II

(Acte fără caracter legislativ)

REGULAMENTE

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2023/203 AL COMISIEI

din 27 octombrie 2022

de stabilire a normelor de aplicare a Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului în ceea ce privește cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, impuse organizațiilor care intră sub incidența Regulamentelor (UE) nr. 1321/2014, (UE) nr. 965/2012, (UE) nr. 1178/2011, (UE) 2015/340 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei, precum și autorităților competente care intră sub incidența Regulamentelor (UE) nr. 748/2012, (UE) nr. 1321/2014, (UE) nr. 965/2012, (UE) nr. 1178/2011, (UE) 2015/340 și (UE) nr. 139/2014 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei, și de modificare a Regulamentelor (UE) nr. 1178/2011, (UE) nr. 748/2012, (UE) nr. 965/2012, (UE) nr. 139/2014, (UE) nr. 1321/2014, (UE) 2015/340 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2018/1139 al Parlamentului European și al Consiliului din 4 iulie 2018 privind normele comune în domeniul aviației civile și de înființare a Agenției Uniunii Europene pentru Siguranța Aviației, de modificare a Regulamentelor (CE) nr. 2111/2005, (CE) nr. 1008/2008, (UE) nr. 996/2010, (UE) nr. 376/2014 și a Directivelor 2014/30/UE și 2014/53/UE ale Parlamentului European și ale Consiliului, precum și de abrogare a Regulamentelor (CE) nr. 552/2004 și (CE) nr. 216/2008 ale Parlamentului European și ale Consiliului și a Regulamentului (CEE) nr. 3922/91 al Consiliului [1], în special articolul 17 alineatul (1) litera (b), articolul 27 alineatul (1) litera (a), articolul 31 alineatul (1) litera (b), articolul 43 alineatul (1) litera (b), articolul 53 alineatul (1) litera (a) și articolul 62 alineatul (15) litera (c),

întrucât:

(1) În conformitate cu cerințele esențiale prevăzute la punctul 3.1 litera (b) din anexa II la Regulamentul (UE) 2018/1139, organizațiile de management al continuității navigabilității și organizațiile de întreținere trebuie să instituie și să mențină un sistem de management pentru gestionarea riscurilor în materie de siguranță.

(2) În conformitate cu cerințele esențiale prevăzute la punctul 3.3 litera (b) și la punctul 5 litera (b) din anexa IV la Regulamentul (UE) 2018/1139, organizațiile de pregătire a piloților, organizațiile de pregătire a echipajului de cabină, centrele de medicină aeronautică pentru personalul aeronautic navigant și operatorii de echipamente de pregătire sintetică pentru zbor trebuie de asemenea să instituie și să mențină un sistem de management pentru gestionarea riscurilor în materie de siguranță.

(3) În conformitate cu cerințele esențiale prevăzute la punctul 8.1 litera (c) din anexa V la Regulamentul (UE) 2018/1139, operatorii aerieni trebuie, la rândul lor, să instituie și să mențină un sistem de management pentru gestionarea riscurilor în materie de siguranță.

(4) În conformitate cu cerințele esențiale prevăzute la punctul 5.1 litera (c) și la punctul 5.4 litera (b) din anexa VIII la Regulamentul (UE) 2018/1139, și furnizorii de servicii de management al traficului aerian, furnizorii de servicii de navigație aeriană, furnizorii de servicii U-space, furnizorii unici de servicii de informații comune, organizațiile de pregătire și centrele de medicină aeronautică pentru controlorii de trafic aerian trebuie să instituie și să mențină un sistem de management pentru gestionarea riscurilor în materie de siguranță.

[1] JO L 212, 22.8.2018, p. 1.

(5) Respectivele riscuri în materie de siguranță pot proveni din diferite surse, cum ar fi deficiențe de proiectare și de întreținere, aspecte ale performanțelor umane, amenințări la adresa mediului și amenințări la adresa securității informațiilor. Prin urmare, sistemele de management instituite de Agenția Uniunii Europene pentru Siguranța Aviației (denumită în continuare „agenția"), de autoritățile naționale competente și de organizațiile menționate în considerentele de mai sus trebuie să țină seama nu doar de riscurile în materie de siguranță care decurg din evenimente fortuite, ci și de riscurile în materie de siguranță care decurg din amenințări la adresa securității informațiilor, atunci când deficiențele existente pot fi exploatate de persoane cu intenții răuvoitoare. Aceste riscuri în materie de securitate a informațiilor sunt în continuă creștere în mediul aviației civile, pe măsură ce sistemele informatice actuale devin tot mai interconectate și devin tot mai des ținta unor actori răuvoitori.

(6) Riscurile asociate acestor sisteme informatice nu se limitează la posibile atacuri asupra spațiului cibernetic, ci includ și amenințări care pot afecta procesele și procedurile, precum și performanțele ființelor umane.

(7) Un număr semnificativ de organizații utilizează deja standarde internaționale, cum ar fi ISO 27001, pentru a aborda securitatea informațiilor și a datelor digitale. Este posibil ca respectivele standarde să nu abordeze pe deplin toate specificitățile aviației civile. Prin urmare, este oportun să se prevadă cerințe privind managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației.

(8) Este esențial ca respectivele cerințe să acopere toate domeniile aviației și interfețele acestora, dat fiind că aviația este un sistem de sisteme cu grad înalt de interconectare. Prin urmare, aceste cerințe trebuie să se aplice tuturor organizațiilor și autorităților competente care intră sub incidența Regulamentelor (UE) nr. 748/2012 ([2]), (UE) nr. 1321/2014 ([3]), (UE) nr. 965/2012 ([4]), (UE) nr. 1178/2011 ([5]), (UE) 2015/340 ([6]), (UE) nr. 139/2014 ([7]) ale Comisiei și a Regulamentului de punere în aplicare (UE) 2021/664 al Comisiei ([8]), inclusiv celor care au deja obligația de a dispune de un sistem de management în conformitate cu legislația existentă a Uniunii în domeniul siguranței aviației. Unele organizații trebuie totuși să fie excluse din domeniul de aplicare al prezentului regulament, pentru a se asigura proporționalitatea corespunzătoare cu gradul mai scăzut de riscuri în materie de securitate a informațiilor pe care acestea le prezintă pentru sistemul aviatic.

(9) Cerințele stabilite în prezentul regulament trebuie să asigure o punere în aplicare consecventă în toate domeniile aviației, creând în același timp un impact minim asupra legislației Uniunii din domeniul siguranței aviației, aplicabilă deja respectivelor domenii.

([2]) Regulamentul (UE) nr. 748/2012 al Comisiei din 3 august 2012 de stabilire a normelor de punere în aplicare privind certificarea pentru navigabilitate și mediu a aeronavelor și a produselor, pieselor și echipamentelor aferente, precum și certificarea organizațiilor de proiectare și producție (JO L 224, 21.8.2012, p. 1).

([3]) Regulamentul (UE) nr. 1321/2014 al comisiei din 26 noiembrie 2014 privind menținerea navigabilității aeronavelor și a produselor, reperelor și dispozitivelor aeronautice și autorizarea întreprinderilor și a personalului cu atribuții în domeniu (JO L 362, 17.12.2014, p. 1).

([4]) Regulamentul (UE) nr. 965/2012 al Comisiei din 5 octombrie 2012 de stabilire a cerințelor tehnice și a procedurilor administrative referitoare la operațiunile aeriene în temeiul Regulamentului (CE) nr. 216/2008 al Parlamentului European și al Consiliului (JO L 296, 25.10.2012, p. 1).

([5]) Regulamentul (UE) nr. 1178/2011 al Comisiei din 3 noiembrie 2011 de stabilire a cerințelor tehnice și a procedurilor administrative referitoare la personalul navigant din aviația civilă în temeiul Regulamentului (CE) nr. 216/2008 al Parlamentului European și al Consiliului (JO L 311, 25.11.2011, p. 1).

([6]) Regulamentul (UE) 2015/340 al Comisiei din 20 februarie 2015 de stabilire a cerințelor tehnice și a procedurilor administrative referitoare la licențele și certificatele controlorilor de trafic aerian în conformitate cu Regulamentul (CE) nr. 216/2008 al Parlamentului European și al Consiliului, de modificare a Regulamentului de punere în aplicare (UE) nr. 923/2012 al Comisiei și de abrogare a Regulamentului (UE) nr. 805/2011 al Comisiei (JO L 63, 6.3.2015, p. 1).

([7]) Regulamentul (UE) nr. 139/2014 al Comisiei din 12 februarie 2014 de stabilire a cerințelor tehnice și a procedurilor administrative referitoare la aerodromuri în temeiul Regulamentului (CE) nr. 216/2008 al Parlamentului European și al Consiliului (JO L 44, 14.2.2014, p. 1).

([8]) Regulamentul de punere în aplicare (UE) 2021/664 al Comisiei din 22 aprilie 2021 privind un cadru de reglementare pentru U-space (JO L 139, 23.4.2021, p. 161).

(10) Cerințele stabilite în prezentul regulament nu trebuie să aducă atingere cerințelor de securitate a informațiilor și de securitate cibernetică stabilite la punctul 1.7 din anexa la Regulamentul de punere în aplicare (UE) 2015/1998 al Comisiei ([9]) și la articolul 14 din Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului ([10]).

(11) Cerințele de securitate stabilite în titlul V, „Securitatea programului", articolele 33-43 din Regulamentul (UE) 2021/696 al Parlamentului European și al Consiliului ([11]) sunt considerate echivalente cu cerințele stabilite în prezentul regulament, cu excepția punctului IS.I.OR.230 din anexa II la prezentul regulament, care trebuie respectat.

(12) Pentru a se asigura securitatea juridică, interpretarea termenului „securitatea informațiilor", astfel cum este definit în prezentul regulament, interpretare care reflectă utilizarea obișnuită a acestuia în aviația civilă la nivel mondial, trebuie să fie considerată consecventă cu interpretarea termenului „securitatea rețelelor și a sistemelor informatice", astfel cum este definit la articolul 4 punctul 2 din Directiva (UE) 2016/1148. Definiția securității informațiilor utilizată în sensul prezentului regulament nu trebuie să fie interpretată ca îndepărtându-se de definiția securității rețelelor și a sistemelor informatice stabilită în Directiva (UE) 2016/1148.

(13) Pentru a se evita suprapunerea cerințelor juridice, în cazurile în care organizațiile care intră sub incidența prezentului regulament sunt deja supuse unor cerințe de securitate, decurgând din acte ale Uniunii menționate în considerentele 10 și 11 și având un efect echivalent cu dispozițiile prevăzute în prezentul regulament, trebuie să se considere că îndeplinirea respectivelor cerințe de securitate constituie o îndeplinire a cerințelor stabilite în prezentul regulament.

(14) Organizațiile care intră sub incidența prezentului regulament și care sunt deja supuse cerințelor de securitate decurgând din Regulamentul de punere în aplicare (UE) 2015/1998, din Regulamentul (UE) 2021/696 sau din ambele trebuie să îndeplinească și cerințele din anexa II (partea IS.I.OR.230 – „Sistemul de raportare externă în materie de securitate a informațiilor") la prezentul regulament, întrucât niciunul dintre regulamente nu conține dispoziții referitoare la raportarea externă a incidentelor de securitate a informațiilor.

(15) Din motive de exhaustivitate, Regulamentele (UE) nr. 1178/2011, (UE) nr. 748/2012, (UE) nr. 965/2012, (UE) nr. 139/2014, (UE) nr. 1321/2014, (UE) 2015/340 și Regulamentele de punere în aplicare (UE) 2017/373 ([12]) și (UE) 2021/664 trebuie modificate pentru a se introduce cerințele prevăzute în prezentul regulament cu privire la sistemele de management al securității informațiilor împreună cu sistemele de management prevăzute în acesta și pentru a se stabili cerințele pe care trebuie să le îndeplinească autoritățile competente în ceea ce privește supravegherea organizațiilor care pun în aplicare cerințele de management al securității informațiilor, menționate anterior.

(16) Pentru a se oferi organizațiilor suficient timp să asigure conformitatea cu noile norme și proceduri, prezentul regulament trebuie să intre în aplicare după trei ani de la data intrării în vigoare, mai puțin pentru furnizorul de servicii de navigație aeriană al Serviciului european geostaționar mixt de navigare (EGNOS), definit în Regulamentul de punere în aplicare (UE) 2017/373, în cazul căruia, dat fiind că procesul de acreditare de securitate al sistemului și serviciilor EGNOS este în curs, în conformitate cu Regulamentul (UE) 2021/696, ar trebui să devină aplicabil de la 1 ianuarie 2026.

(17) Cerințele stabilite în prezentul regulament se bazează pe Avizul nr. 3/2021 ([13]), emis de agenție în conformitate cu articolul 75 alineatul (2) literele (b) și (c) și cu articolul 76 alineatul (1) din Regulamentul (UE) 2018/1139.

([9]) Regulamentul de punere în aplicare (UE) 2015/1998 al Comisiei din 5 noiembrie 2015 de stabilire a măsurilor detaliate de implementare a standardelor de bază comune în domeniul securității aviației (JO L 299, 14.11.2015, p. 1).

([10]) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

([11]) Regulamentul (UE) 2021/696 al Parlamentului European și al Consiliului din 28 aprilie 2021 de instituire a Programului spațial al Uniunii și a Agenției Uniunii Europene pentru Programul spațial și de abrogare a Regulamentelor (UE) nr. 912/2010, (UE) nr. 1285/2013 și (UE) nr. 377/2014 și a Deciziei nr. 541/2014/UE (JO L 170, 12.5.2021, p. 69).

([12]) Regulamentul de punere în aplicare (UE) 2017/373 al Comisiei din 1 martie 2017 de stabilire a unor cerințe comune pentru furnizorii de management al traficului aerian/servicii de navigație aeriană și de alte funcții ale rețelei de management al traficului aerian și pentru supravegherea acestora, de abrogare a Regulamentului (CE) nr. 482/2008, a Regulamentelor de punere în aplicare (UE) nr. 1034/2011, (UE) nr. 1035/2011 și (UE) 2016/1377, precum și de modificare a Regulamentului (UE) nr. 677/2011 (JO L 62, 8.3.2017, p. 1).

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

(18) Cerințele stabilite în prezentul regulament sunt conforme cu avizul Comitetului pentru aplicarea de norme comune de siguranță în domeniul aviației civile, instituit în temeiul articolului 127 din Regulamentul (UE) 2018/1139,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Obiect

În prezentul regulament sunt prevăzute cerințele pe care trebuie să le îndeplinească organizațiile și autoritățile competente în vederea:

(a) identificării și a managementului riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care ar putea afecta sistemele de tehnologie a informației și comunicațiilor și datele utilizate în scopul aviației civile;

(b) detectării evenimentelor de securitate a informațiilor și a identificării celor care sunt considerate incidente de securitate a informațiilor cu impact potențial asupra siguranței aviației;

(c) asigurării unui răspuns la respectivele incidente de securitate a informațiilor și a redresării în urma acestora.

Articolul 2

Domeniu de aplicare

(1) Prezentul regulament se aplică următoarelor organizații:

(a) organizații de întreținere supuse dispozițiilor din secțiunea A din anexa II (partea 145) la Regulamentul (UE) nr. 1321/2014, cu excepția celor implicate exclusiv în întreținerea aeronavelor în conformitate cu anexa Vb (partea ML) la Regulamentul (UE) nr. 1321/2014;

(b) organizații de management al continuității navigabilității (CAMO-uri) supuse dispozițiilor din secțiunea A din anexa Vc (partea CAMO) la Regulamentul (UE) nr. 1321/2014, cu excepția celor implicate exclusiv în managementul continuității navigabilității aeronavelor în conformitate cu anexa Vb (partea ML) la Regulamentul (UE) nr. 1321/2014;

(c) operatori aerieni supuși dispozițiilor din anexa III (partea ORO) la Regulamentul (UE) nr. 965/2012, cu excepția celor implicați exclusiv în operarea oricăreia dintre următoarele:

(i) o aeronavă ELA 2, astfel cum este definită la articolul 1 alineatul (2) litera (j) din Regulamentul (UE) nr. 748/2012;

(ii) avioane monomotoare cu elice cu o configurație maximă operațională de cinci locuri pentru pasageri sau mai puțin, care nu sunt clasificate drept aeronave complexe motorizate, atunci când decolează și aterizează pe același aerodrom sau loc de operare și când operează în conformitate cu regulile de zbor la vedere (VFR) pe timp de zi;

(iii) elicoptere monomotoare cu o configurație maximă operațională de cinci locuri pentru pasageri sau mai puțin, care nu sunt clasificate drept aeronave complexe motorizate, atunci când decolează și aterizează pe același aerodrom sau loc de operare și când operează în conformitate cu regulile de zbor la vedere (VFR) pe timp de zi;

(d) organizații de pregătire aprobate (ATO-uri) supuse dispozițiilor din anexa VII (partea ORA) la Regulamentul (UE) nr. 1178/2011, cu excepția celor implicate exclusiv în activități de pregătire aferente aeronavelor ELA 2, astfel cum sunt definite la articolul 1 alineatul (2) litera (j) din Regulamentul (UE) nr. 748/2012, sau implicate exclusiv în pregătire teoretică;

(e) centre de medicină aeronautică pentru personalul navigant supuse dispozițiilor din anexa VII (partea ORA) la Regulamentul (UE) nr. 1178/2011;

(f) operatori de echipamente de pregătire sintetică pentru zbor (FSTD-uri) supuși dispozițiilor din anexa VII (partea ORA) la Regulamentul (UE) nr. 1178/2011, cu excepția celor implicați exclusiv în operarea FSTD-urilor aferente aeronavelor ELA 2, astfel cum sunt definite la articolul 1 alineatul (2) litera (j) din Regulamentul (UE) nr. 748/2012;

(g) organizații de pregătire a controlorilor de trafic aerian (ATCO) și centre de medicină aeronautică pentru ATCO supuse dispozițiilor din anexa III (partea ATCO.OR) la Regulamentul (UE) 2015/340;

(h) organizații supuse dispozițiilor din anexa III (partea ATM/ANS.OR) la Regulamentul de punere în aplicare (UE) 2017/373, cu excepția următorilor furnizori de servicii:

(i) furnizori de servicii de navigație aeriană care dețin un certificat limitat în conformitate cu punctul ATM/ANS.OR.A.010 din anexa menționată;

(ii) furnizori de servicii de informare a zborurilor care își declară activitățile în conformitate cu punctul ATM/ANS.OR.A.015 din anexa menționată;

(i) furnizori de servicii U-space și furnizori unici de servicii de informații comune care sunt supuși dispozițiilor din Regulamentul de punere în aplicare (UE) 2021/664.

(2) Prezentul regulament se aplică autorităților competente, inclusiv Agenției Uniunii Europene pentru Siguranța Aviației („agenția”), astfel cum sunt menționate la articolul 6 din prezentul regulament și la articolul 5 din Regulamentul delegat (UE) 2022/1645 al Comisiei ([14]).

(3) Prezentul regulament se aplică, de asemenea, autorității competente responsabile cu eliberarea, prelungirea, modificarea, suspendarea sau revocarea licențelor de întreținere a aeronavelor în conformitate cu anexa III (partea 66) la Regulamentul (UE) nr. 1321/2014.

(4) Prezentul regulament nu aduce atingere cerințelor privind securitatea informațiilor și securitatea cibernetică stabilite la punctul 1.7 din anexa la Regulamentul de punere în aplicare (UE) 2015/1998 și la articolul 14 din Directiva (UE) 2016/1148.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „securitate a informațiilor” înseamnă păstrarea confidențialității, integrității, autenticității și disponibilității rețelelor și sistemelor informatice;

2. „eveniment de securitate a informațiilor” înseamnă un eveniment identificat al unui sistem, al unui serviciu sau al unei rețele, care indică o posibilă încălcare a politicii de securitate a informațiilor sau o deficiență a controalelor de securitate a informațiilor ori o situație necunoscută anterior care poate fi relevantă pentru securitatea informațiilor;

3. „incident” înseamnă orice eveniment care are un efect negativ real asupra securității rețelelor și sistemelor informatice, astfel cum este definit la articolul 4 punctul 7 din Directiva (UE) 2016/1148;

4. „risc în materie de securitate a informațiilor” înseamnă riscul la adresa organizării operațiunilor de aviație civilă, precum și la adresa activelor, a persoanelor fizice și a altor organizații, atribuibil unui posibil eveniment de securitate a informațiilor. Riscurile în materie de securitate a informațiilor sunt asociate cu posibilitatea ca amenințările să exploateze vulnerabilitățile unui activ informațional sau ale unui grup de active informaționale;

([14]) Regulamentul delegat (UE) 2022/1645 al Comisiei din 14 iulie 2022 de stabilire a normelor de aplicare a Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului în ceea ce privește cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației impuse organizațiilor care intră sub incidența Regulamentelor (UE) nr. 748/2012 și (UE) nr. 139/2014 ale Comisiei și de modificare a Regulamentelor (UE) nr. 748/2012 și (UE) nr. 139/2014 ale Comisiei (JO L 248, 26.9.2022, p. 18).

5. „amenințare” înseamnă o încălcare potențială a securității informațiilor care există atunci când o entitate, o circumstanță, o acțiune sau un eveniment ar putea cauza prejudicii;

6. „vulnerabilitate” înseamnă o deficiență sau slăbiciune a unui activ sau a unui sistem, a procedurilor, a concepției, a implementării sau a măsurilor de securitate a informațiilor, care ar putea fi exploatată și s-ar putea solda cu o încălcare sau nerespectare a politicii de securitate a informațiilor.

Articolul 4

Cerințe pentru organizații și pentru autorități competente

(1) Organizațiile menționate la articolul 2 alineatul (1) trebuie să respecte cerințele din anexa II (partea IS.I.OR) la prezentul regulament.

(2) Autoritățile competente menționate la articolul 2 alineatele (2) și (3) trebuie să respecte cerințele din anexa I (partea IS.AR) la prezentul regulament.

Articolul 5

Cerințe care decurg din alte acte legislative ale Uniunii

(1) Atunci când o organizație menționată la articolul 2 alineatul (1) îndeplinește cerințe de securitate stabilite în conformitate cu articolul 14 din Directiva (UE) 2016/1148 care sunt echivalente cu cerințele stabilite în prezentul regulament, se consideră că îndeplinirea respectivelor cerințe de securitate constituie îndeplinirea cerințelor stabilite în prezentul regulament.

(2) În cazul în care o organizație menționată la articolul 2 alineatul (1) este un operator sau o entitate menționată în programele naționale de securitate a aviației civile ale statelor membre, stabilite în conformitate cu articolul 10 din Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului ([15]), cerințele de securitate cibernetică de la punctul 1.7 din anexa la Regulamentul de punere în aplicare (UE) 2015/1998 trebuie considerate echivalente cu cerințele stabilite în prezentul regulament, cu excepția punctului IS.I.OR.230 din anexa II la prezentul regulament, care trebuie respectat ca atare.

(3) În cazul în care organizația menționată la articolul 2 alineatul (1) este furnizorul de servicii de navigație aeriană al Serviciului european geostaționar mixt de navigare (EGNOS) menționat în Regulamentul (UE) 2021/696, cerințele de securitate prevăzute în titlul V articolele 33-43 din regulamentul respectiv sunt considerate echivalente cu cerințele stabilite în prezentul regulament, cu excepția punctului IS.I.OR.230 din anexa II la prezentul regulament, care trebuie respectat ca atare.

(4) După consultarea agenției și a grupului de cooperare menționat la articolul 11 din Directiva (UE) 2016/1148, Comisia poate să emită orientări pentru evaluarea echivalenței cerințelor stabilite în prezentul regulament și în Directiva (UE) 2016/1148.

Articolul 6

Autoritatea competentă

(1) Fără a aduce atingere sarcinilor încredințate consiliului de acreditare de securitate menționat la articolul 36 din Regulamentul (UE) 2021/696, autoritatea responsabilă cu certificarea și supravegherea respectării prezentului regulament este:

(a) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) litera (a), autoritatea competentă desemnată în conformitate cu anexa II (partea 145) la Regulamentul (UE) nr. 1321/2014;

(b) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) litera (b), autoritatea competentă desemnată în conformitate cu anexa Vc (partea CAMO) la Regulamentul (UE) nr. 1321/2014;

([15]) Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului din 11 martie 2008 privind norme comune în domeniul securității aviației civile și de abrogare a Regulamentului (CE) nr. 2320/2002 (JO L 97, 9.4.2008, p. 72).

(c) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) litera (c), autoritatea competentă desemnată în conformitate cu anexa III (partea ORO) la Regulamentul (UE) nr. 965/2012;

(d) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) literele (d)-(f), autoritatea competentă desemnată în conformitate cu anexa VII (partea ORA) la Regulamentul (UE) nr. 1178/2011;

(e) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) litera (g), autoritatea competentă desemnată în conformitate cu articolul 6 alineatul (2) din Regulamentul (UE) 2015/340;

(f) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) litera (h), autoritatea competentă desemnată în conformitate cu articolul 4 alineatul (1) din Regulamentul de punere în aplicare (UE) 2017/373;

(g) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) litera (i), autoritatea competentă desemnată în conformitate cu articolul 14 alineatul (1) sau cu articolul 14 alineatul (2) din Regulamentul de punere în aplicare (UE) 2021/664, după caz.

(2) În sensul prezentului regulament, statele membre pot desemna o entitate independentă și autonomă care să îndeplinească rolul și responsabilitățile atribuite autorităților competente menționate la alineatul (1). În acest caz, trebuie stabilite măsuri de coordonare între entitatea respectivă și autoritățile competente, astfel cum se menționează la alineatul (1), pentru a se asigura supravegherea efectivă a tuturor cerințelor care trebuie respectate de către organizație.

(3) Agenția cooperează, în deplină conformitate cu normele aplicabile privind confidențialitatea, protecția datelor cu caracter personal și protecția informațiilor clasificate, cu Agenția Uniunii Europene pentru Programul spațial (EUSPA) și cu consiliul de acreditare de securitate menționat la articolul 36 din Regulamentul (UE) 2021/696, pentru a asigura supravegherea eficace a cerințelor aplicabile furnizorului de servicii de navigație aeriană al EGNOS.

Articolul 7

Transmiterea informațiilor relevante către autoritățile competente din domeniul NIS

Autoritățile competente în temeiul prezentului regulament comunică, fără întârzieri nejustificate, punctului unic de contact desemnat în conformitate cu articolul 8 din Directiva (UE) 2016/1148 orice informație relevantă inclusă în notificările transmise în temeiul punctului IS.I.OR.230 din anexa II la prezentul regulament și în temeiul punctului IS.D.OR.230 din anexa I la Regulamentul delegat (UE) 2022/1645 de către operatorii de servicii esențiale identificați în conformitate cu articolul 5 din Directiva (UE) 2016/1148.

Articolul 8

Modificarea Regulamentului (UE) nr. 1178/2011

Anexele VI (partea ARA) și VII (partea ORA) la Regulamentul (UE) nr. 1178/2011 se modifică în conformitate cu anexa III la prezentul regulament.

Articolul 9

Modificarea Regulamentului (UE) nr. 748/2012

Anexa I (partea 21) la Regulamentul (UE) nr. 748/2012 se modifică în conformitate cu anexa IV la prezentul regulament.

Articolul 10

Modificarea Regulamentului (UE) nr. 965/2012

Anexele II (partea ARO) și III (partea ORO) la Regulamentul (UE) nr. 965/2012 se modifică în conformitate cu anexa V la prezentul regulament.

Articolul 11

Modificarea Regulamentului (UE) nr. 139/2014

Anexa II (partea ADR.AR) la Regulamentul (UE) nr. 139/2014 se modifică în conformitate cu anexa VI la prezentul regulament.

Articolul 12

Modificarea Regulamentului (UE) nr. 1321/2014

Anexele II (partea 145), III (partea 66) și Vc (partea CAMO) la Regulamentul (UE) nr. 1321/2014 se modifică în conformitate cu anexa VII la prezentul regulament.

Articolul 13

Modificarea Regulamentului (UE) 2015/340

Anexele II (partea ATCO.AR) și III (partea ATCO.OR) la Regulamentul (UE) 2015/340 se modifică în conformitate cu anexa VIII la prezentul regulament.

Articolul 14

Modificarea Regulamentului de punere în aplicare (UE) 2017/373

Anexele II (partea ATM/ANS.AR) și III (partea ATM/ANS.OR) la Regulamentul de punere în aplicare (UE) 2017/373 se modifică în conformitate cu anexa IX la prezentul regulament.

Articolul 15

Modificarea Regulamentului de punere în aplicare (UE) 2021/664

Regulamentul de punere în aplicare (UE) 2021/664 se modifică după cum urmează:

1. La articolul 15 alineatul (1), litera (f) se înlocuiește cu următorul text:

„(f) implementează și menține un sistem de management al securității în conformitate cu punctul ATM/ANS.OR.D.010 din subpartea D a anexei III la Regulamentul de punere în aplicare (UE) 2017/373 și un sistem de management al securității informațiilor în conformitate cu anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203.”

2. La articolul 18 se adaugă următoarea literă (l):

„(l) instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203.”

Articolul 16

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Se aplică de la 22 februarie 2026.

În cazul furnizorului de servicii de navigație aeriană al EGNOS, care se supune dispozițiilor Regulamentului de punere în aplicare (UE) 2017/373, prezentul regulament se aplică însă de la 1 ianuarie 2026.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 27 octombrie 2022.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXA I

SECURITATEA INFORMAȚIILOR – CERINȚE APLICABILE AUTORITĂȚILOR

[PARTEA IS.AR]

IS.AR.100 Domeniul de aplicare

Prezenta parte stabilește cerințele în materie de management care trebuie îndeplinite de organizațiile menționate la articolul 2 alineatul (2) din prezentul regulament.

Cerințele pe care trebuie să le îndeplinească autoritățile competente respective când își desfășoară activitățile de certificare, de supraveghere și de asigurare a respectării sunt cuprinse în regulamentele menționate la articolul 2 alineatul (1) din prezentul regulament și la articolul 2 din Regulamentul delegat (UE) 2022/1645.

IS.AR.200 Sistemul de management al securității informațiilor (SMSI)

(a) Pentru a atinge obiectivele prevăzute la articolul 1, autoritatea competentă trebuie să instituie, să implementeze și să mențină un sistem de management al securității informațiilor (SMSI) care asigură faptul că autoritatea competentă:

1. instituie o politică de securitate a informațiilor în care sunt prevăzute principiile generale ale autorității competente în ceea ce privește impactul potențial al riscurilor în materie de securitate a informațiilor asupra siguranței aviației;

2. identifică și examinează riscurile în materie de securitate a informațiilor în conformitate cu punctul IS.AR.205;

3. definește și implementează măsurile de tratare a riscurilor în materie de securitate a informațiilor în conformitate cu punctul IS.AR.210;

4. definește și implementează, în conformitate cu punctul IS.AR.215, măsurile necesare pentru detectarea evenimentelor de securitate a informațiilor, le identifică pe cele care sunt considerate incidente cu impact potențial asupra siguranței aviației, asigură un răspuns la respectivele incidente de securitate a informațiilor și se redresează în urma acestora;

5. îndeplinește cerințele de la punctul IS.AR.220 când subcontractează altor organizații orice parte a activităților descrise la punctul IS.AR.200;

6. îndeplinește cerințele în materie de personal de la punctul IS.AR.225;

7. îndeplinește cerințele de păstrare a evidențelor de la punctul IS.AR.230;

8. monitorizează îndeplinirea de către propria organizație a cerințelor din prezentul regulament și transmite persoanei menționate la punctul IS.AR.225 litera (a) feedback cu privire la constatări, pentru a asigura implementarea efectivă a măsurilor corective;

9. protejează confidențialitatea oricăror informații pe care autoritatea competentă le-ar putea avea cu privire la organizații care fac obiectul supravegherii sale și a informațiilor primite prin intermediul sistemelor de raportare externă ale organizației, instituite în conformitate cu punctul IS.I.OR.230 din anexa II (partea IS.I.OR) la prezentul regulament și cu punctul IS.D.OR.230 din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645;

10. notifică agenției schimbările care afectează capacitatea autorității competente de a-și executa sarcinile și de a-și îndeplini responsabilitățile definite în prezentul regulament;

11. definește și pune în aplicare proceduri pentru transmiterea informațiilor pertinente, în funcție de necesități și într-un mod practic și rapid, pentru a ajuta alte autorități și agenții competente, precum și organizațiile supuse dispozițiilor prezentului regulament să efectueze evaluări eficace ale riscurilor în materie de securitate asociate activităților lor.

(b) Pentru a îndeplini în permanență cerințele menționate la articolul 1, autoritatea competentă trebuie să implementeze un proces de îmbunătățire continuă în conformitate cu punctul IS.AR.235.

(c) Autoritatea competentă trebuie să documenteze toate procesele, procedurile, rolurile și responsabilitățile cheie necesare pentru a se conforma punctului IS.AR.200 litera (a) și să instituie un proces de modificare a acestei documentații.

(d) Procesele, procedurile, rolurile și responsabilitățile instituite de autoritatea competentă pentru a se conforma punctului IS.AR.200 litera (a) trebuie să corespundă naturii și complexității activităților sale, pe baza unei evaluări a riscurilor în materie de securitate a informațiilor inerente activităților respective, și pot fi integrate în alte sisteme de management existente care sunt deja implementate de autoritatea competentă.

IS.AR.205 Evaluarea riscurilor în materie de securitate a informațiilor

(a) Autoritatea competentă trebuie să identifice toate elementele propriei organizații care ar putea fi expuse unor riscuri în materie de securitate a informațiilor. Acestea cuprind:

1. activitățile, instalațiile și resursele autorității competente și serviciile pe care le operează, furnizează, primește sau menține autoritatea competentă;

2. echipamentele, sistemele, datele și informațiile care contribuie la funcționarea elementelor menționate la subpunctul 1.

(b) Autoritatea competentă trebuie să identifice interfețele pe care propria organizație le are cu alte organizații și care ar putea conduce la expunerea reciprocă la riscuri în materie de securitate a informațiilor.

(c) Pentru elementele și interfețele menționate la literele (a) și (b), autoritatea competentă trebuie să identifice riscurile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației.

Pentru fiecare risc identificat, autoritatea competentă trebuie:

1. să atribuie un nivel de risc în conformitate cu o clasificare predefinită stabilită de autoritatea competentă;

2. să asocieze fiecare risc și nivelul său aferent cu elementul sau interfața corespunzătoare identificată în conformitate cu literele (a) și (b).

Clasificarea predefinită menționată la subpunctul 1 trebuie să țină seama de potențialul de producere a scenariului de amenințare și de gravitatea consecințelor acestuia asupra siguranței. Prin această clasificare și în funcție de existența sau absența, în cadrul autorității competente, a unui proces structurat și repetabil de management al riscurilor pentru operațiuni, autoritatea competentă trebuie să fie în măsură să stabilească dacă riscul este acceptabil sau dacă trebuie tratat în conformitate cu punctul IS.AR.210.

Pentru a se facilita comparabilitatea reciprocă a evaluărilor riscurilor, la atribuirea nivelului de risc în conformitate cu subpunctul 1 se ține seama de informațiile relevante obținute în coordonare cu organizațiile menționate la litera (b).

(d) Autoritatea competentă trebuie să revizuiască și să actualizeze evaluarea riscurilor efectuată în conformitate cu literele (a), (b) și (c) în oricare dintre următoarele cazuri:

1. când există o modificare a elementelor expuse unor riscuri în materie de securitate a informațiilor;

2. când există o modificare a interfețelor dintre autoritatea competentă și alte organizații sau o modificare a riscurilor comunicate de celelalte organizații;

3. când există o modificare a informațiilor sau a cunoștințelor utilizate pentru identificarea, analizarea și clasificarea riscurilor;

4. când analiza incidentelor de securitate a informațiilor a permis desprinderea de învățăminte.

IS.AR.210 Tratarea riscurilor în materie de securitate a informațiilor

(a) Autoritatea competentă trebuie să elaboreze măsuri de abordare a riscurilor inacceptabile identificate în conformitate cu punctul IS.AR.205, să le implementeze în timp util și să verifice menținerea eficacității acestora. Respectivele măsuri trebuie să permită autorității competente:

1. să controleze circumstanțele care contribuie la apariția efectivă a scenariului de amenințare;

2. să diminueze consecințele pentru siguranța aviației care sunt asociate materializării scenariului de amenințare;

3. să evite riscurile.

Respectivele măsuri nu trebuie să introducă noi riscuri potențiale inacceptabile pentru siguranța aviației.

(b) Persoana menționată la punctul IS.AR.225 litera (a) și ceilalți membri vizați ai personalului autorității competente trebuie să fie informați de rezultatul evaluării riscurilor efectuate în conformitate cu punctul IS.AR.205, de scenariile de amenințare corespunzătoare și de măsurile care trebuie implementate.

Autoritatea competentă trebuie să informeze, de asemenea, organizațiile cu care are o interfață în conformitate cu punctul IS.AR.205 litera (b) cu privire la orice risc comun autorității competente și organizației în cauză.

IS.AR.215 Incidentele de securitate a informațiilor – detectare, răspuns și redresare

(a) În funcție de rezultatul evaluării riscurilor, efectuată în conformitate cu punctul IS.AR.205, și de rezultatul tratării riscurilor, efectuată în conformitate cu punctul IS.AR.210, autoritatea competentă trebuie să implementeze măsuri de detectare a evenimentelor care indică materializarea potențială a unor riscuri inacceptabile și care pot avea un impact potențial asupra siguranței aviației. Respectivele măsuri de detectare trebuie să permită autorității competente:

1. să identifice abaterile de la valorile de referință predeterminate ale performanței funcționale;

2. să declanșeze avertizări pentru activarea unor măsuri de răspuns adecvate, în cazul oricărei abateri.

(b) Autoritatea competentă trebuie să implementeze măsuri pentru a răspunde oricăror evenimente identificate în conformitate cu litera (a) care se pot transforma ori s-au transformat într-un incident de securitate a informațiilor. Respectivele măsuri de răspuns trebuie să permită autorității competente:

1. să declanșeze reacția propriei organizații la avertizările menționate la litera (a) subpunctul 2 prin activarea unor resurse și planuri de acțiune predefinite;

2. să limiteze răspândirea unui atac și să evite materializarea deplină a unui scenariu de amenințare;

3. să controleze modul de defectare al elementelor afectate definite la punctul IS.AR.205 litera (a).

(c) Autoritatea competentă trebuie să implementeze măsuri de redresare în urma incidentelor de securitate a informațiilor, inclusiv măsuri de urgență, dacă este necesar. Respectivele măsuri de redresare trebuie să permită autorității competente:

1. să elimine situația care a cauzat incidentul sau să o limiteze la un nivel tolerabil;

2. să restabilească starea de siguranță a elementelor afectate definite la punctul IS.AR.205 litera (a) în timpul de redresare definit în prealabil de propria organizație.

IS.AR.220 Subcontractarea activităților de management al securității informațiilor

Autoritatea competentă trebuie să se asigure, atunci când subcontractează altor organizații orice parte a activităților menționate la punctul IS.AR.200, că activitățile subcontractate respectă cerințele din prezentul regulament și că organizația subcontractată lucrează sub supravegherea sa. Autoritatea competentă trebuie să se asigure că riscurile asociate activităților subcontractate sunt gestionate în mod corespunzător.

IS.AR.225 Cerințele în materie de personal

Autoritatea competentă trebuie:

(a) să dispună de o persoană care are drepturile statutare necesare pentru a institui și a menține structurile organizaționale, politicile, procesele și procedurile necesare pentru punerea în aplicare a prezentului regulament.

Această persoană trebuie:

1. să aibă drepturile statutare pentru accesarea deplină a resurselor necesare pentru ca autoritatea competentă să îndeplinească toate sarcinile prevăzute în prezentul regulament;

2. să dețină delegarea de competențe necesară pentru îndeplinirea atribuțiilor primite;

(b) să dispună de o procedură prin care să se asigure că are suficient personal disponibil pentru desfășurarea activităților reglementate de prezenta anexă;

(c) să dispună de o procedură prin care să se asigure că personalul menționat la litera (b) are competența necesară pentru a-și îndeplini sarcinile;

(d) să dispună de o procedură prin care să se asigure că personalul este informat de responsabilitățile aferente rolurilor și sarcinilor atribuite;

(e) să se asigure că identitatea și fiabilitatea personalului care are acces la sistemele informatice și la datele care fac obiectul cerințelor prezentului regulament sunt stabilite în mod corespunzător.

IS.AR.230 Păstrarea evidențelor

(a) Autoritatea competentă trebuie să păstreze evidența activităților sale de management al securității informațiilor.

1. Autoritatea competentă trebuie să se asigure că următoarele evidențe sunt arhivate și trasabile:

(i) contractele pentru activitățile menționate la punctul IS.AR.200 litera (a) subpunctul 5;

(ii) evidențele proceselor-cheie menționate la punctul IS.AR.200 litera (d);

(iii) evidențele riscurilor identificate în evaluarea riscurilor menționată la punctul IS.AR.205, împreună cu măsurile conexe de tratare a riscurilor menționate la punctul IS.AR.210;

(iv) evidențele evenimentelor de securitate a informațiilor care ar putea necesita o reevaluare în vederea depistării unor incidente sau vulnerabilități nedetectate în materie de securitate a informațiilor.

2. Evidențele menționate la subpunctul 1 punctul (i) se păstrează timp de cel puțin cinci ani de la data la care contractul a fost modificat sau reziliat.

3. Evidențele menționate la subpunctul 1 punctele (ii) și (iii) se păstrează timp de cel puțin cinci ani.

4. Evidențele menționate la subpunctul 1 punctul (iv) se păstrează până la reevaluarea respectivelor evenimente de securitate a informațiilor, efectuată cu o periodicitate definită în cadrul unei proceduri instituite de autoritatea competentă.

(b) Autoritatea competentă trebuie să păstreze evidența calificărilor și a experienței personalului propriu implicat în activități de management al securității informațiilor.

1. Evidențele calificărilor și experienței personalului se păstrează atât timp cât persoana lucrează pentru autoritatea competentă și timp de cel puțin trei ani după ce persoana a părăsit autoritatea competentă.

2. Membrii personalului trebuie să primească, la cerere, acces la evidențele personale. În plus, la cererea membrilor personalului, autoritatea competentă trebuie să le furnizeze acestora, la părăsirea autorității competente, o copie a evidențelor personale.

(c) Formatul evidențelor se specifică în procedurile autorității competente.

(d) Evidențele se stochează astfel încât să fie protejate împotriva deteriorării, alterării și furtului, informațiile fiind identificate, după caz, conform nivelului lor de clasificare de securitate. Autoritatea competentă trebuie să se asigure că evidențele sunt stocate prin mijloace care să asigure integritatea, autenticitatea și accesul autorizat.

IS.AR.235 Îmbunătățirea continuă

(a) Autoritatea competentă trebuie să evalueze, cu ajutorul unor indicatori de performanță adecvați, eficacitatea și maturitatea propriului SMSI. Evaluarea trebuie efectuată pe baza unui calendar predefinit, stabilit de autoritatea competentă, sau în urma unui incident de securitate a informațiilor.

(b) Dacă în urma evaluării efectuate în conformitate cu litera (a) se constată deficiențe, autoritatea competentă trebuie să ia măsurile de îmbunătățire necesare pentru a se asigura că SMSI-ul continuă să respecte cerințele aplicabile și că el menține riscurile în materie de securitate a informațiilor la un nivel acceptabil. În plus, autoritatea competentă trebuie să reevalueze elementele SMSI-ului vizate de măsurile adoptate.

ANEXA II

SECURITATEA INFORMAȚIILOR – CERINȚE APLICABILE ORGANIZAȚIILOR

[PARTEA IS.I.OR]

IS.I.OR.100 Domeniul de aplicare

Prezenta parte stabilește cerințele care trebuie îndeplinite de organizațiile menționate la articolul 2 alineatul (1) din prezentul regulament.

IS.I.OR.200 Sistemul de management al securității informațiilor (SMSI)

(a) Pentru a atinge obiectivele prevăzute la articolul 1, organizația trebuie să instituie, să implementeze și să mențină un sistem de management al securității informațiilor (SMSI) care asigură faptul că organizația:

1. instituie o politică de securitate a informațiilor în care sunt prevăzute principiile generale ale organizației în ceea ce privește impactul potențial al riscurilor în materie de securitate a informațiilor asupra siguranței aviației;
2. identifică și examinează riscurile în materie de securitate a informațiilor în conformitate cu punctul IS.I.OR.205;
3. definește și implementează măsurile de tratare a riscurilor în materie de securitate a informațiilor în conformitate cu punctul IS.I.OR.210;
4. implementează un sistem de raportare internă în materie de securitate a informațiilor în conformitate cu punctul IS.I.OR.215;
5. definește și implementează, în conformitate cu punctul IS.I.OR.220, măsurile necesare pentru detectarea evenimentelor de securitate a informațiilor, le identifică pe cele care sunt considerate incidente cu impact potențial asupra siguranței aviației, cu excepția cazurilor permise conform punctului IS.I.OR.205 litera (e), asigură un răspuns la respectivele incidentele de securitate a informațiilor și se redresează în urma acestora;

6. implementează măsurile care au fost notificate de autoritatea competentă ca reacție imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației;

7. ia măsurile corespunzătoare, în conformitate cu punctul IS.I.OR.225, pentru abordarea constatărilor notificate de autoritatea competentă;

8. implementează un sistem de raportare externă în conformitate cu punctul IS.I.OR.230, astfel încât autoritatea competentă să poată lua măsuri corespunzătoare;

9. îndeplinește cerințele de la punctul IS.I.OR.235 când subcontractează altor organizații orice parte a activităților menționate la punctul IS.I.OR.200;

10. îndeplinește cerințele în materie de personal stabilite la punctul IS.I.OR.240;

11. îndeplinește cerințele de păstrare a evidențelor stabilite la punctul IS.I.OR.245;

12. monitorizează îndeplinirea de către organizație a cerințelor din prezentul regulament și transmite managerului responsabil feedback cu privire la constatări, pentru a asigura implementarea efectivă a măsurilor corective;

13. protejează, fără a aduce atingere cerințelor aplicabile în materie de raportare a incidentelor, confidențialitatea oricăror informații pe care organizația le-ar fi putut primi de la alte organizații, în funcție de nivelul de sensibilitate a informațiilor respective.

(b) Pentru a îndeplini în permanență cerințele menționate la articolul 1, organizația trebuie să implementeze un proces de îmbunătățire continuă în conformitate cu punctul IS.I.OR.260.

(c) Organizația trebuie să documenteze, în conformitate cu punctul IS.I.OR.250, toate procesele, procedurile, rolurile și responsabilitățile cheie necesare pentru a se conforma punctului IS.I.OR.200 litera (a) și să instituie un proces de modificare a documentației respective. Modificările aduse respectivelor procese, proceduri, roluri și responsabilități se gestionează în conformitate cu punctul IS.I.OR.255.

(d) Procesele, procedurile, rolurile și responsabilitățile instituite de organizație pentru a se conforma punctului IS.I.OR.200 litera (a) trebuie să corespundă naturii și complexității activităților sale, pe baza unei evaluări a riscurilor în materie de securitate a informațiilor inerente activităților respective, și pot fi integrate în alte sisteme de management existente care sunt deja implementate de organizație.

(e) Fără a se aduce atingere obligației de conformitate cu cerințele de raportare stabilite în Regulamentul (UE) nr. 376/2014 și cu cerințele stabilite la punctul IS.I.OR.200 litera (a) subpunctul 13, organizația poate primi din partea autorității competente aprobarea de a nu implementa cerințele menționate la literele (a)-(d) și cerințele aferente de la punctele IS.I.OR.205-IS.I.OR.260 dacă demonstrează într-un mod considerat satisfăcător de autoritatea respectivă că activitățile, instalațiile și resursele sale, precum și serviciile pe care le operează, furnizează, primește și menține nu prezintă niciun risc în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației pentru organizația în sine sau pentru alte organizații. Aprobarea trebuie să se bazeze pe o evaluare documentată a riscurilor în materie de securitate a informațiilor, efectuată de organizație sau de o parte terță în conformitate cu punctul IS.I.OR.205 și examinată și aprobată de autoritatea sa competentă.

Menținerea valabilității respectivei aprobări va fi examinată de autoritatea competentă în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.

IS.I.OR.205 Evaluarea riscurilor în materie de securitate a informațiilor

(a) Organizația trebuie să identifice toate elementele sale care ar putea fi expuse unor riscuri în materie de securitate a informațiilor. Acestea trebuie să includă:

1. activitățile, instalațiile și resursele organizației, precum și serviciile pe care le operează, furnizează, primește sau menține organizația;

2. echipamentele, sistemele, datele și informațiile care contribuie la funcționarea elementelor enumerate la subpunctul 1.

(b) Organizația trebuie să identifice interfețele pe care le are cu alte organizații și care ar putea conduce la expunerea reciprocă la riscuri în materie de securitate a informațiilor.

(c) În ceea ce privește elementele și interfețele menționate la literele (a) și (b), organizația trebuie să identifice riscurile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației. Pentru fiecare risc identificat, organizația trebuie:

1. să atribuie un nivel de risc în conformitate cu o clasificare predefinită stabilită de organizație;

2. să asocieze fiecare risc și nivelul său aferent cu elementul sau interfața corespunzătoare identificată în conformitate cu literele (a) și (b).

Clasificarea predefinită menționată la subpunctul 1 trebuie să țină seama de potențialul de producere a scenariului de amenințare și de gravitatea consecințelor acestuia asupra siguranței. Pe baza acestei clasificări și în funcție de existența sau absența, în cadrul organizației, a unui proces structurat și repetabil de management al riscurilor pentru operațiuni, organizația trebuie să fie în măsură să stabilească dacă riscul este acceptabil sau dacă trebuie tratat în conformitate cu punctul IS.I.OR.210.

Pentru a se facilita comparabilitatea reciprocă a evaluărilor riscurilor, la atribuirea nivelului de risc în temeiul subpunctului 1 se ține seama de informațiile relevante obținute în coordonare cu organizațiile menționate la litera (b).

(d) Organizația trebuie să revizuiască și să actualizeze evaluarea riscurilor efectuată în conformitate cu literele (a), (b) și, după caz, (c) sau (e) în oricare dintre următoarele situații:

1. când există o modificare a elementelor expuse unor riscuri în materie de securitate a informațiilor;

2. când există o modificare a interfețelor dintre organizație și alte organizații sau o modificare a riscurilor comunicate de celelalte organizații;

3. când există o modificare a informațiilor sau a cunoștințelor utilizate pentru identificarea, analizarea și clasificarea riscurilor;

4. când analiza incidentelor de securitate a informațiilor a permis desprinderea de învățăminte.

(e) Prin derogare de la litera (c), organizațiile care trebuie să respecte subpartea C din anexa III (partea ATM/ANS.OR) la Regulamentul de punere în aplicare (UE) 2017/373 înlocuiesc analiza impactului asupra siguranței aviației cu o analiză a impactului asupra serviciilor lor, în conformitate cu evaluarea în sprijinul siguranței prevăzută la punctul ATM/ANS.OR.C.005. Această evaluare în sprijinul siguranței se pune la dispoziția furnizorilor de servicii de trafic aerian cărora organizațiile le furnizează servicii, iar respectivii furnizori de servicii de trafic aerian sunt responsabili cu evaluarea impactului asupra siguranței aviației.

IS.I.OR.210 Tratarea riscurilor în materie de securitate a informațiilor

(a) Organizația trebuie să elaboreze măsuri de abordare a riscurilor inacceptabile identificate în conformitate cu punctul IS.I.OR.205, să le implementeze în timp util și să verifice menținerea eficacității acestora. Respectivele măsuri trebuie să permită organizației:

1. să controleze circumstanțele care contribuie la apariția efectivă a scenariului de amenințare;

2. să diminueze consecințele asupra siguranței aviației care sunt asociate materializării scenariului de amenințare;

3. să evite riscurile.

Respectivele măsuri nu trebuie să introducă noi riscuri potențiale inacceptabile pentru siguranța aviației.

(b) Persoana menționată la punctul IS.I.OR.240 literele (a) și (b) și ceilalți membri vizați ai personalului organizației trebuie să fie informați de rezultatul evaluării riscurilor efectuate în conformitate cu punctul IS.I.OR.205, de scenariile de amenințare corespunzătoare și de măsurile care trebuie implementate.

Organizația trebuie să informeze, de asemenea, organizațiile cu care are o interfață în conformitate cu punctul IS.I.OR.205 litera (b) cu privire la orice risc comun celor două organizații.

IS.I.OR.215 Sistemul de raportare internă în materie de securitate a informațiilor

(a) Organizația trebuie să instituie un sistem de raportare internă pentru a permite colectarea și evaluarea evenimentelor legate de securitatea informațiilor, inclusiv a celor care trebuie raportate în temeiul punctului IS.I.OR.230.

(b) Sistemul respectiv și procesul menționat la punctul IS.I.OR.220 trebuie să permită organizației:

1. să identifice care dintre evenimentele raportate în temeiul literei (a) sunt considerate incidente de securitate a informațiilor sau vulnerabilități cu impact potențial asupra siguranței aviației;

2. să identifice cauzele și factorii determinanți ai incidentelor de securitate a informațiilor și vulnerabilitățile identificate în conformitate cu subpunctul 1 și să le abordeze în cadrul procesului de management al riscurilor în materie de securitate a informațiilor în conformitate cu punctele IS.I.OR.205 și IS.I.OR.220;

3. să asigure o evaluare a tuturor informațiilor cunoscute și relevante legate de incidentele de securitate a informațiilor și vulnerabilitățile identificate în conformitate cu subpunctul 1;

4. să asigure implementarea unei metode de distribuire internă a informațiilor, după caz.

(c) Orice organizație subcontractată care ar putea expune organizația la riscuri în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației are obligația de a raporta organizației evenimentele de securitate a informațiilor. Rapoartele respective se transmit prin procedurile stabilite în angajamentele contractuale specifice și se evaluează în conformitate cu litera (b).

(d) Organizația trebuie să coopereze în cadrul investigațiilor cu orice altă organizație care are o contribuție semnificativă la securitatea informațiilor în cadrul propriilor sale activități.

(e) Organizația poate integra sistemul de raportare respectiv în alte sisteme de raportare pe care le-a implementat deja.

IS.I.OR.220 Incidentele de securitate a informațiilor – detectare, răspuns și redresare

(a) În funcție de rezultatul evaluării riscurilor, efectuată în conformitate cu punctul IS.I.OR.205, și de rezultatul tratării riscurilor, efectuată în conformitate cu punctul IS.I.OR.210, organizația trebuie să implementeze măsuri de detectare a incidentelor și vulnerabilităților care să indice materializarea potențială a unor riscuri inacceptabile și care pot avea un impact potențial asupra siguranței aviației. Respectivele măsuri de detectare trebuie să permită organizației:

1. să identifice abaterile de la valorile de referință predeterminate ale performanței funcționale;

2. să declanșeze avertizări pentru activarea unor măsuri de răspuns adecvate, în cazul oricărei abateri.

(b) Organizația trebuie să implementeze măsuri pentru a răspunde oricăror evenimente identificate în conformitate cu litera (a) care se pot transforma ori s-au transformat într-un incident de securitate a informațiilor. Respectivele măsuri de răspuns trebuie să permită organizației:

1. să declanșeze reacția la avertizările menționate la litera (a) subpunctul 2 prin activarea unor resurse și planuri de acțiune predefinite;

2. să limiteze răspândirea unui atac și să evite materializarea deplină a unui scenariu de amenințare;

3. să controleze modul de defectare al elementelor afectate definite la punctul IS.I.OR.205 litera (a).

(c) Organizația trebuie să implementeze măsuri de redresare în urma incidentelor de securitate a informațiilor, inclusiv măsuri de urgență, dacă este necesar. Respectivele măsuri de redresare trebuie să permită organizației:

1. să elimine situația care a cauzat incidentul sau să o limiteze la un nivel tolerabil;

2. să asigure atingerea unei stări de siguranță a elementelor afectate definite la punctul IS.I.OR.205 litera (a) în timpul de redresare definit în prealabil de organizație.

IS.I.OR.225 Răspunsul la constatările notificate de autoritatea competentă

(a) După primirea notificării constatărilor de la autoritatea competentă, organizația trebuie:

1. să identifice atât cauza sau cauzele profunde ale apariției neconformității, cât și factorii care contribuie la aceasta;

2. să definească un plan de acțiuni corective;

3. să demonstreze corectarea neconformității într-un mod considerat satisfăcător de către autoritatea competentă.

(b) Acțiunile menționate la litera (a) trebuie întreprinse în termenul convenit cu autoritatea competentă.

IS.I.OR.230 Sistemul de raportare externă în materie de securitate a informațiilor

(a) Organizația trebuie să implementeze un sistem de raportare în materie de securitate a informațiilor care să fie conform cu cerințele stabilite în Regulamentul (UE) nr. 376/2014 și în actele delegate și de punere în aplicare ale acestuia, dacă regulamentul respectiv îi este aplicabil.

(b) Fără a aduce atingere obligațiilor prevăzute în Regulamentul (UE) nr. 376/2014, organizația trebuie să se asigure că orice incident sau vulnerabilitate în materie de securitate a informațiilor care poate reprezenta un risc semnificativ pentru siguranța aviației este raportată autorității sale competente. În plus:

1. atunci când un astfel de incident sau o astfel de vulnerabilitate afectează o aeronavă ori un sistem sau o componentă asociată, organizația trebuie să raporteze acest lucru și titularului aprobării de proiect;

2. atunci când un astfel de incident sau o astfel de vulnerabilitate afectează un sistem sau element constitutiv utilizat de organizație, ea trebuie să raporteze acest lucru organizației responsabile cu proiectarea sistemului sau a elementului constitutiv.

(c) Organizația trebuie să raporteze situațiile menționate la litera (b) după cum urmează:

1. se transmite o notificare autorității competente și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv, de îndată ce organizația ia cunoștință de situație;

2. se transmite un raport autorității competente și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv, cât mai curând posibil, însă fără a depăși 72 de ore de la momentul în care organizația a luat cunoștință de situație, în afara cazului în care circumstanțe excepționale împiedică acest lucru.

   Raportul se întocmește în forma definită de autoritatea competentă și trebuie să conțină toate informațiile relevante despre situația de care a luat cunoștință organizația;

3. se transmite autorității competente și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv un raport de urmărire în care se oferă detalii privind acțiunile întreprinse sau pe care organizația intenționează să le întreprindă în urma incidentului, precum și privind acțiunile pe care organizația intenționează să le întreprindă pentru a preveni, în viitor, producerea unor incidente similare de securitate a informațiilor.

   Raportul de urmărire se transmite de îndată ce au fost identificate respectivele acțiuni și se întocmește în forma definită de autoritatea competentă.

IS.I.OR.235 Subcontractarea activităților de management al securității informațiilor

(a) Organizația trebuie să se asigure că, atunci când subcontractează altor organizații orice parte a activităților menționate la punctul IS.I.OR.200, activitățile subcontractate respectă cerințele din prezentul regulament și că organizația subcontractată lucrează sub supravegherea sa. Organizația trebuie să se asigure că riscurile asociate activităților subcontractate sunt gestionate în mod corespunzător.

(b) Organizația trebuie să se asigure că autoritatea competentă poate avea acces, la cerere, la organizația subcontractată, pentru a determina menținerea conformității cu cerințele aplicabile stabilite în prezentul regulament.

IS.I.OR.240 Cerințele în materie de personal

(a) Managerul responsabil, desemnat în conformitate cu Regulamentele (UE) nr. 1321/2014, (UE) nr. 965/2012, (UE) nr. 1178/2011, (UE) 2015/340, cu Regulamentul de punere în aplicare (UE) 2017/373 sau cu Regulamentul de punere în aplicare (UE) 2021/664, după caz, al organizației menționate la articolul 2 alineatul (1) din prezentul regulament trebuie să aibă drepturile statutare necesare pentru a se asigura că toate activitățile prevăzute în prezentul regulament pot fi finanțate și efectuate. Persoana respectivă trebuie:

1. să se asigure că sunt disponibile toate resursele necesare pentru a se asigura conformitatea cu cerințele prezentului regulament;

2. să stabilească și să promoveze politica de securitate a informațiilor menționată la punctul IS.I.OR.200 litera (a) subpunctul 1;

3. să demonstreze că are o înțelegere de bază a prezentului regulament.

(b) Managerul responsabil trebuie să numească o persoană sau un grup de persoane pentru a se asigura că organizația respectă cerințele prezentului regulament și trebuie să definească nivelul de autoritate al acestora. Persoana sau grupul de persoane au obligația să raporteze direct managerului responsabil și trebuie să dețină pregătirea, cunoștințele și experiența necesare îndeplinirii responsabilităților asumate. În cadrul procedurilor trebuie să se stabilească cine suplinește o anumită persoană în cazul unei absențe îndelungate a persoanei respective.

(c) Managerul responsabil trebuie să însărcineze o persoană sau un grup de persoane cu responsabilitatea de a gestiona funcția de monitorizare a conformității menționată la punctul IS.I.OR.200 litera (a) subpunctul 12.

(d) Atunci când organizația partajează structuri organizaționale, politici, procese și proceduri în materie de securitate a informațiilor cu alte organizații sau cu domenii ale propriei organizații care nu fac parte din aprobare sau din declarație, managerul responsabil își poate delega activitățile unei persoane responsabile comune.

Într-un astfel de caz, se stabilesc măsuri de coordonare între managerul responsabil al organizației și persoana responsabilă comună pentru a se asigura integrarea adecvată a managementului securității informațiilor în cadrul organizației.

(e) Managerul responsabil sau persoana responsabilă comună menționată la litera (d) trebuie să aibă drepturile statutare necesare pentru a institui și menține structurile organizaționale, politicile, procesele și procedurile necesare pentru implementarea punctului IS.I.OR.200.

(f) Organizația trebuie să dispună de o procedură prin care să se asigure că are suficient personal disponibil pentru îndeplinirea activităților reglementate de prezenta anexă.

(g) Organizația trebuie să dispună de o procedură prin care să se asigure că personalul menționat la litera (f) are competența necesară pentru a-și îndeplini sarcinile.

(h) Organizația trebuie să dispună de o procedură prin care să se asigure că personalul este informat de responsabilitățile aferente rolurilor și sarcinilor atribuite.

(i) Organizația trebuie să se asigure că identitatea și fiabilitatea personalului care are acces la sistemele informatice și la datele care fac obiectul cerințelor prezentului regulament sunt stabilite în mod corespunzător.

IS.I.OR.245 Păstrarea evidențelor

(a) *Organizația trebuie să păstreze evidența activităților sale de management al securității informațiilor.*

1. Organizația trebuie să se asigure că următoarele evidențe sunt arhivate și trasabile:

(i) orice aprobare primită și orice evaluare conexă a riscurilor în materie de securitate a informațiilor în conformitate cu punctul IS.I.OR.200 litera (e);

(ii) contractele pentru activitățile menționate la punctul IS.I.OR.200 litera (a) subpunctul 9;

(iii) evidențele proceselor-cheie menționate la punctul IS.I.OR.200 litera (d);

(iv) evidențele riscurilor identificate în evaluarea riscurilor menționată la punctul IS.I.OR.205, împreună cu măsurile conexe de tratare a riscurilor menționate la punctul IS.I.OR.210;

(v) evidențele incidentelor și vulnerabilităților în materie de securitate a informațiilor raportate în conformitate cu sistemele de raportare menționate la punctele IS.I.OR.215 și IS.I.OR.230;

(vi) evidențele evenimentelor de securitate a informațiilor care ar putea necesita o reevaluare în vederea depistării unor incidente sau vulnerabilități nedetectate în materie de securitate a informațiilor.

2. Evidențele menționate la subpunctul 1 punctul (i) se păstrează timp de cel puțin cinci ani de la data la care aprobarea și-a pierdut valabilitatea.

3. Evidențele menționate la subpunctul 1 punctul (ii) se păstrează timp de cel puțin cinci ani de la data la care contractul a fost modificat sau reziliat.

4. Evidențele menționate la subpunctul 1 punctele (iii), (iv) și (v) se păstrează timp de cel puțin cinci ani.

5. Evidențele menționate la subpunctul 1 punctul (vi) se păstrează până la reevaluarea respectivelor evenimente de securitate a informațiilor, efectuată cu o periodicitate definită în cadrul unei proceduri instituite de organizație.

(b) *Organizația trebuie să păstreze evidența calificărilor și a experienței personalului propriu implicat în activități de management al securității informațiilor.*

1. Evidențele calificărilor și experienței personalului se păstrează atât timp cât persoana lucrează pentru organizație și timp de cel puțin trei ani după ce persoana a părăsit organizația.

2. Membrii personalului trebuie să primească, la cerere, acces la evidențele personale. În plus, la cererea membrilor personalului, organizația trebuie să le furnizeze acestora, la părăsirea organizației, o copie a evidențelor personale.

(c) Formatul evidențelor se specifică în procedurile organizației.

(d) Evidențele se stochează astfel încât să fie protejate împotriva deteriorării, alterării și furtului, informațiile fiind identificate, după caz, conform nivelului lor de clasificare de securitate. Organizația trebuie să se asigure că evidențele sunt stocate prin mijloace care să asigure integritatea, autenticitatea și accesul autorizat.

IS.I.OR.250 Manualul de management al securității informațiilor (MMSI)

(a) Organizația trebuie să pună la dispoziția autorității competente un manual de management al securității informațiilor (MMSI) și, când este cazul, eventualele manuale și proceduri conexe la care se face trimitere în manualul respectiv, conținând:

1. o declarație semnată de managerul responsabil prin care se confirmă că organizația își va desfășura în permanență activitatea în conformitate cu prezenta anexă și cu MMSI. Dacă managerul responsabil nu este directorul general al organizației, declarația trebuie să fie contrasemnată de directorul general;

2. funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanei sau persoanelor definite la punctul IS.I.OR.240 literele (b) și (c);

3. funcția, numele, atribuțiile, răspunderile, responsabilitățile și competența persoanei responsabile comune definite la punctul IS.I.OR.240 litera (d), dacă este cazul;

4. politica de securitate a informațiilor instituită de organizație, astfel cum este menționată la punctul IS.I.OR.200 litera (a) subpunctul 1;

5. o descriere generală a resurselor umane, din punctul de vedere al efectivelor și categoriilor, precum și a sistemului instituit pentru planificarea disponibilității personalului, astfel cum se prevede la punctul IS.I.OR.240;

6. funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanelor-cheie responsabile cu implementarea punctului IS.I.OR.200, inclusiv ale persoanei sau persoanelor responsabile cu funcția de monitorizare a conformității, menționată la punctul IS.I.OR.200 litera (a) subpunctul 12;

7. o organigramă ilustrând liniile ierarhice conexe în materie de răspundere și responsabilitate pentru persoanele menționate la subpunctele 2 și 6;

8. descrierea sistemului de raportare internă menționat la punctul IS.I.OR.215;

9. procedurile în care se specifică modul în care organizația asigură conformitatea cu prezenta parte, în particular:

   (i) documentația menționată la punctul IS.I.OR.200 litera (c);

   (ii) procedurile care definesc modul în care organizația controlează eventualele activități subcontractate, astfel cum se menționează la punctul IS.I.OR.200 litera (a) subpunctul 9;

   (iii) procedura de modificare a MMSI-ului, menționată la litera (c);

10. informații detaliate referitoare la mijloace de conformare alternative aprobate în prezent.

(b) Ediția inițială a MMSI-ului trebuie să fie aprobată, iar o copie trebuie să fie păstrată de autoritatea competentă. MMSI-ul trebuie modificat în funcție de necesități, astfel încât să reprezinte o descriere actualizată a SMSI-ului organizației. O copie a oricăror modificări aduse MMSI-ului trebuie transmisă autorității competente.

(c) Modificările aduse MMSI-ului se gestionează în cadrul unei proceduri instituite de organizație. Orice modificare care nu este acoperită de domeniul de aplicare al acestei proceduri și orice modificare legată de modificările menționate la punctul IS.I.OR.255 litera (b) trebuie să fie aprobată de autoritatea competentă.

(d) Organizația poate integra MMSI-ul în alte specificații sau manuale de management pe care le deține, cu condiția să existe o referință încrucișată clară indicând părțile din specificațiile sau manualul de management care corespund diferitelor cerințe cuprinse în prezenta anexă.

IS.I.OR.255 Modificări ale sistemului de management al securității informațiilor

(a) Modificările aduse SMSI-ului pot fi gestionate și notificate autorității competente în cadrul unei proceduri elaborate de organizație. Procedura respectivă trebuie să fie aprobată de autoritatea competentă.

(b) În ceea ce privește modificările SMSI-ului care nu fac obiectul procedurii menționate la litera (a), organizația trebuie să solicite și să obțină o aprobare din partea autorității competente.

În ceea ce privește respectivele modificări:

1. cererea se depune înainte să intervină modificarea respectivă, pentru a i se permite autorității competente să stabilească continuitatea conformității cu prezentul regulament și să modifice, dacă este necesar, certificatul organizației și condițiile de aprobare anexate acestuia;

2. organizația trebuie să pună la dispoziția autorității competente toate informațiile solicitate pentru evaluarea modificării;

3. modificarea se implementează numai după primirea unei aprobări oficiale din partea autorității competente;

4. organizația trebuie să își desfășoare activitatea în condițiile stabilite de autoritatea competentă în timpul implementării modificărilor respective.

IS.I.OR.260 Îmbunătățirea continuă

(a) Organizația trebuie să evalueze, cu ajutorul unor indicatori de performanță adecvați, eficacitatea și maturitatea SMSI-ului. Respectiva evaluare trebuie efectuată pe baza unui calendar predefinit de organizație sau în urma unui incident de securitate a informațiilor.

(b) Dacă în urma evaluării efectuate în conformitate cu litera (a) se constată deficiențe, organizația trebuie să ia măsurile de îmbunătățire necesare pentru a se asigura că SMSI-ul continuă să respecte cerințele aplicabile și că el menține riscurile în materie de securitate a informațiilor la un nivel acceptabil. În plus, organizația trebuie să reevalueze elementele SMSI vizate de măsurile adoptate.

ANEXA III

Anexele VI (partea ARA) și VII (partea ORA) la Regulamentul (UE) nr. 1178/2011 se modifică după cum urmează:

1. Anexa VI (partea ARA) se modifică după cum urmează:

(a) la punctul ARA.GEN.125 se adaugă următoarea literă (c):

„(c) Autoritatea competentă a statului membru furnizează agenției cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul punctului IS.I.OR.230 din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203”;

(b) după punctul ARA.GEN.135 se introduce punctul ARA.GEN.135A cu următorul text:

„**ARA.GEN.135A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) Autoritatea competentă implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul ARA.GEN.125 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare.

(c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.”;

(c) la punctul ARA.GEN.200 se adaugă litera (e) cu următorul text:

„(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;

(d) punctul ARA.GEN.205 se modifică după cum urmează:

(i) titlul se înlocuiește cu următorul text:

„**ARA.GEN.205 Atribuirea de sarcini**”;

(ii) se adaugă litera (c) cu următorul text:

„(c) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ORA.GEN.200A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu punctul ARA.GEN.200 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.";

(e) la punctul ARA.GEN.300 se adaugă litera (g) cu următorul text:

„(g) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ORA.GEN.200A, în plus față de respectarea dispozițiilor de la literele (a)-(f), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.";

(f) după punctul ARA.GEN.330 se introduce punctul ARA.GEN.330A cu următorul text:

„**ARA.GEN.330A Modificări ale sistemului de management al securității informațiilor**

(a) În ceea ce privește modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul ARA.GEN.300. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul ARA.GEN.350.

(b) În ceea ce privește alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203:

1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea."

2. Anexa VII (partea ORA) se modifică după cum urmează:

După punctul ORA.GEN.200 se introduce punctul ORA.GEN.200A cu următorul text:

„**ORA.GEN.200A Sistemul de management al securității informațiilor**

Pe lângă sistemul de management menționat la punctul ORA.GEN.200, organizația instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației."

ANEXA IV

Anexa I (partea 21) la Regulamentul (UE) nr. 748/2012 se modifică după cum urmează:

1. Cuprinsul se modifică după cum urmează:

   (a) după titlul 21.B.20 se introduce următorul titlu:

   „21.B.20A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației";

   (b) titlul punctului 21.B.30 se înlocuiește cu următorul text:

   „21.B.30 Atribuirea de sarcini";

   (c) după titlul 21.B.240 se introduce următorul titlu:

   „21.B.240A Modificări ale sistemului de management al securității informațiilor";

   (d) după titlul 21.B.435 se introduce următorul titlu:

   „21.B.435A Modificări ale sistemului de management al securității informațiilor".

2. La punctul 21.B.15 se adaugă litera (c) cu următorul text:

   „(c) Autoritatea competentă a statului membru furnizează agenției cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul punctului IS.D.OR.230 din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645."

3. După punctul 21.B.20 se introduce punctul 21.B.20A cu următorul text:

   „**21.B.20A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

   (a) Autoritatea competentă implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

   (b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul 21.B.15 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare.

   (c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

   (d) Măsurile luate în conformitate cu litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate."

4. La punctul 21.B.25 se adaugă litera (e) cu următorul text:

   „(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației."

5. Punctul 21.B.30 se modifică după cum urmează:

(a) titlul se înlocuiește cu următorul text:

„21.B.30 Atribuirea de sarcini";

(b) se adaugă litera (c) cu următorul text:

„(c) Pentru certificarea și supravegherea conformității organizației cu punctele 21.A.139A și 21.A.239A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu punctul 21.B.25 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său."

6. La punctul 21.B.221 se adaugă litera (g) cu următorul text:

„(g) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul 21.A.139A, în plus față de respectarea dispozițiilor de la literele (a)-(f), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației."

7. După punctul 21.B.240 se introduce punctul 21.B.240A cu următorul text:

„**21.B.240A Modificări ale sistemului de management al securității informațiilor**

(a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.D.OR.255 litera (a) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645, autoritatea competentă include examinarea acestor modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul 21.B.221. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul 21.B.225.

(b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.D.OR.255 litera (b) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645:

1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea."

8. La punctul 21.B.431 se adaugă litera (d) cu următorul text:

„(d) Pentru certificarea și supravegherea conformității organizației cu punctul 21.A.239A, în plus față de respectarea dispozițiilor de la literele (a)-(c), autoritatea competentă respectă următoarele principii:

1. autoritatea competentă examinează interfețele și riscurile asociate identificate în conformitate cu punctul IS.D.OR.205 litera (b) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645 de fiecare organizație care face obiectul supravegherii sale;

2. dacă se constată discrepanțe în interfețele reciproce și riscurile asociate identificate de diferite organizații, autoritatea competentă le examinează împreună cu organizațiile vizate și, dacă este necesar, formulează constatări corespunzătoare pentru a asigura implementarea de măsuri corective;

3. dacă din examinarea documentației, efectuată în temeiul subpunctului 2, reiese că există riscuri semnificative asociate interfețelor cu organizații supravegheate de altă autoritate competentă din același stat membru, aceste informații se comunică autorității competente corespunzătoare."

9. După punctul 21.B.435 se introduce punctul 21.B.435A cu următorul text:

„**21.B.435A Modificări ale sistemului de management al securității informațiilor**

(a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.D.OR.255 litera (a) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645, autoritatea competentă include examinarea acestor modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul 21.B.431. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul 21.B.433.

(b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.D.OR.255 litera (b) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645:

1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea."

ANEXA V

Anexele II (partea ARO) și III (partea ORO) la Regulamentul (UE) nr. 965/2012 se modifică după cum urmează:

1. Anexa II (partea ARO) se modifică după cum urmează:

(a) la punctul ARO.GEN.125 se adaugă litera (c) cu următorul text:

„(c) Autoritatea competentă a statului membru furnizează agenției cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul punctului IS.I.OR.230 din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203.";

(b) după punctul ARO.GEN.135 se introduce punctul ARO.GEN.135A cu următorul text:

„**ARO.GEN.135A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) Autoritatea competentă implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul ARO.GEN.125 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare.

(c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.";

(c) la punctul ARO.GEN.200 se adaugă litera (e) cu următorul text:

„(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.";

(d) punctul ARO.GEN.205 se modifică după cum urmează:

(i) titlul se înlocuiește cu următorul text:

„**ARO.GEN.205 Atribuirea de sarcini**";

(ii) se adaugă litera (c) cu următorul text:

„(c) Pentru certificarea și supravegherea conformității organizației cu punctul ORO.GEN.200A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu punctul ARO.GEN.200 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.";

(e) la punctul ARO.GEN.300 se adaugă litera (g) cu următorul text:

„(g) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ORO.GEN.200A, în plus față de respectarea dispozițiilor de la literele (a)-(f), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.";

(f) după punctul ARO.GEN.330 se introduce punctul ARO.GEN.330A cu următorul text:

„**ARO.GEN.330A Modificări ale sistemului de management al securității informațiilor**

(a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul ARO.GEN.300. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul ARO.GEN.350.

(b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203:

1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea."

2. Anexa III (partea ORO) se modifică după cum urmează:

După punctul ORO.GEN.200 se introduce punctul ORO.GEN.200A cu următorul text:

„**ORO.GEN.200A Sistemul de management al securității informațiilor**

Pe lângă sistemul de management menționat la punctul ORO.GEN.200, operatorul instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației."

ANEXA VI

Anexa II (partea ADR.AR) la Regulamentul (UE) nr. 139/2014 se modifică după cum urmează:

1. La punctul ADR.AR.A.025 se adaugă litera (c) cu următorul text:

„(c) Autoritatea competentă a statului membru furnizează agenției cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul punctului IS.D.OR.230 din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645."

2. După punctul ADR.AR.A.030 se introduce punctul ADR.AR.A.030A cu următorul text:

„**ADR.AR.A.030A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) Autoritatea competentă implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul ADR.AR.A.025 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare.

(c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate."

3. La punctul ADR.AR.B.005 se adaugă litera (d) cu următorul text:

„(d) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației."

4. Punctul ADR.AR.B.010 se modifică după cum urmează:

(i) titlul se înlocuiește cu următorul text:

„**ADR.AR.B.010 Atribuirea de sarcini**";

(ii) se adaugă litera (c) cu următorul text:

„(c) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ADR.OR.D.005A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu punctul ADR.AR.B.005 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său."

5. La punctul ADR.AR.C.005 se adaugă litera (f) cu următorul text:

„(f) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ADR.OR.D.005A, în plus față de respectarea dispozițiilor de la literele (a)-(e), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației."

6. După punctul ADR.AR.C.040 se introduce punctul ADR.AR.C.040A cu următorul text:

„**ADR.AR.C.040A Modificări ale sistemului de management al securității informațiilor**

(a) În ceea ce privește modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.D.OR.255 litera (a) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645, autoritatea competentă include examinarea acestor modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul ADR.AR.C.005. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul ADR.AR.C.055.

(b) În privința altor modificări care necesită o cerere de aprobare în conformitate cu punctul IS.D.OR.255 litera (b) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645:

1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea."

ANEXA VII

Anexele II (partea 145), III (partea 66) și Vc (partea CAMO) la Regulamentul (UE) nr. 1321/2014 se modifică după cum urmează:

1. Anexa II (partea 145) se modifică după cum urmează:

(a) cuprinsul se modifică după cum urmează:

(i) după titlul 145.A.200 se introduce următorul titlu:

„145.A.200A Sistemul de management al securității informațiilor";

(ii) după titlul 145.B.135 se introduce următorul titlu:

„145.B.135A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației";

(iii) titlul punctului 145.B.205 se înlocuiește cu următorul text:

„145.B.205 Atribuirea de sarcini";

(iv) după titlul 145.B.330 se introduce următorul titlu:

„145.B.330A Modificări ale sistemului de management al securității informațiilor";

(b) după punctul 145.A.200 se introduce punctul 145.A.200A cu următorul text:

„145.A.200A **Sistemul de management al securității informațiilor**

Pe lângă sistemul de management menționat la punctul 145.A.200, organizația de întreținere instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.";

(c) la punctul 145.B.125 se adaugă litera (c) cu următorul text:

„(c) Autoritatea competentă a statului membru furnizează agenției cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul punctului IS.I.OR.230 din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203.";

(d) după punctul 145.B.135 se introduce punctul 145.B.135A cu următorul text:

„145.B.135A **Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) Autoritatea competentă implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul 145.B.125 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare.

(c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.";

(e) la punctul 145.B.200 se adaugă litera (e) cu următorul text:

„(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.";

(f) punctul 145.B.205 se modifică după cum urmează:

(i) titlul se înlocuiește cu următorul text:

„145.B.205 **Atribuirea de sarcini**";

(ii) se adaugă litera (c) cu următorul text:

„(c) Pentru certificarea și supravegherea conformității organizației cu punctul 145.A.200A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu punctul 145.B.200 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.";

(g) la punctul 145.B.300 se adaugă litera (g) cu următorul text:

„(g) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul 145.A.200A, în plus față de respectarea dispozițiilor de la literele (a)-(f), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.";

(h) după punctul 145.B.330 se introduce punctul 145.B.330A cu următorul text:

„145.B.330A **Modificări ale sistemului de management al securității informațiilor**

(a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul 145.B.300. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul 145.B.350.

(b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203:

1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea."

2. Anexa III (partea 66) se modifică după cum urmează:

(a) în cuprins, după titlul 66.B.10 se introduce următorul titlu:

„66.B.15 Sistemul de management al securității informațiilor";

(b) după punctul 66.B.10 se introduce punctul 66.B.15 cu următorul text:

„66.B.15 **Sistemul de management al securității informațiilor**

Autoritatea competentă instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației."

3. Anexa Vc (partea CAMO) se modifică după cum urmează:

(a) cuprinsul se modifică după cum urmează:

(i) după titlul CAMO.A.200 se introduce următorul titlu:

„CAMO.A.200A Sistemul de management al securității informațiilor";

(ii) după titlul CAMO.B.135 se introduce următorul titlu:

„CAMO.B.135A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației";

(iii) titlul punctului CAMO.B.205 se înlocuiește cu următorul text:

„CAMO.B.205 Atribuirea de sarcini";

(iv) după titlul CAMO.B.330 se introduce următorul titlu:

„CAMO.B.330A Modificări ale sistemului de management al securității informațiilor";

(b) după punctul CAMO.A.200 se introduce punctul CAMO.A.200A cu următorul text:

„CAMO.A.200A **Sistemul de management al securității informațiilor**

Pe lângă sistemul de management menționat la punctul CAMO.A.200, organizația instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.";

(c) la punctul CAMO.B.125 se adaugă litera (c) cu următorul text:

„(c) Autoritatea competentă a statului membru furnizează agenției cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul punctului IS.I.OR.230 din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203.";

(d) după punctul CAMO.B.135 se introduce punctul CAMO.B.135A cu următorul text:

„CAMO.B.135A **Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) Autoritatea competentă implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul CAMO.B.125 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare.

(c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.";

(e) la punctul CAMO.B.200 se adaugă litera (e) cu următorul text:

„(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.";

(f) punctul CAMO.B.205 se modifică după cum urmează:

(i) titlul se înlocuiește cu următorul text:

„CAMO.B.205 **Atribuirea de sarcini**";

(ii) se adaugă litera (c) cu următorul text:

„(c) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul CAMO.A.200A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu punctul CAMO.B.200 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.";

(g) la punctul CAMO.B.300 se adaugă litera (g) cu următorul text:

„(g) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul CAMO.A.200A, în plus față de respectarea dispozițiilor de la literele (a)-(f), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.";

(h) după punctul CAMO.B.330 se introduce punctul CAMO.B.330A cu următorul text:

„CAMO.B.330A **Modificări ale sistemului de management al securității informațiilor**

(a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul CAMO.B.300. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul CAMO.B.350.

(b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203:

1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea."

ANEXA VIII

Anexele II (partea ATCO.AR) și III (partea ATCO.OR) la Regulamentul (UE) 2015/340 se modifică după cum urmează:

1. Anexa II (partea ATCO.AR) se modifică după cum urmează:

(a) la punctul ATCO.AR.A.020 se adaugă litera (c) cu următorul text:

„(c) Autoritatea competentă a statului membru furnizează agenției cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul punctului IS.I.OR.230 din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203";

(b) după punctul ATCO.AR.A.025 se introduce punctul ATCO.AR.A.025A cu următorul text:

„**ATCO.AR.A.025A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) Autoritatea competentă implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul ATCO.AR.A.020 și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare.

(c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.";

(c) la punctul ATCO.AR.B.001 se adaugă litera (e) cu următorul text:

„(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.";

(d) punctul ATCO.AR.B.005 se modifică după cum urmează:

(i) titlul se înlocuiește cu următorul text:

„**ATCO.AR.B.005 Atribuirea de sarcini**";

(ii) se adaugă litera (c) cu următorul text:

„(c) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ATCO.OR.C.001A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu punctul ATCO.AR.B.001 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.";

(e) la punctul ATCO.AR.C.001 se adaugă litera (f) cu următorul text:

„(f) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ATCO.OR.C.001A, în plus față de respectarea dispozițiilor de la literele (a)-(e), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.";

(f) după punctul ATCO.AR.E.010 se introduce punctul ATCO.AR.E.010A cu următorul text:

„**ATCO.AR.E.010A Modificări ale sistemului de management al securității informațiilor**

(a) În ceea ce privește modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul ATCO.AR.C.001. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul ATCO.AR.C.010.

(b) În ceea ce privește alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203:

1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea."

2. Anexa III (partea ATCO.OR) se modifică după cum urmează:

După punctul ATCO.OR.C.001 se introduce punctul ATCO.OR.C.001A cu următorul text:

„**ATCO.OR.C.001A Sistemul de management al securității informațiilor**

Pe lângă sistemul de management menționat la punctul ATCO.OR.C.001, organizația de pregătire instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației."

ANEXA IX

Anexele II (partea ATM/ANS.AR) și III (partea ATM/ANS.OR) la Regulamentul de punere în aplicare (UE) 2017/373 se modifică după cum urmează:

1. Anexa II (partea ATM/ANS.AR) se modifică după cum urmează:

(a) la punctul ATM/ANS.AR.A.020 se adaugă litera (c) cu următorul text:

„(c) Autoritatea competentă a statului membru furnizează agenției cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul punctului IS.I.OR.230 din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203”;

(b) după punctul ATM/ANS.AR.A.025 se introduce punctul ATM/ANS.AR.A.025A cu următorul text:

„**ATM/ANS.AR.A.025A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) Autoritatea competentă implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul ATM/ANS.AR.A.020 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare.

(c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.”;

(c) la punctul ATM/ANS.AR.B.001 se adaugă litera (e) cu următorul text:

„(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;

(d) punctul ATM/ANS.AR.B.005 se modifică după cum urmează:

(i) titlul se înlocuiește cu următorul text:

„**ATM/ANS.AR.B.005 Atribuirea de sarcini**”;

(ii) se adaugă litera (c) cu următorul text:

„(c) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ATM/ANS.OR.B.005A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu punctul ATM/ANS.AR.B.001 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.";

(e) la punctul ATM/ANS.AR.C.010 se adaugă litera (d) cu următorul text:

„(d) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ATM/ANS.OR.B.005A, în plus față de respectarea dispozițiilor de la literele (a)-(c), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.";

(f) după punctul ATM/ANS.AR.C.025 se introduce punctul ATM/ANS.AR.C.025A cu următorul text:

„**ATM/ANS.AR.C.025A Modificări ale sistemului de management al securității informațiilor**

(a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul ATM/ANS.AR.C.010. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul ATM/ANS.AR.C.050.

(b) În ceea ce privește alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203:

1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea."

2. Anexa III (partea ATM/ANS.OR) se modifică după cum urmează:

(a) după punctul ATM/ANS.OR.B.005 se introduce punctul ATM/ANS.OR.B.005A cu următorul text:

„**ATM/ANS.OR.B.005A Sistemul de management al securității informațiilor**

Pe lângă sistemul de management menționat la punctul ATM/ANS.OR.B.005, furnizorul de servicii instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.";

(b) punctul ATM/ANS.OR.D.010 se înlocuiește cu următorul text:

„**ATM/ANS.OR.D.010 Managementul securității**

(a) Furnizorii de servicii de navigație aeriană și de management al fluxului de trafic aerian și administratorul rețelei, ca parte integrantă a sistemului lor de management, astfel cum se prevede la punctul ATM/ANS.OR.B.005, trebuie să instituie un sistem de management al securității pentru a asigura:

1. securitatea facilităților și a personalului lor, în vederea prevenirii actelor de intervenție ilicită în furnizarea serviciilor;

2. securitatea datelor operaționale pe care le primesc, le produc sau le utilizează în alt mod, astfel încât accesul la acestea să fie rezervat exclusiv persoanelor autorizate.

(b) Sistemul de management al securității trebuie să definească:

1. procesele și procedurile referitoare la evaluarea și reducerea riscurilor de securitate, monitorizarea și îmbunătățirea securității, examinările de securitate și diseminarea rezultatelor;

2. mijloacele destinate să identifice, să monitorizeze și să detecteze breșele de securitate și să alerteze personalul prin semnale de avertizare adecvate cu privire la securitate;

3. mijloacele de control al efectelor cauzate de breșele de securitate și de identificare a măsurilor de remediere și a procedurilor de reducere a riscurilor pentru prevenirea repetării acestora.

(c) Furnizorii de servicii de navigație aeriană și de management al fluxului de trafic aerian și administratorul rețelei trebuie să asigure autorizarea de securitate a personalului propriu, dacă este cazul, și să se coordoneze cu autoritățile civile și militare relevante pentru a asigura securitatea facilităților, a personalului și a datelor lor.

(d) Aspectele legate de securitatea informațiilor trebuie gestionate în conformitate cu punctul ATM/ANS.OR.B.005A.”