II

*(Nelegislativní akty)*

# NAŘÍZENÍ

## PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2023/203

**ze dne 27. října 2022,**

**prováděcí nařízení Komise ze dne 27. října 2022, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2018/1139, pokud jde o požadavky na řízení rizik v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví pro organizace, na které se vztahují nařízení Komise (EU) č. 1321/2014, (EU) č. 965/2012, (EU) č. 1178/2011, (EU) 2015/340, prováděcí nařízení Komise (EU) 2017/373 a (EU) 2021/664, a pro příslušné orgány, na které se vztahují nařízení Komise (EU) č. 748/2012, (EU) č. 1321/2014, (EU) č. 965/2012, (EU) č. 1178/2011, (EU) 2015/340 a (EU) č. 139/2014, prováděcí nařízení Komise (EU) 2017/373 a (EU) 2021/664, a kterým se mění nařízení Komise (EU) č. 1178/2011, (EU) č. 748/2012, (EU) č. 965/2012, (EU) č. 139/2014, (EU) č. 1321/2014, (EU) 2015/340 a prováděcí nařízení Komise (EU) 2017/373 a (EU) 2021/664**

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2018/1139 ze dne 4. července 2018 o společných pravidlech v oblasti civilního letectví a o zřízení Agentury Evropské unie pro bezpečnost letectví, kterým se mění nařízení (ES) č. 2111/2005, (ES) č. 1008/2008, (EU) č. 996/2010, (EU) č. 376/2014 a směrnice Evropského parlamentu a Rady 2014/30/EU a 2014/53/EU a kterým se zrušuje nařízení Evropského parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nařízení Rady (EHS) č. 3922/91 ([1]), a zejména čl. 17 odst. 1 písm. b), čl. 27 odst. 1 písm. a), čl. 31 odst. 1 písm. b), čl. 43 odst. 1 písm. b), čl. 53 odst. 1 písm. a) a čl. 62 odst. 15 písm. c) uvedeného nařízení,

vzhledem k těmto důvodům:

(1) V souladu s hlavními požadavky stanovenými v bodě 3.1 písm. b) přílohy II nařízení (EU) 2018/1139 mají organizace k řízení zachování letové způsobilosti a organizace údržby zavést a udržovat systém řízení bezpečnostních rizik.

(2) Kromě toho, v souladu s hlavními požadavky stanovenými v bodu 3.3 písm. b) a bodu 5 písm. b) přílohy IV nařízení (EU) 2018/1139 mají organizace provádějící výcvik pilotů, organizace provádějící výcvik palubních průvodčích, letecká zdravotní střediska pro posádky letadel a provozovatelé zařízení pro výcvik pomocí letové simulace navíc zavést a udržovat systém řízení bezpečnostních rizik.

(3) V souladu s hlavními požadavky stanovenými v bodu 8.1 písm. c) přílohy V nařízení (EU) 2018/1139 musí letečtí provozovatelé zavést a udržovat systém řízení bezpečnostních rizik.

(4) Dále v souladu s hlavními požadavky stanovenými v bodu 5.1 písm. c) a bodu 5.4 písm. b) přílohy VIII nařízení (EU) 2018/1139 mají poskytovatelé uspořádání letového provozu a letových navigačních služeb, poskytovatelé služeb U-space a poskytovatelé jednotné společné informační služby a organizace provádějící výcvik a letecká zdravotní střediska pro řídící letového provozu zavést a udržovat systém řízení pro řízení bezpečnostních rizik.

([1]) Úř. věst. L 212, 22.8.2018, s. 1.

(5) Tato bezpečnostní rizika mohou pocházet z různých zdrojů, jako jsou chyby v konstrukci a údržbě, aspekty lidské výkonnosti, hrozby pro životní prostředí a hrozby pro bezpečnost informací. Systémy řízení zavedené Agenturou Evropské unie pro bezpečnost letectví (dále jen „agentura“) a příslušnými vnitrostátními orgány a organizacemi uvedenými ve výše uvedených bodech odůvodnění by proto měly zohledňovat nejen bezpečnostní rizika vyplývající z náhodných událostí, ale také bezpečnostní rizika vyplývající z hrozeb pro bezpečnost informací, kdy mohou existující nedostatky zneužít osoby se zlým úmyslem. Tato rizika v oblasti bezpečnosti informací se v prostředí civilního letectví neustále zvyšují, protože současné informační systémy jsou stále propojenější a stále častěji se stávají cílem zlovolných aktérů.

(6) Rizika spojená s těmito informačními systémy se neomezují pouze na možné útoky na kybernetický prostor, ale patří mezi ně i hrozby, které mohou ovlivnit procesy a postupy, jakož i výkonnost lidí.

(7) Značný počet organizací již používá mezinárodní normy, jako například ISO 27001, s cílem řešit bezpečnost digitálních informací a údajů. Tyto normy však nemusí plně řešit všechny specifičnosti civilního letectví. Proto je vhodné stanovit požadavky na řízení rizik bezpečnosti informací s potenciálním dopadem na bezpečnost letectví.

(8) Je nezbytné, aby se tyto požadavky vztahovaly na všechny oblasti letectví a jejich rozhraní, neboť letectví je vysoce propojeným systémem systémů. Proto by se měly vztahovat na všechny organizace a příslušné orgány, na které se vztahují nařízení Komise (EU) č. 748/2012 ([2]), (EU) č. 1321/2014 ([3]), (EU) č. 965/2012 ([4]), (EU) č. 1178/2011 ([5]), (EU) 2015/340 ([6]), (EU) č. 139/2014 ([7]) a prováděcí nařízení Komise (EU) 2021/664 ([8]), a to i na ty, které již musí mít systém řízení v souladu se stávajícími právními předpisy Unie v oblasti bezpečnosti letectví. Některé organizace by však měly být z oblasti působnosti tohoto nařízení vyňaty, aby se zajistila odpovídající přiměřenost vzhledem k nižším rizikům v oblasti bezpečnosti informací, která pro letecký systém představují.

(9) Požadavky stanovené v tomto nařízení by měly zajistit důsledné provádění ve všech oblastech letectví a současně by měly mít minimální dopad na právní předpisy Unie v oblasti bezpečnosti letectví, které se na tyto oblasti již vztahují.

([2]) Nařízení Komise (EU) č. 748/2012 ze dne 3. srpna 2012, kterým se stanoví prováděcí pravidla pro certifikaci letové způsobilosti letadel a souvisejících výrobků, letadlových částí a zařízení a certifikaci ochrany životního prostředí, jakož i pro certifikaci projekčních a výrobních organizací (Úř. věst. L 224, 21.8.2012, s. 1).

([3]) Nařízení Komise (EU) č. 1321/2014 ze dne 26. listopadu 2014 o zachování letové způsobilosti letadel a leteckých výrobků, letadlových částí a zařízení a schvalování organizací a personálu zapojených do těchto úkolů (přepracované znění) (Úř. věst. L 362, 17.12.2014, s. 1).

([4]) Nařízení Komise (EU) č. 965/2012 ze dne 5. října 2012, kterým se stanoví technické požadavky a správní postupy týkající se letového provozu podle nařízení Evropského parlamentu a Rady (ES) č. 216/2008 (Úř. věst. L 296, 25.10.2012, s. 1).

([5]) Nařízení Komise (EU) č. 1178/2011 ze dne 3. listopadu 2011, kterým se stanoví technické požadavky a správní postupy týkající se posádek v civilním letectví podle nařízení Evropského parlamentu a Rady (ES) č. 216/2008 (Úř. věst. L 311, 25.11.2011, s. 1).

([6]) Nařízení Komise (EU) 2015/340 ze dne 20. února 2015, kterým se stanoví technické požadavky a správní postupy týkající se průkazů způsobilosti a osvědčení řídících letového provozu podle nařízení Evropského parlamentu a Rady (ES) č. 216/2008, kterým se mění prováděcí nařízení Komise (EU) č. 923/2012 a kterým se zrušuje nařízení Komise (EU) č. 805/2011 (Úř. věst. L 63, 6.3.2015, s. 1).

([7]) Nařízení Komise (EU) č. 139/2014 ze dne 12. února 2014, kterým se stanoví požadavky a správní postupy týkající se letišť podle nařízení Evropského parlamentu a Rady (ES) č. 216/2008 (Úř. věst. L 44, 14.2.2014, s. 1).

([8]) Prováděcí nařízení Komise (EU) 2021/664 ze dne 22. dubna 2021 o regulačním rámci pro vzdušný prostor U-space (Úř. věst. L 139, 23.4.2021, s. 161).

(10) Požadavky stanovenými v tomto nařízení by neměly být dotčeny požadavky na bezpečnost informací a kybernetickou bezpečnost stanovené v bodě 1.7 přílohy prováděcího nařízení Komise (EU) 2015/1998 ([9]) a v článku 14 směrnice Evropského parlamentu a Rady (EU) 2016/1148 ([10]).

(11) Bezpečnostní požadavky stanovené v článcích 33 až 43 hlavy V „Bezpečnost programu" nařízení Evropského parlamentu a Rady (EU) 2021/696 ([11]) se považují za rovnocenné požadavkům stanoveným v tomto nařízení, s výjimkou bodu IS.I.OR.230 přílohy II tohoto nařízení, který by měl být dodržen.

(12) V zájmu zajištění právní jistoty by se mělo v případě výkladu pojmu „bezpečnost informací", jak je definován v tomto nařízení, odrážející jeho běžné používání v civilním letectví na celém světě, mít za to, že je v souladu s výkladem pojmu „bezpečnost sítí a informačních systémů", jak je definován v čl. 4 bodě 2 směrnice (EU) 2016/1148. Definice bezpečnosti informací použitá pro účely tohoto nařízení by neměla být vykládána odchylně od definice bezpečnosti sítí a informačních systémů stanovené ve směrnici (EU) 2016/1148.

(13) Aby se zabránilo zdvojování právních požadavků, pokud organizace, na něž se vztahuje toto nařízení, již podléhají bezpečnostním požadavkům vyplývajícím z aktů Unie uvedených v (10). a 11. bodě odůvodnění, které jsou ve svém důsledku rovnocenné ustanovením tohoto nařízení, měl by být soulad s uvedenými bezpečnostními požadavky považován za soulad s požadavky stanovenými v tomto nařízení.

(14) Organizace, na něž se vztahuje toto nařízení a které již podléhají bezpečnostním požadavkům vyplývajícím z prováděcího nařízení (EU) 2015/1998 nebo nařízení (EU) 2021/696, by měly rovněž splňovat požadavky přílohy II (část IS.I.OR.230 „Systém externího hlášení v oblasti bezpečnosti informací") tohoto nařízení, neboť ani jedno z těchto nařízení neobsahuje žádná ustanovení týkající se externího hlášení incidentů bezpečnosti informací.

(15) Pro úplnost je třeba změnit nařízení (EU) č. 1178/2011, (EU) č. 748/2012, (EU) č. 965/2012, (EU) č. 139/2014, (EU) č. 1321/2014, (EU) 2015/340 a prováděcí nařízení (EU) 2017/373 ([12]) a (EU) 2021/664 tak, aby byly zavedeny požadavky na systém řízení bezpečnosti informací stanovené v tomto nařízení spolu se systémy řízení v něm uvedenými a aby byly stanoveny požadavky příslušných orgánů, pokud jde o dohled nad organizacemi, které provádějí výše uvedené požadavky na řízení bezpečnosti informací.

(16) Aby měly organizace dostatek času na zajištění souladu s novými pravidly a postupy, mělo by se toto nařízení začít používat tři roky po vstupu v platnost, s výjimkou poskytovatele letových navigačních služeb evropské služby pro pokrytí geostacionární navigací (EGNOS) definovaného v prováděcím nařízení (EU) 2017/373, v jehož případě by se mělo začít používat od 1. ledna 2026 vzhledem k probíhající bezpečnostní akreditaci systému a služeb EGNOS v souladu s nařízením (EU) 2021/696.

(17) Požadavky stanovené tímto nařízením vycházejí ze stanoviska č. 03/2021 ([13]) vydaného agenturou v souladu s čl. 75 odst. 2 písm. b) a c) a čl. 76 odst. 1 nařízení (EU) 2018/1139.

([9]) Prováděcí nařízení Komise (EU) 2015/1998 ze dne 5. listopadu 2015, kterým se stanoví prováděcí opatření ke společným základním normám letecké bezpečnosti (Úř. věst. L 299, 14.11.2015, s. 1).

([10]) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

([11]) Nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU (Úř. věst. L 170, 12.5.2021, s. 69).

([12]) Prováděcí nařízení Komise (EU) 2017/373 ze dne 1. března 2017, kterým se stanoví společné požadavky na poskytovatele služeb v oblasti uspořádání letového provozu / letových navigačních služeb a jiných funkcí sítě uspořádání letového provozu a dohled nad nimi, zrušují nařízení (ES) č. 482/2008, prováděcí nařízení (EU) č. 1034/2011, (EU) č. 1035/2011 a (EU) 2016/1377 a mění nařízení (EU) č. 677/2011 (Úř. věst. L 62, 8.3.2017, s. 1).

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

(18) Požadavky stanovené v tomto nařízení jsou v souladu se stanoviskem výboru pro uplatňování společných bezpečnostních pravidel v oblasti civilního letectví zřízeného článkem 127 nařízení (EU) 2018/1139,

PŘIJALA TOTO NAŘÍZENÍ:

*Článek 1*

**Předmět**

Toto nařízení stanoví požadavky, které musí organizace a příslušné orgány splnit s cílem:

a) identifikovat a řídit rizika v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, která by mohla ovlivnit systémy a údaje informačních a komunikačních technologií používaných pro účely civilního letectví;

b) zjistit události v oblasti bezpečnosti informací a určit ty, které jsou považovány za incidenty v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví;

c) reagovat na tyto incidenty v oblasti bezpečnosti informací a zotavit se z nich.

*Článek 2*

**Oblast působnosti**

1. Toto nařízení se vztahuje na tyto organizace:

a) organizace údržby, na které se vztahuje oddíl A přílohy II (část 145) nařízení (EU) č. 1321/2014, s výjimkou těch, které se zabývají výhradně údržbou letadel v souladu s přílohou Vb (část ML) nařízení Komise (EU) č. 1321/2014;

b) organizace k řízení zachování letové způsobilosti, na které se vztahuje oddíl A přílohy Vc (část CAMO) nařízení (EU) č. 1321/2014, s výjimkou těch, které se zabývají výhradně řízením zachování letové způsobilosti letadel v souladu s přílohou Vb (část ML) nařízení Komise (EU) č. 1321/2014;

c) letečtí provozovatelé, na které se vztahuje příloha III (část ORO) nařízení (EU) č. 965/2012, s výjimkou těch, kteří se podílejí výhradně na provozu některého z následujících letadel:

   i) letadlo ELA2 podle definice v čl. 1 odst. 2 písm. j) nařízení (EU) č. 748/2012;

   ii) jednomotorové vrtulové letouny s maximální provozní konfigurací sedadel pro cestující 5 nebo méně, které nejsou klasifikovány jako složitá motorová letadla, při vzletu a přistání na stejném letišti nebo provozním místě a při provozu podle pravidel letu za viditelnosti ve dne;

   iii) jednomotorové vrtulníky s maximální provozní konfigurací sedadel pro cestující 5 nebo méně, které nejsou klasifikovány jako složitá motorová letadla, při vzletu a přistání na stejném letišti nebo provozním místě a při provozu podle pravidel letu za viditelnosti ve dne;

d) schválené organizace pro výcvik, na které se vztahuje příloha VII (část ORA) nařízení (EU) č. 1178/2011, s výjimkou těch, které se zabývají výhradně výcvikovými činnostmi u letadel ELA2 podle definice v čl. 1 odst. 2 písm. j) nařízení (EU) č. 748/2012 nebo se zabývají výhradně teoretickým výcvikem;

e) letecká zdravotnická střediska pro posádky letadel, na která se vztahuje příloha VII (část ORA) nařízení (EU) č. 1178/2011;

f) provozovatelé zařízení pro výcvik pomocí letové simulace (FSTD), na které se vztahuje příloha VII (část ORA) nařízení (EU) č. 1178/2011, s výjimkou těch, kteří se podílejí výhradně na provozu zařízení FSTD pro letadla ELA2, jak jsou definována v čl. 1 odst. 2 písm. j) nařízení (EU) č. 748/2012;

g) organizace pro výcvik řídících letového provozu a letecká zdravotní střediska těchto organizací, na které se vztahuje příloha III (část ATCO.OR) nařízení (EU) 2015/340;

h) organizace, na které se vztahuje příloha III (část ATM/ANS.OR) prováděcího nařízení (EU) 2017/373, s výjimkou následujících poskytovatelů služeb:

i) poskytovatelé letových navigačních služeb, kteří jsou držiteli omezeného osvědčení v souladu s bodem ATM/ANS.OR.A.010 uvedené přílohy;

ii) poskytovatelé letových informačních služeb, kteří ohlašují své činnosti v souladu s bodem ATM/ANS.OR.A.015 uvedené přílohy;

i) poskytovatelé služeb U-space a poskytovatelé jednotných společných informačních služeb, na které se vztahuje prováděcí nařízení (EU) 2021/664.

2. Toto nařízení se vztahuje na příslušné orgány, včetně Agentury Evropské unie pro bezpečnost letectví (dále jen „agentura"), uvedené v článku 6 tohoto nařízení a v článku 5 nařízení v přenesené pravomoci (EU) 2022/1645 ([14]).

3. Toto nařízení se rovněž vztahuje na příslušný orgán odpovědný za vydávání, prodlužování platnosti, změnu, pozastavování platnosti a rušení průkazů způsobilosti k údržbě letadel v souladu s přílohou III (část 66) nařízení w(EU) č. 1321/2014.

4. Tímto nařízením nejsou dotčeny požadavky na bezpečnost informací a kybernetickou bezpečnost stanovené v bodě 1.7 přílohy prováděcího nařízení (EU) 2015/1998 a v článku 14 směrnice (EU) 2016/1148.

*Článek 3*

**Definice**

Pro účely tohoto nařízení se rozumí:

1) „bezpečností informací" zachování důvěrnosti, integrity, autenticity a dostupnosti sítí a informačních systémů;

2) „událostí bezpečnosti informací" zjištěný výskyt stavu systému, služby nebo sítě, který poukazuje na možné narušení politiky bezpečnosti informací nebo na selhání kontrol bezpečnosti informací, nebo předem neznámá situace, která může být významná pro bezpečnost informací;

3) „incidentem" jakákoliv událost, která má reálný negativní dopad na bezpečnost sítí a informačních systémů ve smyslu čl. 4 bodu 7 směrnice (EU) 2016/1148;

4) „rizikem bezpečnosti informací" riziko pro organizační provoz civilního letectví, aktiva, jednotlivce a jiné organizace v důsledku potenciálu události bezpečnosti informací. Rizika bezpečnosti informací jsou spojena s potenciální možností, že hrozby zneužijí zranitelností informačního aktiva nebo skupiny informačních aktiv;

([14]) Nařízení Komise v přenesené pravomoci (EU) 2022/1645 ze dne 14. července 2022, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2018/1139, pokud jde o požadavky na řízení rizik bezpečnosti informací s potenciálním dopadem na bezpečnost letectví pro organizace, na něž se vztahují nařízení Komise (EU) č. 748/2012 a (EU) č. 139/2014, a kterým se mění nařízení Komise (EU) č. 748/2012 a (EU) č. 139/2014 (Úř. věst. L 248, 26.9.2022, s. 18).

5) „hrozbou“ potenciální porušení bezpečnosti informací, které existuje v případě výskytu subjektu, okolnosti, akce nebo události, které by mohly způsobit škodu;

6) „zranitelností“ nedostatek nebo slabina aktiva nebo systému, postupů, projekce, provádění nebo opatření v oblasti bezpečnosti informací, která by mohla být zneužita a vést k narušení nebo porušení politiky bezpečnosti informací.

*Článek 4*

**Požadavky na organizace a příslušné orgány**

1. Organizace uvedené v čl. 2 odst. 1 musí splňovat požadavky přílohy II (část IS.I.OR) tohoto nařízení.

2. Příslušné orgány uvedené v čl. 2 odst. 2 a 3 musí splňovat požadavky přílohy I (část IS.AR) tohoto nařízení.

*Článek 5*

**Požadavky vyplývající z jiných právních předpisů Unie**

1. Pokud organizace uvedená v čl. 2 odst. 1 splňuje bezpečnostní požadavky stanovené v souladu s článkem 14 směrnice (EU) 2016/1148, které jsou rovnocenné požadavkům stanoveným v tomto nařízení, má se za to, že soulad s uvedenými bezpečnostními požadavky zakládá soulad s požadavky stanovenými v tomto nařízení.

2. Pokud je organizace uvedená v čl. 2 odst. 1 provozovatelem nebo subjektem uvedeným v národních bezpečnostních programech ochrany civilního letectví před protiprávními činy vypracovaných členskými státy stanovených v souladu s článkem 10 nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ([15]), považují se požadavky na kybernetickou bezpečnost obsažené v bodě 1.7 přílohy prováděcího nařízení (EU) 2015/1998 za rovnocenné požadavkům stanoveným v tomto nařízení, s výjimkou bodu IS.I.OR.230 přílohy II tohoto nařízení, který musí být splněn.

3. Pokud je organizace uvedená v čl. 2 odst. 1 poskytovatelem letových navigačních služeb evropské služby pro pokrytí geostacionární navigací (EGNOS) podle nařízení (EU) 2021/696, považují se bezpečnostní požadavky obsažené v článcích 33 až 43 hlavy V uvedeného nařízení za rovnocenné požadavkům stanoveným v tomto nařízení, s výjimkou bodu IS.I.OR.230 přílohy II tohoto nařízení, který se jako takový dodržuje.

4. Komise může po konzultaci s agenturou a skupinou pro spolupráci uvedenou v článku 11 směrnice (EU) 2016/1148 vydat pokyny pro posuzování rovnocennosti požadavků stanovených v tomto nařízení a ve směrnici (EU) 2016/1148.

*Článek 6*

**Příslušný orgán**

1. Aniž jsou dotčeny úkoly svěřené Komisi pro bezpečnostní akreditaci uvedené v článku 36 nařízení (EU) 2021/696, orgánem odpovědným za certifikaci a dohled nad dodržováním tohoto nařízení je:

a) pokud jde o organizace uvedené v čl. 2 odst. 1 písm. a), příslušný orgán určený v souladu s přílohou II (část 145) nařízení (EU) č. 1321/2014;

b) pokud jde o organizace uvedené v čl. 2 odst. 1 písm. b), příslušný orgán určený v souladu s přílohou Vc (část CAMO) nařízení (EU) č. 1321/2014;

([15]) Nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ze dne 11. března 2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy a o zrušení nařízení (ES) č. 2320/2002 (Úř. věst. L 97, 9.4.2008, s. 72).

c) pokud jde o organizace uvedené v čl. 2 odst. 1 písm. c), příslušný orgán určený v souladu s přílohou III (část ORO) nařízení (EU) č. 965/2012;

d) pokud jde o organizace uvedené v čl. 2 odst. 1 písm. d) až f), příslušný orgán určený v souladu s přílohou VII (část ORA) nařízení (EU) č. 1178/2011;

e) pokud jde o organizace uvedené v čl. 2 odst. 1 písm. g), příslušný orgán určený v souladu s čl. 6 odst. 2 nařízení (EU) 2015/340;

f) pokud jde o organizace uvedené v čl. 2 odst. 1 písm. h), příslušný orgán určený v souladu s čl. 4 odst. 1 prováděcího nařízení (EU) 2017/373;

g) pokud jde o organizace uvedené v čl. 2 odst. 1 písm. i), příslušný orgán určený v souladu s čl. 14 odst. 1, případně čl. 14 odst. 2 prováděcího nařízení (EU) 2021/664.

2. Členské státy mohou pro účely tohoto nařízení určit nezávislý a autonomní subjekt, který bude plnit přidělenou úlohu a povinnosti příslušných úřadů uvedených v odstavci 1. V takovém případě se stanoví koordinační opatření mezi uvedeným subjektem a příslušnými úřady uvedenými v odstavci 1 s cílem zajistit účinný dozor nad všemi požadavky, které má organizace splňovat.

3. Agentura v plném souladu s platnými pravidly o utajení, ochraně osobních údajů a ochraně utajovaných informací spolupracuje s Agenturou Evropské unie pro Kosmický program (EUSPA) a s Komisí pro bezpečnostní akreditaci podle článku 36 nařízení (EU) 2021/696, aby byl zajištěn účinný dohled nad požadavky vztahujícími se na poskytovatele letových navigačních služeb EGNOS.

*Článek 7*

**Předložení relevantních informací příslušným orgánům bezpečnosti sítí a informačních systémů**

Příslušné orgány podle tohoto nařízení bez zbytečného odkladu informují jednotné kontaktní místo určené v souladu s článkem 8 směrnice (EU) 2016/1148 o všech relevantních informacích obsažených v oznámeních předložených podle bodu IS.I.OR.230 přílohy II tohoto nařízení a bodu IS.D.OR.230 přílohy I nařízení v přenesené pravomoci 2022/1645 provozovateli základních služeb určenými v souladu s článkem 5 směrnice (EU) 2016/1148.

*Článek 8*

**Změna nařízení (EU) č. 1178/2011**

Přílohy VI (část ARA) a VII (část ORA) nařízení (EU) č. 1178/2011 se mění v souladu s přílohou III tohoto nařízení.

*Článek 9*

**Změna nařízení (EU) č. 748/2012**

Příloha I (část 21) nařízení (EU) č. 748/2012 se mění v souladu s přílohou IV tohoto nařízení.

*Článek 10*

**Změna nařízení (EU) č. 965/2012**

Přílohy II (část ARO) a III (část ORO) nařízení (EU) č. 965/2012 se mění v souladu s přílohou V tohoto nařízení.

*Článek 11*

**Změna nařízení (EU) č. 139/2014**

Příloha II (část ADR.AR) nařízení (EU) č. 139/2014 se mění v souladu s přílohou VI tohoto nařízení.

*Článek 12*

**Změna nařízení (EU) č. 1321/2014**

Přílohy II (část 145), III (část 66) a Vc (část CAMO) nařízení (EU) č. 1321/2014 se mění v souladu s přílohou VII tohoto nařízení.

*Článek 13*

**Změna nařízení (EU) 2015/340**

Přílohy II (část ATCO.AR) a III (část ATCO.OR) nařízení (EU) 2015/340 se mění v souladu s přílohou VIII tohoto nařízení.

*Článek 14*

**Změna prováděcího nařízení (EU) 2017/373**

Přílohy II (část ATM/ANS.AR) a III (část ATM/ANS.OR) prováděcího nařízení (EU) 2017/373 se mění v souladu s přílohou IX tohoto nařízení.

*Článek 15*

**Změna prováděcího nařízení (EU) 2021/664**

Prováděcí nařízení (EU) 2021/664 se mění takto:

1) v čl. 15 odst. 1 se písmeno f) nahrazuje tímto:

„f) zavést a udržovat systém řízení bezpečnosti v souladu s bodem ATM/ANS.OR.D.010 v hlavě D přílohy III prováděcího nařízení (EU) 2017/373 a systém řízení bezpečnosti informací v souladu s přílohou II (část IS.I.OR) prováděcího nařízení (EU) 2023/203.;“

2) v článku 18 se doplňuje nové písmeno l), které zní:

„l) zřídit, zavést a udržovat systém řízení bezpečnosti informací v souladu s přílohou I (část IS.AR) prováděcího nařízení (EU) 2023/203.“

*Článek 16*

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Použije se od 22. února 2026.

Pokud však jde o poskytovatele letových navigačních služeb EGNOS, na kterého se vztahuje prováděcí nařízení (EU) 2017/373, použije se od 1. ledna 2026.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 27. října 2022.

*Za Komisi*
*předsedkyně*
Ursula VON DER LEYEN

*PŘÍLOHA I*

**BEZPEČNOST INFORMACÍ – POŽADAVKY NA ORGÁN**

**[PART-IS.AR]**



**IS.AR.100 Oblast působnosti**

Tato část stanoví požadavky na řízení, které musí splňovat příslušné orgány uvedené v čl. 2 odst. 2 tohoto nařízení.

Požadavky, které musí tyto příslušné orgány splňovat pro výkon svých činností v oblasti certifikace, dozoru a prosazování, jsou obsaženy v nařízeních uvedených v čl. 2 odst. 1 tohoto nařízení a v článku 2 nařízení v přenesené pravomoci (EU) 2022/1645.

**IS.AR.200 Systém řízení bezpečnosti informací (ISMS)**

a) Za účelem dosažení cílů stanovených v článku 1 příslušný orgán vytvoří, provádí a udržuje systém řízení bezpečnosti informací (ISMS), který zajišťuje, že příslušný orgán:

1) zavede politiku v oblasti bezpečnosti informací, která stanoví obecné zásady příslušného orgánu s ohledem na potenciální dopad rizik bezpečnosti informací na bezpečnost letectví;

2) identifikuje a přezkoumává rizika bezpečnosti informací v souladu s bodem IS.AR.205;

3) definuje a provádí opatření k řešení rizik bezpečnosti informací v souladu s bodem IS.AR.210;

4) definuje a provádí v souladu s bodem IS.AR.215 opatření potřebná k odhalení událostí bezpečnosti informací, identifikuje ty, které jsou považovány za incidenty s potenciálním dopadem na bezpečnost letectví, a reaguje na tyto incidenty bezpečnosti informací a zotavuje se z nich;

5) splňuje požadavky uvedené v bodě IS.AR.220 při uzavírání smluv na jakoukoli část činností popsaných v bodě IS.AR.200 s jinými organizacemi;

6) splňuje požadavky na personál obsažené v bodě IS.AR.225;

7) splňuje požadavky na vedení záznamů obsažené v bodě IS.AR.230;

8) sleduje dodržování požadavků tohoto nařízení svou organizací a poskytuje zpětnou vazbu o zjištěních osobě uvedené v bodě IS.AR.225 písm. a), aby zajistila účinné provádění nápravných opatření;

9) chrání důvěrnost veškerých informací, které může mít příslušný orgán k dispozici v souvislosti s organizacemi podléhajícími jeho dozoru, a informací získaných prostřednictvím systémů externího hlášení organizací zřízených v souladu s bodem IS.I.OR.230 přílohy II (část IS.I.OR) tohoto nařízení a bodem IS.D.OR.230 přílohy (část IS.D.OR) nařízení v přenesené pravomoci (EU) 2022/1645.

10) oznámí agentuře změny, které mají vliv na schopnost příslušného orgánu plnit své úkoly a povinnosti stanovené v tomto nařízení;

11) definuje a provádí postupy pro sdílení relevantních informací, pokud je to vhodné a praktickým způsobem a včas, s cílem pomoci ostatním příslušným orgánům a agenturám, jakož i organizacím, na které se vztahuje toto nařízení, provádět účinné hodnocení bezpečnostních rizik souvisejících s jejich činnostmi.

b) Aby příslušný orgán splňoval požadavky uvedené v článku 1, provádí proces neustálého zlepšování v souladu s bodem IS.AR.235.

c) Příslušný orgán dokumentuje všechny klíčové procesy, postupy, úlohy a povinnosti požadované za účelem dosažení souladu s bodem IS.AR.200 písm. a) a zavede proces pro změnu této dokumentace.

d) Procesy, postupy, úlohy a povinnosti zavedené příslušným orgánem za účelem dosažení souladu s bodem IS.AR.200 písm. a) musí odpovídat povaze a složitosti jeho činností na základě posouzení rizik bezpečnosti informací spojených s uvedenými činnostmi a mohou být začleněny do jiných stávajících systémů řízení, které již příslušný orgán provádí.

**IS.AR.205 Posouzení rizik bezpečnosti informací**

a) Příslušný orgán identifikuje všechny své prvky, které by mohly být vystaveny rizikům bezpečnosti informací. Ty zahrnují:

1) činnosti, zařízení a zdroje příslušného orgánu a služby, které příslušný orgán provozuje, poskytuje, přijímá nebo udržuje;

2) zařízení, systémy, údaje a informace, které přispívají k fungování prvků uvedených v bodě 1.

b) Příslušný orgán identifikuje rozhraní, která má jeho vlastní organizace s jinými organizacemi a která by mohla vést k vzájemné expozici rizikům v oblasti bezpečnosti informací.

c) U prvků a rozhraní uvedených v písmenech a) a b) příslušný orgán identifikuje rizika v oblasti bezpečnosti informací, která případně mohou mít dopad na bezpečnost letectví.

Pro každé zjištěné riziko příslušný orgán:

1) přiřadí úroveň rizika podle předem stanovené klasifikace stanovené příslušným orgánem;

2) přiřadí každé riziko a jeho úroveň odpovídajícímu prvku nebo rozhraní identifikovanému podle písmen a) a b).

Předem stanovená klasifikace uvedená v bodě 1 zohledňuje možnost výskytu scénáře hrozeb a závažnost jeho bezpečnostních důsledků. Prostřednictvím této klasifikace a s přihlédnutím k tomu, zda má příslušný orgán pro svůj provoz strukturovaný a opakovatelný proces řízení rizik, musí být příslušný orgán schopen stanovit, zda je riziko přijatelné, nebo zda je třeba s ním zacházet v souladu s bodem IS.AR.210.

V zájmu usnadnění vzájemné srovnatelnosti hodnocení rizik se při přidělování úrovně rizika podle bodu 1 zohlední příslušné informace získané v koordinaci s organizacemi uvedenými v písmenu b).

d) Příslušný orgán přezkoumá a aktualizuje posouzení rizik provedené v souladu s písmeny a), b) a c) v kterémkoli z následujících případů:

1) dojde ke změně prvků, na které se vztahují rizika v oblasti bezpečnosti informací;

2) dojde ke změně rozhraní mezi organizací příslušného orgánu a ostatními organizacemi nebo ke změně rizik, o kterých ostatní organizace informují;

3) dojde ke změně informací nebo znalostí používaných k identifikaci, analýze a klasifikaci rizik;

4) z analýzy incidentů v oblasti bezpečnosti informací vyplývají poučení.

**IS.AR.210 Řešení rizik bezpečnosti informací**

a) Příslušný orgán vypracuje opatření k řešení nepřijatelných rizik zjištěných v souladu s bodem IS.AR.205, včas je provede a kontroluje jejich trvalou účinnost. Tato opatření umožní příslušnému orgánu:

1) kontrolovat okolnosti, které přispívají ke skutečnému výskytu scénáře hrozeb;

2) snížit důsledky pro bezpečnost letectví spojené s naplněním scénáře hrozeb;

3) vyhnout se rizikům.

Tato opatření nesmí přinést žádná nová možná nepřijatelná rizika pro bezpečnost letectví.

b) Osoba uvedená v bodě IS.AR.225 písm. a) a další dotčení pracovníci příslušného orgánu jsou informováni o výsledku posouzení rizik provedeného v souladu s bodem IS.AR.205, odpovídajících scénářích hrozeb a opatřeních, která mají být provedena.

Příslušný orgán rovněž informuje organizace, s nimiž má rozhraní v souladu s bodem IS.AR.205 písm. b), o všech rizicích sdílených mezi příslušným orgánem a organizací.

**IS.AR.215 Incidenty bezpečnosti informací – odhalení, reakce a zotavení**

a) Na základě výsledku posouzení rizik provedeného v souladu s bodem IS.AR.205 a výsledku řešení rizik provedeného v souladu s bodem IS.AR.210 provede příslušný orgán opatření k odhalování událostí, které naznačují možné naplnění nepřijatelných rizik a které mohou mít možný dopad na bezpečnost letectví. Tato opatření pro odhalování musí příslušnému orgánu umožnit:

1) zjistit odchylky od předem stanovených základních hodnot funkční výkonnosti;

2) spustit varování, aby se v případě jakékoli odchylky aktivovala vhodná opatření.

b) Příslušný orgán zavede opatření pro reakci na všechny podmínky události zjištěné v souladu s písmenem a), které mohou přerůst nebo přerostly v incident v oblasti bezpečnosti informací. Tato reaktivní opatření musí příslušnému orgánu umožnit:

1) iniciovat reakci své vlastní organizace na varování uvedená v písm. a) bodě 2 aktivací předem definovaných zdrojů a postupů;

2) omezit šíření útoku a zabránit úplnému naplnění scénáře hrozby;

3) kontrolovat poruchový režim dotčených prvků definovaných v bodě IS.AR.205 písm. a).

c) Příslušný orgán zavede opatření zaměřená na zotavení se z incidentů v oblasti bezpečnosti informací, včetně případných mimořádných opatření. Tato opatření k zotavení umožňují příslušnému orgánu:

1) odstranit stav, který incident způsobil, nebo jej omezit na únosnou míru;

2) obnovit bezpečný stav dotčených prvků definovaných v bodě IS.AR.205 písm. a) během doby obnovy předem stanovené vlastní organizací.

**IS.AR.220 Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací**

Příslušný orgán zajistí, aby při zadávání jakékoli části činností uvedených v bodě IS.AR.200 jiným organizacím byly smluvní činnosti v souladu s požadavky tohoto nařízení a aby smluvní organizace pracovala pod jeho dozorem. Příslušný orgán zajistí, aby rizika spojená se smluvními činnostmi byla vhodně řízena.

**IS.AR.225 Požadavky na personál**

Příslušný orgán:

a) má osobu, která je oprávněna vytvářet a udržovat organizační struktury, politiky, procesy a postupy nezbytné k provádění tohoto nařízení.

Tato osoba:

1) má oprávnění k úplnému přístupu ke zdrojům, které příslušný orgán potřebuje k plnění všech úkolů požadovaných tímto nařízením;

2) má přenesené pravomoci potřebné k výkonu přidělených úkolů;

b) má zaveden proces, který zajistí, aby měla ve službě dostatečný počet pracovníků za účelem provádění činností, na něž se vztahuje tato příloha;

c) má zaveden proces, který zajistí, aby pracovníci uvedení v písmenu b) měli k plnění svých úkolů nezbytnou způsobilost;

d) má zaveden proces, který zajistí, aby pracovníci uznali povinnosti spojené s přidělenými úlohami a úkoly;

e) zajistí, aby byla náležitě prokázána totožnost a důvěryhodnost pracovníků, kteří mají přístup k informačním systémům a údajům, na něž se vztahují požadavky tohoto nařízení.

**IS.AR.230 Vedení záznamů**

a) Příslušný orgán vede záznamy o svých činnostech v oblasti řízení bezpečnosti informací.

1) Příslušný orgán zajistí, aby byly archivovány a byly vysledovatelné tyto záznamy:

i) smlouvy na činnosti uvedené v bodě IS.AR.200 písm. a) bodě 5;

ii) záznamy o klíčových procesech uvedených v bodě IS.AR.200 písm. d);

iii) záznamy o rizicích identifikovaných v posouzení rizik uvedeném v bodě IS.AR.205 spolu se souvisejícími opatřeními k řešení rizik uvedenými v bodě IS.AR.210;

iv) záznamy o událostech bezpečnosti informací, které může být třeba znovu posoudit, aby se odhalily nezjištěné incidenty nebo zranitelnosti bezpečnosti informací.

2) Záznamy uvedené v bodě 1 podbodě i) se uchovávají nejméně po dobu pěti let poté, co byla smlouva pozměněna nebo ukončena.

3) Záznamy uvedené v bodě 1 podbodech ii) a iii) se uchovávají nejméně po dobu pěti let.

4) Záznamy uvedené v bodě 1 podbodě iv) se uchovávají do té doby, než budou uvedené události bezpečnosti informací znovu posouzeny v souladu s periodicitou vymezenou v postupu stanoveném příslušným orgánem.

b) Příslušný orgán vede záznamy o kvalifikaci a zkušenostech svých zaměstnanců zapojených do činností v oblasti řízení bezpečnosti informací.

1) Záznamy o kvalifikaci a zkušenostech pracovníků se uchovávají po dobu, po kterou daná osoba pracuje pro příslušný orgán, a po dobu alespoň tří let poté, co daná osoba příslušný orgán opustila.

2) Pracovníkům se na jejich žádost poskytne přístup k jejich individuálním záznamům. Kromě toho jim příslušný orgán na jejich žádost poskytne kopii jejich individuálních záznamů při odchodu z příslušného orgánu.

c) Formát záznamů je upřesněn v postupech příslušného orgánu.

d) Záznamy jsou uchovávány způsobem zajišťujícím jejich ochranu před poškozením, pozměňováním a krádeží, přičemž informace se, je-li to vyžadováno, identifikují podle svého stupně utajení. Příslušný orgán zajistí, aby záznamy byly uchovávány za použití prostředků, které zajistí integritu, pravost a oprávněný přístup. information being identified, when required, according to its security classification level.

**IS.AR.235 Soustavné zlepšování**

a) Příslušný orgán pomocí vhodných ukazatelů výkonnosti posoudí účinnost a vyspělost svého vlastního ISMS. Hodnocení se provádí na předem definovaném kalendářním základě vymezeném příslušným orgánem nebo po incidentu v oblasti bezpečnosti informací.

b) Pokud jsou po posouzení provedeném podle písmene a) zjištěny nedostatky, přijme příslušný orgán nezbytná opatření ke zlepšení, aby zajistil, že systém ISMS bude i nadále splňovat platné požadavky a udrží rizika v oblasti bezpečnosti informací na přijatelné úrovni. Kromě toho příslušný orgán znovu posoudí ty prvky systému ISMS, na které mají přijatá opatření vliv.

*PŘÍLOHA II*

**BEZPEČNOST INFORMACÍ – POŽADAVKY ORGANIZACE**

**[ČÁST-IS.I.OR]**



**IS.I.OR.100 Oblast působnosti**

Tato část stanoví požadavky, které musí splňovat organizace uvedené v čl. 2 odst. 1 tohoto nařízení.

**IS.I.OR.200 Systém řízení bezpečnosti informací (ISMS)**

a) Za účelem dosažení cílů stanovených v článku 1 organizace vytvoří, zavede a udržuje systém řízení bezpečnosti informací (ISMS), který zajistí, že organizace:

   1) stanoví politiku bezpečnosti informací, která určí celkové zásady organizace s ohledem na možný dopad rizik bezpečnosti informací na bezpečnost letectví;

   2) identifikuje a přezkoumává rizika bezpečnosti informací v souladu s bodem IS.I.OR.205;

   3) definuje a provádí opatření k řešení rizik bezpečnosti informací v souladu s bodem IS.I.OR.210;

   4) zavede systém interního hlášení v oblasti bezpečnosti informací v souladu s bodem IS.I.OR.215;

   5) definuje a provede v souladu s bodem IS.I.OR.220 opatření potřebná k odhalování událostí v oblasti bezpečnosti informací, určuje události, které jsou považovány za incidenty s možným dopadem na bezpečnost letectví, s výjimkou případů povolených v bodě IS.I.OR.205 písm. e), reaguje na tyto incidenty v oblasti bezpečnosti informací a odstraňuje jejich následky;

6) provádí opatření, která příslušný orgán oznámil jako okamžitou reakci na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví;

7) přijme vhodná opatření v souladu s bodem IS.I.OR.225 k řešení zjištění oznámených příslušným orgánem;

8) zavede systém externího hlášení v souladu s bodem IS.I.OR.230, aby mohl příslušný orgán přijmout vhodná opatření;

9) dodržuje požadavky obsažené v bodě IS.I.OR.235, pokud zadává jakoukoli část činností uvedených v bodě IS.I.OR.200 jiným organizacím;

10) splňuje požadavky na zaměstnance stanovené v bodě IS.I.OR.240;

11) splňuje požadavky na vedení záznamů stanovené v bodě IS.I.OR.245;

12) sleduje, jak organizace plní požadavky tohoto nařízení a poskytuje zpětnou vazbu o zjištěních odpovědnému vedoucímu pracovníkovi, aby zajistil účinné provádění nápravných opatření;

13) chrání, aniž by byly dotčeny platné požadavky na hlášení incidentů, důvěrnost všech informací, které organizace mohla obdržet od jiných organizací, a to podle úrovně jejich citlivosti.

b) Za účelem trvalého plnění požadavků uvedených v článku 1 musí organizace zavést proces trvalého zlepšování v souladu s bodem IS.I.OR.260.

c) Organizace musí v souladu s bodem IS.I.OR.250 zdokumentovat všechny klíčové procesy, postupy, role a odpovědnosti požadované pro splnění bodu IS.I.OR.200 písm. a) a musí zavést proces pro změnu této dokumentace. Změny těchto procesů, postupů, rolí a odpovědností se řídí podle bodu IS.I.OR.255.

d) Procesy, postupy, úlohy a povinnosti zavedené organizací za účelem dosažení souladu s bodem IS.I.OR.200 písm. a) musí odpovídat povaze a složitosti jejích činností na základě posouzení rizik bezpečnosti informací spojených s uvedenými činnostmi a mohou být začleněny do jiných stávajících systémů řízení, které již organizace provádí.

e) Aniž je dotčena povinnost dodržovat požadavky týkající se hlášení uvedené v nařízení (EU) č. 376/2014 a požadavky bodu IS.I.OR.200 písm. a) bodu 13, může příslušný úřad organizaci udělit oprávnění neprovádět požadavky uvedené v písmenech a) až d) a související požadavky uvedené v bodech IS.I.OR.205 až IS.I.OR.260, pokud ke spokojenosti uvedeného úřadu prokáže, že její činnosti, zařízení a zdroje, jakož i služby, které provozuje, poskytuje, přijímá a udržuje, nepředstavují ani pro ni, ani pro jiné organizace žádná rizika bezpečnosti informací s potenciálním dopadem na bezpečnost letectví. Schválení musí vycházet z dokumentovaného posouzení rizik bezpečnosti informací, které provede organizace nebo třetí strana v souladu s bodem IS.I.OR.205 a které přezkoumá a schválí její příslušný orgán.

Platnost tohoto schválení bude přezkoumána příslušným orgánem v návaznosti na příslušný cyklus dozorových auditů a vždy, když dojde ke změnám v rozsahu činnosti organizace.

**IS.I.OR.205 Posouzení rizik bezpečnosti informací**

a) Organizace identifikuje všechny své prvky, které by mohly být vystaveny rizikům bezpečnosti informací. Patří sem:

1) činnosti, zařízení a zdroje organizace, jakož i služby, které organizace provozuje, poskytuje, přijímá nebo udržuje;

2) vybavení, systémy, údaje a informace, které přispívají k fungování prvků uvedených v bodě 1.

b) Organizace identifikuje rozhraní, která má s jinými organizacemi a která by mohla vést k vzájemné expozici rizikům v oblasti bezpečnosti informací.

c) S ohledem na prvky a rozhraní uvedené v písmenech a) a b) organizace identifikuje rizika v oblasti bezpečnosti informací, která mohou mít možný dopad na bezpečnost letectví. Pro každé identifikované riziko organizace:

1) přiřadí úroveň rizika podle předem definované klasifikace, kterou si stanovila;

2) přiřadí každé riziko a jeho úroveň odpovídajícímu prvku nebo rozhraní identifikovanému podle písmen a) a b).

Předem stanovená klasifikace uvedená v bodě 1 zohledňuje možnost výskytu scénáře hrozeb a závažnost jeho bezpečnostních důsledků. Na základě této klasifikace a s přihlédnutím k tomu, zda má organizace strukturovaný a opakovatelný proces řízení rizik pro svůj provoz, musí být schopna stanovit, zda je riziko přijatelné, nebo zda je třeba s ním zacházet v souladu s bodem IS.I.OR.210.

V zájmu usnadnění vzájemné srovnatelnosti hodnocení rizik se při přidělování úrovně rizika podle bodu 1 zohlední příslušné informace získané v koordinaci s organizacemi uvedenými v písmenu b).

d) Organizace přezkoumá a aktualizuje posouzení rizik provedené podle písmen a), b) a případně podle písmen c) nebo e) v kterékoli z následujících situací:

1) dojde ke změně prvků, na které se vztahují rizika v oblasti bezpečnosti informací;

2) dojde ke změně rozhraní mezi organizací a ostatními organizacemi nebo ke změně rizik, o kterém ostatní organizace informují;

3) dojde ke změně informací nebo znalostí používaných pro identifikaci, analýzu a klasifikaci rizik;

4) z analýzy incidentů v oblasti bezpečnosti informací vyplývají poučení.

e) Odchylně od písmene c) nahradí organizace, které musí splňovat požadavky hlavy C přílohy III (část ATM/ANS.OR) prováděcího nařízení (EU) 2017/373, analýzu dopadu na bezpečnost letectví analýzou dopadu na své služby podle posouzení podpory bezpečnosti požadovaného v bodě ATM/ANS.OR.C.005. Toto posouzení podpory bezpečnosti se zpřístupní poskytovatelům letových provozních služeb, kterým poskytují služby, a tito poskytovatelé letových provozních služeb jsou odpovědní za vyhodnocení dopadu na bezpečnost letectví.

**IS.I.OR.210 Řešení rizik bezpečnosti informací**

a) Organizace vypracuje opatření k řešení nepřijatelných rizik zjištěných v souladu s bodem IS.I.OR.205, včas je provede a kontroluje jejich trvalou účinnost. Tato opatření musí organizaci umožnit:

1) kontrolovat okolnosti, které přispívají ke skutečnému výskytu scénáře hrozeb;

2) snížit důsledky pro bezpečnost letectví spojené s naplněním scénáře hrozeb;

3) vyhnout se rizikům.

Tato opatření nesmí přinést žádná nová možná nepřijatelná rizika pro bezpečnost letectví.

b) Osoba uvedená v bodě IS.I.OR.240 písm. a) a b) a ostatní dotčení pracovníci organizace musí být informováni o výsledku posouzení rizik provedeného v souladu s bodem IS.I.OR.205, o odpovídajících scénářích hrozeb a o opatřeních, která mají být provedena.

Organizace rovněž informuje organizace, s nimiž má rozhraní v souladu s bodem IS.I.OR.205 písm. b), o všech rizicích sdílených mezi oběma organizacemi.

**IS.I.OR.215 Systém interního hlášení v oblasti bezpečnosti informací**

a) Organizace vytvoří systém interního hlášení, který umožní shromažďování a vyhodnocování událostí v oblasti bezpečnosti informací, včetně těch, které mají být hlášeny podle bodu IS.I.OR.230.

b) Tento systém a postup uvedený v bodě IS.I.OR.220 umožní organizaci:

1) identifikovat, které z událostí oznámených podle písmene a) jsou považovány za incidenty nebo zranitelnosti v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví;

2) zjistit příčiny a faktory přispívající k incidentům a zranitelnostem v oblasti bezpečnosti informací zjištěným podle bodu 1 a řešit je v rámci procesu řízení rizik bezpečnosti informací v souladu s body IS.I.OR.205 a IS.I.OR.220;

3) zajistit vyhodnocení všech známých relevantních informací týkajících se incidentů a slabých míst v oblasti bezpečnosti informací zjištěných v souladu s bodem 1;

4) zajistit zavedení metody pro interní distribuci informací podle potřeby.

c) Každá smluvní organizace, která může organizaci vystavit rizikům v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, je povinna této organizaci hlásit události v oblasti bezpečnosti informací. Tato hlášení se předkládají podle postupů stanovených ve zvláštních smluvních ujednáních a vyhodnocují se v souladu s písmenem b).

d) Organizace spolupracuje při vyšetřování s jakoukoli jinou organizací, která významně přispívá k bezpečnosti informací v rámci své vlastní činnosti.

e) Organizace může tento systém podávání hlášení integrovat s jinými systémy podávání hlášení, které již zavedla.

**IS.I.OR.220 Incidenty bezpečnosti informací – odhalení, reakce a zotavení**

a) Na základě výsledku posouzení rizik provedeného podle bodu IS.I.OR.205 a výsledku ošetření rizik provedeného podle bodu IS.I.OR.210 organizace provede opatření k odhalování incidentů a zranitelností, které naznačují možné naplnění nepřijatelných rizik a které mohou mít možný dopad na bezpečnost letectví. Tato opatření pro odhalování musí organizaci umožnit:

1) zjistit odchylky od předem stanovených základních hodnot funkční výkonnosti;

2) spustit varování, aby se v případě jakékoli odchylky aktivovala vhodná opatření.

b) Organizace zavede opatření, která reagují na všechny podmínky události zjištěné v souladu s písmenem a), které se mohou rozvinout nebo se rozvinuly do incidentu v oblasti bezpečnosti informací. Tato reaktivní opatření musí organizaci umožnit:

1) zahájit reakci na varování uvedená v písmenu a) bodě 2 aktivací předem definovaných zdrojů a postupů;

2) omezit šíření útoku a zabránit úplnému naplnění scénáře hrozby;

3) kontrolovat poruchový režim dotčených prvků definovaných v bodě IS.I.OR.205 písm. a).

c) Organizace zavede opatření zaměřená na obnovu po incidentech v oblasti bezpečnosti informací, včetně případných mimořádných opatření. Tato opatření na obnovu musí organizaci umožnit:

1) odstranit stav, který incident způsobil, nebo jej omezit na únosnou míru;

2) dosáhnout bezpečného stavu dotčených prvků definovaných v bodě IS.I.OR.205 písm. a) v době obnovy předem stanovené organizací.

**IS.I.OR.225 Reakce na zjištění oznámená příslušným orgánem**

a) Po obdržení oznámení o zjištěních předloženého příslušným orgánem organizace:

1) zjistí hlavní příčinu nebo příčiny nesouladu a faktory, které k němu přispěly;

2) vytvoří plán nápravných opatření;

3) prokáže nápravu nesouladu ke spokojenosti příslušného orgánu.

b) Opatření uvedená v písmenu a) se provedou ve lhůtě dohodnuté s příslušným orgánem.

**IS.I.OR.230 Systém externího hlášení v oblasti bezpečnosti informací**

a) Organizace zavede systém podávání hlášení o bezpečnosti informací, který splňuje požadavky stanovené v nařízení (EU) č. 376/2014 a jeho aktech v přenesené pravomoci a prováděcích aktech, pokud se toto nařízení na organizaci vztahuje.

b) Aniž jsou dotčeny povinnosti vyplývající z nařízení (EU) č. 376/2014, organizace zajistí, aby každý incident nebo zranitelnost v oblasti bezpečnosti informací, které mohou představovat významné riziko pro bezpečnost letectví, byly oznámeny jejich příslušnému orgánu. Dále:

1) pokud se takový incident nebo zranitelnost týká letadla nebo přidruženého systému či konstrukční části, musí o tom organizace informovat také držitele schválení projektu;

2) pokud se takový incident nebo zranitelnost týká systému nebo prvku používaného organizací, organizace to oznámí organizaci odpovědné za návrh systému nebo prvku.

c) Organizace ohlásí podmínky uvedené v písmenu b) takto:

1) oznámení musí být předloženo příslušnému orgánu a případně držiteli schválení návrhu nebo organizaci odpovědné za návrh systému nebo prvku, jakmile se organizace o tomto stavu dozví;

2) hlášení musí být předloženo příslušnému orgánu a případně držiteli schválení projektu nebo organizaci odpovědné za projekt systému nebo prvku, a to co nejdříve, nejdéle však do 72 hodin od okamžiku, kdy se organizace o tomto stavu dozvěděla, pokud tomu nebrání výjimečné okolnosti.

Hlášení se podává ve formě stanovené příslušným orgánem a musí obsahovat všechny relevantní informace o stavu, které jsou organizaci známy;

3) příslušnému orgánu a případně držiteli schválení návrhu nebo organizaci odpovědné za návrh systému nebo prvku se předloží hlášení o následných opatřeních, v němž se uvedou podrobnosti o opatřeních, která organizace přijala nebo hodlá přijmout k nápravě po incidentu, a o opatřeních, která hodlá přijmout k předcházení podobným incidentům v oblasti bezpečnosti informací v budoucnosti.

Následné hlášení se předkládá, jakmile jsou tato opatření zjištěna, a vypracovává se ve formě stanovené příslušným orgánem.

**IS.I.OR.235 Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací**

a) Organizace zajistí, aby při zadávání jakékoli části činností uvedených v bodě IS.I.OR.200 jiným organizacím byly zadané činnosti v souladu s požadavky tohoto nařízení a aby organizace provádějící zadání pracovala pod jejím dozorem. Organizace zajistí, aby rizika spojená se smluvními činnostmi byla náležitě řízena.

b) Organizace zajistí, aby příslušný orgán mohl mít na požádání přístup do smluvní organizace, a mohl tak zjistit, zda jsou nadále plněny příslušné požadavky stanovené v tomto nařízení.

**IS.I.OR.240 Požadavky na personál**

a) Odpovědný vedoucí organizace určený v souladu s nařízeními (EU) č. 1321/2014, (EU) č. 965/2012, (EU) č. 1178/2011, (EU) 2015/340, prováděcím nařízením (EU) 2017/373 nebo prováděcím nařízením (EU) 2021/664, jak je uvedeno v čl. 2 odst. 1 tohoto nařízení, má podnikovou pravomoc zajistit, aby všechny činnosti požadované tímto nařízením mohly být financovány a prováděny. Tato osoba:

1) zajistí, aby byly k dispozici veškeré zdroje nezbytné ke splnění požadavků tohoto nařízení;

2) zavede a podporuje politiku bezpečnosti informací uvedenou v bodě IS.I.OR.200 písm. a) bodě 1;

3) prokáže základní porozumění tomuto nařízení.

b) Odpovědný vedoucí jmenuje osobu nebo skupinu osob, které zajistí, aby organizace splňovala požadavky tohoto nařízení, a vymezí rozsah jejich pravomoci. Tato osoba (nebo skupina osob) je podřízena přímo odpovědnému vedoucímu a má odpovídající znalosti, kvalifikaci a zkušenosti k plnění svých povinností. V postupech je určeno, kdo zastupuje určitou osobu v případě její dlouhodobé nepřítomnosti.

c) Odpovědný vedoucí jmenuje osobu nebo skupinu osob s odpovědností za řízení funkce sledování souladu uvedené v bodě IS.I.OR.200 písm. a) bodě 12.

d) Pokud organizace sdílí organizační struktury, politiky, procesy a postupy v oblasti bezpečnosti informací s jinými organizacemi nebo s částmi své vlastní organizace, na něž se nevztahuje oprávnění nebo prohlášení, může odpovědný vedoucí pověřit společnou odpovědnou osobu.

V takovém případě se stanoví koordinační opatření mezi odpovědným vedoucím organizace a společnou odpovědnou osobou s cílem zajistit odpovídající integraci řízení bezpečnosti informací v rámci organizace.

e) Odpovědný vedoucí nebo společná odpovědná osoba uvedená v písmenu d) má statutární pravomoc zavádět a udržovat organizační struktury, politiky, procesy a postupy nezbytné k provádění bodu IS.I.OR.200.

f) Organizace musí mít zaveden proces, který zajistí, aby měla ve službě dostatečný počet pracovníků za účelem provádění činností, na něž se vztahuje tato příloha.

g) Organizace musí mít zaveden proces, který zajistí, aby pracovníci uvedení v písmenu f) měli k plnění svých úkolů nezbytnou způsobilost.

h) Organizace musí mít zaveden postup, který zajistí, aby pracovníci uznali povinnosti spojené s přidělenými úlohami a úkoly.

i) Organizace zajistí, aby byla náležitě prokázána totožnost a důvěryhodnost pracovníků, kteří mají přístup k informačním systémům a údajům, na něž se vztahují požadavky tohoto nařízení.

**IS.I.OR.245 Vedení záznamů**

a) *Organizace vede záznamy o svých činnostech v oblasti řízení bezpečnosti informací*

1) Organizace zajistí, aby byly archivovány a byly vysledovatelné tyto záznamy:

i) veškerá obdržená oprávnění a veškerá související posouzení rizik bezpečnosti informací v souladu s bodem IS.I.OR.200 písm. e);

ii) smlouvy na činnosti uvedené v bodě IS.I.OR.200 písm. a) bodě 9;

iii) záznamy o klíčových procesech uvedených v bodě IS.I.OR.200 písm. d);

iv) záznamy o rizicích identifikovaných v posouzení rizik uvedeném v bodě IS.I.OR.205 spolu se souvisejícími opatřeními k řešení rizik uvedenými v bodě IS.I.OR.210;

v) záznamy o incidentech a zranitelnostech bezpečnosti informací hlášených v souladu se systémy hlášení uvedenými v bodech IS.I.OR.215 a IS.I.OR.230;

vi) záznamy o takových událostech bezpečnosti informací, které může být třeba znovu posoudit, aby se odhalily nezjištěné incidenty nebo zranitelnosti bezpečnosti informací.

2) Záznamy uvedené v bodě 1 podbodě i) se uchovávají nejméně po dobu pěti let poté, co oprávnění pozbylo platnosti.

3) Záznamy uvedené v bodě 1 podbodě ii) se uchovávají nejméně po dobu pěti let poté, co byla smlouva pozměněna nebo ukončena.

4) Záznamy uvedené v bodě 1 podbodech iii), iv) a v) se uchovávají nejméně po dobu pěti let.

5) Záznamy uvedené v bodě 1 podbodě vi) se uchovávají do té doby, než budou uvedené události bezpečnosti informací znovu posouzeny v souladu s periodicitou vymezenou v postupu stanoveném organizací.

b) *Organizace vede záznamy o kvalifikaci a zkušenostech vlastních zaměstnanců zapojených do činností řízení bezpečnosti informací*

1) Záznamy o kvalifikaci a zkušenostech pracovníků se uchovávají po dobu, po kterou daná osoba pracuje pro organizaci, a po dobu alespoň tří let poté, co daná osoba organizaci opustila.

2) Pracovníkům se na jejich žádost poskytne přístup k jejich individuálním záznamům. Kromě toho jim organizace na jejich žádost poskytne kopii jejich individuálních záznamů při odchodu z organizace.

c) Formát záznamů je upřesněn v postupech organizace.

d) Záznamy jsou uchovávány způsobem zajišťujícím jejich ochranu před poškozením, pozměňováním a krádeží, přičemž informace se, je-li to vyžadováno, identifikují podle svého stupně utajení. Organizace zajistí, aby záznamy byly uchovávány za použití prostředků, které zajistí integritu, pravost a oprávněný přístup. information being identified, when required, according to its security classification level.

**IS.I.OR.250 Příručka pro řízení bezpečnosti informací (ISMM)**

a) Organizace zpřístupní příslušnému úřadu příručku pro řízení bezpečnosti informací (ISMM) a v příslušných případech veškeré související příručky a postupy, na něž odkazuje, která obsahuje:

1) prohlášení podepsané odpovědným vedoucím, kterým se potvrzuje, že organizace bude svou činnost vždy vykonávat v souladu s touto přílohou a příručkou ISMM. Pokud odpovědný vedoucí pracovník není generálním ředitelem organizace, musí prohlášení spolupodepsat generální ředitel;

2) funkci (funkce), jméno (jména), úkoly, odpovědnosti, povinnosti a pravomoci osoby či osob uvedených v bodě IS.I.OR.240 písm. b) a c);

3) v příslušných případech funkci, jméno, úkoly, odpovědnosti, povinnosti a pravomoc společné odpovědné osoby definované v bodě IS.I.OR.240 písm. d);

4) politiku bezpečnosti informací organizace uvedenou v bodě IS.I.OR.200 písm. a) bodě 1;

5) obecný popis počtu a kategorií pracovníků a zavedeného systému plánování dostupnosti pracovníků, jak je požadováno v bodě IS.I.OR.240;

6) funkci (funkce), jméno (jména), úkoly, odpovědnosti, povinnosti a pravomoci klíčových osob odpovědných za provádění bodu IS.I.OR.200, včetně osoby nebo osob odpovědných za funkci sledování souladu uvedenou v bodě IS.I.OR.200 písm. a) bodě 12;

7) organizační schéma znázorňující související odpovědnostní vztahy mezi osobami uvedenými v bodech 2 a 6;

8) popis systému interního hlášení podle bodu IS.I.OR.215;

9) postupy upřesňující, jak organizace zajišťuje soulad s touto částí, a zejména:

i) dokumentaci uvedenou v bodě IS.I.OR.200 písm. c);

ii) postupy, které definují, jak organizace kontroluje všechny smluvní činnosti, jak je uvedeno v bodě IS.I.OR.200 písm. a) bodě 9;

iii) postup změny příručky ISMM uvedený v písmenu c);

10) podrobnosti o aktuálně schválených alternativních způsobech plnění předpisů.

b) První vydání příručky řízení bezpečnosti informací schvaluje a kopii si ponechá příslušný orgán. Příručka řízení bezpečnosti informací se mění podle potřeby tak, aby byla vždy aktuálním popisem systému ISMS organizace. Kopie všech změn příručky ISMM se poskytne příslušnému orgánu.

c) Změny příručky ISMM se řídí postupem stanoveným organizací. Změny, které nespadají do oblasti působnosti tohoto postupu, a změny týkající se změn uvedených v bodě IS.I.OR.255 písm. b) schvaluje příslušný orgán.

d) Organizace může integrovat příručku ISMM s jinými expozicemi nebo příručkami managementu, které má k dispozici, za předpokladu, že existuje jasný křížový odkaz, který uvádí, které části expozice nebo příručky managementu odpovídají jednotlivým požadavkům obsaženým v této příloze.

**IS.I.OR.255 Změny systému řízení bezpečnosti informací**

a) Změny systému ISMS mohou být řízeny a oznamovány příslušnému orgánu postupem, který organizace vypracuje. Tento postup schvaluje příslušný orgán.

b) Pokud jde o změny systému ISMS, na které se nevztahuje postup uvedený v písmenu a), musí organizace požádat o schválení vydané příslušným orgánem a získat ho.

Pokud jde o tyto změny:

1) Žádost o provedení změny musí být podána předtím, než k jakýmkoli takovým změnám dojde, aby příslušný orgán mohl určit, zda budou i nadále dodrženy požadavky tohoto nařízení a aby v případě potřeby mohl změnit osvědčení organizace a s ním spojené podmínky schválení;

2) organizace poskytne příslušnému orgánu veškeré informace, které si vyžádá k posouzení změny;

3) změna se provede až po získání formálního schválení příslušným orgánem;

4) během provádění těchto změn bude organizace svou činnost provozovat v souladu s platnými podmínkami, které jí příslušný orgán stanovil.

**IS.I.OR.260 Soustavné zlepšování**

a) Organizace musí pomocí vhodných ukazatelů výkonnosti hodnotit účinnost a vyspělost systému ISMS. Toto hodnocení se provádí na kalendářním základě předem stanoveném organizací nebo po incidentu v oblasti bezpečnosti informací.

b) Pokud jsou po posouzení provedeném podle písmene a) zjištěny nedostatky, přijme organizace nezbytná opatření ke zlepšení, aby zajistila, že systém ISMS bude i nadále splňovat platné požadavky a udrží rizika bezpečnosti informací na přijatelné úrovni. Kromě toho organizace přehodnotí ty prvky systému ISMS, které jsou přijatými opatřeními ovlivněny.

*PŘÍLOHA III*

Přílohy VI (část ARA) a VII (část ORA) nařízení (EU) č. 1178/2011 se mění takto:

1) příloha VI (část ARA) se mění takto:

a) v bodě ARA.GEN.125 se doplňuje nové písmeno c), které zní:

„c) Příslušný orgán členského státu poskytne agentuře co nejdříve informace důležité pro bezpečnost vyplývající z hlášení o bezpečnosti informací, které obdržel podle bodu IS.I.OR.230 přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203.“;

b) za bod ARA.GEN.135 se vkládá nový bod ARA.GEN.135A, který zní:

„**ARA.GEN.135A Okamžitá reakce na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví**

a) Příslušný orgán zavede systém pro náležité shromažďování, analýzu a šíření informací týkajících se incidentů a zranitelností v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, které organizace nahlásí. Tato činnost se provádí v koordinaci s dalšími příslušnými orgány odpovědnými za bezpečnost informací nebo kybernetickou bezpečnost v členském státě s cílem zvýšit koordinaci a kompatibilitu systémů podávání hlášení.

b) Agentura zavede systém, jehož prostřednictvím je možné náležitě analyzovat veškeré příslušné informace významné z hlediska bezpečnosti, které obdrží v souladu s bodem ARA.GEN.125 písm. c), a neprodleně členským státům a Komisi poskytovat veškeré informace, včetně doporučení nebo nápravných opatření, která je nutno přijmout a která jsou nezbytná k tomu, aby členské státy a Komise mohly včas reagovat na incident nebo zranitelnost v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví týkající se výrobků, letadlových částí, neinstalovaného zařízení, osob nebo organizací, na něž se vztahuje nařízení (EU) 2018/1139 a jeho akty v přenesené pravomoci a prováděcí akty.

c) Poté, co příslušný orgán obdrží informace uvedené v písmenech a) a b), přijme odpovídající opatření k řešení možného dopadu incidentu nebo zranitelnosti v oblasti ochrany informací na bezpečnost letectví.

d) O opatřeních přijatých podle písmene c) se neprodleně vyrozumí všechny osoby a organizace, které se podle nařízení (EU) 2018/1139 a jeho aktů v přenesené pravomoci a prováděcích aktů těmito opatřeními řídí. Příslušný orgán členského státu o těchto opatřeních vyrozumí rovněž agenturu a v případě, že je třeba, aby se na jejich uplatňování podílelo více členských států, vyrozumí i příslušné orgány dalších dotčených členských států.“;

c) v bodě ARA.GEN.200 se doplňuje nové písmeno e), které zní:

„e) Kromě požadavků uvedených v písmenu a) musí být systém řízení zavedený a udržovaný příslušným orgánem v souladu s přílohou I (část IS.AR) prováděcího nařízení (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“;

d) bod ARA.GEN.205 se mění takto:

i) nadpis se nahrazuje tímto:

„**ARA.GEN.205 Přidělování úkolů**“;

ii) doplňuje se nové písmeno c), které zní:

„c) Pokud jde o certifikaci a dozor nad dodržováním bodu ORA.GEN.200A ze strany organizace, může příslušný orgán přidělit úkoly kvalifikovaným subjektům podle písmene a) nebo jakémukoli příslušnému orgánu odpovědnému za bezpečnost informací nebo kybernetickou bezpečnost v členském státě. Při přidělování úkolů příslušný orgán zajistí, že:

1) všechny aspekty týkající se bezpečnosti letectví jsou koordinovány a zohledněny kvalifikovaným subjektem nebo příslušným orgánem;

2) výsledky certifikačních a dozorových činností prováděných kvalifikovaným subjektem nebo příslušným orgánem jsou začleněny do celkové certifikační a dozorové dokumentace organizace;

3) jeho vlastní systém řízení bezpečnosti informací zavedený v souladu s bodem ARA.GEN.200 písm. e) pokrývá všechny úkoly certifikace a průběžného dozoru prováděné jeho jménem.“;

e) v bodě ARA.GEN.300 se doplňuje nové písmeno g), které zní:

„g) Pokud jde o certifikaci a dozor nad dodržováním bodu ORA.GEN.200A ze strany organizace, musí příslušný orgán kromě dodržování písmen a) až f) přezkoumat každé schválení udělené podle bodu IS.I.OR.200 písm. e) tohoto nařízení nebo bodu IS.D.OR.200 písm. e) nařízení v přenesené pravomoci (EU) 2022/1645 po příslušném cyklu dozorových auditů a vždy, když dojde ke změnám v rozsahu činnosti organizace.“;

f) za bod ARA.GEN.330 se vkládá nový bod ARA.GEN.330A, který zní:

„**ARA.GEN.330A Změny systému řízení bezpečnosti informací**

a) Pokud jde o změny řízené a oznámené příslušnému orgánu v souladu s postupem stanoveným v bodě IS.I.OR.255 písm. a) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203, příslušný orgán zahrne přezkum těchto změn do svého průběžného dozoru v souladu se zásadami stanovenými v bodě ARA.GEN.300. Zjistí-li příslušný orgán jakýkoli nesoulad, oznámí to organizaci, vyžádá si další změny a jedná v souladu s bodem ARA.GEN.350.

b) Pokud jde o další změny vyžadující žádost o schválení podle bodu IS.I.OR.255 písm. b) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203:

1) po obdržení žádosti o změnu zkontroluje příslušný orgán před vydáním oprávnění, zda organizace splňuje příslušné požadavky;

2) příslušný orgán stanoví podmínky, za kterých může organizace během provádění změny fungovat;

3) dojde-li příslušný orgán k závěru, že organizace splňuje platné požadavky, změnu schválí.“;

2) příloha VII (část ORA) se mění takto:

Za bod ORA.GEN.200 se vkládá nový bod ORA.GEN.200A, který zní:

„**ORA.GEN.200A Systém řízení bezpečnosti informací**

Kromě systému řízení uvedeného v bodě ORA.GEN.200 musí organizace vytvořit, zavést a udržovat systém řízení bezpečnosti informací v souladu s prováděcím nařízením (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“

*PŘÍLOHA IV*

Příloha I (část 21) nařízení (EU) č. 748/2012 se mění takto:

1) Obsah se mění takto:

a) za nadpis 21.B.20 se vkládá nový nadpis, který zní:

„21.B.20A Okamžitá reakce na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví“;

b) nadpis bodu 21.B.30 se nahrazuje tímto:

„21.B.30 Přidělování úkolů“;

c) za nadpis 21.B.240 se vkládá nový nadpis, který zní:

„21.B.240A Změny systému řízení bezpečnosti informací“;

d) za nadpis 21.B.435 se vkládá nový nadpis, který zní:

„21.B.435A Změny systému řízení bezpečnosti informací“;

2) v bodě 21.B.15 se doplňuje nové písmeno c), které zní:

„c) Příslušný orgán členského státu poskytne agentuře co nejdříve informace důležité pro bezpečnost vyplývající z hlášení o bezpečnosti informací, které obdržel podle bodu IS.D.OR.230 přílohy (část IS.D.OR) nařízení v přenesené pravomoci (EU) 2022/1645.“;

3) za bod 21.B.20 se vkládá nový bod 21.B.20A, který zní:

**„21.B.20A Okamžitá reakce na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví**

a) Příslušný orgán zavede systém pro náležité shromažďování, analýzu a šíření informací týkajících se incidentů a zranitelností v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, které organizace nahlásí. Tato činnost se provádí v koordinaci s dalšími příslušnými orgány odpovědnými za bezpečnost informací nebo kybernetickou bezpečnost v členském státě s cílem zvýšit koordinaci a kompatibilitu systémů podávání hlášení.

b) Agentura zavede systém, jehož prostřednictvím je možné náležitě analyzovat veškeré příslušné informace významné z hlediska bezpečnosti, které obdrží v souladu s bodem 21.B.15 písm. c), a neprodleně členským státům a Komisi poskytovat veškeré informace, včetně doporučení nebo nápravných opatření, která je nutno přijmout a která jsou nezbytná k tomu, aby členské státy a Komise mohly včas reagovat na incident nebo zranitelnost v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví týkající se výrobků, letadlových částí, neinstalovaného zařízení, osob nebo organizací, na něž se vztahuje nařízení (EU) 2018/1139 a jeho akty v přenesené pravomoci a prováděcí akty.

c) Poté, co příslušný orgán obdrží informace uvedené v písmenech a) a b), přijme odpovídající opatření k řešení možného dopadu incidentu nebo zranitelnosti v oblasti ochrany informací na bezpečnost letectví.

d) O opatřeních přijatých podle písmene c) se neprodleně vyrozumí všechny osoby a organizace, které se podle nařízení (EU) 2018/1139 a jeho aktů v přenesené pravomoci a prováděcích aktů těmito opatřeními řídí. Příslušný orgán členského státu o těchto opatřeních vyrozumí rovněž agenturu a v případě, že je třeba, aby se na jejich uplatňování podílelo více členských států, vyrozumí i příslušné orgány dalších dotčených členských států.“;

4) v bodě 21.B.25 se doplňuje nové písmeno e), které zní:

„e) Kromě požadavků uvedených v písmenu a) musí být systém řízení zavedený a udržovaný příslušným orgánem v souladu s přílohou I (část IS.AR) prováděcího nařízení (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“;

5) bod 21.B.30 se mění takto:

a) nadpis se nahrazuje tímto:

**„21.B.30 Přidělování úkolů“;**

b) doplňuje se nové písmeno c), které zní:

„c) Pro certifikaci a dozor nad dodržováním bodů 21.A.139A a 21.A.239A ze strany organizace může příslušný orgán přidělit úkoly kvalifikovaným subjektům podle písmene a) nebo jakémukoli příslušnému orgánu odpovědnému za bezpečnost informací nebo kybernetickou bezpečnost v členském státě. Při přidělování úkolů příslušný orgán zajistí, že:

1) všechny aspekty týkající se bezpečnosti letectví jsou koordinovány a zohledněny kvalifikovaným subjektem nebo příslušným orgánem;

2) výsledky certifikačních a dozorových činností prováděných kvalifikovaným subjektem nebo příslušným orgánem jsou začleněny do celkové certifikační a dozorové dokumentace organizace;

3) jeho vlastní systém řízení bezpečnosti informací zavedený v souladu s bodem 21.B.25 písm. e) pokrývá všechny úkoly certifikace a průběžného dozoru prováděné jeho jménem.“;

6) v bodě 21.B.221 se doplňuje nové písmeno g), které zní:

„g) Pokud jde o certifikaci a dozor nad dodržováním bodu 21.A.139A ze strany organizace, musí příslušný orgán kromě dodržování písmen a) až f) přezkoumat každé schválení udělené podle bodu IS.I.OR.200 písm. e) tohoto nařízení nebo bodu IS.D.OR.200 písm. e) nařízení v přenesené pravomoci (EU) 2022/1645 po příslušném cyklu dozorových auditů a vždy, když dojde ke změnám v rozsahu činnosti organizace.“;

7) za bod 21.B.240 se vkládá nový bod 21.B.240A, který zní:

„**21.B.240A Změny systému řízení bezpečnosti informací**

a) V případě změn řízených a oznámených příslušnému orgánu v souladu s postupem stanoveným v bodě IS.D.OR.255 písm. a) přílohy (část IS.D.OR) nařízení v přenesené pravomoci (EU) 2022/1645 zahrne příslušný orgán přezkum těchto změn do svého průběžného dozoru v souladu se zásadami stanovenými v bodě 21.B.221. Zjistí-li příslušný orgán jakýkoli nesoulad, oznámí to organizaci, vyžádá si další změny a jedná v souladu s bodem 21.B.225.

b) Pro ostatní změny vyžadující žádost o schválení podle bodu IS.D.OR.255 písm. b) přílohy (část IS.D.OR) nařízení v přenesené pravomoci (EU) 2022/1645:

1) po obdržení žádosti o změnu zkontroluje příslušný orgán před vydáním oprávnění, zda organizace splňuje příslušné požadavky;

2) příslušný orgán stanoví podmínky, za kterých může organizace během provádění změny fungovat;

3) dojde-li příslušný orgán k závěru, že organizace splňuje platné požadavky, změnu schválí.“

8) v bodě bodu 21.B.431 se doplňuje nové písmeno d), které zní:

„d) Při certifikaci a dozoru nad dodržováním bodu 21.A.239A ze strany organizace musí příslušný orgán kromě dodržování písmen a) až c) dodržovat následující zásady:

1) příslušný orgán přezkoumá rozhraní a související rizika zjištěná v souladu s bodem IS.D.OR.205 písm. b) přílohy (část IS.D.OR) nařízení v přenesené pravomoci (EU) 2022/1645 každou organizací podléhající jeho dozoru;

2) pokud různé organizace zjistí nesrovnalosti ve vzájemných rozhraních a souvisejících rizicích, příslušný orgán je přezkoumá společně s dotčenými organizacemi a v případě potřeby předloží příslušná zjištění, aby zajistil provedení nápravných opatření;

3) pokud dokumentace přezkoumaná podle bodu 2 odhalí existenci významných rizik spojených s rozhraními s organizacemi podléhajícími dozoru jiného příslušného orgánu v rámci téhož členského státu, sdělí se tato informace odpovídajícímu příslušnému orgánu.“;

9) za bod 21.B.435 se vkládá nový bod 21.B.435A, který zní:

„**21.B.435A Změny systému řízení bezpečnosti informací**

a) V případě změn řízených a oznámených příslušnému orgánu v souladu s postupem stanoveným v bodě IS.D.OR.255 písm. a) přílohy (část IS.D.OR) nařízení v přenesené pravomoci (EU) 2022/1645 zahrne příslušný orgán přezkum těchto změn do svého průběžného dozoru v souladu se zásadami stanovenými v bodě 21.B.431. Zjistí-li příslušný orgán jakýkoli nesoulad, oznámí to organizaci, vyžádá si další změny a jedná v souladu s bodem 21.B.433.

b) Pro ostatní změny vyžadující žádost o schválení podle bodu IS.D.OR.255 písm. b) přílohy (část IS.D.OR) nařízení v přenesené pravomoci (EU) 2022/1645:

1) po obdržení žádosti o změnu zkontroluje příslušný orgán před vydáním oprávnění, zda organizace splňuje příslušné požadavky;

2) příslušný orgán stanoví podmínky, za kterých může organizace během provádění změny fungovat;

3) dojde-li příslušný orgán k závěru, že organizace splňuje platné požadavky, změnu schválí.“

*PŘÍLOHA V*

Přílohy II (část ARO) a III (část ORO) nařízení (EU) č. 965/2012 se mění takto:

1) příloha II (část ARO) se mění takto:

a) v bodě ARO.GEN.125 se doplňuje nové písmeno c), které zní:

„c) Příslušný orgán členského státu poskytne agentuře co nejdříve informace důležité pro bezpečnost vyplývající z hlášení o bezpečnosti informací, které obdržel podle bodu IS.I.OR.230 přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203.“;

b) za bod ARO.GEN.135 se vkládá nový bod ARO.GEN.135A, který zní:

„**ARO.GEN.135A Okamžitá reakce na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví**

a) Příslušný orgán zavede systém pro náležité shromažďování, analýzu a šíření informací týkajících se incidentů a zranitelností v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, které organizace nahlásí. Tato činnost se provádí v koordinaci s dalšími příslušnými orgány odpovědnými za bezpečnost informací nebo kybernetickou bezpečnost v členském státě s cílem zvýšit koordinaci a kompatibilitu systémů podávání hlášení.

b) Agentura zavede systém, jehož prostřednictvím je možné náležitě analyzovat veškeré příslušné informace významné z hlediska bezpečnosti, které obdrží v souladu s bodem ARO.GEN.125 písm. c), a neprodleně členským státům a Komisi poskytovat veškeré informace, včetně doporučení nebo nápravných opatření, která je nutno přijmout a která jsou nezbytná k tomu, aby členské státy a Komise mohly včas reagovat na incident nebo zranitelnost v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví týkající se výrobků, letadlových částí, neinstalovaného zařízení, osob nebo organizací, na něž se vztahuje nařízení (EU) 2018/1139 a jeho akty v přenesené pravomoci a prováděcí akty.

c) Poté, co příslušný orgán obdrží informace uvedené v písmenech a) a b), přijme odpovídající opatření pro řešení možného dopadu incidentu nebo zranitelnosti v oblasti ochrany informací na bezpečnost letectví.

d) O opatřeních přijatých podle písmene c) se neprodleně vyrozumí všechny osoby a organizace, které se podle nařízení (EU) 2018/1139 a jeho aktů v přenesené pravomoci a prováděcích aktů těmito opatřeními řídí. Příslušný orgán členského státu o těchto opatřeních vyrozumí rovněž agenturu a v případě, že je třeba, aby se na jejich uplatňování podílelo více členských států, vyrozumí i příslušné orgány dalších dotčených členských států.“;

c) v bodě ARO.GEN.200 se doplňuje nové písmeno e), které zní:

„e) Kromě požadavků uvedených v písmenu a) musí být systém řízení zavedený a udržovaný příslušným orgánem v souladu s přílohou I (část IS.AR) prováděcího nařízení (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“;

d) bod ARO.GEN.205 se mění takto:

i) nadpis se nahrazuje tímto:

„**ARO.GEN.205 Přidělování úkolů**“;

ii) doplňuje se nové písmeno c), které zní:

„c) Pro certifikaci a dozor nad dodržováním bodu ORO.GEN.200A ze strany organizace může příslušný orgán přidělit úkoly kvalifikovaným subjektům podle písmene a) nebo jakémukoli příslušnému orgánu odpovědnému za bezpečnost informací nebo kybernetickou bezpečnost v členském státě. Při přidělování úkolů příslušný orgán zajistí, že:

1) kvalifikovaným subjektem nebo příslušným orgánem jsou koordinovány a zohledněny všechny aspekty týkající se bezpečnosti letectví;

2) výsledky certifikačních a dozorových činností prováděných kvalifikovaným subjektem nebo příslušným orgánem jsou začleněny do celkové certifikační a dozorové dokumentace organizace;

3) jeho vlastní systém řízení bezpečnosti informací zavedený v souladu s bodem ARO.GEN.200 písm. e) pokrývá všechny úkoly certifikace a průběžného dozoru prováděné jeho jménem.“;

e) v bodě ARO.GEN.300 se doplňuje nové písmeno g), které zní:

„g) Pokud jde o certifikaci a dozor nad dodržováním bodu ORO.GEN.200A ze strany organizace, musí příslušný orgán kromě dodržování písmen a) až f) přezkoumat každé schválení udělené podle bodu IS.I.OR.200 písm. e) tohoto nařízení nebo bodu IS.D.OR.200 písm. e) nařízení v přenesené pravomoci (EU) 2022/1645 po příslušném cyklu dozorových auditů a vždy, když dojde ke změnám v rozsahu činnosti organizace.“;

f) za bod ARO.GEN.330 se vkládá nový bod ARO.GEN.330A, který zní:

„**ARO.GEN.330A Změny systému řízení bezpečnosti informací**

a) Pro změny řízené a oznámené příslušnému orgánu postupem stanoveným v bodě IS.I.OR.255 písm. a) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203, příslušný orgán zahrne přezkum těchto změn do svého průběžného dozoru v souladu se zásadami stanovenými v bodě ARO.GEN.300. Zjistí-li příslušný orgán jakýkoli nesoulad, oznámí to organizaci, vyžádá si další změny a jedná v souladu s bodem ARO.GEN.350.

b) Pro ostatní změny vyžadující žádost o schválení podle bodu IS.I.OR.255 písm. b) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203:

1) po obdržení žádosti o změnu zkontroluje příslušný orgán před vydáním oprávnění, zda organizace splňuje příslušné požadavky;

2) příslušný orgán stanoví podmínky, za kterých může organizace během provádění změny fungovat;

3) dojde-li příslušný orgán k závěru, že organizace splňuje platné požadavky, změnu schválí.“

2) příloha III (část ORO) se mění takto:

za bod ORO.GEN.200 se vkládá nový bod ORO.GEN.200A, který zní:

„**ORO.GEN.200A Systém řízení bezpečnosti informací**

Kromě systému řízení uvedeného v bodě ORO.GEN.200 provozovatel zřídí, zavede a udržuje systém řízení bezpečnosti informací v souladu s prováděcím nařízením (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“

*PŘÍLOHA VI*

Příloha II (část ADR.AR) nařízení (EU) č. 139/2014 se mění takto:

1) v bodě ADR.AR.A.025 se doplňuje nové písmeno c), které zní:

„c) Příslušný orgán členského státu poskytne agentuře co nejdříve informace důležité pro bezpečnost vyplývající z hlášení o bezpečnosti informací, které obdržel podle bodu IS.D.OR.230 přílohy (část IS.D.OR) nařízení v přenesené pravomoci (EU) 2022/1645.“;

2) za bod ADR.AR.A.030 se vkládá nový bod ADR.AR.A.030A, který zní:

„**ADR.AR.A.030A Okamžitá reakce na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví**

a) Příslušný orgán zavede systém pro náležité shromažďování, analýzu a šíření informací týkajících se incidentů a zranitelností v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, které organizace nahlásí. Tato činnost se provádí v koordinaci s dalšími příslušnými orgány odpovědnými za bezpečnost informací nebo kybernetickou bezpečnost v členském státě s cílem zvýšit koordinaci a kompatibilitu systémů podávání hlášení.

b) Agentura zavede systém, jehož prostřednictvím je možné náležitě analyzovat veškeré příslušné informace významné z hlediska bezpečnosti, které obdrží v souladu s bodem ADR.AR.A.025 písm. c), a neprodleně členským státům a Komisi poskytovat veškeré informace, včetně doporučení nebo nápravných opatření, která je nutno přijmout a která jsou nezbytná k tomu, aby členské státy a Komise mohly včas reagovat na incident nebo zranitelnost v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví týkající se výrobků, letadlových částí, neinstalovaného zařízení, osob nebo organizací, na něž se vztahuje nařízení (EU) 2018/1139 a jeho akty v přenesené pravomoci a prováděcí akty.

c) Poté, co příslušný orgán obdrží informace uvedené v písmenech a) a b), přijme odpovídající opatření pro řešení možného dopadu incidentu nebo zranitelnosti v oblasti ochrany informací na bezpečnost letectví.

d) O opatřeních přijatých podle písmene c) se neprodleně vyrozumí všechny osoby a organizace, které se podle nařízení (EU) 2018/1139 a jeho aktů v přenesené pravomoci a prováděcích aktů těmito opatřeními řídí. Příslušný orgán členského státu o těchto opatřeních vyrozumí rovněž agenturu a v případě, že je třeba, aby se na jejich uplatňování podílelo více členských států, vyrozumí i příslušné orgány dalších dotčených členských států.“;

3) v bodě bodu ADR.AR.B.005 se doplňuje nové písmeno d), které zní:

„d) Kromě požadavků uvedených v písmenu a) musí být systém řízení zavedený a udržovaný příslušným orgánem v souladu s přílohou I (část IS.AR) prováděcího nařízení (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“;

4) bod ADR.AR.B.010 se mění takto:

i) nadpis se nahrazuje tímto:

„**ADR.AR.B.010 Přidělování úkolů**“;

ii) doplňuje se nové písmeno c), které zní:

„c) Pokud jde o certifikaci a dozor nad dodržováním bodu ADR.OR.D.005A ze strany organizace, může příslušný orgán přidělit úkoly kvalifikovaným subjektům podle písmene a) nebo jakémukoli příslušnému orgánu odpovědnému za bezpečnost informací nebo kybernetickou bezpečnost v členském státě. Při přidělování úkolů příslušný orgán zajistí, že:

1) kvalifikovaným subjektem nebo příslušným orgánem jsou koordinovány a zohledněny všechny aspekty týkající se bezpečnosti letectví;

2) výsledky certifikačních a dozorových činností prováděných kvalifikovaným subjektem nebo příslušným orgánem jsou začleněny do celkové certifikační a dozorové dokumentace organizace;

3) jeho vlastní systém řízení bezpečnosti informací zavedený v souladu s bodem ADR.AR.B.005 písm. e) pokrývá všechny úkoly certifikace a průběžného dozoru prováděné jeho jménem.“;

5) v bodě ADR.AR.C.005 se doplňuje nové písmeno f), které zní:

„f) Pokud jde o certifikaci a dozor nad dodržováním bodu ADR.OR.D.005A ze strany organizace, musí příslušný orgán kromě dodržování písmen a) až f) přezkoumat každé schválení udělené podle bodu IS.I.OR.200 písm. e) tohoto nařízení nebo bodu IS.D.OR.200 písm. e) nařízení v přenesené pravomoci (EU) 2022/1645 po příslušném cyklu dozorových auditů a vždy, když dojde ke změnám v rozsahu činnosti organizace.“;

6) za bod ADR.AR.C.040 se vkládá nový bod ADR.AR.C.040A, který zní:

„**ADR.AR.C.040A Změny systému řízení bezpečnosti informací**

a) V případě změn řízených a oznámených příslušnému orgánu v souladu s postupem stanoveným v bodě IS.D.OR.255 písm. a) přílohy (část IS.D.OR) nařízení v přenesené pravomoci (EU) 2022/1645 zahrne příslušný orgán přezkum těchto změn do svého průběžného dozoru v souladu se zásadami stanovenými v bodě ADR.AR.C.005. Zjistí-li příslušný orgán jakýkoli nesoulad, oznámí to organizaci, vyžádá si další změny a jedná v souladu s bodem ADR.AR.C.055.

b) V případě ostatních změn vyžadujících žádost o schválení podle bodu IS.D.OR.255 písm. b) přílohy (část IS.D.OR) nařízení v přenesené pravomoci (EU) 2022/1645:

1) po obdržení žádosti o změnu zkontroluje příslušný orgán před vydáním oprávnění, zda organizace splňuje příslušné požadavky;

2) příslušný orgán stanoví podmínky, za kterých může organizace během provádění změny fungovat;

3) dojde-li příslušný orgán k závěru, že organizace splňuje platné požadavky, změnu schválí.“

*PŘÍLOHA VII*

Přílohy II (část 145), III (část 66) a Vc (část CAMO) nařízení (EU) č. 1321/2014 se mění takto:

1) Příloha II (část 145) se mění takto:

a) Obsah se mění takto:

i) za nadpis 145.A.200 se vkládá nový nadpis, který zní:

„145.A.200A Systém řízení bezpečnosti informací“;

ii) za nadpis 145.B.135 se vkládá nový nadpis, který zní:

„145.B.135A Okamžitá reakce na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví“;

iii) nadpis bodu 145.B.205 se nahrazuje tímto:

„145.B.205 Přidělování úkolů“;

iv) za nadpis 145.B.330 se vkládá nový nadpis, který zní:

„145.B.330A Změny systému řízení bezpečnosti informací“;

b) za bod 145.A.200 se vkládá nový bod 145.A.200A, který zní:

„145.A.200A **Systém řízení bezpečnosti informací**

Kromě systému řízení uvedeného v bodě 145.A.200 organizace údržby zavede, uplatňuje a udržuje systém řízení bezpečnosti informací v souladu s prováděcím nařízením (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“;

c) v bodě 145.B.125 se doplňuje nové písmeno c), které zní:

„c) Příslušný orgán členského státu poskytne agentuře co nejdříve informace důležité pro bezpečnost vyplývající z hlášení o bezpečnosti informací, které obdržel podle bodu IS.I.OR.230 přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203.“;

d) za bod 145.B.135 se vkládá nový bod 145.B.135A, který zní:

„145.B.135A **Okamžitá reakce na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví**

a) Příslušný orgán zavede systém pro náležité shromažďování, analýzu a šíření informací týkajících se incidentů a zranitelností v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, které organizace nahlásí. Tato činnost se provádí v koordinaci s dalšími příslušnými orgány odpovědnými za bezpečnost informací nebo kybernetickou bezpečnost v členském státě s cílem zvýšit koordinaci a kompatibilitu systémů podávání hlášení.

b) Agentura zavede systém, jehož prostřednictvím je možné náležitě analyzovat veškeré příslušné informace významné z hlediska bezpečnosti, které obdrží v souladu s bodem 145.B.125 písm. c), a neprodleně členským státům a Komisi poskytovat veškeré informace, včetně doporučení nebo nápravných opatření, která je nutno přijmout a která jsou nezbytná k tomu, aby členské státy a Komise mohly včas reagovat na incident nebo zranitelnost v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví týkající se výrobků, letadlových částí, neinstalovaného zařízení, osob nebo organizací, na něž se vztahuje nařízení (EU) 2018/1139 a jeho akty v přenesené pravomoci a prováděcí akty.

c) Poté, co příslušný orgán obdrží informace uvedené v písmenech a) a b), přijme odpovídající opatření k řešení možného dopadu incidentu nebo zranitelnosti v oblasti ochrany informací na bezpečnost letectví.

d) O opatřeních přijatých podle písmene c) se neprodleně vyrozumí všechny osoby a organizace, které se podle nařízení (EU) 2018/1139 a jeho aktů v přenesené pravomoci a prováděcích aktů těmito opatřeními řídí. Příslušný orgán členského státu o těchto opatřeních vyrozumí rovněž agenturu a v případě, že je třeba, aby se na jejich uplatňování podílelo více členských států, vyrozumí i příslušné orgány dalších dotčených členských států.“;

e) v bodě 145.B.200 se doplňuje nové písmeno e), které zní:

„e) Kromě požadavků uvedených v písmenu a) musí být systém řízení zavedený a udržovaný příslušným orgánem v souladu s přílohou I (část IS.AR) prováděcího nařízení (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“;

f) bod 145.B.205 se mění takto:

i) nadpis se nahrazuje tímto:

„145.B.205 **Přidělování úkolů**“;

ii) doplňuje se nové písmeno c), které zní:

„c) Pro certifikaci a dozor nad dodržováním bodu 145.A.200A ze strany organizace může příslušný orgán přidělit úkoly kvalifikovaným subjektům podle písmene a) nebo jakémukoli příslušnému orgánu odpovědnému za bezpečnost informací nebo kybernetickou bezpečnost v členském státě. Při přidělování úkolů příslušný orgán zajistí, že:

1) kvalifikovaným subjektem nebo příslušným orgánem jsou koordinovány a zohledněny všechny aspekty týkající se bezpečnosti letectví;

2) výsledky certifikačních a dozorových činností prováděných kvalifikovaným subjektem nebo příslušným orgánem jsou začleněny do celkové certifikační a dozorové dokumentace organizace;

3) jeho vlastní systém řízení bezpečnosti informací zavedený v souladu s bodem 145.B.200 písm. e) pokrývá všechny úkoly certifikace a průběžného dozoru prováděné jeho jménem.“;

g) v bodě 145.B.300 se doplňuje nové písmeno g), které zní:

„g) Pokud jde o certifikaci a dozor nad dodržováním bodu 145.A.200A ze strany organizace, musí příslušný orgán kromě dodržování písmen a) až f) přezkoumat každé schválení udělené podle bodu IS.I.OR.200 písm. e) tohoto nařízení nebo bodu IS.D.OR.200 písm. e) nařízení v přenesené pravomoci (EU) 2022/1645 po příslušném cyklu dozorových auditů a vždy, když dojde ke změnám v rozsahu činnosti organizace.“;

h) za bod 145.B.330 se vkládá nový bod 145.B.330A, který zní:

„145.B.330A **Změny systému řízení bezpečnosti informací**

a) Pro změny řízené a oznámené příslušnému orgánu postupem stanoveným v bodě IS.I.OR.255 písm. a) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203, příslušný orgán zahrne přezkum těchto změn do svého průběžného dozoru v souladu se zásadami stanovenými v bodě 145.B.300. Zjistí-li příslušný orgán jakýkoli nesoulad, oznámí to organizaci, vyžádá si další změny a jedná v souladu s bodem 145.B.350.

b) Pro ostatní změny vyžadující žádost o schválení podle bodu IS.I.OR.255 písm. b) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203:

1) po obdržení žádosti o změnu zkontroluje příslušný orgán před vydáním oprávnění, zda organizace splňuje příslušné požadavky;

2) příslušný orgán stanoví podmínky, za kterých může organizace během provádění změny fungovat;

3) dojde-li příslušný orgán k závěru, že organizace splňuje platné požadavky, změnu schválí.“

2) Příloha III (část 66) se mění takto:

a) v obsahu se za nadpis 66.B.10 vkládá nový nadpis, který zní:

„66.B.15 Systém řízení bezpečnosti informací“;

b) za bod 66.B.10 se vkládá nový bod 66.B.15, který zní:

„66.B.15 **Systém řízení bezpečnosti informací**

Příslušný orgán zřídí, zavede a udržuje systém řízení bezpečnosti informací v souladu s přílohou I (část IS.AR) prováděcího nařízení (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“

3) Příloha Vc (část CAMO) se mění takto:

a) Obsah se mění takto:

i) za nadpis CAMO.A.200 se vkládá nový nadpis, který zní:

„CAMO.A.200A Systém řízení bezpečnosti informací“;

ii) za nadpis CAMO.B.135 se vkládá nový nadpis, který zní:

„CAMO.B.135A Okamžitá reakce na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví“;

iii) nadpis bodu CAMO.B.205 se nahrazuje tímto:

„CAMO.B.205 Přidělování úkolů“;

iv) za nadpis CAMO.B.330 se vkládá nový nadpis, který zní:

„CAMO.B.330A Změny systému řízení bezpečnosti informací“;

b) za bod CAMO.A.200 se vkládá nový bod CAMO.A.200A, který zní:

„CAMO.A.200A **Systém řízení bezpečnosti informací**

Kromě systému řízení uvedeného v bodě CAMO.A.200 musí organizace vytvořit, zavést a udržovat systém řízení bezpečnosti informací v souladu s prováděcím nařízením (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“;

c) v bodě CAMO.B.125 se doplňuje nové písmeno c), které zní:

„c) Příslušný orgán členského státu poskytne agentuře co nejdříve informace důležité pro bezpečnost vyplývající z hlášení o bezpečnosti informací, které obdržel podle bodu IS.I.OR.230 přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203.“;

d) za bod CAMO.B.135 se vkládá nový bod CAMO.B.135A, který zní:

„CAMO.B.135A **Okamžitá reakce na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví**

a) Příslušný orgán zavede systém pro náležité shromažďování, analýzu a šíření informací týkajících se incidentů a zranitelností v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, které organizace nahlásí. Tato činnost se provádí v koordinaci s dalšími příslušnými orgány odpovědnými za bezpečnost informací nebo kybernetickou bezpečnost v členském státě s cílem zvýšit koordinaci a kompatibilitu systémů podávání hlášení.

b) Agentura zavede systém, jehož prostřednictvím je možné náležitě analyzovat veškeré příslušné informace významné z hlediska bezpečnosti, které obdrží v souladu s bodem CAMO.B.125 písm. c), a neprodleně členským státům a Komisi poskytovat veškeré informace, včetně doporučení nebo nápravných opatření, která je nutno přijmout a která jsou nezbytná k tomu, aby členské státy a Komise mohly včas reagovat na incident nebo zranitelnost v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví týkající se výrobků, letadlových částí, neinstalovaného zařízení, osob nebo organizací, na něž se vztahuje nařízení (EU) 2018/1139 a jeho akty v přenesené pravomoci a prováděcí akty.

c) Poté, co příslušný orgán obdrží informace uvedené v písmenech a) a b), přijme odpovídající opatření pro řešení možného dopadu incidentu nebo zranitelnosti v oblasti ochrany informací na bezpečnost letectví.

d) O opatřeních přijatých podle písmene c) se neprodleně vyrozumí všechny osoby a organizace, které se podle nařízení (EU) 2018/1139 a jeho aktů v přenesené pravomoci a prováděcích aktů těmito opatřeními řídí. Příslušný orgán členského státu o těchto opatřeních vyrozumí rovněž agenturu a v případě, že je třeba, aby se na jejich uplatňování podílelo více členských států, vyrozumí i příslušné orgány dalších dotčených členských států.“;

e) v bodě CAMO.B.200 se doplňuje nové písmeno e), které zní:

„e) Kromě požadavků uvedených v písmenu a) musí být systém řízení zavedený a udržovaný příslušným orgánem v souladu s přílohou I (část IS.AR) prováděcího nařízení (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“;

f) bod CAMO.B.205 se mění takto:

i) nadpis se nahrazuje tímto:

„CAMO.B.205 **Přidělování úkolů**“;

ii) doplňuje se nové písmeno c), které zní:

„c) Pokud jde o certifikaci a dozor nad dodržováním bodu CAMO.A.200A ze strany organizace, může příslušný orgán přidělit úkoly kvalifikovaným subjektům podle písmene a) nebo jakémukoli příslušnému orgánu odpovědnému za bezpečnost informací nebo kybernetickou bezpečnost v členském státě. Při přidělování úkolů příslušný orgán zajistí, že:

1) kvalifikovaným subjektem nebo příslušným orgánem jsou koordinovány a zohledněny všechny aspekty týkající se bezpečnosti letectví;

2) výsledky certifikačních a dozorových činností prováděných kvalifikovaným subjektem nebo příslušným orgánem jsou začleněny do celkové certifikační a dozorové dokumentace organizace;

3) jeho vlastní systém řízení bezpečnosti informací zavedený v souladu s bodem CAMO.B.200 písm. e) pokrývá všechny úkoly certifikace a průběžného dozoru prováděné jeho jménem.“;

g) v bodě CAMO.B.300 se doplňuje nové písmeno g), které zní:

„g) Pokud jde o certifikaci a dozor nad dodržováním bodu CAMO.A.200A ze strany organizace, musí příslušný orgán kromě dodržování písmen a) až f) přezkoumat každé schválení udělené podle bodu IS.I.OR.200 písm. e) tohoto nařízení nebo bodu IS.D.OR.200 písm. e) nařízení v přenesené pravomoci (EU) 2022/1645 po příslušném cyklu dozorových auditů a vždy, když dojde ke změnám v rozsahu činnosti organizace.“;

h) za bod CAMO.B.330 se vkládá nový bod CAMO.B.330A, který zní:

„CAMO.B.330A **Změny systému řízení bezpečnosti informací**

a) Pro změny řízené a oznámené příslušnému orgánu postupem stanoveným v bodě IS.I.OR.255 písm. a) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203, příslušný orgán zahrne přezkum těchto změn do svého průběžného dozoru v souladu se zásadami stanovenými v bodě CAMO.B.300. Zjistí-li příslušný orgán jakýkoli nesoulad, oznámí to organizaci, vyžádá si další změny a jedná v souladu s bodem CAMO.B.350.

b) Pro ostatní změny vyžadující žádost o schválení podle bodu IS.I.OR.255 písm. b) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203:

1) po obdržení žádosti o změnu zkontroluje příslušný orgán před vydáním oprávnění, zda organizace splňuje příslušné požadavky;

2) příslušný orgán stanoví podmínky, za kterých může organizace během provádění změny fungovat;

3) dojde-li příslušný orgán k závěru, že organizace splňuje platné požadavky, změnu schválí.“

*PŘÍLOHA VIII*

Přílohy II (část ATCO.AR) a III (část ATCO.OR) nařízení (EU) 2015/340 se mění takto:

1) Příloha II (část ATCO.AR) se mění takto:

a) v bodě ATCO.AR.A.020 se doplňuje nové písmeno c), které zní:

„c) Příslušný orgán členského státu poskytne agentuře co nejdříve informace důležité pro bezpečnost vyplývající z hlášení o bezpečnosti informací, které obdržel podle bodu IS.I.OR.230 přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203.“;

b) za bod ATCO.AR.A.025 se vkládá nový bod ATCO.AR.A.025A, který zní:

„**ATCO.AR.A.025A Okamžitá reakce na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví**

a) Příslušný orgán zavede systém pro náležité shromažďování, analýzu a šíření informací týkajících se incidentů a zranitelností v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, které organizace nahlásí. Tato činnost se provádí v koordinaci s dalšími příslušnými orgány odpovědnými za bezpečnost informací nebo kybernetickou bezpečnost v členském státě s cílem zvýšit koordinaci a kompatibilitu systémů podávání hlášení.

b) Agentura zavede systém, jehož prostřednictvím je možné náležitě analyzovat veškeré příslušné informace významné z hlediska bezpečnosti, které obdrží v souladu s bodem ATCO.AR.A.020, a neprodleně členským státům a Komisi poskytne veškeré informace, včetně doporučení nebo nápravných opatření, která je nutno přijmout a která jsou nezbytná k tomu, aby členské státy a Komise mohly včas reagovat na incident nebo zranitelnost v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví týkající se výrobků, letadlových částí, neinstalovaného zařízení, osob nebo organizací, na něž se vztahuje nařízení (EU) 2018/1139 a jeho akty v přenesené pravomoci a prováděcí akty.

c) Poté, co příslušný orgán obdrží informace uvedené v písmenech a) a b), přijme odpovídající opatření pro řešení možného dopadu incidentu nebo zranitelnosti v oblasti ochrany informací na bezpečnost letectví.

d) O opatřeních přijatých podle písmene c) se neprodleně vyrozumí všechny osoby a organizace, které se podle nařízení (EU) 2018/1139 a jeho aktů v přenesené pravomoci a prováděcích aktů těmito opatřeními řídí. Příslušný orgán členského státu o těchto opatřeních vyrozumí rovněž agenturu a v případě, že je třeba, aby se na jejich uplatňování podílelo více členských států, vyrozumí i příslušné orgány dalších dotčených členských států.“;

c) v bodě ATCO.AR.B.001 se doplňuje nové písmeno e), které zní:

„e) Kromě požadavků uvedených v písmenu a) musí být systém řízení zavedený a udržovaný příslušným orgánem v souladu s přílohou I (část IS.AR) prováděcího nařízení (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“;

d) bod ATCO.AR.B.005 se mění takto:

i) nadpis se nahrazuje tímto:

„**ATCO.AR.B.005 Přidělování úkolů**“;

ii) doplňuje se nové písmeno c), které zní:

„c) Pokud jde o certifikaci a dozor nad dodržováním bodu ATCO.OR.C.001A ze strany organizace, může příslušný orgán přidělit úkoly kvalifikovaným subjektům podle písmene a) nebo jakémukoli příslušnému orgánu odpovědnému za bezpečnost informací nebo kybernetickou bezpečnost v členském státě. Při přidělování úkolů příslušný orgán zajistí, že:

1) kvalifikovaným subjektem nebo příslušným orgánem jsou koordinovány a zohledněny všechny aspekty týkající se bezpečnosti letectví;

2) výsledky certifikačních a dozorových činností prováděných kvalifikovaným subjektem nebo příslušným orgánem jsou začleněny do celkové certifikační a dozorové dokumentace organizace;

3) jeho vlastní systém řízení bezpečnosti informací zavedený v souladu s bodem ATCO.AR.B.001 písm. e) pokrývá všechny úkoly certifikace a průběžného dozoru prováděné jeho jménem.“;

e) v bodě ATCO.AR.C.001 se doplňuje nové písmeno f), které zní:

„f) Pokud jde o certifikaci a dozor nad dodržováním bodu ATCO.OR.C.001A ze strany organizace, musí příslušný orgán kromě dodržování písmen a) až f) přezkoumat každé schválení udělené podle bodu IS.I.OR.200 písm. e) tohoto nařízení nebo bodu IS.D.OR.200 písm. e) nařízení v přenesené pravomoci (EU) 2022/1645 po příslušném cyklu dozorových auditů a vždy, když dojde ke změnám v rozsahu činnosti organizace.“;

f) za bod ATCO.AR.E.010 se vkládá nový bod ATCO.AR.E.010A, který zní:

„**ATCO.AR.E.010A Změny systému řízení bezpečnosti informací**

a) Pokud jde o změny řízené a oznámené příslušnému orgánu v souladu s postupem stanoveným v bodě IS.I.OR.255 písm. a) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203, příslušný orgán zahrne přezkum těchto změn do svého průběžného dozoru v souladu se zásadami stanovenými v bodě ATCO.AR.C.001. Zjistí-li příslušný orgán jakýkoli nesoulad, oznámí to organizaci, vyžádá si další změny a jedná v souladu s bodem ATCO.AR.C.010.

b) Pokud jde o další změny vyžadující žádost o schválení podle bodu IS.I.OR.255 písm. b) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203:

1) po obdržení žádosti o změnu zkontroluje příslušný orgán před vydáním oprávnění, zda organizace splňuje příslušné požadavky;

2) příslušný orgán stanoví podmínky, za kterých může organizace během provádění změny fungovat;

3) dojde-li příslušný orgán k závěru, že organizace splňuje platné požadavky, změnu schválí.“

2) Příloha III (část ATCO.OR) se mění takto:

Za bod ATCO.OR.C.001 se vkládá nový bod ATCO.OR.C.001A, který zní:

„**ATCO.OR.C.001A Systém řízení bezpečnosti informací**

Kromě systému řízení uvedeného v bodě ATCO.OR.C.001 organizace pro odborný výcvik zřídí, zavede a udržuje systém řízení bezpečnosti informací v souladu s prováděcím nařízením (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“

*PŘÍLOHA IX*

Přílohy II (část ATM/ANS.AR) a III (část ATM/ANS.OR) prováděcí nařízení (EU) 2017/373 se mění takto:

1) Příloha II (část ATM/ANS.AR) se mění takto:

a) v bodě ATM/ANS.AR.A.020 se doplňuje nové písmeno c), které zní:

„c) Příslušný orgán členského státu poskytne agentuře co nejdříve informace důležité pro bezpečnost vyplývající z hlášení o bezpečnosti informací, které obdržel podle bodu IS.I.OR.230 přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203.“;

b) za bod ATM/ANS.AR.A.025 se vkládá nový bod ATM/ANS.AR.A.025A, který zní:

„**ATM/ANS.AR.A.025A Okamžitá reakce na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví**

a) Příslušný orgán zavede systém pro náležité shromažďování, analýzu a šíření informací týkajících se incidentů a zranitelností v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, které organizace nahlásí. Tato činnost se provádí v koordinaci s dalšími příslušnými orgány odpovědnými za bezpečnost informací nebo kybernetickou bezpečnost v členském státě s cílem zvýšit koordinaci a kompatibilitu systémů podávání hlášení.

b) Agentura zavede systém, jehož prostřednictvím je možné náležitě analyzovat veškeré příslušné informace významné z hlediska bezpečnosti, které obdrží v souladu s bodem ATM/ANS.AR.A.020 písm. c), a neprodleně členským státům a Komisi poskytovat veškeré informace, včetně doporučení nebo nápravných opatření, která je nutno přijmout a která jsou nezbytná k tomu, aby členské státy a Komise mohly včas reagovat na incident nebo zranitelnost v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví týkající se výrobků, letadlových částí, neinstalovaného zařízení, osob nebo organizací, na něž se vztahuje nařízení (EU) 2018/1139 a jeho akty v přenesené pravomoci a prováděcí akty.

c) Poté, co příslušný orgán obdrží informace uvedené v písmenech a) a b), přijme odpovídající opatření pro řešení možného dopadu incidentu nebo zranitelnosti v oblasti ochrany informací na bezpečnost letectví.

d) O opatřeních přijatých podle písmene c) se neprodleně vyrozumí všechny osoby a organizace, které se podle nařízení (EU) 2018/1139 a jeho aktů v přenesené pravomoci a prováděcích aktů těmito opatřeními řídí. Příslušný orgán členského státu o těchto opatřeních vyrozumí rovněž agenturu a v případě, že je třeba, aby se na jejich uplatňování podílelo více členských států, vyrozumí i příslušné orgány dalších dotčených členských států.“;

c) v bodě ATM/ANS.AR.B.001 se doplňuje nové písmeno e), které zní:

„e) Kromě požadavků uvedených v písmenu a) musí být systém řízení zavedený a udržovaný příslušným orgánem v souladu s přílohou I (část IS.AR) prováděcího nařízení (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“;

d) bod ATM/ANS.AR.B.005 se mění takto:

i) nadpis se nahrazuje tímto:

„**ATM/ANS.AR.B.005 Přidělování úkolů**“;

ii) doplňuje se nové písmeno c), které zní:

„c) Pokud jde o certifikaci a dozor nad dodržováním bodu ATM/ANS.OR.B.005A ze strany organizace, může příslušný orgán přidělit úkoly kvalifikovaným subjektům podle písmene a) nebo jakémukoli příslušnému orgánu odpovědnému za bezpečnost informací nebo kybernetickou bezpečnost v členském státě. Při přidělování úkolů příslušný orgán zajistí, že:

1) kvalifikovaným subjektem nebo příslušným orgánem jsou koordinovány a zohledněny všechny aspekty týkající se bezpečnosti letectví;

2) výsledky certifikačních a dozorových činností prováděných kvalifikovaným subjektem nebo příslušným orgánem jsou začleněny do celkové certifikační a dozorové dokumentace organizace;

3) jeho vlastní systém řízení bezpečnosti informací zavedený v souladu s bodem ATM/ANS.AR.B.001 písm. e) pokrývá všechny úkoly certifikace a průběžného dozoru prováděné jeho jménem.“;

e) v bodě ATM/ANS.AR.C.010 se doplňuje nové písmeno d), které zní:

„d) Pokud jde o certifikaci a dozor nad dodržováním bodu ATM/ANS.OR.B.005A ze strany organizace, musí příslušný orgán kromě dodržování písmen a) až c) přezkoumat každé schválení udělené podle bodu IS.I.OR.200 písm. e) tohoto nařízení nebo bodu IS.D.OR.200 písm. e) nařízení v přenesené pravomoci (EU) 2022/1645 po příslušném cyklu dozorových auditů a vždy, když dojde ke změnám v rozsahu činnosti organizace.“;

f) za bod ATM/ANS.AR.C.025 se vkládá nový bod ATM/ANS.AR.C.025A, který zní:

„**ATM/ANS.AR.C.025A Změny systému řízení bezpečnosti informací**

a) Pro změny řízené a oznámené příslušnému orgánu postupem stanoveným v bodě IS.I.OR.255 písm. a) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203 příslušný orgán zahrne přezkum těchto změn do svého průběžného dozoru v souladu se zásadami stanovenými v bodě ATM/ANS.AR.C.010. Zjistí-li příslušný orgán jakýkoli nesoulad, oznámí to organizaci, vyžádá si další změny a jedná v souladu s bodem ATM/ANS.AR.C.050.

b) Pokud jde o další změny vyžadující žádost o schválení podle bodu IS.I.OR.255 písm. b) přílohy II (část IS.I.OR) prováděcího nařízení (EU) 2023/203:

1) po obdržení žádosti o změnu zkontroluje příslušný orgán před vydáním oprávnění, zda organizace splňuje příslušné požadavky;

2) příslušný orgán stanoví podmínky, za kterých může organizace během provádění změny fungovat;

3) Dojde-li příslušný orgán k závěru, že organizace splňuje platné požadavky, změnu schválí.“

2) Příloha III (část ATM/ANS.OR) se mění takto:

a) za bod ATM/ANS.OR.B.005 se vkládá nový bod ATM/ANS.OR.B.005A, který zní:

„**ATM/ANS.OR.B.005A Systém řízení bezpečnosti informací**

Kromě systému řízení uvedeného v bodě ATM/ANS.OR.B.005 poskytovatel služeb zřídí, zavede a udržuje systém řízení bezpečnosti informací v souladu s prováděcím nařízením (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“;

b) bod ATM/ANS.OR.D.010 se nahrazuje tímto:

„**ATM/ANS.OR.D.010 Řízení ochrany**

a) Poskytovatel letových navigačních služeb a poskytovatel uspořádání toku letového provozu a manažer struktury vzdušného prostoru zřídí systém řízení ochrany, jako nedílnou součást svého systému řízení, jak to vyžaduje bod ATM/ANS.OR.B.005, aby zajistili:

1) ochranu svých zařízení a pracovníků před protiprávními činy narušujícími poskytování služeb;

2) ochranu provozních údajů, které přijímají nebo zpracovávají nebo jinak používají, aby k nim měly přístup pouze oprávněné osoby.

b) Systém řízení ochrany vymezí:

1) proces a postupy související s posuzováním a zmírňováním rizika v oblasti ochrany, sledováním a zlepšováním ochrany, hodnocením v oblasti ochrany a šířením poznatků;

2) prostředky určené k identifikaci, monitorování a odhalování narušení ochrany a k upozornění pracovníků prostřednictvím vhodných výstrah;

3) prostředky pro zvládání účinků narušení ochrany a pro určení nápravných opatření a postupů k jejich zmírňování, které zabraňují jejich opětovnému výskytu.

c) Poskytovatel letových navigačních služeb a poskytovatel uspořádání toku letového provozu a manažer struktury vzdušného prostoru zajistí v případě potřeby bezpečnostní prověrku svých pracovníků a koordinují s příslušnými civilními a vojenskými orgány, aby zajistili ochranu svých zařízení, pracovníků a údajů.

d) Aspekty týkající se bezpečnosti informací se řídí podle bodu ATM/ANS.OR.B.005A.“