenu, nadležno tijelo provjerava usklađenost organizacije s primjenjivim zahtjevima prije izdavanja odobrenja;

(2) nadležno tijelo utvrđuje uvjete pod kojima organizacija može raditi tijekom provedbe promjene;

(3) ako utvrdi da organizacija ispunjava primjenjive zahtjeve, nadležno tijelo odobrava promjenu.".

PRILOG VIII.

Prilozi II. (dio ATCO.AR) i III. (dio ATCO.OR) Uredbi (EU) 2015/340 mijenjaju se kako slijedi:

(1) Prilog II. (dio ATCO.AR) mijenja se kako slijedi:

(a) u točki ATCO.AR.A.020 dodaje se sljedeća podtočka (c):

„(c) Nadležno tijelo države članice što prije obavještava Agenciju o informacijama važnima za sigurnost koje proizlaze iz izvješća o informacijskoj sigurnosti koje je zaprimilo u skladu s točkom IS.I.OR.230 Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203.”;

(b) iza točke ATCO.AR.A.025 umeće se sljedeća točka ATCO.AR.A.025A:

„**ATCO.AR.A.025A Neposredna reakcija na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa**

(a) Nadležno tijelo uspostavlja sustav za primjereno prikupljanje, analizu i širenje informacija o incidentima i ranjivostima povezanima s informacijskom sigurnošću koji bi mogli utjecati na sigurnost zračnog prometa i o kojima izvješćuju organizacije. To se provodi u koordinaciji s drugim relevantnim tijelima koja su odgovorna za informacijsku sigurnost ili kibersigurnost u državi članici kako bi se poboljšale koordinacija i usklađenost sustava izvješćivanja.

(b) Agencija uspostavlja sustav za primjerenu analizu svih relevantnih informacija važnih za sigurnost koje zaprimi u skladu s točkom ATCO.AR.A.020 i bez nepotrebne odgode dostavlja državama članicama i Komisiji sve informacije, uključujući preporuke ili korektivne mjere koje se trebaju poduzeti, potrebne za pravodobnu reakciju na incident ili ranjivost povezanu s informacijskom sigurnošću koja bi mogla utjecati na sigurnost zračnog prometa i koja uključuje proizvode, dijelove, neugrađenu opremu, osobe ili organizacije podložne Uredbi (EU) 2018/1139 i njezinim delegiranim i provedbenim aktima.

(c) Nakon što zaprimi informacije iz podtočaka (a) i (b), nadležno tijelo poduzima prikladne mjere kako bi ispravno pristupilo mogućem utjecaju incidenta ili ranjivosti povezane s informacijskom sigurnošću na sigurnost zračnog prometa.

(d) O mjerama poduzetima u skladu s podtočkom (c) odmah se obavješćuju sve osobe ili organizacije koje moraju postupiti u skladu s tim mjerama na temelju Uredbe (EU) 2018/1139 i njezinih delegiranih i provedbenih akata. Nadležno tijelo države članice o tim mjerama također obavješćuje Agenciju i, ako je potrebno zajedničko djelovanje, nadležna tijela drugih predmetnih država članica.”;

(c) u točki ATCO.AR.B.001 dodaje se sljedeća podtočka (e):

„(e) Uz zahtjeve iz podtočke (a) sustav upravljanja koji uspostavlja i održava nadležno tijelo mora biti usklađen s Prilogom I. (dio IS.AR) Provedbenoj uredbi (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.”;

(d) točka ATCO.AR.B.005 mijenja se kako slijedi:

i. naslov se zamjenjuje sljedećim:

„**ATCO.AR.B.005 Dodjeljivanje zadataka**”;

ii. dodaje se sljedeća podtočka (c):

„(c) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom ATCO.OR.C.001A nadležno tijelo može dodijeliti zadatke kvalificiranim subjektima u skladu s podtočkom (a) ili bilo kojem relevantnom tijelu koje je odgovorno za informacijsku sigurnost ili kibersigurnost u državi članici. Pri dodjeljivanju zadataka nadležno tijelo osigurava:

(1) da kvalificirani subjekt ili relevantno tijelo koordinira i uzima u obzir sve aspekte povezane sa sigurnosti zračnog prometa;

(2) da su rezultati aktivnosti certifikacije i nadzora koje obavlja kvalificirani subjekt ili relevantno tijelo uključeni u opće spise organizacije o certifikaciji i nadzoru;

(3) da njegov vlastiti sustav upravljanja informacijskom sigurnošću uspostavljen u skladu s točkom ATCO.AR.B.001 podtočkom (e) obuhvaća sve zadatke certifikacije i kontinuiranog nadzora koji se obavljaju u njegovo ime.";

(e) u točki ATCO.AR.C.001 dodaje se sljedeća podtočka (f):

„(f) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom ATCO.OR.C.001A nadležno tijelo, uz usklađivanje s točkama od (a) do (e), preispituje sva odobrenja izdana na temelju točke IS.I.OR.200 podtočke (e) ove Uredbe ili točke IS.D.OR.200 podtočke (e) Delegirane uredbe (EU) 2022/1645 nakon primjenjivog ciklusa nadzora sigurnosti i kad god se provedu promjene u opsegu rada organizacije.";

(f) iza točke ATCO.AR.E.010 umeće se sljedeća točka ATCO.AR.E.010A:

„**ATCO.AR.E.010A Promjene sustava upravljanja informacijskom sigurnošću**

(a) U vezi s promjenama kojima se upravlja i o kojima se obavješćuje nadležno tijelo u skladu s postupkom iz točke IS.I.OR.255 podtočke (a) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203 nadležno tijelo uključuje preispitivanje tih promjena u svoj kontinuirani nadzor u skladu s načelima utvrđenima u točki ATCO.AR.C.001. Ako se utvrdi bilo kakva neusklađenost, nadležno tijelo o tome obavješćuje organizaciju, zahtijeva daljnje promjene i postupa u skladu s točkom ATCO.AR.C.010.

(b) U vezi s drugim promjenama za koje je potreban zahtjev za odobrenje u skladu s točkom IS.I.OR.255 podtočkom (b) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203:

(1) nakon što zaprimi zahtjev za promjenu, nadležno tijelo provjerava usklađenost organizacije s primjenjivim zahtjevima prije izdavanja odobrenja;

(2) nadležno tijelo utvrđuje uvjete pod kojima organizacija može raditi tijekom provedbe promjene;

(3) ako utvrdi da organizacija ispunjava primjenjive zahtjeve, nadležno tijelo odobrava promjenu.";

(2) Prilog III. (dio ATCO.OR) mijenja se kako slijedi:

iza točke ATCO.OR.C.001 umeće se sljedeća točka ATCO.OR.C.001A:

„**ATCO.OR.C.001A Sustav upravljanja informacijskom sigurnošću**

Uz sustav upravljanja iz točke ATCO.OR.C.001 organizacija za osposobljavanje uspostavlja, provodi i održava sustav upravljanja informacijskom sigurnošću u skladu s Provedbenom uredbom (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.".

PRILOG IX.

Prilozi II. (dio ATM/ANS.AR) i III. (dio ATM/ANS.OR) Provedbenoj uredbi (EU) 2017/373 mijenjaju se kako slijedi:

(1) Prilog II. (dio ATM/ANS.AR) mijenja se kako slijedi:

(a) u točki ATM/ANS.AR.A.020 dodaje se sljedeća podtočka (c):

„(c) Nadležno tijelo države članice što prije obavještava Agenciju o informacijama važnima za sigurnost koje proizlaze iz izvješća o informacijskoj sigurnosti koje je zaprimilo u skladu s točkom IS.I.OR.230 Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203.";

(b) iza točke ATM/ANS.AR.A.025 umeće se sljedeća točka ATM/ANS.AR.A.025A:

„**ATM/ANS.AR.A.025A Neposredna reakcija na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa**

(a) Nadležno tijelo uspostavlja sustav za primjereno prikupljanje, analizu i širenje informacija o incidentima i ranjivostima povezanima s informacijskom sigurnošću koji bi mogli utjecati na sigurnost zračnog prometa i o kojima izvješćuju organizacije. To se provodi u koordinaciji s drugim relevantnim tijelima koja su odgovorna za informacijsku sigurnost ili kibersigurnost u državi članici kako bi se poboljšale koordinacija i usklađenost sustava izvješćivanja.

(b) Agencija uspostavlja sustav za primjerenu analizu svih relevantnih informacija važnih za sigurnost koje zaprimi u skladu s točkom ATM/ANS.AR.A.020 podtočkom (c) i bez nepotrebne odgode dostavlja državama članicama i Komisiji sve informacije, uključujući preporuke ili korektivne mjere koje se trebaju poduzeti, potrebne za pravodobnu reakciju na incident ili ranjivost povezanu s informacijskom sigurnošću koja bi mogla utjecati na sigurnost zračnog prometa i koja uključuje proizvode, dijelove, neugrađenu opremu, osobe ili organizacije podložne Uredbi (EU) 2018/1139 i njezinim delegiranim i provedbenim aktima.

(c) Nakon što zaprimi informacije iz podtočaka (a) i (b), nadležno tijelo poduzima prikladne mjere kako bi ispravno pristupilo mogućem utjecaju incidenta ili ranjivosti povezane s informacijskom sigurnošću na sigurnost zračnog prometa.

(d) O mjerama poduzetima u skladu s podtočkom (c) odmah se obavješćuju sve osobe ili organizacije koje moraju postupiti u skladu s tim mjerama na temelju Uredbe (EU) 2018/1139 i njezinih delegiranih i provedbenih akata. Nadležno tijelo države članice o tim mjerama također obavješćuje Agenciju i, ako je potrebno zajedničko djelovanje, nadležna tijela drugih predmetnih država članica.";

(c) u točki ATM/ANS.AR.B.001 dodaje se sljedeća podtočka (e):

„(e) Uz zahtjeve iz podtočke (a) sustav upravljanja koji uspostavlja i održava nadležno tijelo mora biti usklađen s Prilogom I. (dio IS.AR) Provedbenoj uredbi (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.";

(d) točka ATM/ANS.AR.B.005 mijenja se kako slijedi:

i. naslov se zamjenjuje sljedećim:

„**ATM/ANS.AR.B.005 Dodjeljivanje zadataka**";

ii. dodaje se sljedeća podtočka (c):

„(c) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom ATM/ANS.OR.B.005A nadležno tijelo može dodijeliti zadatke kvalificiranim subjektima u skladu s podtočkom (a) ili bilo kojem relevantnom tijelu koje je odgovorno za informacijsku sigurnost ili kibersigurnost u državi članici. Pri dodjeljivanju zadataka nadležno tijelo osigurava:

(1) da kvalificirani subjekt ili relevantno tijelo koordinira i uzima u obzir sve aspekte povezane sa sigurnosti zračnog prometa;

(2) da su rezultati aktivnosti certifikacije i nadzora koje obavlja kvalificirani subjekt ili relevantno tijelo uključeni u opće spise organizacije o certifikaciji i nadzoru;

(3) da njegov vlastiti sustav upravljanja informacijskom sigurnošću uspostavljen u skladu s točkom ATM/ANS.AR.B.001 podtočkom (e) obuhvaća sve zadatke certifikacije i kontinuiranog nadzora koji se obavljaju u njegovo ime.";

(e) u točki ATM/ANS.AR.C.010 dodaje se sljedeća podtočka (d):

„(d) U vezi s certifikacijom i nadzorom usklađenosti organizacije s točkom ATM/ANS.OR.B.005A nadležno tijelo, uz usklađivanje s točkama od (a) do (c), preispituje sva odobrenja izdana na temelju točke IS.I.OR.200 podtočke (e) ove Uredbe ili točke IS.D.OR.200 podtočke (e) Delegirane uredbe (EU) 2022/1645 nakon primjenjivog ciklusa nadzora sigurnosti i kad god se provedu promjene u opsegu rada organizacije.";

(f) iza točke ATM/ANS.AR.C.025 umeće se sljedeća točka ATM/ANS.AR.C.025A:

„**ATM/ANS.AR.C.025A Promjene sustava upravljanja informacijskom sigurnošću**

(a) Za promjene kojima se upravlja i o kojima se obavješćuje nadležno tijelo u skladu s postupkom iz točke IS.I.OR.255 podtočke (a) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203 nadležno tijelo uključuje preispitivanje tih promjena u svoj kontinuirani nadzor u skladu s načelima utvrđenima u točki ATM/ANS.AR.C.010. Ako se utvrdi bilo kakva neusklađenost, nadležno tijelo o tome obavješćuje organizaciju, zahtijeva daljnje promjene i postupa u skladu s točkom ATM/ANS.AR.C.050.

(b) U vezi s drugim promjenama za koje je potreban zahtjev za odobrenje u skladu s točkom IS.I.OR.255 podtočkom (b) Priloga II. (dio IS.I.OR) Provedbenoj uredbi (EU) 2023/203:

(1) nakon što zaprimi zahtjev za promjenu, nadležno tijelo provjerava usklađenost organizacije s primjenjivim zahtjevima prije izdavanja odobrenja;

(2) nadležno tijelo utvrđuje uvjete pod kojima organizacija može raditi tijekom provedbe promjene;

(3) ako utvrdi da organizacija ispunjava primjenjive zahtjeve, nadležno tijelo odobrava promjenu.";

(2) Prilog III. (dio ATM/ANS.OR) mijenja se kako slijedi:

(a) iza točke ATM/ANS.OR.B.005 umeće se sljedeća točka ATM/ANS.OR.B.005A:

„**ATM/ANS.OR.B.005A Sustav upravljanja informacijskom sigurnošću**

Uz sustav upravljanja iz točke ATM/ANS.OR.B.005 pružatelj usluga uspostavlja, provodi i održava sustav upravljanja informacijskom sigurnošću u skladu s Provedbenom uredbom (EU) 2023/203 kako bi se osiguralo pravilno upravljanje rizicima za informacijsku sigurnost koji mogu utjecati na sigurnost zračnog prometa.";

(b) točka ATM/ANS.OR.D.010 zamjenjuje se sljedećim:

„**ATM/ANS.OR.D.010 Upravljanje zaštitom**

(a) Pružatelji usluga u zračnoj plovidbi i upravljanja protokom zračnog prometa i upravitelj mreže utvrđuju kao sastavni dio svojeg sustava upravljanja u skladu s točkom ATM/ANS.OR.B.005 sustav upravljanja zaštitom kako bi osigurali:

(1) zaštitu svojih objekata, opreme i osoblja kako bi spriječili nezakonito ometanje pružanja usluga;

(2) zaštitu operativnih podataka koje dobivaju ili proizvode ili upotrebljavaju, tako da je pristup tim podacima ograničen samo na one koji su za to ovlašteni.

(b) U okviru sustava upravljanja zaštitom određuje se:

(1) proces i postupke koji se odnose na procjenu i ublažavanje rizika zaštite, praćenje i poboljšanje zaštite, revizije stanja zaštite i širenje novih spoznaja;

(2) sredstva za identifikaciju, praćenje i otkrivanje narušavanja zaštite i za upozoravanje osoblja odgovarajućim signalima upozorenja;

(3) sredstva za otklanjanje posljedica narušavanja zaštite i utvrđivanje postupaka oporavka i postupaka ublažavanja, kako bi se spriječilo ponavljanje situacije.

(c) Pružatelji usluga u zračnoj plovidbi i upravljanja protokom zračnog prometa i upravitelj mreže osiguravaju da njihovo osoblje prođe sigurnosnu provjeru, ako je to primjereno, te surađuju s relevantnim civilnim i vojnim tijelima kako bi osigurali zaštitu svojih tehničkih sredstava i objekata, osoblja i podataka.

(d) Aspektima povezanima s informacijskom sigurnošću upravlja se u skladu s točkom ATM/ANS.OR.B.005A.”.