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

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 19(1), točka (g), in člena 39(1), točka (b), Uredbe,

ob upoštevanju naslednjega:

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

(2) Poleg tega morajo operatorji aerodromov in organizacije, odgovorne za opravljanje storitev upravljanja ploščadi, v skladu z bistvenimi zahtevami iz Priloge VII, točki 2.2.1 in 5.2, k Uredbi (EU) 2018/1139, izvajati in vzdrževati sistem upravljanja za obvladovanje varnostnih tveganj.

(3) Varnostna tveganja iz uvodnih izjav 1 in 2 lahko izhajajo iz različnih virov, vključno s hibami v zasnovi in vzdrževanju, vidikov človeške učinkovitosti, okoljskih groženj in groženj za informacijsko varnost. Zato bi morali sistemi upravljanja, ki jih izvajajo organizacije, kot je navedeno v uvodnih izjavah 1 in 2, upoštevati ne le 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. Ta tveganja za informacijsko varnost se v civilnem letalstvu nenehno povečujejo, saj sedanji informacijski sistemi postajajo vedno bolj medsebojno povezani in postajajo vse bolj tarča zlonamernih akterjev.

(4) Tveganja, povezana s temi informacijskimi sistemi, niso omejena na morebitne napade na kibernetski prostor, marveč vključujejo tudi grožnje, ki lahko vplivajo na procese in postopke ter človeško uspešnost.

(5) Precej organizacij že uporablja mednarodne standarde, kot je ISO 27001, da bi obravnavale varnost digitalnih informacij in podatkov. Ti standardi ne obravnavajo nujno v celoti vseh posebnosti civilnega letalstva.

(6) Zato je primerno določiti zahteve za obvladovanje tveganj za informacijsko varnost, ki bi lahko vplivala na varnost v letalstvu.

(7) Bistveno je, da navedene zahteve zajemajo različna področja letalstva in njihove vmesnike, saj je letalstvo zelo povezan sistem več sistemov. Zato bi se morale uporabljati za vse organizacije, ki morajo že imeti sistem upravljanja v skladu z veljavno zakonodajo Unije o varnosti v letalstvu.

(8) Zahteve iz te uredbe bi bilo treba dosledno uporabljati na vseh področjih letalstva, hkrati pa čim manj vplivati na zakonodajo Unije o varnosti v letalstvu, ki se na teh področjih že uporablja.

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

(9) Zahteve iz te uredbe ne bi smele posegati v zahteve glede informacijske in kibernetske varnosti iz točke 1.7 Priloge Izvedbene uredbe Komisije (EU) 2015/1998 ([2]) in člena 14 Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta ([3]).

(10) Opredelitev informacijske varnosti, ki se uporablja za namene tega pravnega akta, se ne bi smela razlagati drugače kot opredelitev varnosti omrežij in informacijskih sistemov iz Direktive 2016/1148.

(11) Da bi se izognili podvajanju pravnih zahtev, kadar za organizacije, ki so zajete v tej uredbi, že veljajo varnostne zahteve, ki izhajajo iz drugih aktov Unije, navedenih v uvodni izjavi (9), in ki so po svojem učinku enakovredne določbam iz te uredbe, bi bilo treba skladnost s temi varnostnimi zahtevami šteti za skladnost z zahtevami iz te uredbe.

(12) Organizacije, ki so zajete v tej uredbi in za katere že veljajo varnostne zahteve iz Izvedbene uredbe (EU) 2015/1998, bi morale izpolnjevati tudi zahteve iz Priloge I (Del IS.D.OR.230 „Sistem zunanjega poročanja o informacijski varnosti“) k tej uredbi, saj Uredba (EU) 2015/1998 ne vsebuje določb v zvezi z zunanjim poročanjem o informacijskovarnostnih incidentih.

(13) Uredbi Komisije (EU) št. 748/2012 ([4]) in (EU) št. 139/2014 ([5]) bi bilo treba spremeniti, da se vzpostavi povezava med sistemi upravljanja, predpisanimi v zgoraj navedenih uredbah, in zahtevami za upravljanje informacijske varnosti iz te uredbe.

(14) Da se organizacijam zagotovi dovolj časa za zagotovitev skladnosti z novimi pravili in postopki, uvedenimi s to uredbo, bi se morala ta uredba začeti uporabljati tri leta po datumu začetka veljavnosti.

(15) Zahteve iz te uredbe temeljijo na Mnenju št. 03/2021 ([6]), ki ga je Agencija izdala v skladu s členom 75(2), točki (b) in (c), in členom 76(1) Uredbe (EU) 2018/1139.

(16) V skladu s členom 128(4) Uredbe (EU) 2018/1139, se je Komisija posvetovala s strokovnjaki, ki so jih imenovale posamezne države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje ([7]) –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Predmet urejanja

Ta uredba določa zahteve, ki jih morajo izpolnjevati organizacije iz člena 2, da 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, ter da zaznajo dogodke v zvezi z varnostjo informacij in opredelijo tiste, ki se štejejo za informacijskovarnostne incidente, ki bi lahko vplivali na varnost v letalstvu, ter se na te informacijskovarnostne incidente odzovejo in jih sanirajo.

([2]) 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).

([3]) 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).

([4]) 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).

([5]) 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).

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

([7]) UL L 123, 12.5.2016, str. 1.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za naslednje organizacije:

(a) proizvodne organizacije in projektivne organizacije, za katere veljata poddela G in J oddelka A Priloge I (del 21) k Uredbi (EU) št. 748/2012, razen projektivnih in proizvodnih organizacij, ki so vključene izključno v projektiranje in/ali proizvodnjo zrakoplovov ELA2, kot so opredeljeni v členu 1(2), točka (j), Uredbe (EU) št. 748/2012;

(b) operatorji aerodromov in izvajalci storitev upravljanja ploščadi, za katere velja Priloga III „Del Zahteve za organizacije (del ADR.OR)“ k Uredbi (EU) št. 139/2014.

2. Ta uredba ne posega v zahteve glede informacijske in kibernetske varnosti iz točke 1.7 Priloge Izvedbene uredbe (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 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;

(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, ki izhajajo iz druge zakonodaje Unije

1. Kadar organizacija iz člena 2 izpolnjuje varnostne zahteve iz člena 14 Direktive (EU) 2016/1148, ki 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 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 ([8]), 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.D.OR.230 Priloge k tej uredbi, ki morajo biti izpolnjene.

([8]) 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).

3. Komisija lahko po posvetovanju z EASA 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 5

Pristojni organ

1. Organ, pristojen za certifikacijo in nadzor skladnosti s to uredbo, je:

(a) v zvezi z organizacijami iz člena 2, točka (a), pristojni organ, imenovan v skladu s Prilogo I (del 21) k Uredbi (EU) št. 748/2012;

(b) v zvezi z organizacijami iz člena 2, točka (b), pristojni organ, imenovan v skladu s Prilogo III (del ADR.OR) k Uredbi (EU) št. 139/2014.

2. Države članice lahko za namene te uredbe imenujejo neodvisen in avtonomen subjekt za izpolnjevanje dodeljene vloge in obveznosti pristojnih organov v odstavku 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.

Člen 6

Sprememba Uredbe (EU) št. 748/2012

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

(1) Kazalo se spremeni:

(a) za naslovom 21.A.139 se vstavi naslednji naslov:

„**21.A.139A Sistem upravljanja informacijske varnosti**“;

(b) za naslovom 21.A.239 se vstavi naslednji naslov:

„**21.A.239A Sistem upravljanja informacijske varnosti**“;

(2) za točko 21.A.139 se vstavi točka 21.A.139A:

„**21.A.139A Sistem upravljanja informacijske varnosti**

Poleg sistema upravljanja za proizvodnjo, ki se zahteva v točki 21.A.139, proizvodna organizacija vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti v skladu z Delegirano uredbo Komisije (EU) 2022/1645 (*), da se zagotovi ustrezno obvladovanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.

_____

(*) 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).“;

(3) za točko 21.A.239 se vstavi točka 21.A.239A:

„**21.A.239A Sistem upravljanja informacijske varnosti**

Projektivna organizacija poleg sistema upravljanja projektiranja, ki se zahteva v točki 21.A.239, vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti v skladu z Delegirano uredbo (EU) 2022/1645, da se zagotovi ustrezno obvladovanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“.

Člen 7

Sprememba Uredbe (EU) št. 139/2014

Priloga III (del ADR.OR) k Uredbi (EU) št. 139/2014 se spremeni:

(1) za točko ADR.OR.D.005 se vstavi točka ADR.OR.D.005A:

„**ADR.OR.D.005A Sistem upravljanja informacijske varnosti**

Operator aerodroma vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti v skladu z Delegirano uredbo Komisije (EU) 2022/1645 (*), da se zagotovi ustrezno obvladovanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.

_____

(*) 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).“;

(2) točka ADR.OR.D.007 se nadomesti z naslednjim:

„**ADR.OR.D.007 Upravljanje letalskih podatkov in letalskih informacij**

(a) Operator aerodroma v okviru svojega sistema upravljanja izvaja in vzdržuje sistem upravljanja kakovosti, ki zajema naslednje dejavnosti:

(1) dejavnosti v zvezi z letalskimi podatki;

(2) dejavnosti zagotavljanja letalskih informacij.

(b) Kot del svojega sistema upravljanja operator aerodroma vzpostavi sistem upravljanja varovanja, da zagotovi varovanje operativnih podatkov, ki jih prejema, pripravlja ali drugače uporablja, tako da je dostop do navedenih operativnih podatkov omejen le na pooblaščene osebe.

(c) Sistem upravljanja varovanja opredeljuje naslednje elemente:

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

(2) sredstva za odkrivanje kršitev glede varovanja in opozarjanje osebja z ustreznimi opozorili glede varovanja;

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

(d) Operator aerodroma zagotovi varnostno preverjanje svojega osebja glede varovanja letalskih podatkov.

(e) Vidiki, povezani z informacijsko varnostjo, se upravljajo v skladu s točko ADR.OR.D.005A.“;

(3) za točko ADR.OR.F.045 se vstavi točka ADR.OR.F.045A:

„**ADR.OR.F.045A Sistem upravljanja informacijske varnosti**

Organizacija, odgovorna za izvajanje storitev upravljanja ploščadi, vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti v skladu z Delegirano uredbo (EU) 2022/1645, da se zagotovi ustrezno obvladovanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu.“.

Člen 8

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

Uporabljati se začne 16. oktobra 2025.

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

V Bruslju, 14. julija 2022

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA

INFORMACIJSKA VARNOST – ZAHTEVE ZA ORGANIZACIJE

[PART-IS.D.OR]

IS.D.OR.100 Področje uporabe

IS.D.OR.200 Sistem upravljanja informacijske varnosti

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

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

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

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

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

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

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

IS.D.OR.240 Zahteve za osebje

IS.D.OR.245 Vodenje evidenc

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

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

IS.D.OR.260 Stalno izboljševanje

IS.D.OR.100 Področje uporabe

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

IS.D.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.D.OR.205;
3. opredeljuje in izvaja ukrepe za obravnavo tveganj za informacijsko varnost v skladu s točko IS.D.OR.210;
4. izvaja sistem notranjega poročanja o informacijski varnosti v skladu s točko IS.D.OR.215;
5. v skladu s točko IS.D.OR.220 opredeli in izvaja ukrepe, potrebne za zaznavanje dogodkov na področju informacijske varnosti, opredeli tiste dogodke, ki se štejejo za incidente, ki bi lahko vplivali na varnost v letalstvu, razen v primerih, ki jih dovoljuje točka IS.D.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.D.OR.225 za obravnavanje ugotovitev, ki jih je sporočil pristojni organ;
8. izvaja shemo zunanjega poročanja v skladu s točko IS.D.OR.230, da se pristojnemu organu omogoči sprejetje ustreznih ukrepov;
9. izpolnjuje zahteve iz točke IS.D.OR.235, kadar se kateri koli del dejavnosti iz točke IS.D.OR.200 odda v izvajanje drugim organizacijam;

10. izpolnjuje zahteve glede osebja iz točke IS.D.OR.240;

11. izpolnjuje zahteve glede vodenja evidenc iz točke IS.D.OR.245;

12. spremlja skladnost organizacije z zahtevami iz te uredbe in odgovornemu vodji ali, vodji projektivne organizacije v primeru projektivnih organizacij, zagotavlja povratne informacije o ugotovitvah, da se zagotovi učinkovito izvajanje korektivnih 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.D.OR.260.

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

(d) Procesi, postopki, vloge in obveznosti, ki jih organizacija določi za skladnost s točko IS.D.OR.200(a), ustrezajo naravi in kompleksnosti njenih dejavnosti na podlagi ocene tveganj za informacijsko varnost, povezanih s temi dejavnostmi, in 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 ([1]) in v zahteve iz točke IS.D.OR.200(a)(13) lahko pristojni organ organizaciji odobri, da ne izvaja zahtev iz točk (a) do (d) in povezanih zahtev iz točk IS.D.OR.205 do IS.D.OR.260, če navedenemu organu zadovoljivo dokaže, da njene dejavnosti, objekti in viri ter storitve, ki jih izvaja, prejema in vzdržuje, niti zase niti za druge organizacije ne predstavljajo 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.D.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.D.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;

([1]) Uredba (EU) št. 376/2014 Evropskega parlamenta in Sveta z dne 3. aprila 2014 o poročanju, analizi in spremljanju dogodkov v civilnem letalstvu, spremembi Uredbe (EU) št. 996/2010 Evropskega parlamenta in Sveta ter razveljavitvi Direktive 2003/42/ES Evropskega parlamenta in Sveta in uredb Komisije (ES) št. 1321/2007 in (ES) št. 1330/2007 (UL L 122, 24.4.2014, str. 18).

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 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.D.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 posodablja 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 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.D.OR.210 Obravnava tveganja za informacijsko varnost

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

1. nadzor nad okoliščinami, ki prispevajo k učinkovitemu 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.D.OR.240(a) in (b) ter drugo zadevno osebje organizacije se obvestijo o rezultatu ocene tveganja, izvedene v skladu s točko IS.D.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.D.OR.205(b), o kakršnem koli tveganju, ki je skupno obema organizacijama.

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

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

(b) Navedena shema in postopek iz točke IS.D.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.D.OR.205 in IS.D.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, ki lahko organizacijo izpostavi tveganjem za informacijsko varnost, ki bi lahko vplivala na varnost v letalstvu, mora organizaciji poročati o dogodkih v zvezi z informacijsko varnostjo. 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 ta sistem poročanja vključi v druge sisteme poročanja, ki jih je že uvedla.

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

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

(c) Organizacija izvaja ukrepe za saniranje informacijskovarnostnih incidentov, po potrebi vključno z nujnimi ukrepi. Ti 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.D.OR.205(a), v času sanacije, ki ga je predhodno določila organizacija.

IS.D.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. določi načrt korektivnih ukrepov;

3. pristojnemu organu zadovoljivo dokaže odpravo neskladnosti.

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

IS.D.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 informacijsko-varnostnem 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 predloži 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.D.OR.235 Naročanje dejavnosti upravljanja informacijske varnosti

(a) Organizacija zagotovi, da pri oddaji naročila v zvezi s katerim koli delom dejavnosti iz točke IS.D.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 dostopa do organizacije, ki je dejavnost prevzela v izvajanje, da preveri stalno skladnost z ustreznimi zahtevami iz te uredbe.

IS.D.OR.240 Zahteve za osebje

(a) Odgovorni vodja organizacije ali vodja projektivne organizacije v primeru projektivne organizacije, imenovan v skladu z uredbama (EU) št. 748/2012 in (EU) št. 139/2014, kot je navedeno v členu 2, točki 1(a) in (b), 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.D.OR.200(a)(1);

3. izkazuje osnovno razumevanje te uredbe.

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

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

(d) Kadar si 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 ali vodja projektivne organizacije v primeru projektivne organizacije prenese svoje dejavnosti na skupno odgovorno osebo.

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

(e) Odgovorni vodja ali vodja projektivne organizacije 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.D.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 ima osebje iz točke (f) potrebno usposobljenost 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 zaupanje v osebje, ki ima dostop do informacijskih sistemov in podatkov, za katere veljajo zahteve iz te uredbe, ustrezno določena.

IS.D.OR.245 Vodenje evidenc

(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.D.OR.200(e);

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

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

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

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

   (vi) evidence dogodkov v zvezi z varnostjo informacij, ki jih bo morda treba ponovno oceniti, da se razkrijejo nezaznani informacijskovarnostni incidenti ali ranljivosti.

2. Evidence iz točke 1(i) se hranijo najmanj 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 ti dogodki v zvezi z informacijsko varnostjo 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, kadar je potrebno, opredelijo v skladu s stopnjo klasifikacije varnosti. Organizacija zagotovi, da se evidence hranijo s sredstvi za zagotovitev celovitosti, pristnosti in pooblaščenega dostopa.

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

(a) Organizacija da pristojnemu organu na voljo priročnik za upravljanje varnosti informacij (ISMM) in, kadar je ustrezno, vse pripadajoče priročnike in postopke, na katere se sklicuje, ki vsebuje:

1. izjavo, ki jo podpiše odgovorni vodja ali vodja projektivne organizacije v primeru projektivne organizacije, ki potrjuje, da bo organizacija ves čas delala v skladu s to prilogo in ISMM. Če odgovorni vodja ali v primeru projektivne organizacije vodja projektivne organizacije ni izvršni direktor organizacije, potem ta sopodpiše izjavo;

2. nazive, imena, dolžnosti, odgovornosti, obveznosti in pooblastila osebe ali oseb iz točke IS.D.OR.240(b) in (c);

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

4. politiko informacijske varnosti organizacije iz točke IS.D.OR.200(a)(1);

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

6. nazive, imena, dolžnosti, odgovornosti, obveznosti in pooblastila ključnih oseb, odgovornih za izvajanje točke IS.D.OR.200, vključno z osebo ali osebami, odgovornimi za funkcijo spremljanja skladnosti iz točke IS.D.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.D.OR.215;

9. postopke, ki določajo, kako organizacija zagotavlja skladnost s tem delom, in zlasti:

(i) dokumentacijsko točko IS.D.OR.200(c);

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

(iii) postopek spremembe ISMM, opredeljen v točki (c);

10. podrobnosti trenutno odobrenih drugih načinov usklajevanja.

(b) Prva izdaja ISMM se odobri, kopijo pa obdrži pristojni organ. 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. Pristojni organ odobri vse spremembe, ki niso vključene v področje uporabe tega postopka, in vse spremembe, povezane s spremembami, navedenimi v točki IS.D.OR.255(b).

(d) Organizacija lahko ISMM poveže z drugimi priročniki za upravljanje ali priročniki, ki jih hrani, če obstaja jasna navzkrižna referenca, ki navaja, kateri deli priročnika za upravljanje ustrezajo različnim zahtevam iz te priloge.

IS.D.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 s temi spremembami:

1. se zahtevek predloži pred izvedbo vsake takšne spremembe, da bi pristojni organ lahko ugotovil, ali je zagotovljena stalna skladnost s to uredbo, in 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. se sprememba izvede šele po prejemu uradne odobritve pristojnega organa;
4. organizacija med izvajanjem takih sprememb deluje pod pogoji, ki jih predpiše pristojni organ.

IS.D.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.