

UPOZORNĚNÍ:

Ačkoliv jsou tyto texty doslovným překladem originálního textu rozhodnutí výkonného ředitele EASA, slouží příslušné dokumenty připravované ÚCL pouze pro informační účely a ÚCL nenese za jejich obsah odpovědnost. Tyto texty nemají žádnou právní hodnotu. Originální znění naleznete v Úřední publikaci Agentury, tj. na webových stránkách <http://easa.europa.eu>.

Datum aktualizace tohoto dokumentu: 2. 8. 2024

Rozhodnutí výkonného ředitele

2023/008/R

ze dne 12. července 2023

kterým se vydává následující:

1. vydání Přijatelných způsobů průkazu a poradenského materiálu k článkům nařízení Komise v přenesené pravomoci (EU) 2022/1645 a prováděcího nařízení Komise (EU) 2023/203

„AMC a GM k článkům nařízení Komise v přenesené pravomoci (EU) 2022/1645 a prováděcího nařízení Komise (EU) 2023/203 – 1. vydání“

— — —

„Řízení rizik v oblasti bezpečnosti informací – AMC & GM k článkům nařízení Komise v přenesené pravomoci (EU) 2022/1645 a prováděcího nařízení Komise (EU) 2023/203“

VÝKONNÝ ŘEDITEL AGENTURY EVROPSKÉ UNIE PRO BEZPEČNOST LETECTVÍ (EASA)

s ohledem na nařízení (EU) 2018/1139¹, a zejména na článek 76 odst. 3 a článek 104 odst. 3 písm. a) tohoto nařízení,

vzhledem k těmto důvodům:

- (1) Přijatelné způsoby průkazu jsou nezávazné standardy vydané EASA, které jsou osobami a organizacemi využívány k prokázání vyhovění nařízení (EU) 2018/1139 a aktům v přenesené pravomoci a prováděcím aktům přijatým na jeho základě.
- (2) Poradenský materiál je nezávazný materiál vydaný EASA, který pomáhá ilustrovat význam aktů v přenesené pravomoci nebo prováděcích aktů nebo certifikačních specifikací a podrobných specifikací a který se používá k podpoře výkladu nařízení (EU) 2018/1139, aktů v přenesené pravomoci a prováděcích aktů přijatých na jeho základě a certifikačních specifikací a podrobných specifikací.
- (3) EASA je povinna, na základě článku 4 odst. 1 písm. a) nařízení (EU) 2018/1139, zohledňovat současný stav techniky a osvědčené postupy v oblasti letectví a aktualizovat svá rozhodnutí s ohledem na celosvětové zkušenosti v letectví a vědeckotechnický pokrok v daných oblastech.

¹ Nařízení (EU) 2018/1139 Evropského parlamentu a Rady 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 (Úř. věst. L 212, 22.08.2018, s. 1) (<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1535612134845&uri=CELEX:32018R1139>).

- (4) Nařízení Komise v přenesené pravomoci (EU) 2022/1645² a prováděcí nařízení Komise (EU) 2023/203³ stanovují požadavky pro organizace a příslušné úřady týkající se řízení rizik v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví.
- (5) V souvislosti s tím EASA určila potřebu vydat tento soubor přijatelných způsobů průkazu a poradenského materiálu, aby se usnadnilo provádění výše uvedených nových požadavků.
- (6) EASA, v souladu s článkem 115 odst. 1 písm. c) nařízení (EU) 2018/1139 a článkem 6 postupu pro předpisovou činnost EASA⁴, konzultovala své poradní orgány ohledně obsahu tohoto rozhodnutí, a obdržené připomínky zohlednila.

ROZHODL TAKTO:

Článek 1

Přijatelné způsoby průkazu a poradenský materiál k článkům nařízení Komise v přenesené pravomoci (EU) 2022/1645 a prováděcího nařízení Komise (EU) 2023/203 se tímto stanovují v příloze k tomuto rozhodnutí.

Článek 2

Toto rozhodnutí vstupuje v platnost den po jeho uveřejnění v Úřední publikaci EASA.

Použije se od 22. února 2026.

V Kolíně nad Rýnem dne 12. července 2023

*Za Agenturu Evropské unie pro bezpečnost letectví
Výkonný ředitel*

Patrick KY

² 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, 26.09.2022, s. 18) (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1645&qid=1688140452938>).

³ 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 (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R0203&qid=1687859731466>).

⁴ EASA je povinna dodržovat strukturovaný proces tvorby předpisů, jak je požadováno článkem 115 odst. 1 nařízení (EU) 2018/1139. Tento proces byl přijat rozhodnutím správní rady EASA (MB) a je odkazován jako „postup pro předpisovou činnost“. Viz rozhodnutí MB č. 01-2022 ze dne 2. května 2022 ohledně postupu použitého EASA při vydávání stanovisek, certifikačních specifikací a dalších podrobných specifikací, přijatelných způsobů průkazu a poradenského materiálu („postup pro předpisovou činnost“) a kterým se nahrazuje rozhodnutí správní rady č. 18-2015 (<https://www.easa.europa.eu/the-agency/management-board/decisions/easa-mb-decision-no-01-2022-rulemaking-procedure-repealing-mb>).

Přijatelné způsoby průkazu a poradenský materiál k článkům nařízení Komise v přenesené pravomoci (EU) 2022/1645 a prováděcího nařízení Komise (EU) 2023/203

První vydání
12. července 2023¹

¹ Datum vstupu v platnost tohoto vydání prosím viz rozhodnutí 2023/008/R v [Úřední publikaci](#) EASA.

OBSAH

Obsah	2
AMC a GM k článkům nařízení Komise v přenesené pravomoci (EU) 2022/1645 a prováděcího nařízení Komise (EU) 2023/203	3
GM1 Článku 1 – Předmět.....	3
GM1 Článku 3 – Definice	3

AMC A GM K ČLÁNKŮM NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) 2022/1645 A PROVÁDĚCÍHO NAŘÍZENÍ KOMISE (EU) 2023/203

GM1 Článku 1 – Předmět

Při přijímání opatření podle tohoto nařízení se dotčeným subjektům – bez ohledu na jejich velikost – doporučuje zajistit, aby opatření, která přijímají, byla přiměřená povaze a bezpečnostnímu riziku jejich činností.

GM1 Článku 3 – Definice

V zájmu obecného porozumění je níže uveden popis pojmů používaných v AMC & GM k Části IS.D.OR nařízení Komise v přenesené pravomoci (EU) 2022/1645 a také v AMC & GM k Části IS.AR a Části IS.I.OR prováděcího nařízení Komise (EU) 2023/203:

Posuzování	Assessment	V souvislosti se sledováním výkonnosti systému řízení, neustálým zlepšováním a dozorem se jedná o plánovanou a zdokumentovanou činnost prováděnou příslušnými pracovníky s cílem vyhodnotit a analyzovat dosažené úrovně výkonnosti, efektivnosti a vyspělosti, jakož i vyhovění ve vztahu k politice a cílům organizace. <i>Poznámka: Posuzování se zaměřuje na požadované výsledky a celkovou výkonnost, přičemž pohlíží na organizaci jako na celek. Hlavním cílem posuzování je identifikovat silné a slabé stránky pro řízení neustálého zlepšování.</i> <i>Poznámka: Pro „posuzování rizika“ viz definice uvedená níže.</i>
Vektor útoku (nebo cesta útoku)	Attack vector (or attack path)	Cesta, rozhraní a činnosti, kterými útočník provede útok, jak je definováno v EUROCAE ED-202.
Audit	Audit	Týká se systematického, nezávislého a zdokumentovaného procesu získávání důkazů a jejich objektivního vyhodnocení s cílem určit rozsah, v jakém jsou požadavky splněny. <i>Poznámka: Audity mohou zahrnovat kontroly.</i>
Kompetence / (odborná) způsobilost	Competency	Jde o kombinaci individuálních dovedností, praktických a teoretických znalostí, postoje, školení a zkušeností.
Náprava	Correction	Jedná se o činnost k odstranění zjištěné neshody.
Nápravné opatření	Corrective action	Jsou to kroky přijaté k odstranění nebo zmírnění kořenové příčiny (příčin) a zabránění opakování existující zjištěné neshody nebo jiných nežádoucích stavů nebo situací. Správné určení kořenové příčiny (příčin) je zásadní pro definování účinných (účelných) nápravných opatření, která zabrání opakování.

Nedostatek	Deficiency	Odchylka od vyhovění nebo nesplnění jakéhokoli požadavku nebo cílů, ať už z pohledu regulace nebo organizace, ať už zcela nebo částečně.
Praxe / zkušenost	Experience	Skutečnost nebo stav ovlivnění znalostmi a dovednostmi nebo jejich získání prostřednictvím pozorování, účasti nebo činnosti.
Funkční řetězec	Functional chain	Koncept funkčního řetězce diktuje, že rizika informační bezpečnosti jsou sdílena mezi organizacemi díky jejich příslušným rozhraním, jako jsou vztahy dodavatel-zákazník. Bezpečnostní účinky způsobené hrozbami v oblasti bezpečnosti informací se projevují především na úrovni letadla, prameníce proti proudu od letadla. V konceptu funkčního řetězce každá organizace posuzuje svá rizika informační bezpečnosti, která nemusí být schopna řešit, a tudíž může vystavit rizikům jiné organizace. Měla by předat související informace nejbližším partnerům směrem po proudu za účelem dobře informovaného řízení rizik a zajištění, aby byl celý řetězec přiměřeně chráněn, i když žádná organizace nevidí vše ani nemá plnou kontrolu.
Nebezpečí	Hazard	Stav nebo předmět s potenciálem způsobit nebo přispět k leteckému incidentu nebo nehodě.
Opatření / kontrola v oblasti bezpečnosti informací	Information security control	Opatření, které snižuje riziko.
Záměrná neoprávněná elektronická interakce	Intentional unauthorised electronic interaction	Vztahuje se k úmyslnému zapojení se do elektronických aktivit nebo komunikací (např. přístup nebo úprava počítačových systémů, sítí nebo dat) bez řádného oprávnění nebo povolení, a to ve snaze prozradit citlivé informace, upravit data, narušit běžné úkony (operace), nebo odepřít přístup legitimním uživatelům.
Spravedlivé posouzení	Just culture	Znamená kulturu, ve které nejsou frontoví pracovníci v nebo jiné osoby trestáni za činy, opomenutí nebo rozhodnutí, která přijmou, které jsou úměrné jejich zkušenostem a výcviku, ale ve které se netoleruje hrubá nedbalost, úmyslné porušování a destruktivní činy, jak je definována v článku 2 nařízení (EU) č. 376/2014 ² .
Znalosti	Knowledge	Obsah informací potřebných v práci k podávání adekvátního výkonu na přijatelné úrovni, obvykle získaných prostřednictvím formálního vzdělání a praxe na pracovišti. Tyto znalosti jsou pro výkon práce nezbytné, ale samy o sobě nestačí.
Řízení (činnost)	Management (activity)	V obecném organizačním kontextu se to týká činností zaměřených na řízení, kontrolu a neustálé zlepšování organizace v rámci vhodných struktur. V souvislosti s nařízením Komise v přenesené pravomoci (EU) 2022/1645 a prováděcím nařízením

² 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, 24.04.2014, s. 18) (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0376&qid=1669377456448>).

		Komise (EU) 2023/203 to konkrétněji znamená dohled a přijímání rozhodnutí nezbytných k dosažení cílů organizace v oblasti bezpečnosti a bezpečnosti informací.
Systém řízení	Management system	Odkazuje na soubor vzájemně propojených nebo interagujících prvků systému za účelem stanovení politik, cílů a procesů k dosažení těchto cílů, přičemž prvky systému zahrnují organizační strukturu, role a odpovědnosti, plánování a úkony (operace).
Posuzování rizika	Risk assessment	Je to hodnocení, které je založeno na inženýrském a provozním úsudku a/nebo analytických metodách s cílem stanovit, zda je dosažené nebo vnímané riziko přijatelné.
Registr rizik	Risk register	Odkazuje na fyzické nebo digitální způsoby dokumentace používané jako nástroj řízení rizik, který funguje jako úložiště všech identifikovaných rizik a obsahuje další informace o každém riziku, jako je povaha rizika, opatření ke zmírnění, vlastnictví, status atd.
Bezpečnost	Safety	Odkazuje na stav, při kterém jsou rizika spojená s leteckými činnostmi souvisejícími s provozem letadel nebo jej přímo podporujícími snížena a řízena na přijatelné úrovni, jak je definováno v Annexu 19 ICAO.
Bezpečnostní riziko	Safety risk	Odkazuje na předpokládanou pravděpodobnost a závažnost následků nebo výsledků nebezpečí. <i>Poznámka: V angličtině je pro „pravděpodobnost“ použit výraz „likelihood“ místo výrazu „probability“ proto, aby odrážel subjektivní analýzu možnosti výskytu spíše než čistě statistické hodnocení.</i>