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

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 na čl. 19 odst. 1 písm. g) a čl. 39 odst. 1 písm. b) uvedeného nařízení,

vzhledem k těmto důvodům:

(1) V souladu s hlavními požadavky stanovenými v příloze II bodě 3.1 písm. b) nařízení (EU) 2018/1139 musí projekční a výrobní organizace zavést a udržovat systém řízení za účelem řízení bezpečnostních rizik.

(2) Kromě toho v souladu s hlavními požadavky stanovenými v příloze VII bodech 2.2.1 a 5.2 nařízení (EU) 2018/1139 musí provozovatelé letišť a organizace odpovědné za poskytování služeb řízení provozu na odbavovací ploše zavést a udržovat systém řízení za účelem řízení bezpečnostních rizik.

(3) Bezpečnostní rizika uvedená v 1. a 2. bodě odůvodnění mohou pramenit z různých zdrojů, včetně nedostatků souvisejících s projektováním a údržbou, aspektů lidské výkonnosti, environmentálních hrozeb a hrozeb pro bezpečnost informací. Systémy řízení zavedené organizacemi, jak je uvedeno v 1. a 2. bodě odůvodnění, by proto měly zohledňovat nejen bezpečnostní rizika vyplývající z náhodných událostí, ale také bezpečnostní rizika pramenící z hrozeb pro bezpečnost informací, kdy mohou být stávající nedostatky zneužity osobami se zlým úmyslem. Uvedená rizika bezpečnosti informací se v prostředí civilního letectví neustále zvyšují, neboť stávající informační systémy jsou čím dál tím více propojeny a stále častěji se stávají terčem subjektů s nekalými úmysly.

(4) Rizika spojená s uvedenými informačními systémy se neomezují na možné útoky v kybernetickém prostoru, ale zahrnují rovněž hrozby, které mohou ovlivnit procesy a postupy, jakož i výkonnost lidí.

(5) 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.

(6) Proto je vhodné stanovit požadavky na řízení rizik bezpečnosti informací s potenciálním dopadem na bezpečnost letectví.

(7) Je nezbytné, aby se tyto požadavky vztahovaly na různé oblasti letectví a jejich rozhraní, neboť letectví je vysoce propojeným systémem systémů. Proto by měly platit pro všechny organizace, které již v souladu se stávajícími právními předpisy Unie v oblasti bezpečnosti letectví musí mít systém řízení.

(8) Požadavky stanovené v tomto nařízení by měly být důsledně uplatňovány ve všech oblastech letectví a současně by měly mít minimální dopad na právní předpisy Unie v oblasti bezpečnosti letectví, které již jsou na uvedené oblasti použitelné.

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

(9) 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 ([2]) a v článku 14 směrnice Evropského parlamentu a Rady (EU) 2016/1148 ([3]).

(10) Definice týkající se bezpečnosti informací použitá pro účely tohoto právního aktu by neměla být vykládána tak, že se odchyluje od definice bezpečnosti sítí a informačních systémů stanovené ve směrnici 2016/1148.

(11) Aby se zabránilo zdvojování právních požadavků, pokud organizace, na něž se vztahuje toto nařízení, již podléhají bezpečnostním požadavkům vyplývajícím z jiných aktů Unie uvedených v 9. 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.

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

(13) Nařízení Komise (EU) č. 748/2012 ([4]) a (EU) č. 139/2014 ([5]) by měla být změněna za účelem vytvoření vazby mezi systémy řízení předepsanými ve výše uvedených nařízeních a požadavky na řízení bezpečnosti informací předepsanými tímto nařízením.

(14) Aby měly organizace dostatek času na zajištění souladu s novými pravidly a postupy zavedenými tímto nařízením, mělo by se toto nařízení použít po uplynutí tří let od data vstupu v platnost.

(15) Požadavky stanovené tímto nařízením vycházejí ze stanoviska č. 03/2021 ([6]) vydaného agenturou v souladu s čl. 75 odst. 2 písm. b) a c) a čl. 76 odst. 1 nařízení (EU) 2018/1139.

(16) V souladu s čl. 128 odst. 4 nařízení (EU) 2018/1139 vedla Komise konzultace s odborníky jmenovanými jednotlivými členskými státy v souladu se zásadami stanovenými v interinstitucionální dohodě o zdokonalení tvorby právních předpisů ze dne 13. dubna 2016 ([7]),

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Předmět

Toto nařízení stanoví požadavky, které musí splňovat organizace uvedené v článku 2 za účelem identifikace a řízení rizik bezpečnosti informací s potenciálním dopadem na bezpečnost letectví, která by mohla ovlivnit systémy informačních a komunikačních technologií a údaje používané pro účely civilního letectví, a za účelem odhalování událostí bezpečnosti informací a identifikace těch, které jsou považovány za incidenty bezpečnosti informací s potenciálním dopadem na bezpečnost letectví, a reagování na tyto incidenty bezpečnosti informací a zotavení se z nich.

([2]) 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).

([3]) 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).

([4]) 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).

([5]) 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).

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

([7]) Úř. věst. L 123, 12.5.2016, s. 1.

Článek 2

Oblast působnosti

1. Toto nařízení se vztahuje na tyto organizace:

a) výrobní organizace a projekční organizace, na něž se vztahují hlavy G a J přílohy I oddílu A (část 21) nařízení (EU) č. 748/2012, s výjimkou projekčních a výrobních organizací, které se podílejí výhradně na projektování a/nebo výrobě letadel ELA2 ve smyslu čl. 1 odst. 2 písm. j) nařízení (EU) č. 748/2012;

b) provozovatele letišť a poskytovatele služeb řízení provozu na odbavovací ploše, na něž se vztahuje příloha III „Část: Požadavky na organizace (část ADR.OR)“ nařízení (EU) č. 139/2014.

2. 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 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;

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 vyplývající z jiných právních předpisů Unie

1. Pokud organizace uvedená v článku 2 splňuje bezpečnostní požadavky stanovené v článku 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 článku 2 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 ([8]), 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.D.OR.230 přílohy tohoto nařízení, který musí být splněn.

([8]) 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).

3. Komise může po konzultaci s agenturou EASA 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 5

Příslušný úřad

1. Úřadem odpovědným za certifikaci souladu s tímto nařízením a za dozor nad tímto souladem je:

a) pokud jde o organizace uvedené v čl. 2 písm. a), příslušný úřad určený v souladu s přílohou I (část 21) nařízení (EU) č. 748/2012;

b) pokud jde o organizace uvedené v čl. 2 písm. b), příslušný úřad určený v souladu s přílohou III (část ADR.OR) nařízení (EU) č. 139/2014.

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.

Článek 6

Změna nařízení (EU) č. 748/2012

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

1) Obsah se mění takto:

   a) za položku 21.A.139 se vkládá nová položka, která zní:

      „**21.A.139 A Systém řízení bezpečnosti informací**“;

   b) za položku 21.A.239 se vkládá nová položka, která zní:

      „**21.A.239 A Systém řízení bezpečnosti informací**“.

2) Za bod 21.A.139 se vkládá nový bod 21.A.139 A, který zní:

   „**21.A.139A Systém řízení bezpečnosti informací**

   Vedle systému řízení výroby požadovaného podle bodu 21.A.139 výrobní organizace navíc zavede, provádí a udržuje systém řízení bezpečnosti informací v souladu s nařízením Komise v přenesené pravomoci (EU) 2022/1645 (*) za účelem zajištění řádného řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.

   (*) 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).“

3) Za bod 21.A.239 se vkládá nový bod 21.A.239 A, který zní:

   „**21.A.239A Systém řízení bezpečnosti informací**

   Vedle systému řízení projekce požadovaného podle bodu 21.A.239 projekční organizace navíc zavede, provádí a udržuje systém řízení bezpečnosti informací v souladu s nařízením v přenesené pravomoci (EU) 2022/1645 za účelem zajištění řádného řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“

Článek 7

Změna nařízení (EU) č. 139/2014

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

1) Za bod ADR.OR.D.005 se vkládá nový bod ADR.OR.D.005 A, který zní:

„**ADR.OR.D.005A Systém řízení bezpečnosti informací**

Provozovatel letiště vytvoří, provádí a udržuje systém řízení bezpečnosti informací v souladu s nařízením Komise v přenesené pravomoci (EU) 2022/1645 (*) za účelem zajištění řádného řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.

(*) 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).“

2) Bod ADR.OR.D.007 se nahrazuje tímto:

„**ADR.OR.D.007 Správa leteckých dat a leteckých informací**

a) V rámci svého systému řízení provozovatel letiště provádí a udržuje systém řízení jakosti, který pokrývá tyto činnosti:

1) jeho činnosti související s leteckými daty;

2) jeho činnosti poskytování leteckých informací.

b) V rámci svého systému řízení provozovatel letiště zřídí systém řízení ochrany, aby se zajistila ochrana provozních údajů, které letiště přijímá, vytváří či jinak používá, a to tak, aby přístup k těmto provozním údajům měly pouze oprávněné osoby.

c) Systém řízení ochrany vymezí tyto prvky:

1) postupy související s posuzováním a zmírňováním rizik v oblasti zabezpečení údajů, se sledováním a zlepšováním ochrany, přezkumy v oblasti ochrany a šířením získaných poznatků;

2) prostředky určené k zjišťování narušení ochrany a k upozornění pracovníků prostřednictvím vhodných výstrah;

3) prostředky pro zvládání účinků narušení ochrany a pro určení nápravných opatření a postupů zmírňování, aby se zabránilo jejich opětovnému výskytu.

d) Provozovatel letiště zajistí bezpečnostní prověrku pracovníků letiště, pokud jde o ochranu leteckých dat.

e) Aspekty týkající se bezpečnosti informací se řídí podle bodu ADR.OR.D.005 A.“

3) Za bod ADR.OR.F.045 se vkládá nový bod ADR.OR.F.045 A, který zní:

„**ADR.OR.F.045A Systém řízení bezpečnosti informací**

Organizace odpovědná za poskytování služeb řízení provozu na odbavovací ploše vytvoří, provádí a udržuje systém řízení bezpečnosti informací v souladu s nařízením v přenesené pravomoci (EU) 2022/1645 za účelem zajištění řádného řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“

Článek 8

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

Použije se od 16. října 2025.

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

V Bruselu dne 14. července 2022.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA

BEZPEČNOST INFORMACÍ – POŽADAVKY NA ORGANIZACI

[ČÁST IS.D.OR]

IS.D.OR.100 Oblast působnosti

Tato část stanoví požadavky, které musí splňovat organizace uvedené v článku 2 tohoto nařízení.

IS.D.OR.200 Systém řízení bezpečnosti informací (ISMS)

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

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

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

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

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

5) definuje a provádí v souladu s bodem IS.D.OR.220 opatření potřebná k odhalení událostí bezpečnosti informací, identifikuje takové události, které jsou považovány za incidenty s potenciálním dopadem na bezpečnost letectví, s výjimkou případů povolených bodem IS.D.OR.205 písm. e), a reaguje na tyto incidenty bezpečnosti informací a zotavuje se z nich;

6) provádí opatření, která byla oznámena příslušným úřadem jako okamžitá reakce na incident nebo zranitelnost bezpečnosti informací s dopadem na bezpečnost letectví;

7) přijme v souladu s bodem IS.D.OR.225 vhodné opatření k řešení nálezů oznámených příslušným úřadem;

8) provádí systém externího hlášení v souladu s bodem IS.D.OR.230 s cílem umožnit příslušnému úřadu přijmout vhodná opatření;

9) splňuje požadavky uvedené v bodě IS.D.OR.235 při uzavírání smluv na jakoukoli část činností uvedených v bodě IS.D.OR.200 s jinými organizacemi;

10) splňuje požadavky na personál stanovené v bodě IS.D.OR.240;

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

12) sleduje soulad organizace s požadavky tohoto nařízení a poskytuje zpětnou vazbu v souvislosti s nálezy odpovědnému vedoucímu nebo v případě projekčních organizací vedoucímu projekční organizace za účelem zajištění účinného provádění nápravných opatření;

13) chrání, aniž jsou dotčeny příslušné požadavky na hlášení incidentů, důvěrnost veškerých informací, které organizace případně obdržela od jiných organizací, podle úrovně jejich citlivosti.

b) Aby organizace neustále splňovala požadavky uvedené v článku 1, provádí proces neustálého zlepšování v souladu s bodem IS.D.OR.260.

c) Organizace v souladu s bodem IS.D.OR.250 dokumentuje všechny klíčové procesy, postupy, úlohy a povinnosti požadované za účelem dosažení souladu s bodem IS.D.OR.200 písm. a) a zavede proces pro změnu uvedené dokumentace. Změny uvedených procesů, postupů, úloh a povinností se řídí podle bodu IS.D.OR.255.

d) Procesy, postupy, úlohy a povinnosti zavedené organizací za účelem dosažení souladu s bodem IS.D.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 Evropského parlamentu a Rady (EU) č. 376/2014 ([1]) a požadavky bodu IS.D.OR.200 písm. a) bodu 13, může příslušný úřad organizaci udělit oprávnění neprovádět požadavky uvedené v písmenech a) až d) a související požadavky obsažené v bodech IS.D.OR.205 až IS.D.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. Toto oprávnění musí být založeno na zdokumentovaném posouzení rizik bezpečnosti informací provedeném organizací nebo třetí stranou podle bodu IS.D.OR.205 a přezkoumaném a schváleném jejím příslušným úřadem.

Zachování platnosti uvedeného oprávnění bude přezkoumáno příslušným úřadem v návaznosti na příslušný cyklus auditu dozoru a pokaždé, když jsou provedeny změny v rozsahu činnosti organizace.

IS.D.OR.205 Posouzení rizik bezpečnosti informací

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

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 ke vzájemné expozici rizikům bezpečnosti informací.

c) S ohledem na prvky a rozhraní uvedené v písmenech a) a b), organizace identifikuje rizika bezpečnosti informací, která mohou mít potenciální dopad na bezpečnost letectví. V případě každého identifikovaného rizika organizace:

1) riziku podle předem definované klasifikace stanovené organizací přiřadí příslušnou úroveň rizika;

([1]) Nařízení Evropského parlamentu a Rady (EU) č. 376/2014 ze dne 3. dubna 2014 o hlášení událostí v civilním letectví, analýze těchto hlášení a navazujících opatřeních a o změně nařízení Evropského parlamentu a Rady (EU) č. 996/2010 a zrušení směrnice Evropského parlamentu a Rady 2003/42/ES, nařízení Komise (ES) č. 1321/2007 a nařízení Komise (ES) č. 1330/2007 (Úř. věst. L 122, 24.4.2014, s. 18).

2) spojí každé riziko a jeho úroveň s odpovídajícím prvkem nebo rozhraním identifikovaným v souladu s písmeny a) a b).

Předem definovaná klasifikace uvedená v bodě 1 zohlední potenciál výskytu scénáře hrozby a závažnost jeho bezpečnostních důsledků. Na základě uvedené klasifikace a s přihlédnutím k tomu, zda má organizace pro provoz strukturovaný a opakovatelný proces řízení rizik, musí být organizace schopna stanovit, zda je riziko přijatelné, nebo zda je třeba jej řešit v souladu s bodem IS.D.OR.210.

Aby se usnadnila vzájemná srovnatelnost posouzení rizik, zohlední se při přiřazení úrovně rizika podle bodu 1 relevantní informace získané v koordinaci s organizacemi uvedenými v písmenu b).

d) Organizace přezkoumá a aktualizuje posouzení rizik provedené v souladu s písmeny a), b) a c) v kterékoli z těchto situací:

1) došlo ke změně prvků, na něž se vztahují rizika bezpečnosti informací;

2) došlo ke změně rozhraní mezi organizací a jinými organizacemi nebo ke změně rizik sdělených jinými organizacemi;

3) došlo ke změně informací nebo poznatků použitých pro identifikaci, analýzu a klasifikaci rizik;

4) z analýzy incidentů bezpečnosti informací byla vyvozena ponaučení.

IS.D.OR.210 Řešení rizik bezpečnosti informací

a) Organizace vypracuje opatření k řešení nepřijatelných rizik identifikovaných podle bodu IS.D.OR.205, včas je provede a kontroluje jejich trvalou účinnost. Uvedená opatření umožní organizaci:

1) řídit okolnosti, které přispívají k faktickému výskytu scénáře hrozby;

2) zmírnit důsledky pro bezpečnost letectví, které jsou spojeny s naplněním scénáře hrozby;

3) vyhnout se rizikům.

Uvedená opatření nesmí přinášet žádná nová potenciální nepřijatelná rizika pro bezpečnost letectví.

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

Organizace rovněž informuje organizace, s nimiž má rozhraní v souladu s bodem IS.D.OR.205 písm. b), o jakémkoli riziku sdíleném oběma organizacemi.

IS.D.OR.215 Systém interního hlášení v oblasti bezpečnosti informací

a) Organizace zavede systém interního hlášení, který umožní shromažďování a hodnocení událostí bezpečnosti informací, včetně takových událostí, které mají být hlášeny podle bodu IS.D.OR.230.

b) Zmíněný systém a proces uvedený v bodě IS.D.OR.220 umožní organizaci:

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

2) identifikovat příčiny incidentů a zranitelností bezpečnosti informací identifikovaných v souladu s bodem 1 a faktory, které k nim přispívají, a řešit je v rámci procesu řízení rizik bezpečnosti informací v souladu s body IS.D.OR.205 a IS.D.OR.220;

3) zajistit hodnocení všech známých relevantních informací týkajících se incidentů a zranitelností bezpečnosti informací identifikovaných v souladu s bodem 1;

4) zajistit provádění metody pro interní šíření informací podle potřeby.

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

d) Organizace při vyšetřování spolupracuje s jakoukoli jinou organizací, která významně přispívá k bezpečnosti informací týkající se jejích vlastních činností.

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

IS.D.OR.220 Incidenty bezpečnosti informací — odhalení, reakce a zotavení

a) Na základě výsledku posouzení rizik uskutečněného v souladu s bodem IS.D.OR.205 a výsledku řešení rizik vykonaného v souladu s bodem IS.D.OR.210 provede organizace opatření k odhalení incidentů a zranitelností, které naznačují potenciální naplnění nepřijatelných rizik a jež mohou mít potenciální dopad na bezpečnost letectví. Uvedená odhalovací opatření umožní organizaci:

1) identifikovat odchylky od předem stanovených základních stavů funkční výkonnosti;

2) v případě jakékoli odchylky spustit varování za účelem aktivace vhodných reakčních opatření.

b) Organizace provede opatření za účelem reakce na jakékoli podmínky události identifikované v souladu s písmenem a), z nichž by se mohl vyvinout nebo z nichž se vyvinul incident bezpečnosti informací. Uvedená reakční opatření umožní organizaci:

1) zahájit reakci na varování uvedená v písm. a) bodě 2 tím, že se aktivují předem stanovené zdroje a postup;

2) zabránit šíření útoku a vyhnout se úplnému naplnění scénáře hrozby;

3) regulovat režim poruchy dotčených prvků vymezených v bodě IS.D.OR.205 písm. a).

c) Organizace provede opatření zaměřená na zotavení se z incidentů bezpečnosti informací, v případě potřeby včetně mimořádných opatření. Uvedená zotavovací opatření umožní organizaci:

1) odstranit stav, kterým byl incident způsoben, nebo jej omezit na přípustnou úroveň;

2) dosáhnout bezpečného stavu dotčených prvků vymezených v bodě IS.D.OR.205 písm. a) během doby pro zotavení, jež byla předem stanovena organizací.

IS.D.OR.225 Reakce na nálezy oznámené příslušným úřadem

a) Po obdržení oznámení o nálezech předloženého příslušným úřadem organizace:

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

2) vytvoří plán nápravných opatření;

3) prokáže nápravu nesouladu ke spokojenosti příslušného úřadu.

b) Kroky uvedené v písmenu a) se provedou ve lhůtě dohodnuté s příslušným úřadem.

IS.D.OR.230 Systém externího hlášení v oblasti bezpečnosti informací

a) Organizace provede systém hlášení v oblasti bezpečnosti informací, který splňuje požadavky stanovené v nařízení (EU) č. 376/2014 a jeho aktech v přenesené pravomoci a prováděcích aktech, pokud se uvedené nařízení na danou organizaci vztahuje.

b) Aniž jsou dotčeny povinnosti podle nařízení (EU) č. 376/2014, organizace zajistí, aby byly veškeré incidenty nebo zranitelnosti bezpečnosti informací, které mohou představovat významné riziko pro bezpečnost letectví, hlášeny jejich příslušnému úřadu. Mimoto:

1) dotýká-li se takový incident nebo taková zranitelnost letadla nebo přidruženého systému či letadlového celku, hlásí je organizace rovněž držiteli schválení návrhu;

2) dotýká-li se takový incident nebo taková zranitelnost systému, který organizace používá, nebo jeho součásti, hlásí je organizace organizaci odpovědné za návrh systému nebo jeho součásti.

c) Organizace hlásí stavy uvedené v písmenu b) takto:

1) jakmile se organizace o stavu dozví, musí být příslušnému úřadu a v příslušném případě držiteli schválení návrhu nebo organizaci odpovědné za návrh systému nebo jeho součásti podáno oznámení;

2) co nejdříve, avšak nejpozději 72 hodin od okamžiku, kdy se organizace o stavu dozví, pokud tomu nebrání výjimečné okolnosti, musí být příslušnému úřadu a v příslušném případě držiteli schválení návrhu nebo organizaci odpovědné za návrh systému nebo jeho součásti podáno hlášení.

Hlášení se podává ve formě stanovené příslušným úřadem a obsahuje všechny důležité informace o stavu, který je organizaci znám;

3) příslušnému úřadu a v příslušném případě držiteli schválení návrhu nebo organizaci odpovědné za návrh systému nebo jeho součásti musí být předložena zpráva o následných opatřeních, v níž jsou uvedeny podrobnosti o opatřeních, která organizace přijala nebo hodlá přijmout, aby se z incidentu zotavila, a o opatřeních, která hodlá přijmout, aby podobným incidentům bezpečnosti informací v budoucnu zabránila.

Zpráva o následných opatřeních se předloží, jakmile budou uvedená opatření identifikována, a vypracuje se ve formě stanovené příslušným úřadem.

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

a) Organizace zajistí, aby při uzavírání smluv na jakoukoli část činností uvedených v bodě IS.D.OR.200 s jinými organizacemi byly smluvní činnosti v souladu s požadavky tohoto nařízení a aby smluvní organizace pracovala pod jejím dohledem. Organizace zajistí, aby rizika spojená se smluvními činnostmi byla náležitě řízena.

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

IS.D.OR.240 Požadavky na personál

a) Odpovědný vedoucí organizace nebo v případě projekčních organizací vedoucí projekční organizace určený v souladu s nařízením (EU) č. 748/2012 a nařízením (EU) č. 139/2014, jak se uvádí v čl. 2 odst. 1 písm. a) a b) tohoto nařízení, musí mít statutární pravomoc zajistit, aby mohly být financovány a prováděny všechny činnosti požadované tímto nařízením. Uvedená 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.D.OR.200 písm. a) bodě 1;

3) musí prokázat základní porozumění tomuto nařízení.

b) Odpovědný vedoucí nebo v případě projekčních organizací vedoucí projekční organizace jmenuje osobu nebo skupinu osob, která zajistí, aby organizace splňovala požadavky tohoto nařízení, a vymezí rozsah jejich pravomoci. Uvedená osoba nebo skupina osob jsou podřízeny přímo odpovědnému vedoucímu nebo v případě projekčních organizací vedoucímu projekční organizace a musí mít odpovídající znalosti, kvalifikaci a zkušenosti k plnění svých povinností. V postupech musí být určeno, kdo zastupuje určitou osobu v případě její dlouhodobé nepřítomnosti.

c) Odpovědný vedoucí nebo v případě projekčních organizací vedoucí projekční organizace jmenuje osobu nebo skupinu osob s odpovědností za řízení funkce sledování souladu uvedené v bodě IS.D.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 nebo v případě projekčních organizací vedoucí projekční organizace svými činnostmi pověřit společnou odpovědnou osobu.

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

e) Odpovědný vedoucí či vedoucí projekční organizace nebo společná odpovědná osoba uvedená v písmenu d) musí mít statutární pravomoc zavádět a udržovat organizační struktury, politiky, procesy a postupy nezbytné k provádění bodu IS.D.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.D.OR.245 Vedení záznamů

a) Organizace vede záznamy o svých činnostech týkajících se řízení bezpečnosti informací

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

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

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

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

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

v) záznamy o incidentech a zranitelnostech bezpečnosti informací hlášených v souladu se systémy hlášení uvedenými v bodech IS.D.OR.215 a IS.D.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 svých vlastních pracovníků podílejících se na činnostech týkajících se 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 jejich stupně utajení. Organizace zajistí, aby záznamy byly uchovávány za použití prostředků, které zajistí integritu, pravost a oprávněný přístup.

IS.D.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 nebo v případě projekčních organizací vedoucím projekční organizace potvrzující, že organizace bude vždy postupovat v souladu s touto přílohou a s příručkou ISMM. Pokud odpovědný vedoucí nebo v případě projekčních organizací vedoucí projekční organizace není výkonným ředitelem (CEO) organizace, musí prohlášení spolupodepsat také tento výkonný ředitel;

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

3) v příslušných případech funkci, jméno, úkoly, odpovědnosti, povinnosti a pravomoci společné odpovědné osoby uvedené v bodě IS.D.OR.240 písm. d);

4) politiku bezpečnosti informací organizace uvedenou v bodě IS.D.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.D.OR.240;

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

7) organizační schéma znázorňující související odpovědnostní vztahy pro osoby uvedené v bodech 2 a 6;

8) popis systému interního hlášení uvedeného v bodě IS.D.OR.215;

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

i) dokumentaci podle bodu IS.D.OR.200 písm. c);

ii) postupy, které definují, jak organizace kontroluje veškeré smluvní činnosti uvedené v bodě IS.D.OR.200 písm. a) bodě 9;

iii) postup pro změnu příručky ISMM definovaný v písmenu c);

10) podrobnosti o aktuálně schválených alternativních způsobech průkazu.

b) První vydání příručky ISMM schvaluje příslušný úřad, který si ponechá jednu kopii. Příručka ISMM se podle potřeby pozmění tak, aby zůstala aktuálním popisem systému ISMS organizace. Kopie veškerých změn příručky ISMM se poskytne příslušnému úřadu.

c) Změny příručky ISMM se řídí postupem stanoveným organizací. Veškeré změny, které nespadají do tohoto postupu, a veškeré změny, které se týkají změn uvedených v bodě IS.D.OR.255 písm. b), schvaluje příslušný úřad.

d) Organizace může příručku ISMM začlenit do jiných výkladů řízení nebo příruček, které má k dispozici, za předpokladu, že je uveden jasný křížový odkaz udávající, které části výkladu řízení nebo příručky odpovídají jednotlivým požadavkům obsaženým v této příloze.

IS.D.OR.255 Změny systému řízení bezpečnosti informací

a) Změny ISMS mohou být řízeny a příslušnému úřadu oznamovány v rámci postupu vytvořeného organizací. Tento postup schválí příslušný úřad.

b) Pokud jde o změny ISMS, na něž se nevztahuje postup uvedený v písmenu a), organizace musí požádat o oprávnění, které vydává příslušný úřad, a toto oprávnění získat.

Pokud jde o tyto změny:

1) žádost musí být podána dříve, než jsou změny provedeny, aby příslušný úřad mohl stanovit, zda jsou i nadále plněny požadavky tohoto nařízení, a v případě potřeby změnit osvědčení organizace a k němu připojené související podmínky oprávnění;

2) organizace zpřístupní příslušnému úřadu veškeré informace, které k posouzení změny požaduje;

3) změna se provede až po obdržení formálního souhlasu příslušného úřadu;

4) během provádění těchto změn organizace postupuje podle podmínek předepsaných příslušným úřadem.

IS.D.OR.260 Neustálé zlepšování

a) Organizace za použití odpovídajících ukazatelů výkonnosti posuzuje účinnost a vyspělost ISMS. Uvedené posouzení se provádí na základě harmonogramu předem stanoveného organizací nebo v návaznosti na incident bezpečnosti informací.

b) Jsou-li na základě posouzení provedeného v souladu s písmenem a) zjištěny nedostatky, organizace přijme nezbytná opatření ke zlepšení, aby zajistila, že ISMS nadále splňuje příslušné požadavky a udržuje rizika bezpečnosti informací na přijatelné úrovni. Kromě toho organizace znovu posoudí ty prvky ISMS, jež jsou přijatými opatřeními dotčeny.