II

(Nezakonodajni akti)

UREDBE

IZVEDBENA UREDBA KOMISIJE (EU) 2023/203

z dne 27. oktobra 2022

o določitvi pravil za uporabo Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta glede zahtev za obvladovanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu, za organizacije, zajete v uredbah Komisije (EU) št. 1321/2014, (EU) št. 965/2012, (EU) št. 1178/2011, (EU) 2015/340, izvedbenih uredbah Komisije (EU) 2017/373 in (EU) 2021/664, ter za pristojne organe, zajete v uredbah Komisije (EU) št. 748/2012, (EU) št. 1321/2014, (EU) št. 965/2012, (EU) št. 1178/2011, (EU) 2015/340 in (EU) št. 139/2014, izvedbenih uredbah Komisije (EU) 2017/373 in (EU) 2021/664, ter o spremembi uredb Komisije (EU) št. 1178/2011, (EU) št. 748/2012, (EU) št. 965/2012, (EU) št. 139/2014, (EU) št. 1321/2014, (EU) 2015/340 ter izvedbenih uredb Komisije (EU) 2017/373 in (EU) 2021/664

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta z dne 4. julija 2018 o skupnih pravilih na področju civilnega letalstva in ustanovitvi Agencije Evropske unije za varnost v letalstvu ter spremembi uredb (ES) št. 2111/2005, (ES) št. 1008/2008, (EU) št. 996/2010, (EU) št. 376/2014 ter direktiv 2014/30/EU in 2014/53/EU Evropskega parlamenta in Sveta ter razveljavitvi uredb (ES) št. 552/2004 in (ES) št. 216/2008 Evropskega parlamenta in Sveta ter Uredbe Sveta (EGS) št. 3922/91 ([1]), zlasti člena 17(1), točka (b), člena 27(1), točka (a), člena 31(1), točka (b), člena 43(1), točka (b), člena 53(1), točka (a), ter člena 62(15), točka (c), Uredbe,

ob upoštevanju naslednjega:

(1) V skladu z bistvenimi zahtevami iz Priloge II, točka 3.1(b), k Uredbi (EU) 2018/1139 morajo organizacije za vodenje stalne plovnosti in vzdrževalne organizacije izvajati in vzdrževati sistem upravljanja za obvladovanje varnostnih tveganj.

(2) Tudi organizacije za usposabljanje pilotov, organizacije za usposabljanje kabinskega osebja, zdravstveni centri za letalsko osebje in operatorji naprav za simulacijo letenja morajo v skladu z bistvenimi zahtevami iz Priloge IV, točka 3.3(b) in točka 5(b), k Uredbi (EU) 2018/1139 izvajati in vzdrževati sistem upravljanja za obvladovanje varnostnih tveganj.

(3) Poleg tega morajo letalski prevozniki v skladu z bistvenimi zahtevami iz Priloge V, točka 8.1(c), k Uredbi (EU) 2018/1139 izvajati in vzdrževati sistem upravljanja za obvladovanje varnostnih tveganj.

(4) Tudi izvajalci upravljanja zračnega prometa in navigacijskih služb zračnega prometa, izvajalci služb U-space, enotni izvajalci skupne informacijske službe, organizacije za usposabljanje in zdravstveni centri za letalsko osebje za kontrolorje zračnega prometa morajo v skladu z bistvenimi zahtevami iz Priloge VIII, točka 5.1(c) in točka 5.4(b), k Uredbi (EU) 2018/1139 izvajati in vzdrževati sistem upravljanja za obvladovanje varnostnih tveganj.

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

(5) Navedena varnostna tveganja lahko nastanejo iz različnih razlogov, na primer zaradi hib v zasnovi in vzdrževanju, vidikov človeške učinkovitosti, okoljskih groženj in groženj za informacijsko varnost. Zato bi morali sistemi upravljanja, ki jih izvajajo Agencija Evropske unije za varnost v letalstvu (v nadaljnjem besedilu: Agencija) ter nacionalni pristojni organi in organizacije iz zgornjih uvodnih izjav, upoštevati ne samo varnostna tveganja, ki izhajajo iz naključnih dogodkov, ampak tudi varnostna tveganja, ki izhajajo iz groženj za informacijsko varnost, kadar lahko posamezniki obstoječe pomanjkljivosti izkoristijo zlonamerno. Navedena tveganja za informacijsko varnost se v civilnem letalstvu nenehno povečujejo, saj sedanji informacijski sistemi postajajo čedalje bolj medsebojno povezani in čedalje pogosteje tarča zlonamernih akterjev.

(6) Tveganja, povezana z navedenimi informacijskimi sistemi, niso omejena na morebitne napade na kibernetski prostor, ampak vključujejo tudi grožnje, ki lahko vplivajo na procese in postopke ter človeško uspešnost.

(7) Veliko organizacij že uporablja mednarodne standarde, na primer ISO 27001, da bi obravnavale varnost digitalnih informacij in podatkov. Navedeni standardi ne obravnavajo nujno v celoti vseh posebnosti civilnega letalstva. Zato je primerno določiti zahteve za obvladovanje tveganj za informacijsko varnost, ki bi lahko vplivala na varnost v letalstvu.

(8) Bistveno je, da navedene zahteve zajemajo vsa področja letalstva in njihove vmesnike, saj je letalstvo zelo povezan sistem več sistemov. Zato bi se morale uporabljati za vse organizacije in pristojne organe, zajete v uredbah Komisije (EU) št. 748/2012 ([2]), (EU) št. 1321/2014 ([3]), (EU) št. 965/2012 ([4]), (EU) št. 1178/2011 ([5]), (EU) 2015/340 ([6]), (EU) št. 139/2014 ([7]) in Izvedbeni uredbi Komisije (EU) 2021/664 ([8]), ter za tiste, ki že morajo imeti sistem upravljanja v skladu z veljavno zakonodajo Unije o varnosti v letalstvu. Vendar pa bi morale biti nekatere organizacije izključene s področja uporabe te uredbe, da se zagotovi ustrezna sorazmernost z nižjimi tveganji za informacijsko varnost, ki jo imajo za letalski sistem.

(9) Zahteve iz te uredbe bi morale zagotoviti dosledno izvajanje na vseh področjih letalstva, hkrati pa čim manj vplivati na zakonodajo Unije o varnosti v letalstvu, ki se na teh področjih že uporablja.

([2]) Uredba Komisije (EU) št. 748/2012 z dne 3. avgusta 2012 o določitvi izvedbenih določb za certificiranje zrakoplovov in sorodnih proizvodov, delov in naprav glede plovnosti in okoljske ustreznosti ter potrjevanje projektivnih in proizvodnih organizacij (UL L 224, 21.8.2012, str. 1).

([3]) Uredba Komisije (EU) št. 1321/2014 z dne 26. novembra 2014 o stalni plovnosti zrakoplovov in letalskih izdelkov, delov in naprav ter o potrjevanju organizacij in osebja, ki se ukvarjajo s temi nalogami (UL L 362, 17.12.2014, str. 1).

([4]) Uredba Komisije (EU) št. 965/2012 z dne 5. oktobra 2012 o tehničnih zahtevah in upravnih postopkih za letalske operacije v skladu z Uredbo (ES) št. 216/2008 Evropskega parlamenta in Sveta (UL L 296, 25.10.2012, str. 1).

([5]) Uredba Komisije (EU) št. 1178/2011 z dne 3. novembra 2011 o tehničnih zahtevah in upravnih postopkih za letalsko osebje v civilnem letalstvu v skladu z Uredbo (ES) št. 216/2008 Evropskega parlamenta in Sveta (UL L 311, 25.11.2011, str. 1).

([6]) Uredba Komisije (EU) 2015/340 z dne 20. februarja 2015 o tehničnih zahtevah in upravnih postopkih za licence in certifikate kontrolorjev zračnega prometa v skladu z Uredbo (ES) št. 216/2008 Evropskega parlamenta in Sveta, o spremembi Izvedbene uredbe Komisije (EU) št. 923/2012 ter razveljavitvi Uredbe Komisije (EU) št. 805/2011 (UL L 63, 6.3.2015, str. 1).

([7]) Uredba Komisije (EU) št. 139/2014 z dne 12. februarja 2014 o določitvi zahtev in upravnih postopkov v zvezi z aerodromi v skladu z Uredbo (ES) št. 216/2008 Evropskega parlamenta in Sveta (UL L 44, 14.2.2014, str. 1).

([8]) Izvedbena uredba Komisije (EU) 2021/664 z dne 22. aprila 2021 o regulativnem okviru za U-space (UL L 139, 23.4.2021, str. 161).

(10) Zahteve iz te uredbe ne bi smele posegati v zahteve glede informacijske in kibernetske varnosti iz točke 1.7 Priloge k Izvedbeni uredbi Komisije (EU) 2015/1998 ([9]) in iz člena 14 Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta ([10]).

(11) Varnostne zahteve iz členov 33 do 43 naslova V „Varnost programa“ Uredbe (EU) 2021/696 Evropskega parlamenta in Sveta ([11]) štejejo za enakovredne zahtevam iz te uredbe, razen kar zadeva točko IS.I.OR.230 Priloge II k tej uredbi, katere zahteve bi morale biti izpolnjene.

(12) Da bi se zagotovila pravna varnost, bi bilo razlago izraza „informacijska varnost“, kot je opredeljen v tej uredbi in ki odraža splošno rabo v civilnem letalstvu po vsem svetu, treba šteti za skladno z razlago izraza „varnost omrežij in informacijskih sistemov“, kot je opredeljen v členu 4(2) Direktive (EU) 2016/1148. Opredelitev informacijske varnosti, ki se uporablja za namene te uredbe, se ne bi smela razlagati drugače kot opredelitev varnosti omrežij in informacijskih sistemov iz Direktive (EU) 2016/1148.

(13) Da bi se izognili podvajanju pravnih zahtev, kadar za organizacije, ki so zajete v tej uredbi, že veljajo varnostne zahteve, ki izhajajo iz aktov Unije, navedenih v uvodnih izjavah 10 in 11, in ki so po svojem učinku enakovredne določbam iz te uredbe, bi bilo treba skladnost z navedenimi varnostnimi zahtevami šteti za skladnost z zahtevami iz te uredbe.

(14) Organizacije, ki so zajete v tej uredbi in za katere že veljajo varnostne zahteve iz Uredbe (EU) 2015/1998 ali Uredbe (EU) 2021/696 ali obeh, bi morale izpolnjevati tudi zahteve iz Priloge II (del IS.I.OR.230 „Sistem zunanjega poročanja o informacijski varnosti“) k tej uredbi, saj nobena od obeh uredb ne vsebuje določb v zvezi z zunanjim poročanjem o informacijskovarnostnih incidentih.

(15) Da bi bila zagotovljena popolnost, bi bilo treba uredbe (EU) št. 1178/2011, (EU) št. 748/2012, (EU) št. 965/2012, (EU) št. 139/2014, (EU) št. 1321/2014, (EU) 2015/340 ter izvedbeni uredbi (EU) 2017/373 ([12]) in (EU) 2021/664 spremeniti, da se uvedejo zahteve za sistem upravljanja informacijske varnosti, predpisane v tej uredbi, skupaj s sistemi upravljanja, določenimi v njej, ter da se določijo zahteve za pristojne organe glede nadzora nad tem, ali organizacije izvajajo navedene zahteve za upravljanje informacijske varnosti.

(16) Da se organizacijam zagotovi dovolj časa za zagotovitev skladnosti z novimi pravili in postopki, bi se morala ta uredba začeti uporabljati tri leta po datumu začetka veljavnosti, razen za izvajalca navigacijskih služb zračnega prometa skupne evropske geostacionarne navigacijske storitve (EGNOS), opredeljenega v Izvedbeni uredbi Komisije (EU) 2017/373, za katerega bi se zaradi stalne varnostne akreditacije sistema in storitev EGNOS v skladu z Uredbo (EU) 2021/696 morala začeti uporabljati 1. januarja 2026.

(17) Zahteve iz te uredbe temeljijo na Mnenju št. 03/2021 ([13]), ki ga je Agencija izdala v skladu s členom 75(2), točki (b) in (c), ter členom 76(1) Uredbe (EU) 2018/1139.

([9]) Izvedbena uredba Komisije (EU) 2015/1998 z dne 5. novembra 2015 o določitvi podrobnih ukrepov za izvajanje skupnih osnovnih standardov za varovanje letalstva (UL L 299, 14.11.2015, str. 1).

([10]) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

([11]) Uredba (EU) 2021/696 Evropskega parlamenta in Sveta z dne 28. aprila 2021 o vzpostavitvi Vesoljskega programa Unije in ustanovitvi Agencije Evropske unije za vesoljski program ter razveljavitvi uredb (EU) št. 912/2010, (EU) št. 1285/2013 in (EU) št. 377/2014 in Sklepa št. 541/2014/EU (UL L 170, 12.5.2021, str. 69).

([12]) Izvedbena uredba Komisije (EU) 2017/373 z dne 1. marca 2017 o skupnih zahtevah za izvajalce storitev upravljanja zračnega prometa/izvajanja navigacijskih služb zračnega prometa in drugih funkcij omrežja za upravljanje zračnega prometa ter njihov nadzor, razveljavitvi Uredbe (ES) št. 482/2008, izvedbenih uredb (EU) št. 1034/2011, (EU) št. 1035/2011 in (EU) 2016/1377 ter spremembi Uredbe (EU) št. 677/2011 (UL L 62, 8.3.2017, str. 1).

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

(18) Zahteve iz te uredbe so skladne z mnenjem odbora za uporabo skupnih varnostnih predpisov na področju civilnega letalstva, ustanovljenega na podlagi člena 127 Uredbe (EU) 2018/1139 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Predmet urejanja

Ta uredba določa zahteve, ki jih morajo izpolnjevati organizacije in pristojni organi, da:

(a) opredelijo in obvladujejo tveganja za informacijsko varnost, ki bi lahko vplivala na varnost v letalstvu in sisteme informacijske in komunikacijske tehnologije ter podatke, ki se uporabljajo za namene civilnega letalstva,

(b) zaznajo informacijskovarnostne dogodke in opredelijo tiste, ki se štejejo za informacijskovarnostne incidente, ki bi lahko vplivali na varnost v letalstvu,

(c) se na navedene informacijskovarnostne incidente odzovejo in jih sanirajo.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za naslednje organizacije:

(a) vzdrževalne organizacije, za katere velja Oddelek A Priloge II (del 145) k Uredbi (EU) št. 1321/2014, razen tistih, ki so vključene izključno v vzdrževanje zrakoplovov v skladu s Prilogo Vb (del ML) k Uredbi (EU) št. 1321/2014;

(b) organizacije za vodenje stalne plovnosti (CAMO), za katere velja Oddelek A Priloge Vc (del CAMO) k Uredbi (EU) št. 1321/2014, razen tistih, ki so vključene izključno v vodenje stalne plovnosti zrakoplova v skladu s Prilogo Vb (del ML) k Uredbi (EU) št. 1321/2014;

(c) letalske prevoznike, za katere velja Priloga III (del ORO) k Uredbi (EU) št. 965/2012, razen tistih, ki so vključeni izključno v upravljanje katerega koli od naslednjih zrakoplovov:

(i) zrakoplov ELA2, kot je opredeljen v členu 1(2), točka (j), Uredbe (EU) št. 748/2012;

(ii) enomotorna propelerska letala z največjim operativnim številom potniških sedežev 5 ali manj, ki niso opredeljena kot kompleksni zrakoplovi na motorni pogon, kadar vzletajo in pristajajo na istem letališču ali območju delovanja ter obratujejo v skladu s pravili vizualnega letenja (VFR) podnevi;

(iii) enomotorni helikopterji z največjim operativnim številom potniških sedežev 5 ali manj, ki niso opredeljeni kot kompleksni zrakoplovi na motorni pogon, kadar vzletajo in pristajajo na istem letališču ali območju delovanja ter obratujejo v skladu s pravili VFR podnevi;

(d) odobrene organizacije za usposabljanje (ATO), za katere velja Priloga VII (del ORA) k Uredbi (EU) št. 1178/2011, razen tistih, ki so vključene izključno v dejavnosti usposabljanja za zrakoplov ELA2, kot je opredeljen v členu 1(2), točka (j), Uredbe (EU) št. 748/2012, ali so vključene izključno v teoretično usposabljanje;

(e) zdravstvene centre za letalsko osebje, za katere velja Priloga VII (del ORA) k Uredbi (EU) št. 1178/2011;

(f) operatorje naprav za simulacijo letenja (FSTD), za katere velja Priloga VII (del ORA) k Uredbi (EU) št. 1178/2011, razen tistih, ki so vključeni izključno v upravljanje naprav FSTD za zrakoplov ELA2, kot je opredeljen v členu 1(2), točka (j), Uredbe (EU) št. 748/2012;

(g) organizacije za usposabljanje kontrolorjev zračnega prometa (ATCO TO) in zdravstvene centre za letalsko osebje za kontrolorje zračnega prometa, za katere velja Priloga III (del ATCO.OR) k Uredbi (EU) 2015/340;

(h) organizacije, za katere velja Priloga III (del ATM/ANS.OR) k Izvedbeni uredbi (EU) 2017/373, razen naslednjih izvajalcev storitev:

(i) izvajalci navigacijskih služb zračnega prometa, ki imajo omejen certifikat v skladu s točko ATM/ANS.OR.A.010 navedene priloge;

(ii) izvajalci služb informacij za letenje, ki dajo izjavo o svojih dejavnostih v skladu s točko ATM/ANS.OR.A.015 navedene priloge;

(i) izvajalce služb U-space in enotne izvajalce skupnih informacijskih služb, za katere velja Izvedbena uredba (EU) 2021/664.

2. Ta uredba se uporablja za pristojne organe, vključno z Agencijo Evropske unije za varnost v letalstvu (v nadaljnjem besedilu: Agencija), iz člena 6 te uredbe in člena 5 Delegirane uredbe Komisije (EU) 2022/1645 ([14]).

3. Ta uredba se uporablja tudi za pristojni organ, odgovoren za izdajo, podaljšanje, spremembo, začasno ukinitev ali preklic licenc za vzdrževanje zrakoplova v skladu s Prilogo III (del 66) k Uredbi (EU) št. 1321/2014.

4. Ta uredba ne posega v zahteve glede informacijske in kibernetske varnosti iz točke 1.7 Priloge k Izvedbeni uredbi (EU) 2015/1998 in člena 14 Direktive (EU) 2016/1148.

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „informacijska varnost“ pomeni ohranjanje zaupnosti, celovitosti, avtentičnosti in razpoložljivosti omrežij in informacijskih sistemov;

(2) „informacijskovarnostni dogodek“ pomeni ugotovljen dogodek stanja sistema, storitve ali omrežja, ki kaže na morebitno kršitev politike informacijske varnosti ali neuspeh pri kontrolah informacijske varnosti ali na predhodno neznane razmere, ki so lahko pomembne za informacijsko varnost;

(3) „incident“ pomeni vsak dogodek, ki dejansko negativno vpliva na varnost omrežij in informacijskih sistemov, kot so opredeljeni v členu 4(7) Direktive (EU) 2016/1148;

(4) „tveganje za informacijsko varnost“ pomeni tveganje za organizacijske operacije civilnega letalstva, sredstva, posameznike in druge organizacije zaradi možnosti informacijskovarnostnega dogodka. Tveganja za informacijsko varnost so povezana z možnostjo, da bodo grožnje izkoristile ranljivosti informacijskega sredstva ali skupin informacijskih sredstev;

([14]) Delegirana uredba Komisije (EU) 2022/1645 z dne 14. julija 2022 o določitvi pravil za uporabo Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta glede zahtev za obvladovanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu, za organizacije, zajete v uredbah Komisije (EU) št. 748/2012 in (EU) št. 139/2014, ter o spremembi uredb Komisije (EU) št. 748/2012 in (EU) št. 139/2014 (UL L 248, 26.9.2022, str. 18).

(5) „grožnja“ pomeni morebitno kršitev informacijske varnosti, ki nastane zaradi subjekta, okoliščine, dejanja ali dogodka, ki bi lahko povzročil škodo;

(6) „ranljivost“ pomeni hibo ali pomanjkljivost v sredstvu ali sistemu, postopkih, zasnovi, izvajanju ali ukrepih za informacijsko varnost, ki bi jih bilo mogoče izkoristiti in katerih posledica je kršitev politike informacijske varnosti.

Člen 4

Zahteve za organizacije in pristojne organe

1. Organizacije iz člena 2(1) izpolnjujejo zahteve iz Priloge II (del IS.I.OR) k tej uredbi.

2. Pristojni organi iz člena 2(2) in (3) izpolnjujejo zahteve iz Priloge I (del IS.AR) k tej uredbi.

Člen 5

Zahteve, ki izhajajo iz druge zakonodaje Unije

1. Kadar organizacija iz člena 2(1) izpolnjuje varnostne zahteve, ki so določene v skladu s členom 14 Direktive (EU) 2016/1148 in so enakovredne zahtevam iz te uredbe, se skladnost z navedenimi varnostnimi zahtevami šteje za skladnost z zahtevami iz te uredbe.

2. Kadar je organizacija iz člena 2(1) operator ali subjekt iz nacionalnih programov varovanja v civilnem letalstvu držav članic, določenih v skladu s členom 10 Uredbe (ES) št. 300/2008 Evropskega parlamenta in Sveta ([15]), se zahteve glede kibernetske varnosti iz točke 1.7 Priloge k Izvedbeni uredbi (EU) 2015/1998 štejejo za enakovredne zahtevam iz te uredbe, razen kar zadeva točko IS.I.OR.230 Priloge II k tej uredbi, katere zahteve morajo biti izpolnjene.

3. Kadar je organizacija iz člena 2(1) izvajalec navigacijskih služb zračnega prometa skupne evropske geostacionarne navigacijske storitve (EGNOS) iz Uredbe (EU) 2021/696, se varnostne zahteve iz členov 33 do 43 naslova V navedene uredbe štejejo za enakovredne zahtevam iz te uredbe, razen kar zadeva točko IS.I.OR.230 Priloge II k tej uredbi, katere zahteve morajo biti izpolnjene.

4. Komisija lahko po posvetovanju z Agencijo in skupino za sodelovanje iz člena 11 Direktive (EU) 2016/1148 izda smernice za oceno enakovrednosti zahtev iz te uredbe in Direktive (EU) 2016/1148.

Člen 6

Pristojni organ

1. Brez poseganja v naloge, zaupane odboru za varnostno akreditacijo (SAB) iz člena 36 Uredbe (EU) 2021/696, je organ, pristojen za certificiranje in nadzor skladnosti s to uredbo, naslednji organ:

(a) v zvezi z organizacijami iz člena 2(1), točka (a), pristojni organ, imenovan v skladu s Prilogo II (del 145) k Uredbi (EU) št. 1321/2014;

(b) v zvezi z organizacijami iz člena 2(1), točka (b), pristojni organ, imenovan v skladu s Prilogo Vc (del CAMO) k Uredbi (EU) št. 1321/2014;

([15]) Uredba (ES) št. 300/2008 Evropskega parlamenta in Sveta z dne 11. marca 2008 o skupnih pravilih na področju varovanja civilnega letalstva in o razveljavitvi Uredbe (ES) št. 2320/2002 (UL L 97, 9.4.2008, str. 72).

(c) v zvezi z organizacijami iz člena 2(1), točka (c), pristojni organ, imenovan v skladu s Prilogo III (del ORO) k Uredbi (EU) št. 965/2012;

(d) v zvezi z organizacijami iz člena 2(1), točke (d) do (f), pristojni organ, imenovan v skladu s Prilogo VII (del ORA) k Uredbi (EU) št. 1178/2011;

(e) v zvezi z organizacijami iz člena 2(1), točka (g), pristojni organ, imenovan v skladu s členom 6(2) Uredbe (EU) 2015/340;

(f) v zvezi z organizacijami iz člena 2(1), točka (h), pristojni organ, imenovan v skladu s členom 4(1) Izvedbene uredbe (EU) 2017/373;

(g) v zvezi z organizacijami iz člena 2(1), točka (i), pristojni organ, imenovan v skladu s členom 14(1) ali členom 14(2), kot je ustrezno, Izvedbene uredbe (EU) 2021/664.

2. Države članice lahko za namene te uredbe imenujejo neodvisen in avtonomen subjekt za izpolnjevanje dodeljene vloge in obveznosti pristojnih organov iz odstavka 1. V tem primeru se med navedenim subjektom in pristojnimi organi, kot je navedeno v odstavku 1, vzpostavijo usklajevalni ukrepi, da se zagotovi učinkovit nadzor nad vsemi zahtevami, ki jih mora organizacija izpolnjevati.

3. Agencija ob popolnem upoštevanju veljavnih pravil o zaupnosti, varstvu osebnih podatkov in varovanju tajnih informacij sodeluje z Agencijo Evropske unije za vesoljski program (EUSPA) in odborom SAB iz člena 36 Uredbe (EU) 2021/696, da se zagotovi učinkovit nadzor nad zahtevami, ki se uporabljajo za izvajalca navigacijskih služb zračnega prometa storitve EGNOS.

Člen 7

Predložitev ustreznih informacij pristojnim organom na področju varnosti omrežij in informacijskih sistemov

Pristojni organi iz te uredbe enotno kontaktno točko, določeno v skladu s členom 8 Direktive (EU) 2016/1148, nemudoma obvestijo o vseh ustreznih informacijah, vključenih v obvestila, ki so jih v skladu s točko IS.I.OR.230 Priloge II k tej uredbi in točko IS.D.OR.230 Priloge I k Delegirani uredbi (EU) 2022/1645 (Delegirana uredba) predložili izvajalci bistvenih storitev, določeni v skladu s členom 5 Direktive (EU) 2016/1148.

Člen 8

Sprememba Uredbe (EU) št. 1178/2011

Prilogi VI (del ARA) in VII (del ORA) k Uredbi (EU) št. 1178/2011 se spremenita v skladu s Prilogo III k tej uredbi.

Člen 9

Sprememba Uredbe (EU) št. 748/2012

Priloga I (del 21) k Uredbi (EU) št. 748/2012 se spremeni v skladu s Prilogo IV k tej uredbi.

Člen 10

Sprememba Uredbe (EU) št. 965/2012

Prilogi II (del ARO) in III (del ORO) k Uredbi (EU) št. 965/2012 se spremenita v skladu s Prilogo V k tej uredbi.

Člen 11

Sprememba Uredbe (EU) št. 139/2014

Priloga II (del ADR.AR) k Uredbi (EU) št. 139/2014 se spremeni v skladu s Prilogo VI k tej uredbi.

Člen 12

Sprememba Uredbe (EU) št. 1321/2014

Priloge II (del 145), III (del 66) in Vc (del CAMO) k Uredbi (EU) št. 1321/2014 se spremenijo v skladu s Prilogo VII k tej uredbi.

Člen 13

Sprememba Uredbe (EU) 2015/340

Prilogi II (del ATCO.AR) in III (del ATCO.OR) k Uredbi (EU) 2015/340 se spremenita v skladu s Prilogo VIII k tej uredbi.

Člen 14

Sprememba Izvedbene uredbe (EU) 2017/373

Prilogi II (del ATM/ANS.AR) in III (del ATM/ANS.OR) k Izvedbeni uredbi (EU) 2017/373 se spremenita v skladu s Prilogo IX k tej uredbi.

Člen 15

Sprememba Izvedbene uredbe (EU) 2021/664

Izvedbena uredba (EU) 2021/664 se spremeni:

(1) v členu 15(1) se točka (f) nadomesti z naslednjim:

„(f) da izvajajo in vzdržujejo sistem upravljanja varnosti v skladu s točko ATM/ANS.OR.D.010 v poddelu D Priloge III k Izvedbeni uredbi (EU) 2017/373 ter sistem upravljanja informacijske varnosti v skladu s Prilogo II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203;";

(2) v členu 18 se doda naslednja točka l:

„(l) vzpostavijo, izvajajo in vzdržujejo sistem upravljanja informacijske varnosti v skladu s Prilogo I (del IS.AR) k Izvedbeni uredbi (EU) 2023/203.".

Člen 16

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Uporabljati se začne 22. februarja 2026.

Vendar se, kar zadeva primer izvajalca navigacijskih služb zračnega prometa storitve EGNOS, za katerega velja Izvedbena uredba (EU) 2017/373, začne uporabljati 1. januarja 2026.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 27. oktobra 2022

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA I

INFORMACIJSKA VARNOST – ZAHTEVE ZA ORGANE

[DEL IS.AR]

IS.AR.100 Področje uporabe

IS.AR.200 Sistem upravljanja informacijske varnosti (ISMS)

IS.AR.205 Ocena tveganja za informacijsko varnost

IS.AR.210 Obravnava tveganja za informacijsko varnost

IS.AR.215 Informacijskovarnostni incidenti – zaznavanje, odzivanje in sanacija

IS.AR.220 Naročanje dejavnosti upravljanja informacijske varnosti

IS.AR.225 Zahteve za osebje

IS.AR.230 Vodenje evidenc

IS.AR.235 Stalno izboljševanje

IS.AR.100 Področje uporabe

Ta del določa zahteve za upravljanje, ki jih morajo izpolnjevati pristojni organi iz člena 2(2) te uredbe.

Zahteve, ki jih morajo navedeni pristojni organi izpolnjevati za izvajanje dejavnosti certificiranja, nadzora in izvrševanja, so navedene v uredbah iz člena 2(1) te uredbe in člena 2 Delegirane uredbe (EU) 2022/1645.

IS.AR.200 Sistem upravljanja informacijske varnosti (ISMS)

(a) Za doseganje ciljev iz člena 1 pristojni organ vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti (ISMS), ki zagotavlja, da pristojni organ:

(1) oblikuje politiko o informacijski varnosti, ki določa splošna načela pristojnega organa v zvezi z morebitnim učinkom tveganj za informacijsko varnost na varnost v letalstvu;

(2) opredeli in pregleda tveganja za informacijsko varnost v skladu s točko IS.AR.205;

(3) opredeli in izvaja ukrepe za obravnavo tveganj za informacijsko varnost v skladu s točko IS.AR.210;

(4) v skladu s točko IS.AR.215 opredeli in izvaja ukrepe, potrebne za zaznavanje informacijskovarnostnih dogodkov, opredeli tiste, ki se štejejo za incidente, ki bi lahko vplivali na varnost v letalstvu, ter se odziva na navedene informacijskovarnostne incidente in jih sanira;

(5) izpolnjuje zahteve iz točke IS.AR.220, kadar se kateri koli del dejavnosti iz točke IS.AR.200 odda v izvajanje drugim organizacijam;

(6) izpolnjuje zahteve za osebje iz točke IS.AR.225.

(7) izpolnjuje zahteve za vodenje evidenc iz točke IS.AR.230;

(8) spremlja skladnost svoje organizacije z zahtevami iz te uredbe in osebi iz točke IS.AR.225(a) zagotavlja povratne informacije o ugotovitvah, da se zagotovi učinkovito izvajanje popravnih ukrepov;

(9) varuje zaupnost vseh informacij, ki jih pristojni organ morda sporoči organizacijam, ki so pod njegovim nadzorom, in informacij, prejetih prek sistemov zunanjega poročanja organizacije, vzpostavljenih v skladu s točko IS.I.OR.230 Priloge II (del IS.I.OR) k tej uredbi in točko IS.D.OR.230 Priloge (del IS.D.OR) k Delegirani uredbi (EU) 2022/1645;

(10) Agencijo obvešča o spremembah, ki vplivajo na zmogljivost pristojnega organa za opravljanje njegovih nalog in izvajanje njegovih obveznosti, kot je opredeljeno v tej uredbi;

(11) opredeljuje in izvaja postopke za praktično in pravočasno izmenjavo ustreznih informacij, kot je primerno, da pomaga drugim pristojnim organom in agencijam ter organizacijam, za katere velja ta uredba, da izvajajo učinkovite ocene tveganja za varnost v zvezi s svojimi dejavnostmi.

(b) Za stalno izpolnjevanje zahtev iz člena 1 pristojni organ izvaja postopek stalnega izboljševanja v skladu s točko IS.AR.235.

(c) Pristojni organ dokumentira vse ključne procese, postopke, vloge in obveznosti, potrebne za skladnost s točko IS.AR.200(a), ter vzpostavi proces za spremembo te dokumentacije.

(d) Procesi, postopki, vloge in obveznosti, ki jih pristojni organ določi za skladnost s točko IS.AR.200(a), ustrezajo naravi in kompleksnosti njegovih dejavnosti na podlagi ocene tveganj za informacijsko varnost, povezanih z navedenimi dejavnostmi, ter so lahko vključeni v druge obstoječe sisteme upravljanja, ki jih pristojni organ že izvaja.

IS.AR.205 Ocena tveganja za informacijsko varnost

(a) Pristojni organ opredeli vse elemente svoje organizacije, ki bi lahko bili izpostavljeni tveganjem za informacijsko varnost. To vključuje:

(1) dejavnosti, objekte in vire pristojnega organa ter storitve, ki jih pristojni organ izvaja, zagotavlja, prejema ali vzdržuje;

(2) opremo, sisteme, podatke in informacije, ki prispevajo k delovanju elementov iz točke 1.

(b) Pristojni organ opredeli vmesnike, ki jih ima njegova organizacija z drugimi organizacijami in ki bi lahko povzročili vzajemno izpostavljenost tveganjem za informacijsko varnost.

(c) Za elemente in vmesnike iz točk (a) in (b) pristojni organ opredeli tveganja za informacijsko varnost, ki bi lahko vplivala na varnost v letalstvu.

Pristojni organ za vsako ugotovljeno tveganje:

(1) določi stopnjo tveganja v skladu z vnaprej določeno klasifikacijo pristojnega organa;

(2) poveže vsako tveganje in njegovo raven z ustreznim elementom ali vmesnikom, opredeljenim v skladu s točkama (a) in (b).

Pri vnaprej določeni klasifikaciji iz točke 1 se upoštevata možnost pojava scenarija grožnje in resnost njegovih posledic za varnost. Na podlagi navedene klasifikacije in ob upoštevanju, ali ima pristojni organ strukturiran in ponovljiv postopek upravljanja tveganja za operacije, je pristojni organ sposoben ugotoviti, ali je tveganje sprejemljivo ali ga je treba obravnavati v skladu s točko IS.AR.210.

Za lažjo medsebojno primerljivost ocen tveganj se pri določanju stopnje tveganja v skladu s točko 1 upoštevajo ustrezne informacije, pridobljene v sodelovanju z organizacijami iz točke (b).

(d) Pristojni organ pregleda in posodobi oceno tveganja, opravljeno v skladu s točkami (a), (b) in (c), v katerem koli od naslednjih primerov:

(1) spremenijo se elementi, ki so izpostavljeni tveganjem za informacijsko varnost;

(2) spremenijo se vmesniki med organizacijo pristojnega organa in drugimi organizacijami ali tveganja, ki jih sporočijo druge organizacije;

(3) spremenijo se informacije ali znanje, ki se uporabljajo za opredelitev, analizo in klasifikacijo tveganj;

(4) pridobijo se izkušnje na podlagi analize informacijskovarnostnih incidentov.

IS.AR.210 Obravnava tveganja za informacijsko varnost

(a) Pristojni organ pripravi ukrepe za obravnavanje nesprejemljivih tveganj, ugotovljenih v skladu s točko IS.AR.205, jih pravočasno izvede in preveri njihovo nadaljnjo učinkovitost. Navedeni ukrepi pristojnemu organu omogočajo:

(1) nadzor nad okoliščinami, ki prispevajo k uspešnemu nastanku scenarija grožnje;

(2) zmanjšanje posledic za varnost v letalstvu, povezanih z uresničitvijo scenarija grožnje;

(3) izogibanje tveganjem.

Navedeni ukrepi ne uvajajo novih morebitnih nesprejemljivih tveganj za varnost v letalstvu.

(b) Oseba iz točke IS.AR.225(a) ter drugo zadevno osebje pristojnega organa se obvestijo o rezultatu ocene tveganja, izvedene v skladu s točko IS.AR.205, ustreznih scenarijih grožnje in ukrepih, ki jih je treba izvesti.

Pristojni organ obvesti tudi organizacije, s katerimi ima vmesnik v skladu s točko IS.AR.205(b), o kakršnem koli tveganju, skupnem pristojnemu organu in organizaciji.

IS.AR.215 Informacijskovarnostni incidenti – zaznavanje, odzivanje in sanacija

(a) Pristojni organ na podlagi rezultata ocene tveganja, izvedene v skladu s točko IS.AR.205, in rezultata obravnave tveganja, izvedene v skladu s točko IS.AR.210, izvaja ukrepe za zaznavanje dogodkov, ki kažejo morebitno uresničitev nesprejemljivih tveganj in ki bi lahko vplivali na varnost v letalstvu. Navedeni ukrepi za zaznavanje pristojnemu organu omogočajo, da:

(1) opredeli odstopanja od vnaprej določenih izhodišč za funkcionalno učinkovitost;

(2) sproži opozorila za aktiviranje ustreznih odzivnih ukrepov v primeru kakršnega koli odstopanja.

(b) Pristojni organ izvaja ukrepe za odziv na kakršne koli dogodke, opredeljene v skladu s točko (a), ki so prerasli v informacijskovarnostni incident ali bi vanj lahko prerasli. Navedeni ukrepi za odzivanje pristojnemu organu omogočajo, da:

(1) sproži odziv svoje organizacije na opozorila iz točke (a)(2) z aktiviranjem vnaprej določenih virov in potekov ukrepov;

(2) zajezi širjenje napada in prepreči, da bi se scenarij grožnje v celoti uresničil;

(3) nadzira vrsto okvare prizadetih elementov, opredeljenih v točki IS.AR.205(a).

(c) Pristojni organ izvaja ukrepe za saniranje informacijskovarnostnih incidentov, po potrebi vključno z nujnimi ukrepi. Navedeni sanacijski ukrepi pristojnemu organu omogočajo, da:

(1) odpravi stanje, ki je povzročilo incident, ali ga omeji na sprejemljivo raven;

(2) obnovi varno stanje prizadetih elementov, opredeljenih v točki IS.AR.205(a), v času sanacije, ki ga je predhodno določila njegova organizacija.

IS.AR.220 Naročanje dejavnosti upravljanja informacijske varnosti

Pristojni organ zagotovi, da pri oddaji naročila v zvezi s katerim koli delom dejavnosti iz točke IS.AR.200 drugim organizacijam pogodbene dejavnosti izpolnjujejo zahteve iz te uredbe in da organizacija, ki je dejavnost prevzela v izvajanje, dela pod njegovim nadzorom. Pristojni organ zagotovi, da se tveganja, povezana s pogodbenimi dejavnostmi, ustrezno obvladujejo.

IS.AR.225 Zahteve za osebje

Pristojni organ:

(a) ima na voljo osebo, ki ima pooblastilo, da vzpostavi ter vzdržuje organizacijske strukture, politike, procese in postopke, potrebne za izvajanje te uredbe.

Ta oseba:

(1) ima pooblastilo, da v celoti dostopa do virov, ki jih pristojni organ potrebuje za opravljanje vseh nalog, ki jih zahteva ta uredba;

(2) je pridobila prenos pooblastil, potrebnih za izvajanje dodeljenih obveznosti;

(b) ima vzpostavljen postopek, s katerim zagotovi, da ima na delovnem mestu dovolj osebja za izvajanje dejavnosti iz te priloge;

(c) ima vzpostavljen postopek za zagotovitev, da je osebje iz točke (b) ustrezno usposobljeno za opravljanje svojih nalog;

(d) ima vzpostavljen postopek za zagotovitev, da osebje priznava odgovornosti, povezane z dodeljenimi vlogami in nalogami;

(e) zagotovi, da sta identiteta in zanesljivost osebja, ki ima dostop do informacijskih sistemov in podatkov, za katere veljajo zahteve iz te uredbe, ustrezno določeni.

IS.AR.230 Vodenje evidence

(a) Pristojni organ vodi evidenco svojih dejavnosti upravljanja informacijske varnosti.

(1) Pristojni organ zagotovi, da so naslednje evidence arhivirane in sledljive:

(i) pogodbe za dejavnosti iz točke IS.AR.200(a)(5);

(ii) evidence ključnih procesov iz točke IS.AR.200(d);

(iii) evidence tveganj, opredeljenih v oceni tveganja iz točke IS.AR.205, skupaj s povezanimi ukrepi za obravnavo tveganja iz točke IS.AR.210;

(iv) evidence informacijskovarnostnih dogodkov, ki jih bo morda treba ponovno oceniti, da se razkrijejo neznani informacijskovarnostni incidenti ali ranljivosti.

(2) Evidence iz točke 1(i) se hranijo vsaj pet let po spremembi ali odpovedi pogodbe.

(3) Evidence iz točk 1(ii) in (iii) se hranijo vsaj pet let.

(4) Evidence iz točke 1(iv) se hranijo, dokler se navedeni informacijskovarnostni dogodki ponovno ne ocenijo v skladu s periodičnostjo, opredeljeno v postopku, ki ga določi pristojni organ.

(b) Pristojni organ vodi evidenco usposobljenosti in izkušenj svojega osebja, vključenega v dejavnosti upravljanja informacijske varnosti.

(1) Evidence o usposobljenosti in izkušnjah osebja se hranijo toliko časa, dokler oseba dela za pristojni organ, ter vsaj tri leta po tem, ko oseba zapusti pristojni organ.

(2) Članom osebja se na njihovo zahtevo omogoči dostop do njihovih individualnih evidenc. Poleg tega jim pristojni organ na njihovo zahtevo zagotovi kopijo njihovih individualnih evidenc ob odhodu iz pristojnega organa.

(c) Oblika evidenc se opredeli v postopkih pristojnega organa.

(d) Evidence se hranijo na način, ki zagotavlja zaščito pred škodo, spremembo in tatvino, pri čemer se informacije po potrebi opredelijo v skladu s stopnjo klasifikacije varnosti. Pristojni organ zagotovi, da se evidence hranijo s sredstvi za zagotovitev celovitosti, pristnosti in pooblaščenega dostopa.

IS.AR.235 Stalno izboljševanje

(a) Pristojni organ z ustreznimi kazalniki uspešnosti oceni učinkovitost in zrelost svojega sistema ISMS. Ocena se opravi na podlagi koledarja, ki ga pristojni organ vnaprej določi, ali po informacijskovarnostnem incidentu.

(b) Če se po oceni, opravljeni v skladu s točko (a), ugotovijo pomanjkljivosti, pristojni organ sprejme potrebne ukrepe za izboljšanje, s katerimi zagotovi, da ISMS še naprej izpolnjuje veljavne zahteve in ohranja tveganja za informacijsko varnost na sprejemljivi ravni. Poleg tega pristojni organ ponovno oceni tiste elemente sistema ISMS, na katere so vplivali sprejeti ukrepi.

PRILOGA II

INFORMACIJSKA VARNOST – ZAHTEVE ZA ORGANIZACIJE

[DEL IS.I.OR]

IS.I.OR.100 Področje uporabe

IS.I.OR.200 Sistem upravljanja informacijske varnosti (ISMS)

IS.I.OR.205 Ocena tveganja za informacijsko varnost

IS.I.OR.210 Obravnava tveganja za informacijsko varnost

IS.I.OR.215 Sistem notranjega poročanja o informacijski varnosti

IS.I.OR.220 Informacijskovarnostni incidenti – zaznavanje, odzivanje in sanacija

IS.I.OR.225 Odziv na ugotovitve, ki jih je sporočil pristojni organ

IS.I.OR.230 Sistem zunanjega poročanja o informacijski varnosti

IS.I.OR.235 Naročanje dejavnosti upravljanja informacijske varnosti

IS.I.OR.240 Zahteve za osebje

IS.I.OR.245 Vodenje evidenc

IS.I.OR.250 Priročnik za upravljanje informacijske varnosti (ISMM)

IS.I.OR.255 Spremembe sistema upravljanja informacijske varnosti

IS.I.OR.260 Stalno izboljševanje

IS.I.OR.100 Področje uporabe

Ta del določa zahteve, ki jih morajo izpolnjevati organizacije iz člena 2(1) te uredbe.

IS.I.OR.200 Sistem upravljanja informacijske varnosti (ISMS)

(a) Za doseganje ciljev iz člena 1 organizacija vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti (ISMS), ki zagotavlja, da organizacija:

(1) oblikuje politiko o informacijski varnosti, ki določa splošna načela organizacije v zvezi z morebitnim učinkom tveganj za informacijsko varnost na varnost v letalstvu;

(2) opredeli in pregleda tveganja za informacijsko varnost v skladu s točko IS.I.OR.205;

(3) opredeljuje in izvaja ukrepe za obravnavo tveganj za informacijsko varnost v skladu s točko IS.I.OR.210;

(4) izvaja sistem notranjega poročanja o informacijski varnosti v skladu s točko IS.I.OR.215;

(5) v skladu s točko IS.I.OR.220 opredeli in izvaja ukrepe, potrebne za zaznavanje informacijskovarnostnih dogodkov, opredeli tiste dogodke, ki se štejejo za incidente, ki bi lahko vplivali na varnost v letalstvu, razen v primerih, ki jih dovoljuje točka IS.I.OR.205(e), ter se odziva na te informacijskovarnostne incidente in jih sanira;

(6) izvaja ukrepe, ki jih je pristojni organ sporočil kot takojšen odziv na incident ali ranljivost v zvezi z informacijsko varnostjo, ki vpliva na varnost v letalstvu;

(7) sprejme ustrezne ukrepe v skladu s točko IS.I.OR.225 za obravnavanje ugotovitev, ki jih je sporočil pristojni organ;

(8) izvaja sistem zunanjega poročanja v skladu s točko IS.I.OR.230, da se pristojnemu organu omogoči sprejetje ustreznih ukrepov;

(9) izpolnjuje zahteve iz točke IS.I.OR.235, kadar se kateri koli del dejavnosti iz točke IS.I.OR.200 odda v izvajanje drugim organizacijam;

(10) izpolnjuje zahteve za osebje iz točke IS.I.OR.240;

(11) izpolnjuje zahteve za vodenje evidenc iz točke IS.I.OR.245;

(12) spremlja skladnost organizacije z zahtevami iz te uredbe in odgovornemu vodji zagotavlja povratne informacije o ugotovitvah, da se zagotovi učinkovito izvajanje popravnih ukrepov;

(13) brez poseganja v veljavne zahteve glede poročanja o incidentih varuje zaupnost vseh informacij glede na njihovo stopnjo občutljivosti, ki jih je organizacija morda prejela od drugih organizacij.

(b) Za stalno izpolnjevanje zahtev iz člena 1 organizacija izvaja postopek stalnega izboljševanja v skladu s točko IS.I.OR.260.

(c) Organizacija v skladu s točko IS.I.OR.250 dokumentira vse ključne procese, postopke, vloge in obveznosti, potrebne za skladnost s točko IS.I.OR.200(a), ter vzpostavi proces za spremembo navedene dokumentacije. Spremembe navedenih procesov, postopkov, vlog in obveznosti se upravljajo v skladu s točko IS.I.OR.255.

(d) Procesi, postopki, vloge in obveznosti, ki jih organizacija določi za skladnost s točko IS.I.OR.200(a), ustrezajo naravi in kompleksnosti njenih dejavnosti na podlagi ocene tveganj za informacijsko varnost, povezanih z navedenimi dejavnostmi, ter so lahko vključeni v druge obstoječe sisteme upravljanja, ki jih organizacija že izvaja.

(e) Brez poseganja v obveznost izpolnjevanja zahtev glede poročanja iz Uredbe (EU) št. 376/2014 in v zahteve iz točke IS.I.OR.200(a)(13) lahko pristojni organ organizaciji odobri, da ne izvaja zahtev iz točk (a) do (d) in povezanih zahtev iz točk IS.I.OR.205 do IS.I.OR.260, če navedenemu organu zadovoljivo dokaže, da njene dejavnosti, objekti in viri ter storitve, ki jih izvaja, zagotavlja, prejema in vzdržuje, niti zase niti za druge organizacije ne pomenijo nobenega tveganja za informacijsko varnost, ki bi lahko vplivalo na varnost v letalstvu. Odobritev temelji na dokumentirani oceni tveganja za informacijsko varnost, ki jo izvede organizacija ali tretja oseba v skladu s točko IS.I.OR.205 ter pregleda in odobri njen pristojni organ.

Nadaljnjo veljavnost navedene odobritve bo pregledal pristojni organ po veljavnem ciklu presoje nadzora in kadar se bodo izvedle spremembe na področju dela organizacije.

IS.I.OR.205 Ocena tveganja za informacijsko varnost

(a) Organizacija opredeli vse svoje elemente, ki bi lahko bili izpostavljeni tveganjem za informacijsko varnost. To vključuje:

(1) dejavnosti, objekte in vire organizacije ter storitve, ki jih organizacija izvaja, zagotavlja, prejema ali vzdržuje;

(2) opremo, sisteme, podatke in informacije, ki prispevajo k delovanju elementov iz točke 1.

(b) Organizacija opredeli vmesnike, ki jih ima z drugimi organizacijami in ki bi lahko povzročili vzajemno izpostavljenost tveganjem za informacijsko varnost.

(c) V zvezi z elementi in vmesniki iz točk (a) in (b) organizacija opredeli tveganja za informacijsko varnost, ki bi lahko vplivala na varnost v letalstvu. Organizacija za vsako ugotovljeno tveganje:

(1) določi stopnjo tveganja v skladu z vnaprej določeno klasifikacijo organizacije;

(2) poveže vsako tveganje in njegovo raven z ustreznim elementom ali vmesnikom, opredeljenim v skladu s točkama (a) in (b).

Pri vnaprej določeni klasifikaciji iz točke 1 se upoštevata možnost pojava scenarija grožnje in resnost njegovih posledic za varnost. Na podlagi navedene klasifikacije ter ob upoštevanju, ali ima organizacija strukturiran in ponovljiv postopek upravljanja tveganja za operacije, je organizacija sposobna ugotoviti, ali je tveganje sprejemljivo ali ga je treba obravnavati v skladu s točko IS.I.OR.210.

Za lažjo medsebojno primerljivost ocen tveganj se pri določanju stopnje tveganja v skladu s točko 1 upoštevajo ustrezne informacije, pridobljene v sodelovanju z organizacijami iz točke (b).

(d) Organizacija pregleda in posodobi oceno tveganja, opravljeno v skladu s točkama (a) in (b) ter po potrebi točkama (c) ali (e), v katerem koli od naslednjih primerov:

(1) spremenijo se elementi, ki so izpostavljeni tveganjem za informacijsko varnost;

(2) spremenijo se vmesniki med organizacijo in drugimi organizacijami ali tveganja, ki jih sporočijo druge organizacije;

(3) spremenijo se informacije ali znanje, ki se uporabljajo za opredelitev, analizo in klasifikacijo tveganj;

(4) pridobijo se izkušnje na podlagi analize informacijskovarnostnih incidentov.

(e) Z odstopanjem od točke (c) organizacije, ki morajo izpolnjevati zahteve iz poddela C Priloge III (del ATM/ANS.OR) k Izvedbeni Uredbi (EU) 2017/373, nadomestijo analizo vpliva na varnost v letalstvu z analizo vpliva na njihove storitve v skladu z oceno varnosti iz točke ATM/ANS.OR.C.005. Ocena varnosti je na voljo izvajalcem služb zračnega prometa, za katere izvajajo storitve, navedeni izvajalci služb zračnega prometa pa so odgovorni za ocenjevanje vpliva na varnost v letalstvu.

IS.I.OR.210 Obravnava tveganja za informacijsko varnost

(a) Organizacija pripravi ukrepe za obravnavanje nesprejemljivih tveganj, ugotovljenih v skladu s točko IS.I.OR.205, jih pravočasno izvede in preveri njihovo nadaljnjo učinkovitost. Navedeni ukrepi organizaciji omogočajo:

(1) nadzor nad okoliščinami, ki prispevajo k uspešnemu nastanku scenarija grožnje;

(2) zmanjšanje posledic za varnost v letalstvu, povezanih z uresničitvijo scenarija grožnje;

(3) izogibanje tveganjem.

Navedeni ukrepi ne uvajajo novih morebitnih nesprejemljivih tveganj za varnost v letalstvu.

(b) Oseba iz točke IS.I.OR.240(a) in (b) ter drugo zadevno osebje organizacije se obvestijo o rezultatu ocene tveganja, izvedene v skladu s točko IS.I.OR.205, ustreznih scenarijih grožnje in ukrepih, ki jih je treba izvesti.

Organizacija obvesti tudi organizacije, s katerimi ima vmesnik v skladu s točko IS.I.OR.205(b), o kakršnem koli tveganju, skupnem obema organizacijama.

IS.I.OR.215 Sistem notranjega poročanja o informacijski varnosti

(a) Organizacija vzpostavi notranji sistem poročanja, da se omogoči zbiranje in ocenjevanje informacijskovarnostnih dogodkov, vključno s tistimi, o katerih je treba poročati v skladu s točko IS.I.OR.230.

(b) Navedena shema in postopek iz točke IS.I.OR.220 organizaciji omogočata, da:

(1) ugotovi, kateri dogodki, sporočeni v skladu s točko (a), se štejejo za informacijskovarnostne incidente ali ranljivosti, ki bi lahko vplivali na varnost v letalstvu;

(2) ugotovi vzroke in dejavnike, ki prispevajo k informacijskovarnostnim incidentom in ranljivostim, opredeljenim v skladu s točko 1, ter jih obravnava v okviru postopka upravljanja tveganja za informacijsko varnost v skladu s točkama IS.I.OR.205 in IS.I.OR.220;

(3) zagotovi oceno vseh znanih, relevantnih informacij v zvezi z informacijskovarnostnimi incidenti in ranljivostmi, opredeljenimi v skladu s točko 1;

(4) zagotovi izvajanje metode za interno razširjanje informacij po potrebi.

(c) Vsaka organizacija, ki je prevzela v izvajanje dejavnost in lahko organizacijo izpostavi tveganjem za informacijsko varnost, ki bi lahko vplivala na varnost v letalstvu, mora organizaciji poročati o informacijskovarnostnih dogodkih. Navedena poročila se predložijo po postopkih, določenih v posebnih pogodbenih dogovorih, in se ocenijo v skladu s točko (b).

(d) Organizacija pri preiskavah sodeluje s katero koli drugo organizacijo, ki znatno prispeva k informacijski varnosti lastnih dejavnosti.

(e) Organizacija lahko navedeni sistem poročanja vključi v druge sisteme poročanja, ki jih je že uvedla.

IS.I.OR.220 Informacijskovarnostni incidenti – zaznavanje, odzivanje in sanacija

(a) Organizacija na podlagi rezultata ocene tveganja, izvedene v skladu s točko IS.I.OR.205, in rezultata obravnave tveganja, izvedene v skladu s točko IS.I.OR.210, izvaja ukrepe za zaznavanje incidentov in ranljivosti, ki kažejo morebitno uresničitev nesprejemljivih tveganj in ki bi lahko vplivali na varnost v letalstvu. Navedeni ukrepi za zaznavanje organizaciji omogočajo, da:

(1) opredeli odstopanja od vnaprej določenih izhodišč za funkcionalno učinkovitost;

(2) sproži opozorila za aktiviranje ustreznih odzivnih ukrepov v primeru kakršnega koli odstopanja.

(b) Organizacija izvaja ukrepe za odziv na kakršne koli dogodke, opredeljene v skladu s točko (a), ki so prerasli v informacijskovarnostni incident ali bi vanj lahko prerasli. Navedeni ukrepi za odzivanje organizaciji omogočajo, da:

(1) sproži odziv na opozorila iz točke (a)(2) z aktiviranjem vnaprej določenih virov in potekov ukrepov;

(2) zajezi širjenje napada in prepreči, da bi se scenarij grožnje v celoti uresničil;

(3) nadzira vrsto okvare prizadetih elementov, opredeljenih v točki IS.I.OR.205(a).

(c) Organizacija izvaja ukrepe za saniranje informacijskovarnostnih incidentov, po potrebi vključno z nujnimi ukrepi. Navedeni sanacijski ukrepi organizaciji omogočajo, da:

(1) odpravi stanje, ki je povzročilo incident, ali ga omeji na sprejemljivo raven;

(2) doseže varno stanje prizadetih elementov, opredeljenih v točki IS.I.OR.205(a), v času sanacije, ki ga je predhodno določila organizacija.

IS.I.OR.225 Odziv na ugotovitve, ki jih je sporočil pristojni organ

(a) Organizacija po prejemu obvestila o ugotovitvah, ki ga predloži pristojni organ:

(1) opredeli temeljni vzrok ali vzroke za neskladnost in dejavnike, ki prispevajo k njej;

(2) opredeli načrt popravnih ukrepov;

(3) pristojnemu organu zadovoljivo dokaže odpravo neskladnosti.

(b) Ukrepi iz točke (a) se izvedejo v roku, dogovorjenem s pristojnim organom.

IS.I.OR.230 Sistem zunanjega poročanja o informacijski varnosti

(a) Organizacija izvaja sistem poročanja o informacijski varnosti, ki izpolnjuje zahteve iz Uredbe (EU) št. 376/2014 ter njenih delegiranih in izvedbenih aktov, če se navedena uredba uporablja za organizacijo.

(b) Brez poseganja v obveznosti iz Uredbe (EU) št. 376/2014 organizacija zagotovi, da se o vsakem informacijskovarnostnem incidentu ali ranljivosti, ki lahko pomeni znatno tveganje za varnost v letalstvu, poroča njenemu pristojnemu organu. Poleg tega:

(1) kadar tak incident ali ranljivost vpliva na zrakoplov ali z njim povezan sistem ali komponento, organizacija o tem poroča tudi nosilcu odobritve projekta;

(2) kadar tak incident ali ranljivost vpliva na sistem ali komponento, ki jo uporablja organizacija, organizacija o tem poroča organizaciji, odgovorni za projektiranje sistema ali komponente.

(c) Organizacija poroča o pogojih iz točke (b), kot sledi:

(1) obvestilo se predloži pristojnemu organu in po potrebi nosilcu odobritve projekta ali organizaciji, odgovorni za projektiranje sistema ali komponente, takoj ko se organizacija seznani s stanjem;

(2) poročilo se predloži pristojnemu organu in po potrebi nosilcu odobritve projekta ali organizaciji, odgovorni za projektiranje sistema ali komponente, čim prej, vendar ne pozneje kot 72 ur od trenutka, ko se je organizacija seznanila s stanjem, razen če to preprečujejo izjemne okoliščine.

Poročilo se pripravi v obliki, ki jo določi pristojni organ, in vsebuje vse ustrezne informacije o stanju, s katerim je organizacija seznanjena;

(3) pristojnemu organu in po potrebi nosilcu odobritve projekta ali organizaciji, odgovorni za projektiranje sistema ali komponente, se predložijo nadaljnje poročilo, v katerem so podrobno navedeni ukrepi, ki jih je organizacija sprejela ali jih namerava sprejeti za sanacijo incidenta, in ukrepi, ki jih namerava sprejeti za preprečitev podobnih informacijskovarnostnih incidentov v prihodnosti.

Nadaljnje poročilo se predloži, takoj ko so opredeljeni navedeni ukrepi, in se pripravi v obliki, ki jo določi pristojni organ.

IS.I.OR.235 Naročanje dejavnosti upravljanja informacijske varnosti

(a) Organizacija zagotovi, da pri oddaji naročila v zvezi s katerim koli delom dejavnosti iz točke IS.I.OR.200 drugim organizacijam pogodbene dejavnosti izpolnjujejo zahteve iz te uredbe in da organizacija, ki je dejavnost prevzela v izvajanje, dela pod njenim nadzorom. Organizacija zagotovi, da se tveganja, povezana s pogodbenimi dejavnostmi, ustrezno obvladujejo.

(b) Organizacija zagotovi, da pristojni organ na zahtevo lahko pridobi dostop do organizacije, ki je dejavnost prevzela v izvajanje, da preveri stalno skladnost z ustreznimi zahtevami iz te uredbe.

IS.I.OR.240 Zahteve za osebje

(a) Odgovorni vodja organizacije, imenovan v skladu z uredbami (EU) št. 1321/2014, (EU) št. 965/2012, (EU) št. 1178/2011, (EU) 2015/340, Izvedbeno uredbo (EU) 2017/373 ali Izvedbeno uredbo (EU) 2021/664, kot se uporablja, iz člena 2(1) te uredbe, ima pooblastilo podjetja, da zagotovi financiranje in izvajanje vseh dejavnosti, ki jih zahteva ta uredba. Ta oseba:

(1) zagotovi, da so na voljo vsi potrebni viri za izpolnjevanje zahtev iz te uredbe;

(2) vzpostavi in spodbuja politiko informacijske varnosti iz točke IS.I.OR.200(a)(1);

(3) izkazuje osnovno razumevanje te uredbe.

(b) Odgovorni vodja imenuje osebo ali skupino oseb za zagotovitev, da organizacija izpolnjuje zahteve iz te uredbe, in opredeli obseg njihovih pooblastil. Navedena oseba ali skupina oseb poroča neposredno odgovornemu vodji ter ima ustrezno znanje, izobrazbo in izkušnje za izvajanje svojih obveznosti. V postopkih se določi, kdo nadomešča neko osebo v primeru njene daljše odsotnosti.

(c) Odgovorni vodja imenuje osebo ali skupino oseb z obveznostjo za upravljanje funkcije spremljanja skladnosti iz točke IS.I.OR.200(a)(12).

(d) Kadar organizacija deli organizacijske strukture, politike, procese in postopke za informacijsko varnost z drugimi organizacijami ali področji svoje organizacije, ki niso del odobritve ali izjave, lahko odgovorni vodja prenese svoje dejavnosti na skupno odgovorno osebo.

V takem primeru se določijo usklajevalni ukrepi med odgovornim vodjo organizacije in skupno odgovorno osebo, da se zagotovi ustrezna vključitev upravljanja informacijske varnosti v organizacijo.

(e) Odgovorni vodja ali skupna odgovorna oseba iz točke (d) ima pooblastilo podjetja za vzpostavitev in vzdrževanje organizacijskih struktur, politik, procesov in postopkov, potrebnih za izvajanje točke IS.I.OR.200.

(f) Organizacija ima vzpostavljen postopek, s katerim zagotovi, da ima na delovnem mestu dovolj osebja za izvajanje dejavnosti iz te priloge.

(g) Organizacija ima vzpostavljen postopek za zagotovitev, da je osebje iz točke (f) ustrezno usposobljeno za opravljanje svojih nalog.

(h) Organizacija ima vzpostavljen postopek za zagotovitev, da osebje priznava odgovornosti, povezane z dodeljenimi vlogami in nalogami.

(i) Organizacija zagotovi, da sta identiteta in zanesljivost osebja, ki ima dostop do informacijskih sistemov in podatkov, za katere veljajo zahteve iz te uredbe, ustrezno določeni.

IS.I.OR.245 Vodenje evidence

(a) *Organizacija vodi evidenco svojih dejavnosti upravljanja informacijske varnosti.*

(1) Organizacija zagotovi, da so naslednje evidence arhivirane in sledljive:

(i) vse prejete odobritve in vse povezane ocene tveganja za informacijsko varnost v skladu s točko IS.I.OR.200(e);

(ii) pogodbe za dejavnosti iz točke IS.I.OR.200(a)(9);

(iii) evidence ključnih procesov iz točke IS.I.OR.200(d);

(iv) evidence tveganj, opredeljenih v oceni tveganja iz točke IS.I.OR.205, skupaj s povezanimi ukrepi za obravnavo tveganja iz točke IS.I.OR.210;

(v) evidence informacijskovarnostnih incidentov in ranljivosti, sporočenih v skladu s shemami poročanja iz točk IS.I.OR.215 in IS.I.OR.230;

(vi) evidence informacijskovarnostnih dogodkov, ki jih bo morda treba ponovno oceniti, da se razkrijejo nezaznani informacijskovarnostni incidenti ali ranljivosti.

(2) Evidence iz točke 1(i) se hranijo vsaj pet let po prenehanju veljavnosti odobritve.

(3) Evidence iz točke 1(ii) se hranijo vsaj pet let po spremembi ali odpovedi pogodbe.

(4) Evidence iz točk 1(iii), (iv) in (v) se hranijo vsaj pet let.

(5) Evidence iz točke 1(vi) se hranijo, dokler se navedeni informacijskovarnostni dogodki ponovno ne ocenijo v skladu s periodičnostjo, opredeljeno v postopku, ki ga določi organizacija.

(b) *Organizacija vodi evidenco usposobljenosti in izkušenj svojega osebja, vključenega v dejavnosti upravljanja informacijske varnosti.*

(1) Evidence o usposobljenosti in izkušnjah osebja se hranijo toliko časa, dokler oseba dela za organizacijo, in vsaj tri leta po tem, ko oseba zapusti organizacijo.

(2) Članom osebja se na njihovo zahtevo omogoči dostop do njihovih individualnih evidenc. Poleg tega jim organizacija na njihovo zahtevo zagotovi kopijo njihovih individualnih evidenc ob odhodu iz organizacije.

(c) Oblika evidenc se opredeli v postopkih organizacije.

(d) Evidence se hranijo na način, ki zagotavlja zaščito pred škodo, spremembo in tatvino, pri čemer se informacije po potrebi opredelijo v skladu s stopnjo klasifikacije varnosti. Organizacija zagotovi, da se evidence hranijo s sredstvi za zagotovitev celovitosti, pristnosti in pooblaščenega dostopa.

IS.I.OR.250 Priročnik za upravljanje informacijske varnosti (ISMM)

(a) Organizacija da pristojnemu organu na voljo priročnik za upravljanje informacijske varnosti (ISMM) ter, kadar je ustrezno, vse pripadajoče priročnike in postopke, na katere se sklicuje, z naslednjo vsebino:

(1) izjava, ki jo je podpisal odgovorni vodja in ki potrjuje, da bo organizacija vedno delovala v skladu s to prilogo in ISMM. Če odgovorni vodja ni glavni direktor organizacije, potem glavni direktor sopodpiše izjavo;

(2) nazivi, imena, dolžnosti, odgovornosti, obveznosti in pooblastila osebe ali oseb iz točk IS.I.OR.240(b) in (c);

(3) naziv, ime, dolžnosti, odgovornosti, obveznosti in pooblastilo skupne odgovorne osebe iz točke IS.I.OR.240(d), če je ustrezno;

(4) politika informacijske varnosti organizacije iz točke IS.I.OR.200(a)(1);

(5) splošen opis števila in kategorij članov osebja ter sistema, vzpostavljenega za načrtovanje razpoložljivosti osebja, kot se zahteva v točki IS.I.OR.240;

(6) nazivi, imena, dolžnosti, odgovornosti, obveznosti in pooblastila ključnih oseb, odgovornih za izvajanje točke IS.I.OR.200, vključno z osebo ali osebami, odgovornimi za funkcijo spremljanja skladnosti iz točke IS.I.OR.200(a)(12);

(7) organigram, ki prikazuje povezane verige odgovornosti in obveznosti za osebe iz točk 2 in 6;

(8) opis sistema notranjega poročanja iz točke IS.I.OR.215;

(9) postopki, ki določajo, kako organizacija zagotavlja skladnost s tem delom, in zlasti:

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

(ii) postopki, ki opredeljujejo, kako organizacija nadzira katere koli pogodbene dejavnosti iz točke IS.I.OR.200(a)(9);

(iii) postopek spremembe ISMM iz točke (c);

(10) podrobnosti trenutno odobrenih drugih načinov usklajevanja.

(b) Prvo izdajo ISMM odobri pristojni organ in obdrži njeno kopijo. ISMM se po potrebi spremeni, da ostaja ažuren opis sistema ISMS organizacije. Pristojnemu organu se predloži kopija vseh sprememb ISMM.

(c) Spremembe ISMM se upravljajo po postopku, ki ga določi organizacija. Vse spremembe, ki niso vključene v področje uporabe tega postopka, in vse spremembe, povezane s spremembami, navedenimi v točki IS.I.OR.255(b), odobri pristojni organ.

(d) Organizacija lahko ISMM poveže z drugimi priročniki za upravljanje, ki jih ima na voljo, če obstaja jasno navzkrižno sklicevanje, ki kaže, kateri deli priročnika za upravljanje ustrezajo različnim zahtevam iz te priloge.

IS.I.OR.255 Spremembe sistema upravljanja informacijske varnosti

(a) Spremembe sistema ISMS se lahko upravljajo in sporočijo pristojnemu organu s postopkom, ki ga razvije organizacija. Ta postopek odobri pristojni organ.

(b) V zvezi s spremembami sistema ISMS, ki niso zajete v postopku iz točke (a), organizacija zaprosi za odobritev pristojnega organa in jo pridobi.

V zvezi z navedenimi spremembami:

(1) se predloži zahtevek pred izvedbo vsake take spremembe, da bi pristojni organ lahko ugotovil, ali je zagotovljena stalna skladnost s to uredbo, ter da bi po potrebi spremenil certifikat organizacije in z njim povezane pogoje za odobritev, ki so mu priloženi;

(2) organizacija da pristojnemu organu na voljo vse informacije, ki jih zahteva za oceno spremembe;

(3) sprememba se izvede šele po prejemu uradne odobritve pristojnega organa;

(4) organizacija med izvajanjem takih sprememb deluje pod pogoji, ki jih predpiše pristojni organ.

IS.I.OR.260 Stalno izboljševanje

(a) Organizacija z ustreznimi kazalniki uspešnosti oceni učinkovitost in zrelost sistema ISMS. Ta ocena se izvede na podlagi koledarja, ki ga organizacija vnaprej določi, ali po informacijskovarnostnem incidentu.

(b) Če se po oceni, opravljeni v skladu s točko (a), ugotovijo pomanjkljivosti, organizacija sprejme potrebne ukrepe za izboljšanje, s katerimi zagotovi, da ISMS še naprej izpolnjuje veljavne zahteve in tveganja za informacijsko varnost ohranja na sprejemljivi ravni. Poleg tega organizacija ponovno oceni tiste elemente sistema ISMS, na katere so vplivali sprejeti ukrepi.

PRILOGA III

Prilogi VI (del ARA) in VII (del ORA) k Uredbi (EU) št. 1178/2011 se spremenita na naslednji način:

(1) Priloga VI (del ARA) se spremeni:

(a) v točki ARA.GEN.125 se doda naslednja točka (c):

„(c) Pristojni organ države članice Agenciji čim prej zagotovi informacije, pomembne za varnost, ki izhajajo iz poročil o informacijski varnosti, ki jih je prejel na podlagi točke IS.I.OR.230 Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203.“;

(b) za točko ARA.GEN.135 se vstavi naslednja točka ARA.GEN.135A:

„**ARA.GEN.135A Takojšen odziv na informacijskovarnostni incident ali ranljivost, ki vpliva na varnost v letalstvu**

(a) Pristojni organ vzpostavi sistem za ustrezno zbiranje, analiziranje in razširjanje informacij v zvezi z informacijskovarnostnimi incidenti in ranljivostmi, ki lahko vplivajo na varnost v letalstvu, o katerih poročajo organizacije. To se izvede ob usklajevanju z vsemi drugimi ustreznimi organi, odgovornimi za informacijsko ali kibernetsko varnost v državi članici, da se okrepita usklajevanje in združljivost sistemov poročanja.

(b) Agencija vzpostavi sistem za ustrezno analiziranje vseh ustreznih informacij, pomembnih za varnost in prejetih v skladu s točko ARA.GEN.125(c), ter državam članicam in Komisiji nemudoma zagotovi vse informacije, vključno s priporočili ali popravnimi ukrepi, ki jih morajo sprejeti za pravočasen odziv na informacijskovarnostni incident ali ranljivost, ki lahko vpliva na varnost v letalstvu in je v zvezi s proizvodi, deli, nenameščeno opremo, osebami ali organizacijami, za katere se uporabljajo Uredba (EU) 2018/1139 ter njeni delegirani in izvedbeni akti.

(c) Pristojni organ po prejemu informacij iz točk (a) in (b) sprejme ustrezne ukrepe za obravnavo morebitnega vpliva informacijskovarnostnega incidenta ali ranljivosti na varnost v letalstvu.

(d) Ukrepi, sprejeti v skladu s točko (c), se takoj sporočijo vsem osebam ali organizacijam, ki jih upoštevajo v skladu z Uredbo (EU) 2018/1139 ter njenimi delegiranimi in izvedbenimi akti. Pristojni organ države članice o navedenih ukrepih obvesti tudi Agencijo, in, če se zahteva skupno ukrepanje, pristojne organe drugih zadevnih držav članic.“;

(c) v točki ARA.GEN.200 se doda naslednja točka (e):

„(e) Sistem upravljanja, ki ga vzpostavi in vzdržuje pristojni organ, poleg zahtev iz točke (a) izpolnjuje tudi zahteve iz Priloge I (del IS.AR) k Izvedbeni uredbi (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(d) točka ARA.GEN.205 se spremeni:

(i) naslov se nadomesti z naslednjim:

„**ARA.GEN.205 Dodelitev nalog**“;

(ii) doda se naslednja točka (c):

„(c) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko ORA.GEN.200A, lahko pristojni organ dodeli naloge kvalificiranim subjektom v skladu s točko (a) ali kateremu koli ustreznemu organu, odgovornemu za informacijsko ali kibernetsko varnost v državi članici. Pri dodelitvi nalog pristojni organ zagotovi, da:

(1) kvalificirani subjekt ali ustrezni organ usklajuje in upošteva vse vidike v zvezi z varnostjo v letalstvu;

(2) se rezultati dejavnosti certificiranja in nadzora, ki jih izvede kvalificirani subjekt ali ustrezni organ, vključijo v splošno dokumentacijo organizacije v zvezi s certificiranjem in nadzorom;

(3) njegov sistem upravljanja informacijske varnosti, vzpostavljen v skladu s točko ARA.GEN.200(e), zajema vse naloge certificiranja in stalnega nadzora, ki se izvajajo v njegovem imenu.“;

(e) v točki ARA.GEN.300 se doda naslednja točka (g):

„(g) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko ORA.GEN.200A, pristojni organ poleg upoštevanja točk od (a) do (f) pregleda tudi vse odobritve, izdane v skladu s točko IS.I.OR.200(e) te uredbe ali točko IS.D.OR.200(e) Delegirane uredbe (EU) 2022/1645, potem ko se izvede veljavni cikel presoje nadzora in kadar se izvedejo spremembe na področju dela organizacije.“;

(f) za točko ARA.GEN.330 se vstavi naslednja točka ARA.GEN.330A:

„**ARA.GEN.330A Spremembe sistema upravljanja informacijske varnosti**

(a) Kar zadeva spremembe, ki se upravljajo in sporočijo pristojnemu organu v skladu s postopkom iz točke IS.I.OR.255(a) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203, pristojni organ vključi pregled takih sprememb v svoj stalni nadzor v skladu z načeli iz točke ARA.GEN.300. V primeru ugotovljene neskladnosti pristojni organ o tem obvesti organizacijo, zahteva nadaljnje spremembe in ukrepa v skladu s točko ARA.GEN.350.

(b) Kar zadeva druge spremembe, za katere je treba vložiti vlogo za odobritev v skladu s točko IS.I.OR.255(b) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203:

(1) pristojni organ ob prejemu vloge za spremembo pred izdajo odobritve preveri skladnost organizacije z veljavnimi zahtevami;

(2) pristojni organ določi pogoje, pod katerimi lahko organizacija deluje med izvajanjem spremembe;

(3) če se pristojni organ prepriča, da organizacija izpolnjuje veljavne zahteve, odobri spremembo.“;

(2) Priloga VII (del ORA) se spremeni:

za točko ORA.GEN.200 se vstavi naslednja točka ORA.GEN.200A:

„**ORA.GEN.200A Sistem upravljanja informacijske varnosti**

Organizacija poleg sistema upravljanja iz točke ORA.GEN.200 vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti v skladu z Izvedbeno uredbo (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“.

PRILOGA IV

Priloga I (del 21) k Uredbi (EU) št. 748/2012 se spremeni na naslednji način:

(1) kazalo se spremeni:

(a) za naslovom 21.B.20 se vstavi naslednji naslov:

„21.B.20A Takojšen odziv na informacijskovarnostni incident ali ranljivost, ki vpliva na varnost v letalstvu“;

(b) naslov točke 21.B.30 se nadomesti z naslednjim:

„21.B.30 Dodelitev nalog“;

(c) za naslovom 21.B.240 se vstavi naslednji naslov:

„21.B.240A Spremembe sistema upravljanja informacijske varnosti“;

(d) za naslovom 21.B.435 se vstavi naslednji naslov:

„21.B.435A Spremembe sistema upravljanja informacijske varnosti“;

(2) v točki 21.B.15 se doda naslednja točka (c):

„(c) Pristojni organ države članice Agenciji čim prej zagotovi informacije, pomembne za varnost, ki izhajajo iz poročil o informacijski varnosti, ki jih je prejel na podlagi točke IS.D.OR.230 Priloge (del IS.D.OR) k Delegirani uredbi (EU) 2022/1645.“;

(3) za točko 21.B.20 se vstavi naslednja točka 21.B.20A:

„**21.B.20A Takojšen odziv na informacijskovarnostni incident ali ranljivost, ki vpliva na varnost v letalstvu**

(a) Pristojni organ vzpostavi sistem za ustrezno zbiranje, analiziranje in razširjanje informacij v zvezi z informacijskovarnostnimi incidenti in ranljivostmi, ki lahko vplivajo na varnost v letalstvu, o katerih poročajo organizacije. To se izvede ob usklajevanju z vsemi drugimi ustreznimi organi, odgovornimi za informacijsko ali kibernetsko varnost v državi članici, da se okrepita usklajevanje in združljivost sistemov poročanja.

(b) Agencija vzpostavi sistem za ustrezno analiziranje vseh ustreznih informacij, pomembnih za varnost in prejetih v skladu s točko 21.B.15(c), ter državam članicam in Komisiji nemudoma zagotovi vse informacije, vključno s priporočili ali popravnimi ukrepi, ki jih morajo sprejeti za pravočasen odziv na informacijskovarnostni incident ali ranljivost, ki lahko vpliva na varnost v letalstvu in je v zvezi s proizvodi, deli, nenameščeno opremo, osebami ali organizacijami, za katere se uporabljajo Uredba (EU) 2018/1139 ter njeni delegirani in izvedbeni akti.

(c) Pristojni organ po prejemu informacij iz točk (a) in (b) sprejme ustrezne ukrepe za obravnavo morebitnega vpliva informacijskovarnostnega incidenta ali ranljivosti na varnost v letalstvu.

(d) Ukrepi, sprejeti v skladu s točko (c), se takoj sporočijo vsem osebam ali organizacijam, ki jih upoštevajo v skladu z Uredbo (EU) 2018/1139 ter njenimi delegiranimi in izvedbenimi akti. Pristojni organ države članice o navedenih ukrepih obvesti tudi Agencijo, in, če se zahteva skupno ukrepanje, pristojne organe drugih zadevnih držav članic.“;

(4) v točki 21.B.25 se doda naslednja točka (e):

„(e) Sistem upravljanja, ki ga vzpostavi in vzdržuje pristojni organ, poleg zahtev iz točke (a) izpolnjuje tudi zahteve iz Priloge I (del IS.AR) k Izvedbeni uredbi (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(5) točka 21.B.30 se spremeni:

(a) naslov se nadomesti z naslednjim:

„**21.B.30 Dodelitev nalog“;**

(b) doda se naslednja točka (c):

„(c) Za certificiranje in nadzor skladnosti organizacije s točkama 21.A.139A in 21.A.239A lahko pristojni organ dodeli naloge kvalificiranim subjektom v skladu s točko (a) ali kateremu koli ustreznemu organu, odgovornemu za informacijsko ali kibernetsko varnost v državi članici. Pri dodelitvi nalog pristojni organ zagotovi, da:

(1) kvalificirani subjekt ali ustrezni organ usklajuje in upošteva vse vidike v zvezi z varnostjo v letalstvu;

(2) se rezultati dejavnosti certificiranja in nadzora, ki jih izvede kvalificirani subjekt ali ustrezni organ, vključijo v splošno dokumentacijo organizacije v zvezi s certificiranjem in nadzorom;

(3) njegov sistem upravljanja informacijske varnosti, vzpostavljen v skladu s točko 21.B.25(e), zajema vse naloge certificiranja in stalnega nadzora, ki se izvajajo v njegovem imenu.“;

(6) v točki 21.B.221 se doda naslednja točka (g):

„(g) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko 21.A.139A, pristojni organ poleg upoštevanja točk od (a) do (f) pregleda tudi vse odobritve, izdane v skladu s točko IS.I.OR.200(e) te uredbe ali točko IS.D.OR.200(e) Delegirane uredbe (EU) 2022/1645, potem ko se izvede veljavni cikel presoje nadzora in kadar se izvedejo spremembe na področju dela organizacije.“;

(7) za točko 21.B.240 se vstavi naslednja točka 21.B.240A:

„**21.B.240A Spremembe sistema upravljanja informacijske varnosti**

(a) Pri spremembah, ki se upravljajo in sporočijo pristojnemu organu v skladu s postopkom iz točke IS.D.OR.255(a) Priloge (del IS.D.OR) k Delegirani uredbi (EU) 2022/1645, pristojni organ vključi pregled takih sprememb v svoj stalni nadzor v skladu z načeli iz točke 21.B.221. V primeru ugotovljene neskladnosti pristojni organ o tem obvesti organizacijo, zahteva nadaljnje spremembe in ukrepa v skladu s točko 21.B.225.

(b) Za druge spremembe, za katere je treba vložiti vlogo za odobritev v skladu s točko IS.D.OR.255(b) Priloge (del IS.D.OR) k Delegirani uredbi (EU) 2022/1645:

(1) pristojni organ ob prejemu vloge za spremembo pred izdajo odobritve preveri skladnost organizacije z veljavnimi zahtevami;

(2) pristojni organ določi pogoje, pod katerimi lahko organizacija deluje med izvajanjem spremembe;

(3) če se pristojni organ prepriča, da organizacija izpolnjuje veljavne zahteve, odobri spremembo.“;

(8) v točki 21.B.431 se doda naslednja točka (d):

„(d) Za certificiranje in nadzor skladnosti organizacije s točko 21.A.239A pristojni organ poleg upoštevanja točk od (a) do (c) upošteva naslednja načela:

(1) pristojni organ pregleda vmesnike in povezana tveganja, ki jih v skladu s točko IS.D.OR.205(b) Priloge (del IS.D.OR) k Delegirani uredbi (EU) 2022/1645 opredeli vsaka organizacija, ki je pod njegovim nadzorom;

(2) če so ugotovljena razhajanja pri medsebojnih vmesnikih in povezanih tveganjih, ki jih opredelijo različne organizacije, jih pristojni organ pregleda z zadevnimi organizacijami ter po potrebi sprejme ustrezne ugotovitve, da zagotovi izvajanje popravnih ukrepov;

(3) če pregled dokumentacije iz točke 2 razkrije obstoj bistvenih tveganj, povezanih z vmesniki z organizacijami, ki so pod nadzorom drugega pristojnega organa v isti državi članici, se o tem obvesti ustrezen pristojni organ.“;

(9) za točko 21.B.435 se vstavi naslednja točka 21.B.435A:

„**21.B.435A Spremembe sistema upravljanja informacijske varnosti**

(a) Pri spremembah, ki se upravljajo in sporočijo pristojnemu organu v skladu s postopkom iz točke IS.D.OR.255(a) Priloge (del IS.D.OR) k Delegirani uredbi (EU) 2022/1645, pristojni organ vključi pregled takih sprememb v svoj stalni nadzor v skladu z načeli iz točke 21.B.431. V primeru ugotovljene neskladnosti pristojni organ o tem obvesti organizacijo, zahteva nadaljnje spremembe in ukrepa v skladu s točko 21.B.433.

(b) Za druge spremembe, za katere je treba vložiti vlogo za odobritev v skladu s točko IS.D.OR.255(b) Priloge (del IS.D.OR) k Delegirani uredbi (EU) 2022/1645:

(1) pristojni organ ob prejemu vloge za spremembo pred izdajo odobritve preveri skladnost organizacije z veljavnimi zahtevami;

(2) pristojni organ določi pogoje, pod katerimi lahko organizacija deluje med izvajanjem spremembe;

(3) če se pristojni organ prepriča, da organizacija izpolnjuje veljavne zahteve, odobri spremembo.“.

PRILOGA V

Prilogi II (del ARO) in III (del ORO) k Uredbi (EU) št. 965/2012 se spremenita na naslednji način:

(1) Priloga II (del ARO) se spremeni:

(a) v točki ARO.GEN.125 se doda naslednja točka (c):

„(c) Pristojni organ države članice Agenciji čim prej zagotovi informacije, pomembne za varnost, ki izhajajo iz poročil o informacijski varnosti, ki jih je prejel na podlagi točke IS.I.OR.230 Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203.“;

(b) za točko ARO.GEN.135 se vstavi naslednja točka ARO.GEN.135A:

„**ARO.GEN.135A Takojšen odziv na informacijskovarnostni incident ali ranljivost, ki vpliva na varnost v letalstvu**

(a) Pristojni organ vzpostavi sistem za ustrezno zbiranje, analiziranje in razširjanje informacij v zvezi z informacijskovarnostnimi incidenti in ranljivostmi, ki lahko vplivajo na varnost v letalstvu, o katerih poročajo organizacije. To se izvede ob usklajevanju z vsemi drugimi ustreznimi organi, odgovornimi za informacijsko ali kibernetsko varnost v državi članici, da se okrepita usklajevanje in združljivost sistemov poročanja.

(b) Agencija vzpostavi sistem za ustrezno analiziranje vseh ustreznih informacij, pomembnih za varnost in prejetih v skladu s točko ARO.GEN.125(c), ter državam članicam in Komisiji nemudoma zagotovi vse informacije, vključno s priporočili ali popravnimi ukrepi, ki jih morajo sprejeti za pravočasen odziv na informacijskovarnostni incident ali ranljivost, ki lahko vpliva na varnost v letalstvu in je v zvezi s proizvodi, deli, nenameščeno opremo, osebami ali organizacijami, za katere se uporabljajo Uredba (EU) 2018/1139 ter njeni delegirani in izvedbeni akti.

(c) Pristojni organ po prejemu informacij iz točk (a) in (b) sprejme ustrezne ukrepe za obravnavo morebitnega vpliva informacijskovarnostnega incidenta ali ranljivosti na varnost v letalstvu.

(d) Ukrepi, sprejeti v skladu s točko (c), se takoj sporočijo vsem osebam ali organizacijam, ki jih upoštevajo v skladu z Uredbo (EU) 2018/1139 ter njenimi delegiranimi in izvedbenimi akti. Pristojni organ države članice o navedenih ukrepih obvesti tudi Agencijo, in, če se zahteva skupno ukrepanje, pristojne organe drugih zadevnih držav članic.“;

(c) v točki ARO.GEN.200 se doda naslednja točka (e):

„(e) Sistem upravljanja, ki ga vzpostavi in vzdržuje pristojni organ, poleg zahtev iz točke (a) izpolnjuje tudi zahteve iz Priloge I (del IS.AR) k Izvedbeni uredbi (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(d) točka ARO.GEN.205 se spremeni:

(i) naslov se nadomesti z naslednjim:

„**ARO.GEN.205 Dodelitev nalog**“;

(ii) doda se naslednja točka (c):

„(c) Za certificiranje in nadzor skladnosti organizacije s točko ORO.GEN.200A lahko pristojni organ dodeli naloge kvalificiranim subjektom v skladu s točko (a) ali kateremu koli ustreznemu organu, odgovornemu za informacijsko ali kibernetsko varnost v državi članici. Pri dodelitvi nalog pristojni organ zagotovi, da:

(1) kvalificirani subjekt ali ustrezni organ usklajuje in upošteva vse vidike v zvezi z varnostjo v letalstvu;

(2) se rezultati dejavnosti certificiranja in nadzora, ki jih izvede kvalificirani subjekt ali ustrezni organ, vključijo v splošno dokumentacijo organizacije v zvezi s certificiranjem in nadzorom;

(3) njegov sistem upravljanja informacijske varnosti, vzpostavljen v skladu s točko ARO.GEN.200(e), zajema vse naloge certificiranja in stalnega nadzora, ki se izvajajo v njegovem imenu.“;

(e) v točki ARO.GEN.300 se doda naslednja točka (g):

„(g) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko ORO.GEN.200A, pristojni organ poleg upoštevanja točk od (a) do (f) pregleda tudi vse odobritve, izdane v skladu s točko IS.I.OR.200(e) te uredbe ali točko IS.D.OR.200(e) Delegirane uredbe (EU) 2022/1645, potem ko se izvede veljavni cikel presoje nadzora in kadar se izvedejo spremembe na področju dela organizacije.“;

(f) za točko ARO.GEN.330 se vstavi naslednja točka ARO.GEN.330A:

„**ARO.GEN.330A Spremembe sistema upravljanja informacijske varnosti**

(a) Za spremembe, ki se upravljajo in sporočijo pristojnemu organu v skladu s postopkom iz točke IS.I.OR.255 (a) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203, pristojni organ vključi pregled takih sprememb v svoj stalni nadzor v skladu z načeli iz točke ARO.GEN.300. V primeru ugotovljene neskladnosti pristojni organ o tem obvesti organizacijo, zahteva nadaljnje spremembe in ukrepa v skladu s točko ARO.GEN.350.

(b) Za druge spremembe, za katere je treba vložiti vlogo za odobritev v skladu s točko IS.I.OR.255(b) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203:

(1) pristojni organ ob prejemu vloge za spremembo pred izdajo odobritve preveri skladnost organizacije z veljavnimi zahtevami;

(2) pristojni organ določi pogoje, pod katerimi lahko organizacija deluje med izvajanjem spremembe;

(3) če se pristojni organ prepriča, da organizacija izpolnjuje veljavne zahteve, odobri spremembo.“;

(2) Priloga III (del ORO) se spremeni:

za točko ORO.GEN.200 se vstavi naslednja točka ORO.GEN.200A:

„**ORO.GEN.200A Sistem upravljanja informacijske varnosti**

Operator poleg sistema upravljanja iz točke ORO.GEN.200 vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti v skladu z Izvedbeno uredbo (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“.

PRILOGA VI

Priloga II (del ADR.AR) k Uredbi (EU) št. 139/2014 se spremeni na naslednji način:

(1) v točki ADR.AR.A.025 se doda naslednja točka (c):

„(c) Pristojni organ države članice Agenciji čim prej zagotovi informacije, pomembne za varnost, ki izhajajo iz poročil o informacijski varnosti, ki jih je prejel na podlagi točke IS.D.OR.230 Priloge (del IS.D.OR) k Delegirani uredbi (EU) 2022/1645.“;

(2) za točko ADR.AR.A.030 se vstavi naslednja točka ADR.AR.A.030A:

„**ADR.AR.A.030A Takojšen odziv na informacijskovarnostni incident ali ranljivost, ki vpliva na varnost v letalstvu**

(a) Pristojni organ vzpostavi sistem za ustrezno zbiranje, analiziranje in razširjanje informacij v zvezi z informacijskovarnostnimi incidenti in ranljivostmi, ki lahko vplivajo na varnost v letalstvu, o katerih poročajo organizacije. To se izvede ob usklajevanju z vsemi drugimi ustreznimi organi, odgovornimi za informacijsko ali kibernetsko varnost v državi članici, da se okrepita usklajevanje in združljivost sistemov poročanja.

(b) Agencija vzpostavi sistem za ustrezno analiziranje vseh ustreznih informacij, pomembnih za varnost in prejetih v skladu s točko ADR.AR.A.025(c), ter državam članicam in Komisiji nemudoma zagotovi vse informacije, vključno s priporočili ali popravnimi ukrepi, ki jih morajo sprejeti za pravočasen odziv na informacijskovarnostni incident ali ranljivost, ki lahko vpliva na varnost v letalstvu in je v zvezi s proizvodi, deli, nenameščeno opremo, osebami ali organizacijami, za katere se uporabljajo Uredba (EU) 2018/1139 ter njeni delegirani in izvedbeni akti.

(c) Pristojni organ po prejemu informacij iz točk (a) in (b) sprejme ustrezne ukrepe za obravnavo morebitnega vpliva informacijskovarnostnega incidenta ali ranljivosti na varnost v letalstvu.

(d) Ukrepi, sprejeti v skladu s točko (c), se takoj sporočijo vsem osebam ali organizacijam, ki jih upoštevajo v skladu z Uredbo (EU) 2018/1139 ter njenimi delegiranimi in izvedbenimi akti. Pristojni organ države članice o navedenih ukrepih obvesti tudi Agencijo, in, če se zahteva skupno ukrepanje, pristojne organe drugih zadevnih držav članic.“;

(3) v točki ADR.AR.B.005 se doda naslednja točka (d):

„(d) Sistem upravljanja, ki ga vzpostavi in vzdržuje pristojni organ, poleg zahtev iz točke (a) izpolnjuje tudi zahteve iz Priloge I (del IS.AR) k Izvedbeni uredbi (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(4) točka ADR.AR.B.010 se spremeni:

(i) naslov se nadomesti z naslednjim:

„**ADR.AR.B.010 Dodelitev nalog**“;

(ii) doda se naslednja točka (c):

„(c) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko ADR.OR.D.005A, lahko pristojni organ dodeli naloge kvalificiranim subjektom v skladu s točko (a) ali kateremu koli ustreznemu organu, odgovornemu za informacijsko ali kibernetsko varnost v državi članici. Pri dodelitvi nalog pristojni organ zagotovi, da:

(1) kvalificirani subjekt ali ustrezni organ usklajuje in upošteva vse vidike v zvezi z varnostjo v letalstvu;

(2) se rezultati dejavnosti certificiranja in nadzora, ki jih izvede kvalificirani subjekt ali ustrezni organ, vključijo v splošno dokumentacijo organizacije v zvezi s certificiranjem in nadzorom;

(3) njegov sistem upravljanja informacijske varnosti, vzpostavljen v skladu s točko ADR.AR.B.005(e), zajema vse naloge certificiranja in stalnega nadzora, ki se izvajajo v njegovem imenu.“;

(5) v točki ADR.AR.C.005 se doda naslednja točka (f):

„(f) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko ADR.OR.D.005A, pristojni organ poleg upoštevanja točk od (a) do (e) pregleda tudi vse odobritve, izdane v skladu s točko IS.I.OR.200(e) te uredbe ali točko IS.D.OR.200(e) Delegirane uredbe (EU) 2022/1645, potem ko se izvede veljavni cikel presoje nadzora in kadar se izvedejo spremembe na področju dela organizacije.“;

(6) za točko ADR.AR.C.040 se vstavi točka ADR.AR.C.040A:

„**ADR.AR.C.040A Spremembe sistema upravljanja informacijske varnosti**

(a) Pri spremembah, ki se upravljajo in sporočijo pristojnemu organu v skladu s postopkom iz točke IS.D.OR.255(a) Priloge (del IS.D.OR) k Delegirani uredbi (EU) 2022/1645, pristojni organ vključi pregled takih sprememb v svoj stalni nadzor v skladu z načeli iz točke ADR.AR.C.005. V primeru ugotovljene neskladnosti pristojni organ o tem obvesti organizacijo, zahteva nadaljnje spremembe in ukrepa v skladu s točko ADR.AR.C.055.

(b) Pri drugih spremembah, za katere je treba vložiti vlogo za odobritev v skladu s točko IS.D.OR.255(b) Priloge (del IS.D.OR) k Delegirani uredbi (EU) 2022/1645:

(1) pristojni organ ob prejemu vloge za spremembo pred izdajo odobritve preveri skladnost organizacije z veljavnimi zahtevami;

(2) pristojni organ določi pogoje, pod katerimi lahko organizacija deluje med izvajanjem spremembe;

(3) če se pristojni organ prepriča, da organizacija izpolnjuje veljavne zahteve, odobri spremembo.“.

PRILOGA VII

Priloge II (del 145), III (del 66) in Vc (del CAMO) k Uredbi (EU) št. 1321/2014 se spremenijo na naslednji način:

(1) Priloga II (del 145) se spremeni:

(a) kazalo se spremeni:

(i) za naslovom 145.A.200 se vstavi naslednji naslov:

„145.A.200A Sistem upravljanja informacijske varnosti“;

(ii) za naslovom 145.B.135 se vstavi naslednji naslov:

„145.B.135A Takojšen odziv na informacijskovarnostni incident ali ranljivost, ki vpliva na varnost v letalstvu“;

(iii) naslov točke 145.B.205 se nadomesti z naslednjim:

„145.B.205 Dodelitev nalog“;

(iv) za naslovom 145.B.330 se vstavi naslednji naslov:

„145.B.330A Spremembe sistema upravljanja informacijske varnosti“;

(b) za točko 145.A.200 se vstavi točka 145.A.200A:

„145.A.200A **Sistem upravljanja informacijske varnosti**

Vzdrževalna organizacija poleg sistema upravljanja iz točke 145.A.200 vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti v skladu z Izvedbeno uredbo (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(c) v točki 145.B.125 se doda naslednja točka (c):

„(c) Pristojni organ države članice Agenciji čim prej zagotovi informacije, pomembne za varnost, ki izhajajo iz poročil o informacijski varnosti, ki jih je prejel na podlagi točke IS.I.OR.230 Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203.“;

(d) za točko 145.B.135 se vstavi točka 145.B.135A:

„145.B.135A **Takojšen odziv na informacijskovarnostni incident ali ranljivost, ki vpliva na varnost v letalstvu**

(a) Pristojni organ vzpostavi sistem za ustrezno zbiranje, analiziranje in razširjanje informacij v zvezi z informacijskovarnostnimi incidenti in ranljivostmi, ki lahko vplivajo na varnost v letalstvu, o katerih poročajo organizacije. To se izvede ob usklajevanju z vsemi drugimi ustreznimi organi, odgovornimi za informacijsko ali kibernetsko varnost v državi članici, da se okrepita usklajevanje in združljivost sistemov poročanja.

(b) Agencija vzpostavi sistem za ustrezno analiziranje vseh ustreznih informacij, pomembnih za varnost in prejetih v skladu s točko 145.B.125(c), ter državam članicam in Komisiji nemudoma zagotovi vse informacije, vključno s priporočili ali popravnimi ukrepi, ki jih morajo sprejeti za pravočasen odziv na informacijskovarnostni incident ali ranljivost, ki lahko vpliva na varnost v letalstvu in je v zvezi s proizvodi, deli, nenameščeno opremo, osebami ali organizacijami, za katere se uporabljajo Uredba (EU) 2018/1139 ter njeni delegirani in izvedbeni akti.

(c) Pristojni organ po prejemu informacij iz točk (a) in (b) sprejme ustrezne ukrepe za obravnavo morebitnega vpliva informacijskovarnostnega incidenta ali ranljivosti na varnost v letalstvu.

(d) Ukrepi, sprejeti v skladu s točko (c), se takoj sporočijo vsem osebam ali organizacijam, ki jih upoštevajo v skladu z Uredbo (EU) 2018/1139 ter njenimi delegiranimi in izvedbenimi akti. Pristojni organ države članice o navedenih ukrepih obvesti tudi Agencijo, in, če se zahteva skupno ukrepanje, pristojne organe drugih zadevnih držav članic.“;

(e) v točki 145.B.200 se doda naslednja točka (e):

„(e) Sistem upravljanja, ki ga vzpostavi in vzdržuje pristojni organ, poleg zahtev iz točke (a) izpolnjuje tudi zahteve iz Priloge I (del IS.AR) k Izvedbeni uredbi (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(f) točka 145.B.205 se spremeni:

(i) naslov se nadomesti z naslednjim:

„145.B.205 **Dodelitev nalog**“;

(ii) doda se naslednja točka (c):

„(c) Za certificiranje in nadzor skladnosti organizacije s točko 145.A.200A lahko pristojni organ dodeli naloge kvalificiranim subjektom v skladu s točko (a) ali kateremu koli ustreznemu organu, odgovornemu za informacijsko ali kibernetsko varnost v državi članici. Pri dodelitvi nalog pristojni organ zagotovi, da:

(1) kvalificirani subjekt ali ustrezni organ usklajuje in upošteva vse vidike v zvezi z varnostjo v letalstvu;

(2) se rezultati dejavnosti certificiranja in nadzora, ki jih izvede kvalificirani subjekt ali ustrezni organ, vključijo v splošno dokumentacijo organizacije v zvezi s certificiranjem in nadzorom;

(3) njegov sistem upravljanja informacijske varnosti, vzpostavljen v skladu s točko 145.B.200(e), zajema vse naloge certificiranja in stalnega nadzora, ki se izvajajo v njegovem imenu.“;

(g) v točki 145.B.300 se doda naslednja točka (g):

„(g) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko 145.A.200A, pristojni organ poleg upoštevanja točk od (a) do (f) pregleda tudi vse odobritve, izdane v skladu s točko IS.I.OR.200(e) te uredbe ali točko IS.D.OR.200(e) Delegirane uredbe (EU) 2022/1645, potem ko se izvede veljavni cikel presoje nadzora in kadar se izvedejo spremembe na področju dela organizacije.“;

(h) za točko 145.B.330 se vstavi točka 145.B.330A:

„145.B.330A **Spremembe sistema upravljanja informacijske varnosti**

(a) Za spremembe, ki se upravljajo in sporočijo pristojnemu organu v skladu s postopkom iz točke IS.I.OR.255(a) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203, pristojni organ vključi pregled takih sprememb v svoj stalni nadzor v skladu z načeli iz točke 145.B.300. V primeru ugotovljene neskladnosti pristojni organ o tem obvesti organizacijo, zahteva nadaljnje spremembe in ukrepa v skladu s točko 145.B.350.

(b) Za druge spremembe, za katere je treba vložiti vlogo za odobritev v skladu s točko IS.I.OR.255(b) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203:

(1) pristojni organ ob prejemu vloge za spremembo pred izdajo odobritve preveri skladnost organizacije z veljavnimi zahtevami;

(2) pristojni organ določi pogoje, pod katerimi lahko organizacija deluje med izvajanjem spremembe;

(3) če se pristojni organ prepriča, da organizacija izpolnjuje veljavne zahteve, odobri spremembo.“;

(2) Priloga III (del 66) se spremeni:

(a) v kazalu se za naslovom 66.B.10 vstavi naslednji naslov:

„66.B.15 Sistem upravljanja informacijske varnosti“;

(b) za točko 66.B.10 se vstavi naslednja točka 66.B.15:

„66.B.15 **Sistem upravljanja informacijske varnosti**

Pristojni organ vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti v skladu s Prilogo I (del IS.AR) k Izvedbeni uredbi (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(3) Priloga Vc (del CAMO) se spremeni:

(a) kazalo se spremeni:

(i) za naslovom CAMO.A.200 se vstavi naslednji naslov:

„CAMO.A.200A Sistem upravljanja informacijske varnosti“;

(ii) za naslovom CAMO.B.135 se vstavi naslednji naslov:

„CAMO.B.135A Takojšen odziv na informacijskovarnostni incident ali ranljivost, ki vpliva na varnost v letalstvu“;

(iii) naslov točke CAMO.B.205 se nadomesti z naslednjim:

„CAMO.B.205 Dodelitev nalog“;

(iv) za naslovom CAMO.B.330 se vstavi naslednji naslov:

„CAMO.B.330A Spremembe sistema upravljanja informacijske varnosti“;

(b) za točko CAMO.A.200 se vstavi naslednja točka CAMO.A.200A:

„CAMO.A.200A **Sistem upravljanja informacijske varnosti**

Organizacija poleg sistema upravljanja iz točke CAMO.A.200 vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti v skladu z Izvedbeno uredbo (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(c) v točki CAMO.B.125 se doda naslednja točka (c):

„(c) Pristojni organ države članice Agenciji čim prej zagotovi informacije, pomembne za varnost, ki izhajajo iz poročil o informacijski varnosti, ki jih je prejel na podlagi točke IS.I.OR.230 Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203.“;

(d) za CAMO.B.135 se vstavi naslednja točka CAMO.B.135A:

„CAMO.B.135A **Takojšen odziv na informacijskovarnostni incident ali ranljivost, ki vpliva na varnost v letalstvu**

(a) Pristojni organ vzpostavi sistem za ustrezno zbiranje, analiziranje in razširjanje informacij v zvezi z informacijskovarnostnimi incidenti in ranljivostmi, ki lahko vplivajo na varnost v letalstvu, o katerih poročajo organizacije. To se izvede ob usklajevanju z vsemi drugimi ustreznimi organi, odgovornimi za informacijsko ali kibernetsko varnost v državi članici, da se okrepita usklajevanje in združljivost sistemov poročanja.

(b) Agencija vzpostavi sistem za ustrezno analiziranje vseh ustreznih informacij, pomembnih za varnost in prejetih v skladu s točko CAMO.B.125(c), ter državam članicam in Komisiji nemudoma zagotovi vse informacije, vključno s priporočili ali popravnimi ukrepi, ki jih morajo sprejeti za pravočasen odziv na informacijskovarnostni incident ali ranljivost, ki lahko vpliva na varnost v letalstvu in je v zvezi s proizvodi, deli, nenameščeno opremo, osebami ali organizacijami, za katere se uporabljajo Uredba (EU) 2018/1139 ter njeni delegirani in izvedbeni akti.

(c) Pristojni organ po prejemu informacij iz točk (a) in (b) sprejme ustrezne ukrepe za obravnavo morebitnega vpliva informacijskovarnostnega incidenta ali ranljivosti na varnost v letalstvu.

(d) Ukrepi, sprejeti v skladu s točko (c), se takoj sporočijo vsem osebam ali organizacijam, ki jih upoštevajo v skladu z Uredbo (EU) 2018/1139 ter njenimi delegiranimi in izvedbenimi akti. Pristojni organ države članice o navedenih ukrepih obvesti tudi Agencijo, in, če se zahteva skupno ukrepanje, pristojne organe drugih zadevnih držav članic.“;

(e) v točki CAMO.B.200 se doda naslednja točka (e):

„(e) Sistem upravljanja, ki ga vzpostavi in vzdržuje pristojni organ, poleg zahtev iz točke (a) izpolnjuje tudi zahteve iz Priloge I (del IS.AR) k Izvedbeni uredbi (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(f) točka CAMO.B.205 se spremeni:

(i) naslov se nadomesti z naslednjim:

„CAMO.B.205 **Dodelitev nalog**“;

(ii) doda se naslednja točka (c):

„(c) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko CAMO.A.200A, lahko pristojni organ dodeli naloge kvalificiranim subjektom v skladu s točko (a) ali kateremu koli ustreznemu organu, odgovornemu za informacijsko ali kibernetsko varnost v državi članici. Pri dodelitvi nalog pristojni organ zagotovi, da:

(1) kvalificirani subjekt ali ustrezni organ usklajuje in upošteva vse vidike v zvezi z varnostjo v letalstvu;

(2) se rezultati dejavnosti certificiranja in nadzora, ki jih izvede kvalificirani subjekt ali ustrezni organ, vključijo v splošno dokumentacijo organizacije v zvezi s certificiranjem in nadzorom;

(3) njegov sistem upravljanja informacijske varnosti, vzpostavljen v skladu s točko CAMO.B.200(e), zajema vse naloge certificiranja in stalnega nadzora, ki se izvajajo v njegovem imenu.“;

(g) v točki CAMO.B.300 se doda naslednja točka (g):

„(g) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko CAMO.A.200A, pristojni organ poleg upoštevanja točk od (a) do (f) pregleda tudi vse odobritve, izdane v skladu s točko IS.I.OR.200(e) te uredbe ali točko IS.D.OR.200(e) Delegirane uredbe (EU) 2022/1645, potem ko se izvede veljavni cikel presoje nadzora in kadar se izvedejo spremembe na področju dela organizacije.“;

(h) za točko CAMO.B.330 se vstavi naslednja točka CAMO.B.330A:

„CAMO.B.330A **Spremembe sistema upravljanja informacijske varnosti**

(a) Za spremembe, ki se upravljajo in sporočijo pristojnemu organu v skladu s postopkom iz točke IS.I.OR.255(a) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203, pristojni organ vključi pregled takih sprememb v svoj stalni nadzor v skladu z načeli iz točke CAMO.B.300. V primeru ugotovljene neskladnosti pristojni organ o tem obvesti organizacijo, zahteva nadaljnje spremembe in ukrepa v skladu s točko CAMO.B.350.

(b) Za druge spremembe, za katere je treba vložiti vlogo za odobritev v skladu s točko IS.I.OR.255(b) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203:

(1) pristojni organ ob prejemu vloge za spremembo pred izdajo odobritve preveri skladnost organizacije z veljavnimi zahtevami;

(2) pristojni organ določi pogoje, pod katerimi lahko organizacija deluje med izvajanjem spremembe;

(3) če se pristojni organ prepriča, da organizacija izpolnjuje veljavne zahteve, odobri spremembo.“.

PRILOGA VIII

Prilogi II (del ATCO.AR) in III (del ATCO.OR) k Uredbi (EU) 2015/340 se spremenita na naslednji način:

(1) Priloga II (del ATCO.AR) se spremeni:

(a) v točki ATCO.AR.A.020 se doda naslednja točka (c):

„(c) Pristojni organ države članice Agenciji čim prej zagotovi informacije, pomembne za varnost, ki izhajajo iz poročil o informacijski varnosti, ki jih je prejel na podlagi točke IS.I.OR.230 Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203.“;

(b) za točko ATCO.AR.A.025 se vstavi naslednja točka ATCO.AR.A.025A:

„**ATCO.AR.A.025A Takojšen odziv na informacijskovarnostni incident ali ranljivost, ki vpliva na varnost v letalstvu**

(a) Pristojni organ vzpostavi sistem za ustrezno zbiranje, analiziranje in razširjanje informacij v zvezi z informacijskovarnostnimi incidenti in ranljivostmi, ki lahko vplivajo na varnost v letalstvu, o katerih poročajo organizacije. To se izvede ob usklajevanju z vsemi drugimi ustreznimi organi, odgovornimi za informacijsko ali kibernetsko varnost v državi članici, da se okrepita usklajevanje in združljivost sistemov poročanja.

(b) Agencija vzpostavi sistem za ustrezno analiziranje vseh ustreznih informacij, pomembnih za varnost in prejetih v skladu s točko ATCO.AR.A.020, ter državam članicam in Komisiji nemudoma zagotovi vse informacije, vključno s priporočili ali popravnimi ukrepi, ki jih morajo sprejeti za pravočasen odziv na informacijskovarnostni incident ali ranljivost, ki lahko vpliva na varnost v letalstvu in je v zvezi s proizvodi, deli, nenameščeno opremo, osebami ali organizacijami, za katere se uporabljajo Uredba (EU) 2018/1139 ter njeni delegirani in izvedbeni akti.

(c) Pristojni organ po prejemu informacij iz točk (a) in (b) sprejme ustrezne ukrepe za obravnavo morebitnega vpliva informacijskovarnostnega incidenta ali ranljivosti na varnost v letalstvu.

(d) Ukrepi, sprejeti v skladu s točko (c), se takoj sporočijo vsem osebam ali organizacijam, ki jih upoštevajo v skladu z Uredbo (EU) 2018/1139 ter njenimi delegiranimi in izvedbenimi akti. Pristojni organ države članice o navedenih ukrepih obvesti tudi Agencijo, in, če se zahteva skupno ukrepanje, pristojne organe drugih zadevnih držav članic.“;

(c) v točki ATCO.AR.B.001 se doda naslednja točka (e):

„(e) Sistem upravljanja, ki ga vzpostavi in vzdržuje pristojni organ, poleg zahtev iz točke (a) izpolnjuje tudi zahteve iz Priloge I (del IS.AR) k Izvedbeni uredbi (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(d) točka ATCO.AR.B.005 se spremeni:

(i) naslov se nadomesti z naslednjim:

„**ATCO.AR.B.005 Dodelitev nalog**“;

(ii) doda se naslednja točka (c):

„(c) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko ATCO.OR.C.001A, lahko pristojni organ dodeli naloge kvalificiranim subjektom v skladu s točko (a) ali kateremu koli ustreznemu organu, odgovornemu za informacijsko ali kibernetsko varnost v državi članici. Pri dodelitvi nalog pristojni organ zagotovi, da:

(1) kvalificirani subjekt ali ustrezni organ usklajuje in upošteva vse vidike v zvezi z varnostjo v letalstvu;

(2) se rezultati dejavnosti certificiranja in nadzora, ki jih izvede kvalificirani subjekt ali ustrezni organ, vključijo v splošno dokumentacijo organizacije v zvezi s certificiranjem in nadzorom;

(3) njegov sistem upravljanja informacijske varnosti, vzpostavljen v skladu s točko ATCO.AR.B.001(e), zajema vse naloge certificiranja in stalnega nadzora, ki se izvajajo v njegovem imenu.“;

(e) v točki ATCO.AR.C.001 se doda naslednja točka (f):

„(f) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko ATCO.OR.C.001A, pristojni organ poleg upoštevanja točk od (a) do (e) pregleda tudi vse odobritve, izdane v skladu s točko IS.I.OR.200(e) te uredbe ali točko IS.D.OR.200(e) Delegirane uredbe (EU) 2022/1645, potem ko se izvede veljavni cikel presoje nadzora in kadar se izvedejo spremembe na področju dela organizacije.“;

(f) za točko ATCO.AR.E.010 se vstavi naslednja točka ATCO.AR.E.010A:

„**ATCO.AR.E.010A Spremembe sistema upravljanja informacijske varnosti**

(a) Kar zadeva spremembe, ki se upravljajo in sporočijo pristojnemu organu v skladu s postopkom iz točke IS.I.OR.255(a) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203, pristojni organ vključi pregled takih sprememb v svoj stalni nadzor v skladu z načeli iz točke ATCO.AR.C.001. V primeru ugotovljene neskladnosti pristojni organ o tem obvesti organizacijo, zahteva nadaljnje spremembe in ukrepa v skladu s točko ATCO.AR.C.010.

(b) Kar zadeva druge spremembe, za katere je treba vložiti vlogo za odobritev v skladu s točko IS.I.OR.255(b) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203:

(1) pristojni organ ob prejemu vloge za spremembo pred izdajo odobritve preveri skladnost organizacije z veljavnimi zahtevami;

(2) pristojni organ določi pogoje, pod katerimi lahko organizacija deluje med izvajanjem spremembe;

(3) če se pristojni organ prepriča, da organizacija izpolnjuje veljavne zahteve, odobri spremembo.“;

(2) Priloga III (del ATCO.OR) se spremeni:

za točko ATCO.OR.C.001 se vstavi naslednja točka ATCO.OR.C.001A:

„**ATCO.OR.C.001A Sistem upravljanja informacijske varnosti**

Organizacija za usposabljanje poleg sistema upravljanja iz točke ATCO.OR.C.001 vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti v skladu z Izvedbeno uredbo (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“.

PRILOGA IX

Prilogi II (del ATM/ANS.AR) in III (del ATM/ANS.OR) k Izvedbeni uredbi (EU) 2017/373 se spremenita na naslednji način:

(1) Priloga II (del ATM/ANS.AR) se spremeni:

(a) v točki ATM/ANS.AR.A.020 se doda naslednja točka (c):

„(c) Pristojni organ države članice Agenciji čim prej zagotovi informacije, pomembne za varnost, ki izhajajo iz poročil o informacijski varnosti, ki jih je prejel na podlagi točke IS.I.OR.230 Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203.“;

(b) za točko ATM/ANS.AR.A.025 se vstavi naslednja točka ATM/ANS.AR.A.025A:

„ATM/ANS.AR.A.025A Takojšen odziv na informacijskovarnostni incident ali ranljivost, ki vpliva na varnost v letalstvu

(a) Pristojni organ vzpostavi sistem za ustrezno zbiranje, analiziranje in razširjanje informacij v zvezi z informacijskovarnostnimi incidenti in ranljivostmi, ki lahko vplivajo na varnost v letalstvu, o katerih poročajo organizacije. To se izvede ob usklajevanju z vsemi drugimi ustreznimi organi, odgovornimi za informacijsko ali kibernetsko varnost v državi članici, da se okrepita usklajevanje in združljivost sistemov poročanja.

(b) Agencija vzpostavi sistem za ustrezno analiziranje vseh ustreznih informacij, pomembnih za varnost in prejetih v skladu s točko ATM/ANS.AR.A.020(c), ter državam članicam in Komisiji nemudoma zagotovi vse informacije, vključno s priporočili ali popravnimi ukrepi, ki jih morajo sprejeti za pravočasen odziv na informacijskovarnostni incident ali ranljivost, ki lahko vpliva na varnost v letalstvu in je v zvezi s proizvodi, deli, nenameščeno opremo, osebami ali organizacijami, za katere se uporabljajo Uredba (EU) 2018/1139 ter njeni delegirani in izvedbeni akti.

(c) Pristojni organ po prejemu informacij iz točk (a) in (b) sprejme ustrezne ukrepe za obravnavo morebitnega vpliva informacijskovarnostnega incidenta ali ranljivosti na varnost v letalstvu.

(d) Ukrepi, sprejeti v skladu s točko (c), se takoj sporočijo vsem osebam ali organizacijam, ki jih upoštevajo v skladu z Uredbo (EU) 2018/1139 ter njenimi delegiranimi in izvedbenimi akti. Pristojni organ države članice o navedenih ukrepih obvesti tudi Agencijo, in, če se zahteva skupno ukrepanje, pristojne organe drugih zadevnih držav članic.“;

(c) v točki ATM/ANS.AR.B.001 se doda naslednja točka (e):

„(e) Sistem upravljanja, ki ga vzpostavi in vzdržuje pristojni organ, poleg zahtev iz točke (a) izpolnjuje tudi zahteve iz Priloge I (del IS.AR) k Izvedbeni uredbi (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(d) točka ATM/ANS.AR.B.005 se spremeni:

(i) naslov se nadomesti z naslednjim:

„**ATM/ANS.AR.B.005 Dodelitev nalog**“;

(ii) doda se naslednja točka (c):

„(c) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko ATM/ANS.OR.B.005A, lahko pristojni organ dodeli naloge kvalificiranim subjektom v skladu s točko (a) ali kateremu koli ustreznemu organu, odgovornemu za informacijsko ali kibernetsko varnost v državi članici. Pri dodelitvi nalog pristojni organ zagotovi, da:

(1) kvalificirani subjekt ali ustrezni organ usklajuje in upošteva vse vidike v zvezi z varnostjo v letalstvu;

(2) se rezultati dejavnosti certificiranja in nadzora, ki jih izvede kvalificirani subjekt ali ustrezni organ, vključijo v splošno dokumentacijo organizacije v zvezi s certificiranjem in nadzorom;

(3) njegov sistem upravljanja informacijske varnosti, vzpostavljen v skladu s točko ATM/ANS.AR.B.001 (e), zajema vse naloge certificiranja in stalnega nadzora, ki se izvajajo v njegovem imenu.“;

(e) v točki ATM/ANS.AR.C.010 se doda naslednja točka (d):

„(d) Kar zadeva certificiranje in nadzor skladnosti organizacije s točko ATM/ANS.OR.B.005A, pristojni organ poleg upoštevanja točk od (a) do (c) pregleda tudi vse odobritve, izdane v skladu s točko IS.I.OR.200(e) te uredbe ali točko IS.D.OR.200(e) Delegirane uredbe (EU) 2022/1645, potem ko se izvede veljavni cikel presoje nadzora in kadar se izvedejo spremembe na področju dela organizacije.“;

(f) za točko ATM/ANS.AR.C.025 se vstavi naslednja točka ATM/ANS.AR.C.025A:

„**ATM/ANS.AR.C.025A Spremembe sistema upravljanja informacijske varnosti**

(a) Za spremembe, ki se upravljajo in sporočijo pristojnemu organu v skladu s postopkom iz točke IS.I.OR.255(a) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203, pristojni organ vključi pregled takih sprememb v svoj stalni nadzor v skladu z načeli iz točke ATM/ANS.AR.C.010. V primeru ugotovljene neskladnosti pristojni organ o tem obvesti organizacijo, zahteva nadaljnje spremembe in ukrepa v skladu s točko ATM/ANS.AR.C.050.

(b) Kar zadeva druge spremembe, za katere je treba vložiti vlogo za odobritev v skladu s točko IS.I.OR.255(b) Priloge II (del IS.I.OR) k Izvedbeni uredbi (EU) 2023/203:

(1) pristojni organ ob prejemu vloge za spremembo pred izdajo odobritve preveri skladnost organizacije z veljavnimi zahtevami;

(2) pristojni organ določi pogoje, pod katerimi lahko organizacija deluje med izvajanjem spremembe;

(3) če se pristojni organ prepriča, da organizacija izpolnjuje veljavne zahteve, odobri spremembo.“;

(2) Priloga III (del ATM/ANS.OR) se spremeni:

(a) za točko ATM/ANS.OR.B.005 se vstavi naslednja točka ATM/ANS.OR.B.005A:

„**ATM/ANS.OR.B.005A Sistem upravljanja informacijske varnosti**

Izvajalec storitev poleg sistema upravljanja iz točke ATM/ANS.OR.B.005 vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti v skladu z Izvedbeno uredbo (EU) 2023/203, da se zagotovi primerno upravljanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“;

(b) točka ATM/ANS.OR.D.010 se nadomesti z naslednjim:

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

(a) Izvajalci navigacijskih služb zračnega prometa in upravljavci pretoka zračnega prometa ter upravljavec omrežja v okviru svojega sistema upravljanja, kot se zahteva v točki ATM/ANS.OR.B.005, vzpostavijo sistem za upravljanje varovanja, da zagotovijo:

(1) varovanje svojih objektov in osebja, s čimer se prepreči nezakonito poseganje v izvajanje storitev;

(2) varovanje operativnih podatkov, ki jih prejmejo, pripravijo ali kako drugače uporabljajo, tako da je dostop do njih omejen in omogočen le pooblaščenim.

(b) Sistem upravljanja varovanja opredeljuje:

(1) proces in postopke v zvezi z oceno in ublažitvijo tveganja glede varovanja, spremljanjem in izboljšanjem varovanja, pregledi varovanja ter razširjanjem pridobljenih novih spoznanj;

(2) sredstva za določanje, spremljanje in odkrivanje kršitev varnosti in opozarjanje osebja z ustreznimi varnostnimi opozorili;

(3) sredstva za obvladovanje posledic kršitev varnosti ter določitev sanacijskih ukrepov in postopkov za zmanjšanje tveganja, s katerimi se prepreči ponovna kršitev.

(c) Izvajalci navigacijskih služb zračnega prometa in upravljavci pretoka zračnega prometa ter upravljavec omrežja zagotovijo varnostno preverjanje svojega osebja, če je ustrezno, ter se usklajujejo z ustreznimi civilnimi in vojaškimi organi za zagotovitev varovanja svojih objektov, osebja in podatkov.

(d) Vidiki, povezani z informacijsko varnostjo, se upravljajo v skladu s točko ATM/ANS.OR.B.005A.“.