II

(Nem jogalkotási aktusok)

RENDELETEK

A BIZOTTSÁG (EU) 2023/203 VÉGREHAJTÁSI RENDELETE

(2022. október 27.)

az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek az 1321/2014/EU, a 965/2012/EU, az 1178/2011/EU és az (EU) 2015/340 bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet hatálya alá tartozó szervezetek, valamint a 748/2012/EU, az 1321/2014/EU, a 965/2012/EU, az 1178/2011/EU, az (EU) 2015/340 és a 139/2014/EU bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet hatálya alá tartozó illetékes hatóságok tekintetében a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésére vonatkozó követelmények tekintetében történő alkalmazására vonatkozó szabályok megállapításáról, valamint az 1178/2011/EU, a 748/2012/EU, a 965/2012/EU, a 139/2014/EU, az 1321/2014/EU és az (EU) 2015/340 bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet módosításáról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a polgári légi közlekedés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról és a 2111/2005/EK, az 1008/2008/EK, a 996/2010/EU, a 376/2014/EU európai parlamenti és tanácsi rendelet és a 2014/30/EU és a 2014/53/EU európai parlamenti és tanácsi irányelv módosításáról, valamint az 552/2004/EK és a 216/2008/EK európai parlamenti és tanácsi rendelet és a 3922/91/EGK tanácsi rendelet hatályon kívül helyezéséről szóló, 2018. július 4-i (EU) 2018/1139 európai parlamenti és tanácsi rendeletre [1] és különösen annak 17. cikke (1) bekezdésének b) pontjára, 27. cikke (1) bekezdésének a) pontjára, 31. cikke (1) bekezdésének b) pontjára, 43. cikke (1) bekezdésének b) pontjára, 53. cikke (1) bekezdésének a) pontjára, valamint 62. cikke (15) bekezdésének c) pontjára,

mivel:

(1) Az (EU) 2018/1139 rendelet II. melléklete 3.1. pontjának b) alpontjában meghatározott alapvető követelményekkel összhangban a légialkalmasság-irányító szervezeteknek és a karbantartó szervezeteknek olyan irányítási rendszert kell létrehozniuk és fenntartaniuk, amely kezeli a biztonsági kockázatokat.

(2) Emellett az (EU) 2018/1139 rendelet IV. melléklete 3.3. pontjának b) alpontjában és 5. pontjának b) alpontjában meghatározott alapvető követelményekkel összhangban a pilótaképző szervezeteknek, a kabinszemélyzet-képző szervezeteknek, a légi személyzettel foglalkozó repülőorvosi központoknak és a repülésszimulációs oktatóeszközök üzemeltetőinek szintén olyan irányítási rendszert kell létrehozniuk és fenntartaniuk, amely kezeli a biztonsági kockázatokat.

(3) Hasonlóképpen, az (EU) 2018/1139 rendelet V. melléklete 8.1. pontjának c) alpontjában meghatározott alapvető követelményekkel összhangban a légijármű-üzembentartóknak is olyan irányítási rendszert kell létrehozniuk és fenntartaniuk, amely kezeli a biztonsági kockázatokat.

(4) Ezenfelül az (EU) 2018/1139 rendelet VIII. melléklete 5.1. pontjának c) alpontjában és 5.4. pontjának b) alpontjában meghatározott alapvető követelményekkel összhangban a légiforgalmi szolgáltatóknak és a léginavigációs szolgáltatóknak, a U-space szolgáltatóknak és a kizárólagos közös információs szolgáltatóknak, valamint a légiforgalmi irányítók képzési szervezeteinek és repülőorvosi központjainak szintén olyan irányítási rendszert kell létrehozniuk és fenntartaniuk, amely kezeli a biztonsági kockázatokat.

[1] HL L 212., 2018.8.22., 1. o.

(5) Az említett biztonsági kockázatok származhatnak különböző forrásokból, többek között tervezési és karbantartási hibákból, az emberi teljesítőképességgel kapcsolatos szempontokból, környezeti és információbiztonsági fenyegetésekből. Ezért az Európai Unió Repülésbiztonsági Ügynöksége (a továbbiakban: az Ügynökség), valamint a fenti preambulumbekezdésekben említett nemzeti illetékes hatóságok és szervezetek által alkalmazott irányítási rendszereknek nemcsak a véletlenszerű eseményekből eredő biztonsági kockázatokat kell figyelembe venniük, hanem az információbiztonsági fenyegetésekből eredő olyan biztonsági kockázatokat is, amelyek akkor következhetnek be, ha a meglévő hiányosságokat valaki ártó szándékkal kihasználja. Ezek az információbiztonsági kockázatok folyamatosan nőnek a polgári légi közlekedés területén, mivel a jelenlegi információs rendszerek egyre inkább összekapcsolódnak, és egyre gyakrabban válnak rosszindulatú szereplők célpontjává.

(6) A szóban forgó információs rendszerekkel kapcsolatos kockázatok nem korlátozódnak a kibertér elleni lehetséges támadásokra, hanem magukban foglalják azokat a fenyegetéseket is, amelyek hatással lehetnek a folyamatokra és eljárásokra, valamint az emberi teljesítőképességre.

(7) A digitális információk és adatok biztonságának kezelése érdekében már számos szervezet alkalmaz nemzetközi szabványokat, például az ISO 27001 szabványt. Előfordulhat, hogy ezek a szabványok nem veszik teljes mértékben figyelembe a polgári légi közlekedés valamennyi sajátosságát. Ezért helyénvaló követelményeket megállapítani a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésére vonatkozóan.

(8) Alapvető fontosságú, hogy ezek a követelmények kiterjedjenek a légi közlekedés minden területére és azok kapcsolódási pontjaira, mivel a légi közlekedés több rendszer nagy mértékű összekapcsolása révén létrejött rendszer. Ezért az említett követelményeket alkalmazni kell a 748/2012/EU ([2]), az 1321/2014/EU ([3]), a 965/2012/EU ([4]), az 1178/2011/EU ([5]), az (EU) 2015/340 ([6]) és a 139/2014/EU bizottsági rendelet ([7]), valamint az (EU) 2021/664 bizottsági végrehajtási rendelet ([8]) hatálya alá tartozó valamennyi szervezetre és illetékes hatóságra, továbbá azon szervezetekre és illetékes hatóságokra is, amelyeknek a meglévő uniós repülésbiztonsági jogszabályokkal összhangban már rendelkezniük kell irányítási rendszerrel. Egyes szervezetek esetében alacsonyabbak a légi közlekedési rendszerre gyakorolt információbiztonsági kockázatok, így a megfelelő arányosság biztosítása érdekében e szervezeteket helyénvaló kizárni e rendelet hatálya alól.

(9) Az e rendeletben meghatározott követelmények várhatóan következetes alkalmazást biztosítanak a légi közlekedés valamennyi területén, ugyanakkor minimális hatást gyakorolnak az e területeken már alkalmazandó uniós repülésbiztonsági jogszabályokra.

([2]) A Bizottság 748/2012/EU rendelete (2012. augusztus 3.) a légi járművek és kapcsolódó termékek, alkatrészek és berendezések légialkalmassági és környezetvédelmi tanúsítása, valamint a tervező és gyártó szervezetek tanúsítása végrehajtási szabályainak megállapításáról (HL L 224., 2012.8.21., 1. o.).

([3]) A Bizottság 1321/2014/EU rendelete (2014. november 26.) a légi járművek és repüléstechnikai termékek, alkatrészek és berendezések folyamatos légi alkalmasságának biztosításáról és az ezzel összefüggő feladatokban részt vevő szervezetek és személyek jóváhagyásáról (átdolgozás) (HL L 362., 2014.12.17., 1. o.).

([4]) A Bizottság 965/2012/EU rendelete (2012. október 5.) a légi járművek üzemben tartásához kapcsolódó műszaki követelményeknek és igazgatási eljárásoknak a 216/2008/EK európai parlamenti és tanácsi rendelet értelmében történő meghatározásáról (HL L 296., 2012.10.25., 1. o.).

([5]) A Bizottság 1178/2011/EU rendelete (2011. november 3.) a polgári légi közlekedéshez kapcsolódó műszaki követelményeknek és igazgatási eljárásoknak a 216/2008/EK európai parlamenti és tanácsi rendelet értelmében történő rögzítéséről (HL L 311., 2011.11.25., 1. o.).

([6]) A Bizottság (EU) 2015/340 rendelete (2015. február 20.) a légiforgalmi irányítói szakszolgálati engedélyekre és tanúsítványokra vonatkozó formai követelményeknek és igazgatási eljárásoknak a 216/2008/EK európai parlamenti és tanácsi rendelet értelmében történő meghatározásáról, a 923/2012/EU bizottsági végrehajtási rendelet módosításáról és a 805/2011/EU bizottsági rendelet hatályon kívül helyezéséről (HL L 63., 2015.3.6., 1. o.).

([7]) A Bizottság 139/2014/EU rendelete (2014. február 12.) a repülőterekhez kapcsolódó követelményeknek és igazgatási eljárásoknak a 216/2008/EK európai parlamenti és tanácsi rendelet értelmében történő meghatározásáról (HL L 44., 2014.2.14., 1. o.).

([8]) A Bizottság (EU) 2021/664 végrehajtási rendelete (2021. április 22.) a U-space szabályozási keretéről (HL L 139., 2021.4.23., 161. o.).

(10) Az e rendeletben meghatározott követelmények nem sérthetik az (EU) 2015/1998 bizottsági végrehajtási rendelet ([9]) mellékletének 1.7. pontjában és az (EU) 2016/1148 európai parlamenti és tanácsi irányelv ([10]) 14. cikkében meghatározott információbiztonsági és kiberbiztonsági követelményeket.

(11) Az (EU) 2021/696 európai parlamenti és tanácsi rendelet ([11]) V. címének (A program biztonsága) 33–43. cikkében meghatározott biztonsági követelmények egyenértékűnek tekintendők az e rendeletben meghatározott követelményekkel, kivéve az e rendelet II. mellékletének IS.I.OR.230 pontját, amelyet be kell tartani.

(12) A jogbiztonság érdekében az e rendeletben meghatározott „információbiztonság" fogalmának a polgári légi közlekedésben világszerte bevett használatot tükröző értelmezése az (EU) 2016/1148 irányelv 4. cikkének (2) bekezdésében meghatározott „hálózati és információs rendszerek biztonsága" fogalommal összhangban lévőnek tekintendő. Az „információbiztonság" fogalmának e rendeletben foglalt meghatározása nem értelmezhető úgy, mint amely eltér a „hálózati és információs rendszerek biztonsága" fogalmának az (EU) 2016/1148 irányelvben foglalt meghatározásától.

(13) A jogszabályi követelmények megkettőzésének elkerülése érdekében, amennyiben az e rendelet hatálya alá tartozó szervezetekre már vonatkoznak olyan, a (10) és (11) preambulumbekezdésben említett uniós jogi aktusokból eredő biztonsági követelmények, amelyek jellegüknél fogva egyenértékűek az e rendeletben megállapított rendelkezésekkel, az említett biztonsági követelményeknek való megfelelést az e rendeletben meghatározott követelményeknek való megfelelésnek kell tekinteni.

(14) Az e rendelet hatálya alá tartozó azon szervezeteknek, amelyekre már vonatkoznak az (EU) 2015/1998 végrehajtási rendeletből, az (EU) 2021/696 rendeletből, vagy mindkét említett rendeletből eredő biztonsági követelmények, meg kell felelniük az e rendelet II. mellékletében (IS.I.OR.230 rész, „Információbiztonsági külső jelentéstételi rendszer") foglalt követelményeknek is, mivel egyik rendelet sem tartalmaz az információbiztonsági incidensek külső bejelentésére vonatkozó rendelkezéseket.

(15) A teljesség érdekében az 1178/2011/EU, a 748/2012/EU, a 965/2012/EU, a 139/2014/EU, az 1321/2014/EU, az (EU) 2015/340 bizottsági rendeletet, valamint az (EU) 2017/373 ([12]) és az (EU) 2021/664 végrehajtási rendeletet módosítani kell annak érdekében, hogy bevezessék az e rendeletben előírt információbiztonsági irányítási rendszerre vonatkozó követelményeket és az e rendeletben meghatározott irányítási rendszereket, valamint hogy meghatározzák az illetékes hatóságokkal szemben támasztott, a fent említett információbiztonsági irányítási követelményeket végrehajtó szervezetek felügyeletére vonatkozó követelményeket.

(16) Annak érdekében, hogy a szervezeteknek elegendő idejük legyen arra, hogy gondoskodjanak az új szabályoknak és eljárásoknak való megfelelésről, e rendelet alkalmazását három évvel a hatálybalépését követően kell megkezdeni, kivéve az (EU) 2017/373 végrehajtási rendeletben meghatározott európai geostacionárius navigációs lefedési szolgáltatás (EGNOS) léginavigációs szolgáltatójával kapcsolatos rendelkezést, amelynek esetében az EGNOS-rendszernek és -szolgáltatásoknak az (EU) 2021/696 rendelettel összhangban folyamatban lévő biztonsági akkreditációja miatt a rendeletet 2026. január 1-jétől kell alkalmazni.

(17) Az e rendeletben meghatározott követelmények az Ügynökség által az (EU) 2018/1139 rendelet 75. cikke (2) bekezdésének b) és c) pontjával, valamint 76. cikkének (1) bekezdésével összhangban kiadott 03/2021. sz. véleményen ([13]) alapulnak.

([9]) A Bizottság (EU) 2015/1998 végrehajtási rendelete (2015. november 5.) a közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról (HL L 299., 2015.11.14., 1. o.).

([10]) Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

([11]) Az Európai Parlament és a Tanács (EU) 2021/696 rendelete (2021. április 28.) az uniós űrprogram és az Európai Unió Űrprogram-ügynökségének a létrehozásáról, valamint a 912/2010/EU, az 1285/2013/EU és a 377/2014/EU rendelet és az 541/2014/EU határozat hatályon kívül helyezéséről (HL L 170., 2021.5.12., 69. o.).

([12]) A Bizottság (EU) 2017/373 végrehajtási rendelete (2017. március 1.) a légiforgalmi szolgáltatást/léginavigációs szolgálatokat és más légiforgalmi szolgáltatási hálózati funkciókat és azok felügyeletét ellátó szolgáltatókra vonatkozó közös követelmények meghatározásáról, valamint a 482/2008/EK rendelet, az 1034/2011/EU, az 1035/2011/EU és az (EU) 2016/1377 végrehajtási rendelet hatályon kívül helyezéséről, továbbá a 677/2011/EU rendelet módosításáról (HL L 62., 2017.3.8., 1. o.).

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

(18) Az e rendeletben meghatározott követelmények összhangban vannak az (EU) 2018/1139 rendelet 127. cikkével létrehozott, a polgári repülés területén érvényes közös biztonsági szabályok alkalmazásáért felelős bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

Tárgy

Ez a rendelet meghatározza azokat a követelményeket, amelyeket a szervezeteknek és az illetékes hatóságoknak teljesíteniük kell annak érdekében, hogy:

a) azonosítsák és kezeljék a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatokat, amelyek hatással lehetnek a polgári repülés céljaira használt információs és kommunikációs technológiai rendszerekre és adatokra,

b) észleljék az információbiztonsági incidenseket és azonosítsák közülük azokat, amelyek a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensnek minősülnek,

c) reagáljanak, illetve megoldást találjanak az említett információbiztonsági incidensekre.

2. cikk

Hatály

(1) Ez a rendelet az alábbi szervezetekre alkalmazandó:

a) az 1321/2014/EU rendelet II. melléklete (145. rész) A. szakaszának hatálya alá tartozó karbantartó szervezetek, kivéve azokat, amelyek kizárólag az 1321/2014/EU rendelet Vb. melléklete (ML. rész) szerinti repülőgép-karbantartásban vesznek részt;

b) az 1321/2014/EU rendelet Vc. melléklete (CAMO rész) A. szakaszának hatálya alá tartozó légialkalmasság-irányító szervezetek (CAMO-k), kivéve azokat, amelyek kizárólag az 1321/2014/EU rendelet Vb. melléklete (ML. rész) szerinti légialkalmasság-irányításban vesznek részt;

c) a 965/2012/EU rendelet III. mellékletének (ORO rész) hatálya alá tartozó légijármű-üzembentartók, kivéve azokat, amelyek kizárólag a következők bármelyikének üzemeltetésében vesznek részt:

i. a 748/2012/EU rendelet 1. cikke (2) bekezdésének j) pontjában meghatározott ELA2 légi járművek;

ii. egyhajtóműves, légcsavaros, legfeljebb 5 maximális utasülésszám-konfigurációjú repülőgépek, amelyek nem minősülnek hajtóművel rendelkező komplex légi járműnek, amennyiben ugyanazon a repülőtéren vagy műveleti területen fel- és leszállva, nappali látvarepülési szabályok (VFR) szerint hajtanak végre repülést;

iii. egyhajtóműves, legfeljebb 5 maximális utasülésszám-konfigurációjú helikopterek, amelyek nem minősülnek hajtóművel rendelkező komplex légi járműnek, amennyiben ugyanazon a repülőtéren vagy műveleti területen fel- és leszállva, nappali látvarepülési szabályok (VFR) szerint hajtanak végre repülést;

d) az 1178/2011/EU rendelet VII. mellékletének (ORA rész) hatálya alá tartozó jóváhagyott képzési szervezetek, kivéve azokat, amelyek kizárólag a 748/2012/EU rendelet 1. cikke (2) bekezdésének j) pontjában meghatározott ELA2 légi járművek esetében vesznek részt képzési tevékenységekben, vagy kizárólag elméleti képzésben vesznek részt;

e) az 1178/2011/EU rendelet VII. mellékletének (ORA rész) hatálya alá tartozó, a légi személyzettel foglalkozó repülőorvosi központok;

f) az 1178/2011/EU rendelet VII. mellékletének (ORA rész) hatálya alá tartozó repülésszimulációs oktatóeszközök üzemeltetői, kivéve azokat, amelyek kizárólag a 748/2012/EU rendelet 1. cikke (2) bekezdésének j) pontjában meghatározott ELA2 légi járművek esetében vesznek részt repülésszimulációs oktatóeszközök üzemeltetésében;

g) az (EU) 2015/340 rendelet III. mellékletének (ATCO.OR rész) hatálya alá tartozó légiforgalmi irányítói képzési szervezetek (ATCO TO-k) és repülőorvosi központok;

h) az (EU) 2017/373 végrehajtási rendelet III. mellékletének (ATM/ANS.OR rész) hatálya alá tartozó szervezetek, kivéve a következő szolgáltatókat:

i. az említett melléklet ATM/ANS.OR.A.010 pontja szerinti korlátozott tanúsítvánnyal rendelkező léginavigációs szolgáltatók;

ii. az említett melléklet ATM/ANS.OR.A.015 pontjának megfelelően tevékenységükről nyilatkozatot tevő repüléstájékoztató szolgáltatók;

i) az (EU) 2021/664 végrehajtási rendelet hatálya alá tartozó U-space szolgáltatók és kizárólagos közös információs szolgáltatók.

(2) Ez a rendelet az e rendelet 6. cikkében és az (EU) 2022/1645 felhatalmazáson alapuló bizottsági rendelet ([14]) 5. cikkében említett illetékes hatóságokra, köztük az Európai Unió Repülésbiztonsági Ügynökségére (a továbbiakban: Ügynökség) alkalmazandó.

(3) Ez a rendelet az 1321/2014/EU rendelet III. mellékletének (66. rész) megfelelően a légijármű-karbantartási engedélyek kiadásáért, meghosszabbításáért, módosításáért, felfüggesztéséért vagy visszavonásáért felelős illetékes hatóságra is alkalmazandó.

(4) Ez a rendelet nem sérti az (EU) 2015/1998 végrehajtási rendelet mellékletének 1.7. pontjában és az (EU) 2016/1148 irányelv 14. cikkében meghatározott információbiztonsági és kiberbiztonsági követelményeket.

3. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „információbiztonság”: a hálózati és információs rendszerek bizalmas jellegének, integritásának, hitelességének és rendelkezésre állásának megőrzése;

2. „információbiztonsági esemény”: egy rendszer-, szolgáltatás- vagy hálózati állapot olyan azonosított előfordulása, amely az információbiztonsági szabályok esetleges megsértésére vagy az információbiztonsági ellenőrzések hibájára utal, vagy olyan, korábban ismeretlen helyzet, amely az információbiztonság szempontjából releváns lehet;

3. „incidens”: minden olyan esemény, amely kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára az (EU) 2016/1148 irányelv 4. cikkének 7. pontjában meghatározottak szerint;

4. „információbiztonsági kockázat”: valamely szervezet polgári légiközlekedési műveleteit, vagyoni eszközeit, magánszemélyeket és más szervezeteket érintő, egy esetleges információbiztonsági eseményből eredő kockázat. Az információbiztonsági kockázatok azzal a veszéllyel járnak, hogy a fenyegetések kihasználhatják egy információs eszköz vagy információseszköz-csoport sebezhetőségét;

([14]) A Bizottság (EU) 2022/1645 felhatalmazáson alapuló rendelete (2022. július 14.) az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek a 748/2012/EU és a 139/2014/EU bizottsági rendelet hatálya alá tartozó szervezetekre vonatkozó, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésével kapcsolatos követelmények tekintetében történő alkalmazására irányadó szabályok megállapításáról, valamint a 748/2012/EU és a 139/2014/EU bizottsági rendelet módosításáról (EHL L 248., 2022.9.26., 18. o).

5. „fenyegetés”: az információbiztonság olyan lehetséges megsértése, amely akkor áll fenn, ha egy szervezet, körülmény, cselekmény vagy esemény kárt okozhat;

6. „sebezhetőség”: egy eszköz, rendszer, eljárás, tervezés, végrehajtás vagy információbiztonsági intézkedés olyan hiányossága vagy gyengesége, amely kihasználható, és amely az információbiztonsági szabályok megsértését eredményezi.

4. cikk

A szervezetekre és az illetékes hatóságokra vonatkozó követelmények

(1) A 2. cikk (1) bekezdésében említett szervezeteknek meg kell felelniük az e rendelet II. mellékletében (IS.I.OR rész) foglalt követelményeknek.

(2) A 2. cikk (2) és (3) bekezdésében említett illetékes hatóságoknak meg kell felelniük az e rendelet I. mellékletében (IS.AR rész) foglalt követelményeknek.

5. cikk

Egyéb uniós jogszabályokból eredő követelmények

(1) Amennyiben a 2. cikk (1) bekezdésében említett szervezet megfelel az (EU) 2016/1148 irányelv 14. cikkének megfelelően meghatározott, az e rendeletben foglalt követelményekkel egyenértékű biztonsági követelményeknek, az említett biztonsági követelményeknek való megfelelés az e rendeletben foglalt követelményeknek való megfelelésnek minősül.

(2) Amennyiben a 2. cikk (1) bekezdésében említett szervezet a tagállamoknak a 300/2008/EK európai parlamenti és tanácsi rendelet ([15]) 10. cikkével összhangban meghatározott nemzeti polgári légiközlekedés-védelmi programjai összefüggésében említett üzemben tartó vagy jogalany, az (EU) 2015/1998 végrehajtási rendelet mellékletének 1.7. pontjában foglalt kiberbiztonsági követelmények egyenértékűnek tekintendők az e rendeletben meghatározott követelményekkel, kivéve az e rendelet II. mellékletének IS.I.OR.230 pontját, amelyet be kell tartani.

(3) Amennyiben a 2. cikk (1) bekezdésében említett szervezet az (EU) 2021/696 rendeletben említett európai geostacionárius navigációs lefedési szolgáltatás (EGNOS) léginavigációs szolgáltatója, az említett rendelet V. címének 33–43. cikkében foglalt biztonsági követelmények egyenértékűnek tekintendők az e rendeletben meghatározott követelményekkel, kivéve az e rendelet II. mellékletének IS.I.OR.230 pontját, amelyet be kell tartani.

(4) A Bizottság az Ügynökséggel és az (EU) 2016/1148 irányelv 11. cikkében említett együttműködési csoporttal folytatott konzultációt követően iránymutatásokat adhat ki az e rendeletben és az (EU) 2016/1148 irányelvben meghatározott követelmények egyenértékűségének értékelésére vonatkozóan.

6. cikk

Illetékes hatóság

(1) Az (EU) 2021/696 rendelet 36. cikkében említett, a Biztonsági Akkreditációs Bizottságra ruházott feladatok sérelme nélkül az e rendeletnek való megfelelés tanúsításáért és felügyeletéért felelős hatóság a következő:

a) a 2. cikk (1) bekezdésének a) pontjában említett szervezetek tekintetében az 1321/2014/EU rendelet II. mellékletének (145. rész) megfelelően kijelölt illetékes hatóság;

b) a 2. cikk (1) bekezdésének b) pontjában említett szervezetek tekintetében az 1321/2014/EU rendelet Vc. mellékletének (CAMO rész) megfelelően kijelölt illetékes hatóság;

([15]) Az Európai Parlament és a Tanács 300/2008/EK rendelete (2008. március 11.) a polgári légi közlekedés védelmének közös szabályairól és a 2320/2002/EK rendelet hatályon kívül helyezéséről (HL L 97., 2008.4.9., 72. o.).

c) a 2. cikk (1) bekezdésének c) pontjában említett szervezetek tekintetében a 965/2012/EU rendelet III. mellékletének (ORO rész) megfelelően kijelölt illetékes hatóság;

d) a 2. cikk (1) bekezdésének d)–f) pontjában említett szervezetek tekintetében az 1178/2011/EU rendelet VII. mellékletének (ORA rész) megfelelően kijelölt illetékes hatóság;

e) a 2. cikk (1) bekezdésének g) pontjában említett szervezetek tekintetében az (EU) 2015/340 rendelet 6. cikke (2) bekezdésének megfelelően kijelölt illetékes hatóság;

f) a 2. cikk (1) bekezdésének h) pontjában említett szervezetek tekintetében az (EU) 2017/373 végrehajtási rendelet 4. cikke (1) bekezdésének megfelelően kijelölt illetékes hatóság;

g) a 2. cikk (1) bekezdésének i) pontjában említett szervezetek tekintetében az (EU) 2021/664 végrehajtási rendelet 14. cikke (1), illetve (2) bekezdésének megfelelően kijelölt illetékes hatóság.

(2) E rendelet alkalmazásában az (1) bekezdésben említett illetékes hatóságok számára kijelölt szerep és feladatok ellátására a tagállamok kijelölhetnek egy független és önálló jogalanyt. Ebben az esetben a szervezet által teljesítendő valamennyi követelmény hatékony felügyeletének biztosítása érdekében meg kell határozni az adott jogalany és az (1) bekezdésben említett illetékes hatóságok közötti koordinálási intézkedéseket.

(3) Az Ügynökség a titoktartásra, a személyes adatok védelmére és a minősített adatok védelmére vonatkozó alkalmazandó szabályokkal teljes összhangban együttműködik az Európai Unió Űrprogramügynökségével (EUSPA) és az (EU) 2021/696 rendelet 36. cikkében említett Biztonsági Akkreditációs Bizottsággal annak érdekében, hogy biztosítsa az EGNOS léginavigációs szolgáltatójára alkalmazandó követelmények hatékony felügyeletét.

7. cikk

A releváns információk benyújtása a hálózat- és információbiztonság területén illetékes hatóságokhoz

Az e rendelet hatálya alá tartozó illetékes hatóságok indokolatlan késedelem nélkül tájékoztatják az (EU) 2016/1148 irányelv 8. cikkével összhangban kijelölt egyedüli kapcsolattartó pontot az e rendelet II. mellékletének IS.I.OR.230 pontja és az (EU) 2022/1645 felhatalmazáson alapuló rendelet I. mellékletének IS.D.OR.230 pontja alapján az (EU) 2016/1148 irányelv 5. cikkével összhangban azonosított, alapvető szolgáltatásokat nyújtó szereplők által benyújtott értesítésekben foglalt releváns információkról.

8. cikk

Az 1178/2011/EU rendelet módosítása

Az 1178/2011/EU rendelet VI. melléklete (ARA rész) és VII. melléklete (ORA rész) e rendelet III. mellékletének megfelelően módosul.

9. cikk

A 748/2012/EU rendelet módosítása

A 748/2012/EU rendelet I. melléklete (21. rész) e rendelet IV. mellékletének megfelelően módosul.

10. cikk

A 965/2012/EU rendelet módosítása

A 965/2012/EU rendelet II. melléklete (ARO rész) és III. melléklete (ORO rész) e rendelet V. mellékletének megfelelően módosul.

11. cikk

A 139/2014/EU rendelet módosítása

A 139/2014/EU rendelet II. melléklete (ADR.AR rész) e rendelet VI. mellékletének megfelelően módosul.

12. cikk

Az 1321/2014/EU rendelet módosítása

Az 1321/2014/EU rendelet II. melléklete (145. rész), III. melléklete (66. rész) és Vc. melléklete (CAMO rész) e rendelet VII. mellékletének megfelelően módosul.

13. cikk

Az (EU) 2015/340 rendelet módosítása

Az (EU) 2015/340 rendelet II. melléklete (ATCO.AR rész) és III. melléklete (ATCO.OR rész) e rendelet VIII. mellékletének megfelelően módosul.

14. cikk

Az (EU) 2017/373 végrehajtási rendelet módosítása

Az (EU) 2017/373 végrehajtási rendelet II. melléklete (ATM/ANS.AR rész) és III. melléklete (ATM/ANS.OR rész) e rendelet IX. mellékletének megfelelően módosul.

15. cikk

Az (EU) 2021/664 végrehajtási rendelet módosítása

Az (EU) 2021/664 végrehajtási rendelet a következőképpen módosul:

1. a 15. cikk (1) bekezdésének f) pontja helyébe a következő szöveg lép:

„f) az (EU) 2017/373 bizottsági végrehajtási rendelet III. melléklete D. alrészének ATM/ANS.OR.D.010 pontjával összhangban biztonságirányítási rendszert, az (EU) 2023/203 végrehajtási rendelet II. mellékletével (IS.I.OR rész) összhangban pedig információbiztonsági irányítási rendszert vezetnek be és tartanak fenn;”

2. a 18. cikk a következő l) ponttal egészül ki:

„l) az (EU) 2023/203 végrehajtási rendelet I. mellékletének (IS.AR rész) megfelelően információbiztonsági irányítási rendszert hoznak létre, alkalmaznak és tartanak fenn.”

16. cikk

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

E rendelet 2026. február 22-től alkalmazandó.

A rendelet az (EU) 2017/373 végrehajtási rendelet hatálya alá tartozó EGNOS léginavigációs szolgáltató esetében azonban 2026. január 1-jétől alkalmazandó.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2022. október 27-én.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

I. MELLÉKLET

INFORMÁCIÓBIZTONSÁG – HATÓSÁGI KÖVETELMÉNYEK

[IS.AR RÉSZ]

IS.AR.100. Hatály

IS.AR.200. Információbiztonsági irányítási rendszer (ISMS)

IS.AR.205. Információbiztonsági kockázatértékelés

IS.AR.210. Információbiztonsági kockázatkezelés

IS.AR.215. Információbiztonsági incidensek – észlelés, reagálás és helyreállítás

IS.AR.220. Információbiztonsági irányítási tevékenységek kiszervezése

IS.AR.225. Személyzeti követelmények

IS.AR.230. Nyilvántartás

IS.AR.235. Folyamatos fejlesztés

IS.AR.100. Hatály

Ez a rész meghatározza az e rendelet 2. cikkének (2) bekezdésében említett illetékes hatóságok által teljesítendő irányítási követelményeket.

Az említett illetékes hatóságok által a tanúsítási, felügyeleti és végrehajtási tevékenységeik végzése során teljesítendő követelményeket az e rendelet 2. cikkének (1) bekezdésében és az (EU) 2022/1645 felhatalmazáson alapuló rendelet 2. cikkében hivatkozott rendeletek tartalmazzák.

IS.AR.200. Információbiztonsági irányítási rendszer (ISMS)

a) Az 1. cikkben meghatározott célkitűzések megvalósítása érdekében az illetékes hatóság információbiztonsági irányítási rendszert (a továbbiakban: ISMS) hoz létre, alkalmaz és tart fenn, amely biztosítja, hogy az illetékes hatóság:

   1. olyan információbiztonsági szabályokat hozzon létre, amelyek meghatározzák az illetékes hatóság általános elveit az információbiztonsági kockázatok repülésbiztonságra gyakorolt lehetséges hatásaival kapcsolatban;

   2. az IS.AR.205. pontnak megfelelően azonosítsa és felülvizsgálja az információbiztonsági kockázatokat;

   3. az IS.AR.210. pontnak megfelelően információbiztonsági kockázatkezelési intézkedéseket határozzon meg és hajtson végre;

   4. az IS.AR.215. pontnak megfelelően meghatározza és végrehajtsa az információbiztonsági események észleléséhez szükséges intézkedéseket, azonosítsa közülük azokat, amelyek potenciálisan hatással lehetnek a repülésbiztonságra, továbbá reagáljon és megoldást találjon rájuk;

   5. az IS.AR.200. pontban leírt tevékenységek bármely részére vonatkozó, más szervezetekkel létrehozott szerződések megkötésekor megfeleljen az IS.AR.220. pontban foglalt követelményeknek;

   6. megfeleljen az IS.AR.225. pontban foglalt személyzeti követelményeknek;

   7. megfeleljen az IS.AR.230. pontban foglalt nyilvántartási követelményeknek;

   8. ellenőrizze, hogy saját szervezete megfelel-e e rendelet követelményeinek, és a korrekciós intézkedések hatékony végrehajtásának biztosítása érdekében visszajelzést adjon a megállapításokról az IS.AR.225. a) pontban említett személynek;

9. megvédje az illetékes hatóság által a felügyelete alatt álló szervezetekkel esetleg megosztott információknak, valamint a szervezet által az e rendelet II. mellékletének (IS.I.OR rész) IS.I.OR.230. pontja és az (EU) 2022/1645 felhatalmazáson alapuló rendelet mellékletének (IS.D.OR rész) IS.D.OR.230. pontja szerint létrehozott külső jelentéstételi rendszeren keresztül kapott információknak a bizalmas jellegét;

10. értesítse az Ügynökséget az illetékes hatóság e rendelet szerinti feladatainak végrehajtásával és kötelezettségeinek teljesítésével kapcsolatos képességeit érintő változásokról;

11. kialakítson és alkalmazzon olyan eljárásokat, amelyek révén szükség szerint, praktikus módon és kellő időben meg tudja osztani a többi illetékes hatósággal és ügynökséggel, valamint az e rendelet hatálya alá tartozó szervezetekkel a releváns információkat, ezzel segítve őket abban, hogy hatékony biztonsági kockázatértékeléseket végezhessenek tevékenységeikhez kapcsolódóan.

b) Az 1. cikkben említett követelmények folyamatos teljesítése érdekében az illetékes hatóság az IS.AR.235. pontnak megfelelően folyamatos fejlesztést végez.

c) Az illetékes hatóság dokumentálja az IS.AR.200. a) pontnak való megfeleléshez szükséges valamennyi kulcsfontosságú folyamatot, eljárást, szerepet és felelősségi kört, és kialakítja e dokumentáció módosításának folyamatát.

d) Az illetékes hatóság által az IS.AR.200. a) pontnak való megfelelés érdekében megállapított folyamatoknak, eljárásoknak, szerepeknek és felelősségi köröknek összhangban kell lenniük az illetékes hatóság tevékenységeinek jellegével és összetettségével az e tevékenységekkel járó információbiztonsági kockázatok értékelése alapján, és integrálhatóknak kell lenniük az illetékes hatóság által már bevezetett egyéb meglévő irányítási rendszerekbe.

IS.AR.205. Információbiztonsági kockázatértékelés

a) Az illetékes hatóság azonosítja szervezete minden olyan elemét, amely ki lehet téve információbiztonsági kockázatoknak. Idetartoznak többek között:

1. az illetékes hatóság tevékenységei, létesítményei és erőforrásai, valamint az illetékes hatóság által működtetett, nyújtott, kapott vagy fenntartott szolgáltatások;

2. az 1. pontban említett elemek működéséhez hozzájáruló berendezések, rendszerek, adatok és információk.

b) Az illetékes hatóság azonosítja a saját szervezete és más szervezetek között meglévő azon kapcsolódási pontokat, amelyek információbiztonsági kockázatoknak való kölcsönös kitettséget eredményezhetnek.

c) Az a) és b) pontban említett elemeket és kapcsolódási pontokat illetően az illetékes hatóság azonosítja a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatokat.

Az illetékes hatóság minden egyes azonosított kockázat tekintetében:

1. kockázati szintet állapít meg az illetékes hatóság által előre meghatározott osztályozásnak megfelelően;

2. az egyes kockázatokat és azok szintjét társítja az a) és b) pontnak megfelelően azonosított megfelelő elemhez vagy kapcsolódási ponthoz.

Az 1. pontban említett, előre meghatározott osztályozásnak figyelembe kell vennie a fenyegetettségi forgatókönyv megvalósulásának valószínűségét és biztonsági következményeinek súlyosságát. Ezen osztályozás révén és figyelembe véve, hogy a műveletek tekintetében az illetékes hatóság rendelkezik-e strukturált és megismételhető kockázatkezelési eljárással, az illetékes hatóságnak képesnek kell lennie annak megállapítására, hogy a kockázat elfogadható-e, vagy az IS.AR.210. pontnak megfelelően kezelendő.

A kockázatértékelések kölcsönös összehasonlíthatóságának megkönnyítése érdekében a kockázati szint 1. pont szerinti megállapítása során figyelembe kell venni a b) pontban említett szervezetekkel együttműködésben szerzett releváns információkat.

d) Az illetékes hatóság az alábbi esetek bármelyikének fennállása esetén felülvizsgálja és aktualizálja az a), b) és c) pontnak megfelelően elvégzett kockázatértékelést:

1. változás következik be az információbiztonsági kockázatoknak kitett elemek tekintetében;

2. változás következik be az illetékes hatóság szervezete és más szervezetek közötti kapcsolódási pontok vagy a többi szervezet által közölt kockázatok tekintetében;

3. változás következik be a kockázatok azonosításához, elemzéséhez és osztályozásához használt információk vagy ismeretek tekintetében;

4. tanulságok kerültek levonásra az információbiztonsági incidensek elemzéséből.

IS.AR.210. Információbiztonsági kockázatkezelés

a) Az illetékes hatóság intézkedéseket dolgoz ki az IS.AR.205. ponttal összhangban azonosított elfogadhatatlan kockázatok kezelésére, azokat időben végrehajtja, és ellenőrzi folyamatos hatékonyságukat. A szóban forgó intézkedéseknek lehetővé kell tenniük az illetékes hatóság számára, hogy:

1. ellenőrizze a fenyegetettségi forgatókönyv tényleges megvalósulásához hozzájáruló körülményeket;

2. a fenyegetettségi forgatókönyv megvalósulása esetén csökkentse a repülésbiztonsági következmények súlyosságát;

3. elkerülje a kockázatokat.

Ezek az intézkedések nem jelenthetnek potenciális új elfogadhatatlan kockázatot a repülésbiztonságra nézve.

b) Az IS.AR.225. a) pontban említett személyt és az illetékes hatóság egyéb érintett személyzetét tájékoztatni kell az IS.AR.205. pont szerint elvégzett kockázatértékelés eredményéről, a megfelelő fenyegetettségi forgatókönyvekről és a végrehajtandó intézkedésekről.

Az illetékes hatóság emellett tájékoztatja azokat a szervezeteket, amelyekkel az IS.AR.205. b) pontnak megfelelően kapcsolódási ponttal rendelkezik, az illetékes hatóságot és a szervezetet érintő kockázatokról.

IS.AR.215. Információbiztonsági incidensek – észlelés, reagálás és helyreállítás

a) Az IS.AR.205. pont szerint elvégzett kockázatértékelés és az IS.AR.210. szerint elvégzett kockázatkezelés eredménye alapján az illetékes hatóság intézkedéseket tesz az olyan események észlelésére, amelyek elfogadhatatlan kockázatok lehetséges bekövetkezését jelzik, és amelyek potenciálisan hatással lehetnek a repülésbiztonságra. A szóban forgó észlelési intézkedéseknek lehetővé kell tenniük az illetékes hatóság számára, hogy:

1. azonosítsa az előre meghatározott funkcionális teljesítmény-alapértékektől való eltéréseket;

2. bármilyen eltérés esetén figyelmeztetéseket adjon a megfelelő válaszintézkedések aktiválása érdekében.

b) Az illetékes hatóság intézkedéseket tesz annak érdekében, hogy valamely esemény kapcsán reagáljon az a) pontnak megfelelően azonosított bármely olyan körülményre, amelynek teljesülése esetén információbiztonsági incidens következhet vagy következett be. A szóban forgó válaszintézkedéseknek lehetővé kell tenniük az illetékes hatóság számára, hogy:

1. előre meghatározott erőforrások és intézkedések aktiválásával kezdeményezze a saját szervezete az a) pont 2. alpontjában említett figyelmeztetésekre való reagálását;

2. megfékezze a támadás terjedését és elkerülje a fenyegetettségi forgatókönyv teljes körű megvalósulását;

3. ellenőrizze az IS.AR.205. a) pontban meghatározott érintett elemek meghibásodásának típusát.

c) Az illetékes hatóság végrehajtja az információbiztonsági incidensek utáni helyreállítást célzó intézkedéseket, beleértve szükség esetén a vészhelyzeti intézkedéseket is. A szóban forgó helyreállítási intézkedéseknek lehetővé kell tenniük az illetékes hatóság számára, hogy:

1. megszüntesse vagy elfogadható szintre korlátozza az eseményt okozó körülményt;

2. a saját szervezete által előzetesen meghatározott helyreállási időn belül visszaállítsa az IS.AR.205. a) pontban meghatározott érintett elemek biztonságos állapotát.

IS.AR.220. Információbiztonsági irányítási tevékenységek kiszervezése

Az illetékes hatóság biztosítja, hogy az IS.AR.200. pontban említett tevékenységek bármely részére vonatkozó, más szervezetekkel létrehozott szerződések megkötésekor a kiszervezett tevékenységek megfeleljenek e rendelet követelményeinek, és a megbízott szervezet a megbízó szervezet felügyelete alatt működjön. Az illetékes hatóság biztosítja a kiszervezett tevékenységekkel kapcsolatos kockázatok megfelelő kezelését.

IS.AR.225. Személyzeti követelmények

Az illetékes hatóság:

a) rendelkezik olyan személlyel, akinek felhatalmazása van az e rendelet végrehajtásához szükséges szervezeti struktúrák, szabályok, folyamatok és eljárások kialakítására és fenntartására.

A szóban forgó személy:

1. felhatalmazással rendelkezik arra, hogy maradéktalanul hozzáférjen az e rendelet szerinti összes feladat ellátásához az illetékes hatóság számára szükséges forrásokhoz;

2. rendelkezik a kijelölt feladatok ellátásához szükséges felhatalmazással;

b) rendelkezik olyan eljárással, amely biztosítja, hogy elegendő személyzet álljon rendelkezésre az e melléklet hatálya alá tartozó tevékenységek elvégzéséhez;

c) rendelkezik olyan eljárással, amely biztosítja, hogy a b) pontban említett személyzet rendelkezzen a feladatai ellátásához szükséges szakértelemmel;

d) rendelkezik olyan eljárással, amely biztosítja, hogy a személyzet elismerje a kijelölt szerepekhez és feladatokhoz kapcsolódó felelősségi köröket;

e) biztosítja, hogy az információs rendszerekhez és az e rendelet követelményeinek hatálya alá tartozó adatokhoz hozzáféréssel rendelkező személyzet megfelelő és megbízható legyen.

IS.AR.230. Nyilvántartás

a) Az illetékes hatóság nyilvántartást vezet információbiztonsági irányítási tevékenységeiről.

1. Az illetékes hatóság biztosítja a következő nyilvántartások archiválását és nyomonkövethetőségét:

i. az IS.AR.200. a) 5. pontban említett tevékenységekre vonatkozó szerződések;

ii. az IS.AR.200. d) pontban említett kulcsfontosságú folyamatokkal kapcsolatos nyilvántartások;

iii. az IS.AR.205. pontban említett kockázatértékelés eredményeképpen azonosított kockázatok, valamint az IS.AR.210. pontban említett kapcsolódó kockázatkezelési intézkedések nyilvántartása;

iv. azon információbiztonsági események nyilvántartása, amelyeket újra kell értékelni a fel nem tárt információbiztonsági incidensek vagy sebezhetőségek feltárása érdekében.

2. Az 1. pont i. alpontjában említett nyilvántartásokat a szerződés módosítását vagy megszüntetését követően legalább öt évig meg kell őrizni.

3. Az 1. pont ii. és iii. alpontjában említett nyilvántartásokat legalább 5 évig meg kell őrizni.

4. Az 1. pont iv. alpontjában említett nyilvántartásokat mindaddig meg kell őrizni, amíg ezeket az információbiztonsági eseményeket az illetékes hatóság által megállapított eljárásban meghatározott rendszerességgel újraértékelik.

b) Az illetékes hatóság nyilvántartást vezet az információbiztonsági irányítási tevékenységekben részt vevő saját személyzetének képesítéséről és tapasztalatáról.

1. A személyzet képesítéséről és tapasztalatáról vezetett nyilvántartást mindaddig meg kell őrizni, amíg az adott személy az illetékes hatóságnál dolgozik, és legalább három évig azt követően, hogy az adott személy elhagyta az illetékes hatóságot.

2. A személyzet tagjai számára – kérésükre – hozzáférést kell biztosítani egyéni nyilvántartásaikhoz. Ezen túlmenően, amikor az említett személyek elhagyják az illetékes hatóságot, az illetékes hatóság az érintettek kérésére köteles átadni nekik a róluk vezetett egyéni nyilvántartás másolatát.

c) A nyilvántartások formátumát az illetékes hatóság eljárásaiban kell meghatározni.

d) A nyilvántartásokat oly módon kell tárolni, hogy biztosított legyen a sérüléssel, megváltoztatással és lopással szembeni védelmük, és az információk szükség esetén biztonsági besorolási szintjüknek megfelelően azonosíthatók legyenek. Az illetékes hatóság gondoskodik arról, hogy a nyilvántartásokat olyan eszközökkel tárolják, amelyek biztosítják azok integritását és hitelességét, valamint az azokhoz való engedélyezett hozzáférést.

IS.AR.235. Folyamatos fejlesztés

a) Az illetékes hatóság megfelelő teljesítménymutatók alkalmazásával értékeli a saját ISMS-e hatékonyságát és érettségét. Az értékelést az illetékes hatóság által előre meghatározott naptári ütemezés szerint vagy egy információbiztonsági incidenst követően kell elvégezni.

b) Amennyiben az a) pontnak megfelelően elvégzett értékelést követően hiányosságokat tárnak fel, az illetékes hatóság meghozza a szükséges javító intézkedéseket annak biztosítása érdekében, hogy az ISMS továbbra is megfeleljen az alkalmazandó követelményeknek, és elfogadható szinten tartsa az információbiztonsági kockázatokat. Az illetékes hatóság továbbá újraértékeli az ISMS-nek az elfogadott intézkedések által érintett elemeit.

II. MELLÉKLET

INFORMÁCIÓBIZTONSÁG – A SZERVEZETEKRE VONATKOZÓ KÖVETELMÉNYEK

[IS.I.OR RÉSZ]

IS.I.OR.100. Hatály

IS.I.OR.200. Információbiztonsági irányítási rendszer (ISMS)

IS.I.OR.205. Információbiztonsági kockázatértékelés

IS.I.OR.210. Információbiztonsági kockázatkezelés

IS.I.OR.215. Információbiztonsági belső jelentéstételi rendszer

IS.I.OR.220. Információbiztonsági incidensek – észlelés, reagálás és helyreállítás

IS.I.OR.225. Reagálás az illetékes hatóság által közölt megállapításokra

IS.I.OR.230. Információbiztonsági külső jelentéstételi rendszer

IS.I.OR.235. Információbiztonsági irányítási tevékenységek kiszervezése

IS.I.OR.240. Személyzeti követelmények

IS.I.OR.245. Nyilvántartás

IS.I.OR.250. Információbiztonsági irányítási kézikönyv (ISMM)

IS.I.OR.255. Az információbiztonsági irányítási rendszer változásai

IS.I.OR.260. Folyamatos fejlesztés

IS.I.OR.100. Hatály

Ez a rész meghatározza az e rendelet 2. cikkének (1) bekezdésben említett szervezetek által teljesítendő követelményeket.

IS.I.OR.200. Információbiztonsági irányítási rendszer (ISMS)

a) Az 1. cikkben meghatározott célkitűzések megvalósítása érdekében a szervezet információbiztonsági irányítási rendszert (a továbbiakban: ISMS) hoz létre, alkalmaz és tart fenn, amely biztosítja, hogy a szervezet:

   1. olyan információbiztonsági szabályokat hozzon létre, amelyek meghatározzák a szervezet általános elveit az információbiztonsági kockázatok repülésbiztonságra gyakorolt lehetséges hatásaival kapcsolatban;

   2. az IS.I.OR.205. pontnak megfelelően azonosítsa és felülvizsgálja az információbiztonsági kockázatokat;

   3. az IS.I.OR.210. pontnak megfelelően információbiztonsági kockázatkezelési intézkedéseket határozzon meg és hajtson végre;

   4. az IS.I.OR.215. pontnak megfelelően információbiztonsági belső jelentéstételi rendszert alkalmazzon;

   5. az IS.I.OR.220. pontnak megfelelően meghatározza és végrehajtsa az információbiztonsági események észleléséhez szükséges intézkedéseket, azonosítsa közülük azokat, amelyek az IS.I.OR.205. e) pont által megengedettek kivételével potenciálisan hatással lehetnek a repülésbiztonságra, továbbá reagáljon és megoldást találjon rájuk;

6. végrehajtsa az illetékes hatóság által a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre adott azonnali reagálásként bejelentett intézkedéseket;

7. az IS.I.OR.225. pontnak megfelelően meghozza a megfelelő intézkedéseket az illetékes hatóság által közölt megállapítások kezelésére;

8. az IS.I.OR.230. pontnak megfelelően külső jelentéstételi rendszert alkalmazzon annak érdekében, hogy az illetékes hatóság meghozhassa a megfelelő intézkedéseket;

9. az IS.I.OR.200. pontban említett tevékenységek bármely részére vonatkozó, más szervezetekkel létrehozott szerződések megkötésekor megfeleljen az IS.I.OR.235. pontban foglalt követelményeknek;

10. megfeleljen az IS.I.OR.240. pontban meghatározott személyzeti követelményeknek;

11. megfeleljen az IS.I.OR.245. pontban meghatározott nyilvántartási követelményeknek;

12. ellenőrizze, hogy a szervezete megfelel-e e rendelet követelményeinek, és a korrekciós intézkedések hatékony végrehajtásának biztosítása érdekében visszajelzést adjon a megállapításokról a felelős vezetőnek;

13. a biztonsági események jelentésére vonatkozó alkalmazandó követelmények sérelme nélkül védje a szervezet más szervezetektől kapott információinak bizalmas jellegét, az adott információk érzékenységi szintjének megfelelően.

b) Az 1. cikkben említett követelmények folyamatos teljesítése érdekében a szervezet az IS.I.OR.260. pontnak megfelelően folyamatos fejlesztést végez.

c) A szervezet az IS.I.OR.250. pontnak megfelelően dokumentálja az IS.I.OR.200. a) pontnak való megfeleléshez szükséges valamennyi kulcsfontosságú folyamatot, eljárást, szerepet és felelősségi kört, és kialakítja a dokumentáció módosításának folyamatát. Az említett folyamatokat, eljárásokat, szerepeket és felelősségi köröket érintő változásokat az IS.I.OR.255. pontnak megfelelően kell kezelni.

d) A szervezet által az IS.I.OR.200. a) pontnak való megfelelés érdekében megállapított folyamatoknak, eljárásoknak, szerepeknek és felelősségi köröknek összhangban kell lenniük a szervezet tevékenységeinek jellegével és összetettségével az e tevékenységekkel járó információbiztonsági kockázatok értékelése alapján, és azok integrálhatók a szervezet által már bevezetett egyéb meglévő irányítási rendszerekbe.

e) A 376/2014/EU rendeletben rögzített jelentéstételi követelményeknek és az IS.I.OR.200. a) 13. pontban foglalt követelményeknek való megfelelésre vonatkozó kötelezettség sérelme nélkül az illetékes hatóság jóváhagyhatja, hogy a szervezet ne hajtsa végre az a)–d) pontban említett követelményeket, valamint az IS.I.OR.205–IS.I.OR.260. pontban említett kapcsolódó követelményeket, amennyiben a szervezet a szóban forgó hatóság számára kielégítően bizonyítja, hogy tevékenységei, létesítményei és erőforrásai, valamint az általa működtetett, nyújtott, kapott és fenntartott szolgáltatások sem az adott szervezet, sem más szervezetek tekintetében nem jelentenek a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatot. A jóváhagyásnak a szervezet vagy egy harmadik fél által az IS.I.OR.205. pontnak megfelelően elvégzett és dokumentált, valamint a releváns illetékes hatóság által felülvizsgált és jóváhagyott információbiztonsági kockázatértékelésen kell alapulnia.

A jóváhagyás folyamatos érvényességét az illetékes hatóság az alkalmazandó felügyeleti ellenőrzési ciklust követően, valamint minden olyan esetben felülvizsgálja, amikor a szervezet tevékenységi körében változtatásokat hajtanak végre.

IS.I.OR.205. Információbiztonsági kockázatértékelés

a) A szervezet azonosítja minden olyan elemét, amely ki lehet téve információbiztonsági kockázatoknak. Ez a következőket foglalja magában:

1. a szervezet tevékenységei, létesítményei és erőforrásai, valamint a szervezet által működtetett, nyújtott, kapott vagy fenntartott szolgáltatások;

2. az 1. pontban felsorolt elemek működéséhez hozzájáruló berendezések, rendszerek, adatok és információk.

b) A szervezet azonosítja a közte és más szervezetek között meglévő azon kapcsolódási pontokat, amelyek információbiztonsági kockázatoknak való kölcsönös kitettséget eredményezhetnek.

c) Az a) és b) pontban említett elemek és kapcsolódási pontok tekintetében a szervezet azonosítja a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatokat. A szervezet minden egyes azonosított kockázat tekintetében:

1. kockázati szintet állapít meg a szervezet által előre meghatározott osztályozásnak megfelelően;

2. az egyes kockázatokat és azok szintjét társítja az a) és b) pontnak megfelelően azonosított megfelelő elemhez vagy kapcsolódási ponthoz.

Az 1. pontban említett, előre meghatározott osztályozásnak figyelembe kell vennie a fenyegetettségi forgatókönyv megvalósulásának valószínűségét és biztonsági következményeinek súlyosságát. Ezen osztályozás alapján és figyelembe véve, hogy a műveletek tekintetében a szervezet rendelkezik-e strukturált és megismételhető kockázatkezelési eljárással, a szervezetnek képesnek kell lennie annak megállapítására, hogy a kockázat elfogadható-e, vagy az IS.I.OR.210. pontnak megfelelően kezelendő.

A kockázatértékelések kölcsönös összehasonlíthatóságának megkönnyítése érdekében a kockázati szint 1. pont szerinti megállapítása során figyelembe kell venni a b) pontban említett szervezetekkel együttműködésben szerzett releváns információkat.

d) A szervezet az alábbi helyzetek bármelyikének fennállása esetén felülvizsgálja és aktualizálja az a), b) és adott esetben a c) vagy e) pontnak megfelelően elvégzett kockázatértékelést:

1. változás következik be az információbiztonsági kockázatoknak kitett elemek tekintetében;

2. változás következik be a szervezet és más szervezetek közötti kapcsolódási pontok vagy a többi szervezet által közölt kockázatok tekintetében;

3. változás következik be a kockázatok azonosításához, elemzéséhez és osztályozásához használt információk vagy ismeretek tekintetében;

4. tanulságok kerültek levonásra az információbiztonsági incidensek elemzéséből.

e) A c) ponttól eltérve, az (EU) 2017/373 végrehajtási rendelet III. mellékletének (Part-ATM/ANS.OR) C. alrészben foglalt rendelkezések betartására kötelezett szervezeteknek a repülésbiztonságot érintő hatás elemzése helyett a szolgáltatásaikra gyakorolt hatás elemzését kell elvégezniük az ATM/ANS.OR.C.005. pontban előírt repülésbiztonság-támogatási értékelés szerint. Ezt a repülésbiztonság-támogatási értékelést rendelkezésre kell bocsátaniuk azoknak a légiforgalmi szolgáltatóknak, amelyeknek szolgáltatásokat nyújtanak, és e légiforgalmi szolgáltatók feladata lesz a repülésbiztonságot érintő hatás értékelése.

IS.I.OR.210. Információbiztonsági kockázatkezelés

a) A szervezet intézkedéseket dolgoz ki az IS.I.OR.205. ponttal összhangban azonosított elfogadhatatlan kockázatok kezelésére, azokat időben végrehajtja, és ellenőrzi folyamatos hatékonyságukat. A szóban forgó intézkedéseknek lehetővé kell tenniük a szervezet számára, hogy:

1. ellenőrizze a fenyegetettségi forgatókönyv tényleges megvalósulásához hozzájáruló körülményeket;

2. a fenyegetettségi forgatókönyv megvalósulása esetén csökkentse a repülésbiztonsági következmények súlyosságát;

3. elkerülje a kockázatokat.

Ezek az intézkedések nem jelenthetnek potenciális új elfogadhatatlan kockázatot a repülésbiztonságra nézve.

b) Az IS.I.OR.240. a) és b) pontban említett személyt és a szervezet egyéb érintett személyzetét tájékoztatni kell az IS.I.OR.205. pont szerint elvégzett kockázatértékelés eredményéről, a megfelelő fenyegetettségi forgatókönyvekről és a végrehajtandó intézkedésekről.

A szervezet emellett tájékoztatja azokat a szervezeteket, amelyekkel az IS.I.OR.205. b) pontnak megfelelően kapcsolódási ponttal rendelkezik, a mindkét szervezetet érintő kockázatokról.

IS.I.OR.215. Információbiztonsági belső jelentéstételi rendszer

a) A szervezet belső jelentéstételi rendszert hoz létre az információbiztonsági események – köztük az IS.I.OR.230. pont szerint bejelentendő események – összegyűjtésének és értékelésének lehetővé tétele érdekében.

b) A szóban forgó rendszernek és az IS.I.OR.220. pontban említett eljárásnak lehetővé kell tennie a szervezet számára, hogy:

1. megállapítsa, hogy az a) pont szerint bejelentett események közül melyek minősülnek a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidenseknek vagy sebezhetőségeknek;

2. azonosítsa az 1. pontnak megfelelően megállapított információbiztonsági incidensek és sebezhetőségek okait és az azokhoz hozzájáruló tényezőket, és az IS.I.OR.205. és az IS.I.OR.220. pont szerinti információbiztonsági kockázatkezelési eljárás részeként kezelje azokat;

3. biztosítsa az 1. pontnak megfelelően azonosított információbiztonsági incidensekkel és sebezhetőségekkel kapcsolatos valamennyi ismert és releváns információ értékelését;

4. szükség esetén biztosítsa az információk belső terjesztésére szolgáló módszer alkalmazását.

c) Minden olyan, szerződés keretében megbízott szervezetnek, amely a szervezetet a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatnak teheti ki, be kell jelentenie a szervezetnek az információbiztonsági eseményeket. A szóban forgó jelentéseket az egyedi szerződéses megállapodásokban meghatározott eljárások szerint kell benyújtani és a b) ponttal összhangban kell értékelni.

d) A szervezet együttműködik a vizsgálatokban minden más olyan szervezettel, amely jelentős mértékben hozzájárul saját tevékenységeinek információbiztonságához.

e) A szervezet integrálhatja ezt a jelentéstételi rendszert más, már alkalmazott jelentéstételi rendszerekbe.

IS.I.OR.220. Információbiztonsági incidensek – észlelés, reagálás és helyreállítás

a) Az IS.I.OR.205. pont szerint elvégzett kockázatértékelés és az IS.I.OR.210. szerint elvégzett kockázatkezelés eredménye alapján a szervezet intézkedéseket tesz az olyan események és sebezhetőségek észlelésére, amelyek elfogadhatatlan kockázatok lehetséges bekövetkezését jelzik, és amelyek potenciálisan hatással lehetnek a repülésbiztonságra. A szóban forgó észlelési intézkedéseknek lehetővé kell tenniük a szervezet számára, hogy:

1. azonosítsa az előre meghatározott funkcionális teljesítmény-alapértékektől való eltéréseket;

2. bármilyen eltérés esetén figyelmeztetéseket adjon a megfelelő válaszintézkedések aktiválása érdekében.

b) A szervezet intézkedéseket tesz annak érdekében, hogy valamely esemény kapcsán reagáljon az a) pontnak megfelelően azonosított bármely olyan körülményre, amelynek teljesülése esetén információbiztonsági incidens következhet vagy következett be. A szóban forgó válaszintézkedéseknek lehetővé kell tenniük a szervezet számára, hogy:

1. előre meghatározott erőforrások és intézkedések aktiválásával kezdeményezze az a) pont 2. alpontjában említett figyelmeztetésekre való reagálást;

2. megfékezze a támadás terjedését és elkerülje a fenyegetettségi forgatókönyv teljes körű megvalósulását;

3. ellenőrizze az IS.I.OR.205. a) pontban meghatározott érintett elemek meghibásodásának típusát.

c) A szervezet végrehajtja az információbiztonsági incidensek utáni helyreállítást célzó intézkedéseket, beleértve szükség esetén a vészhelyzeti intézkedéseket is. A szóban forgó helyreállítási intézkedéseknek lehetővé kell tenniük a szervezet számára, hogy:

1. megszüntesse vagy elfogadható szintre korlátozza az eseményt okozó körülményt;

2. a szervezet által előzetesen meghatározott helyreállási időn belül biztonságos állapotba hozza az IS.I.OR.205. a) pontban meghatározott érintett elemeket.

IS.I.OR.225. Reagálás az illetékes hatóság által közölt megállapításokra

a) Az illetékes hatóság által benyújtott, a megállapításokról szóló értesítés kézhezvételét követően a szervezet:

1. meghatározza a meg nem felelés kiváltó okát vagy okait, illetve az azt előidéző tényezőket;

2. korrekciós intézkedési tervet dolgoz ki;

3. az illetékes hatóság számára kielégítő módon igazolja a meg nem felelés orvoslását.

b) Az a) pontban említett intézkedéseket az illetékes hatósággal egyeztetett határidőn belül kell végrehajtani.

IS.I.OR.230. Információbiztonsági külső jelentéstételi rendszer

a) A szervezet olyan információbiztonsági jelentéstételi rendszert működtet, amely megfelel a 376/2014/EU rendeletben, valamint az ahhoz kapcsolódó felhatalmazáson alapuló és végrehajtási jogi aktusokban meghatározott követelményeknek, amennyiben a szóban forgó rendelet alkalmazandó a szervezetre.

b) A 376/2014/EU rendeletben foglalt kötelezettségek sérelme nélkül a szervezet biztosítja, hogy az illetékes hatóság bejelentést kapjon minden olyan információbiztonsági incidensről vagy sebezhetőségről, amely jelentős kockázatot jelenthet a repülésbiztonságra. Továbbá:

1. amennyiben egy ilyen incidens vagy sebezhetőség valamely légi járművet vagy kapcsolódó rendszert vagy komponenst érinti, a szervezet azt a tervjóváhagyás jogosultjának is jelenti;

2. amennyiben egy ilyen incidens vagy sebezhetőség a szervezet által használt rendszert vagy rendszerelemet érinti, a szervezet jelenti azt a rendszer vagy rendszerelem tervezéséért felelős szervezetnek.

c) A szervezet az alábbiak szerint jelenti a b) pontban említett körülményeket:

1. amint a szervezet tudomást szerez a körülményről, értesítést nyújt be az illetékes hatóságnak és adott esetben a tervjóváhagyás jogosultjának, illetve a rendszer vagy rendszerelem tervezéséért felelős szervezetnek;

2. a lehető leghamarabb, de legfeljebb 72 órával azt követően, hogy a szervezet tudomást szerez a körülményről, jelentést nyújt be az illetékes hatóságnak és adott esetben a tervjóváhagyás jogosultjának, illetve a rendszer vagy rendszerelem tervezéséért felelős szervezetnek, kivéve, ha ezt rendkívüli körülmények megakadályozzák.

   A jelentést az illetékes hatóság által meghatározott formában kell elkészíteni, és annak tartalmaznia kell a körülményre vonatkozóan a szervezet birtokában lévő valamennyi lényeges információt;

3. nyomonkövetési jelentést nyújt be az illetékes hatóságnak és adott esetben a tervjóváhagyás jogosultjának, illetve a rendszer vagy rendszerelem tervezéséért felelős szervezetnek, amelyben részletesen ismerteti azokat az intézkedéseket, amelyeket a szervezet az incidens utáni helyreállítás érdekében tett vagy szándékozik tenni, valamint a hasonló információbiztonsági incidensek jövőbeli megelőzése érdekében tervezett intézkedéseket.

   A nyomonkövetési jelentést az intézkedések meghatározását követően azonnal be kell nyújtani, és az illetékes hatóság által meghatározott formában kell elkészíteni.

IS.I.OR.235. Információbiztonsági irányítási tevékenységek kiszervezése

a) A szervezet biztosítja, hogy az IS.I.OR.200. pontban említett tevékenységek bármely részére vonatkozó, más szervezetekkel létrehozott szerződések megkötésekor a kiszervezett tevékenységek megfeleljenek e rendelet követelményeinek, és a megbízott szervezet a megbízó szervezet felügyelete alatt működjön. A szervezet biztosítja a kiszervezett tevékenységekkel kapcsolatos kockázatok megfelelő kezelését.

b) A szervezet biztosítja, hogy az illetékes hatóság kérésre felvehesse a kapcsolatot a megbízott szervezettel az e rendeletben meghatározott alkalmazandó követelményeknek való folyamatos megfelelés ellenőrzése céljából.

IS.I.OR.240. Személyzeti követelmények

a) Az e rendelet 2. cikkének (1) bekezdésében említett és adott esetben az 1321/2014/EU, a 965/2012/EU, az 1178/2011/EU, az (EU) 2015/340 rendelet, az (EU) 2017/373 végrehajtási rendelet vagy az (EU) 2021/664 végrehajtási rendelet szerint kijelölt szervezet felelős vezetője vállalati felhatalmazással rendelkezik annak biztosítására, hogy az e rendeletben előírt valamennyi tevékenység finanszírozható és elvégezhető legyen. A szóban forgó személy:

1. biztosítja, hogy minden szükséges erőforrás rendelkezésre álljon az e rendelet követelményeinek való megfeleléshez;

2. kidolgozza és előmozdítja az IS.I.OR.200. a) 1. pontban említett információbiztonsági szabályokat;

3. igazolja, hogy e rendeletet illetően rendelkezik az alapvető ismeretekkel.

b) A felelős vezető kijelöl egy vagy több személyt annak biztosítására, hogy a szervezet megfeleljen e rendelet követelményeinek, és meghatározza az érintett(ek) hatáskörét. A kijelölt személy vagy személyek csoportja közvetlenül a felelős vezetőnek számol be, rendelkezik a feladatai ellátáshoz szükséges megfelelő szaktudással, szakmai háttérrel és tapasztalattal. Az eljárásokban meg kell határozni, hogy az adott személyek hosszabb távolléte esetén ki helyettesíti őket.

c) A felelős vezető kijelöl egy vagy több személyt, aki(k) az IS.I.OR.200. a) 12. pontban említett megfelelőség-ellenőrzés irányításáért felel(nek).

d) Amennyiben a szervezet információbiztonsági szervezeti struktúrákat, szabályokat, folyamatokat és eljárásokat oszt meg más szervezetekkel vagy saját szervezete olyan területeivel, amelyekre nem terjed ki a jóváhagyás vagy a nyilatkozat, a felelős vezető átruházhatja tevékenységét egy közös felelős személyre.

Ebben az esetben az információbiztonság-irányítás szervezeten belüli megfelelő integrációjának biztosítása érdekében meg kell határozni a felelős vezető és a közös felelős személy közötti koordinálási intézkedéseket.

e) A felelős vezető a d) pontban említett közös felelős személy vállalati felhatalmazással rendelkezik az IS.I.OR.200. pont végrehajtásához szükséges szervezeti struktúrák, szabályok, folyamatok és eljárások kialakítására és fenntartására.

f) A szervezetnek rendelkeznie kell egy olyan eljárással, amely biztosítja, hogy elegendő személyzet álljon rendelkezésre az e melléklet hatálya alá tartozó tevékenységek elvégzéséhez.

g) A szervezetnek rendelkeznie kell egy olyan eljárással, amely biztosítja, hogy az f) pontban említett személyzet rendelkezzen a feladatai ellátásához szükséges szakértelemmel.

h) A szervezetnek rendelkeznie kell egy olyan eljárással, amely biztosítja, hogy a személyzet elismerje a kijelölt szerepekhez és feladatokhoz kapcsolódó felelősségi köröket.

i) A szervezet biztosítja, hogy az információs rendszerekhez és az e rendelet követelményeinek hatálya alá tartozó adatokhoz hozzáféréssel rendelkező személyzet megfelelő és megbízható legyen.

IS.I.OR.245. Nyilvántartás

a) *A szervezet nyilvántartást vezet információbiztonsági irányítási tevékenységeiről*

1. A szervezet biztosítja a következő nyilvántartások archiválását és nyomonkövethetőségét:

   i. az IS.I.OR.200. e) ponttal összhangban kapott jóváhagyások és a kapcsolódó információbiztonsági kockázatértékelés;

   ii. az IS.I.OR.200. a) 9. pontban említett tevékenységekre vonatkozó szerződések;

   iii. az IS.I.OR.200. d) pontban említett kulcsfontosságú folyamatokkal kapcsolatos nyilvántartások;

   iv. az IS.I.OR.205. pontban említett kockázatértékelés eredményeképpen azonosított kockázatok, valamint az IS.I.OR.210. pontban említett kapcsolódó kockázatkezelési intézkedések nyilvántartása;

   v. az IS.I.OR.215. és az IS.I.OR.230. pontban említett jelentéstételi rendszerekkel összhangban bejelentett információbiztonsági incidensek és sebezhetőségek nyilvántartása;

   vi. azon információbiztonsági események nyilvántartása, amelyeket újra kell értékelni a fel nem tárt információbiztonsági incidensek vagy sebezhetőségek feltárása érdekében.

2. Az 1. pont i. alpontjában említett nyilvántartásokat a jóváhagyás érvényességének megszűnését követően legalább öt évig meg kell őrizni.

3. Az 1. pont ii. alpontjában említett nyilvántartásokat a szerződés módosítását vagy megszüntetését követően legalább öt évig meg kell őrizni.

4. Az 1. pont iii., iv. és v. alpontjában említett nyilvántartásokat legalább öt évig meg kell őrizni.

5. Az 1. pont vi. alpontjában említett nyilvántartásokat mindaddig meg kell őrizni, amíg ezeket az információbiztonsági eseményeket a szervezet által megállapított eljárásban meghatározott rendszerességgel újraértékelik.

b) *A szervezet nyilvántartást vezet az információbiztonsági irányítási tevékenységekben részt vevő saját személyzetének képesítéséről és tapasztalatáról*

1. A személyzet képesítéséről és tapasztalatáról vezetett nyilvántartást mindaddig meg kell őrizni, amíg az adott személy a szervezetnél dolgozik, és legalább három évig azt követően, hogy az adott személy elhagyta a szervezetet.

2. A személyzet tagjai számára – kérésükre – hozzáférést kell biztosítani egyéni nyilvántartásaikhoz. Ezen túlmenően, amikor az említett személyek elhagyják a szervezetet, a szervezet az érintettek kérésére köteles átadni nekik a róluk vezetett egyéni nyilvántartás másolatát.

c) A nyilvántartások formátumát a szervezet eljárásaiban kell meghatározni.

d) A nyilvántartásokat oly módon kell tárolni, hogy biztosított legyen a sérüléssel, megváltoztatással és lopással szembeni védelmük, és az információk szükség esetén biztonsági besorolási szintjüknek megfelelően azonosíthatók legyenek. A szervezet gondoskodik arról, hogy a nyilvántartásokat olyan eszközökkel tárolják, amelyek biztosítják azok integritását és hitelességét, valamint az azokhoz való engedélyezett hozzáférést.

IS.I.OR.250. Információbiztonsági irányítási kézikönyv (ISMM)

a) A szervezet az illetékes hatóság rendelkezésére bocsát egy információbiztonsági irányítási kézikönyvet (a továbbiakban: ISMM) – és adott esetben bármely hivatkozott kapcsolódó kézikönyvet és eljárást –, amely a következőket tartalmazza:

1. a felelős vezető által aláírt nyilatkozat, amely megerősíti, hogy a szervezet mindenkor e mellékletnek és az ISMM-nek megfelelően fog működni. Amennyiben a felelős vezető nem a szervezet vezérigazgatója, akkor az ilyen nyilatkozatot a vezérigazgatónak ellen kell jegyeznie;

2. az IS.I.OR.240. b) és c) pontban meghatározott személy vagy személyek beosztása, neve, feladatai, elszámoltathatósága, felelősségi köre és hatásköre;

3. adott esetben az IS.I.OR.240. d) pontban meghatározott közös felelős személy beosztása, neve, feladatai, elszámoltathatósága, felelősségi köre és hatásköre;

4. a szervezet IS.I.OR.200. a) 1. pontban említett információbiztonsági szabályai;

5. az IS.I.OR.240. pontban előírt személyzet létszámának és kategóriáinak, valamint a személyzeti rendelkezésre állás tervezésére szolgáló rendszernek az általános leírása;

6. az IS.I.OR.200. pont végrehajtásáért felelős kulcsfontosságú személyek, köztük az IS.I.OR.200. a) 12. pontban említett megfelelés-ellenőrzésért felelős személy vagy személyek beosztása, neve, feladatai, elszámoltathatósága, felelősségi köre és hatásköre;

7. szervezeti ábra, amely bemutatja a kapcsolódó elszámoltathatósági és felelősségi láncokat a 2. és 6. pontban említett személyek tekintetében;

8. az IS.I.OR.215. pontban említett belső jelentéstételi rendszer leírása;

9. azok az eljárások, amelyek meghatározzák, hogy a szervezet hogyan biztosítja az e résznek való megfelelést, és különösen a következők:

i. az IS.I.OR.200. c) pontban említett dokumentáció;

ii. azon eljárások, amelyek meghatározzák, hogy a szervezet hogyan ellenőrzi az IS.I.OR.200. a) 9. pontban említett kiszervezett tevékenységeket;

iii. a c) pontban említett ISMM-módosítási eljárás;

10. a jelenleg jóváhagyott alternatív megfelelési módozatok részletei.

b) Az ISMM első kiadását az illetékes hatóságnak jóvá kell hagynia, és annak egy példányát meg kell őriznie. Az ISMM-et szükség szerint módosítani kell annak érdekében, hogy az a szervezet ISMS-ének naprakész leírása maradjon. Az ISMM módosításainak másolatát az illetékes hatóság rendelkezésére kell bocsátani.

c) Az ISMM módosításait a szervezet által megállapított eljárás szerint kell kezelni. Az ezen eljárás hatálya alá nem tartozó módosításokat és az IS.I.OR.255. b) pontban említett változásokhoz kapcsolódó módosításokat az illetékes hatóságnak jóvá kell hagynia.

d) A szervezet integrálhatja az ISMM-et a birtokában lévő egyéb irányítási szabályzatokkal vagy kézikönyvekkel, feltéve, hogy egyértelmű kereszthivatkozás áll rendelkezésre, amely jelzi, hogy az irányítási szabályzat vagy kézikönyv mely részei felelnek meg az e mellékletben foglalt különböző követelményeknek.

IS.I.OR.255. Az információbiztonsági irányítási rendszer változásai

a) Az ISMS változásait a szervezet által kidolgozott eljárás keretében lehet kezelni és bejelenteni az illetékes hatóságnak. A szóban forgó eljárást az illetékes hatóság hagyja jóvá.

b) Az ISMS-t érintő, az a) pontban említett eljárás hatálya alá nem tartozó változások tekintetében a szervezetnek kérelmeznie kell és meg kell szereznie az illetékes hatóság jóváhagyását.

E változásokat illetően:

1. a kérelmet még a változtatás végrehajtása előtt be kell nyújtani, hogy az illetékes hatóság megállapíthassa, hogy a szervezet továbbra is megfelel-e ennek a rendeletnek, és szükség esetén módosíthassa a szervezet bizonyítványát és a hozzá csatolt jóváhagyási feltételeket;

2. a szervezet az illetékes hatóság rendelkezésére bocsát minden olyan információt, amelyet az a változás értékeléséhez kér;

3. a változtatás csak az illetékes hatóság hivatalos jóváhagyásának kézhezvételét követően hajtható végre;

4. a szervezetnek az ilyen változtatások végrehajtása során az illetékes hatóság által előírt feltételek szerint kell működnie.

IS.I.OR.260. Folyamatos fejlesztés

a) A szervezet megfelelő teljesítménymutatók alkalmazásával értékeli az ISMS hatékonyságát és érettségét. Ezt az értékelést a szervezet által előre meghatározott naptári ütemezés szerint vagy egy információbiztonsági incidenst követően kell elvégezni.

b) Amennyiben az a) pontnak megfelelően elvégzett értékelést követően hiányosságokat tárnak fel, a szervezet meghozza a szükséges javító intézkedéseket annak biztosítása érdekében, hogy az ISMS továbbra is megfeleljen az alkalmazandó követelményeknek, és elfogadható szinten tartsa az információbiztonsági kockázatokat. A szervezet továbbá újraértékeli az ISMS-nek az elfogadott intézkedések által érintett elemeit.

III. MELLÉKLET

Az 1178/2011/EU rendelet VI. (ARA rész) és VII. melléklete (ORA rész) a következőképpen módosul:

1. A VI. melléklet (ARA rész) a következőképpen módosul:

a) az ARA.GEN.125. pont a következő c) alponttal egészül ki:

„c) Az illetékes tagállami hatóságnak a lehető leghamarabb közölnie kell az Ügynökséggel az általa kapott, az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR rész) IS.I.OR.230. pontja szerinti információbiztonsági jelentésekben szereplő, a repülésbiztonság szempontjából jelentős információkat.";

b) a szöveg az ARA.GEN.135. pont után a következő ARA.GEN.135A. ponttal egészül ki:

„**ARA.GEN.135A. Azonnali reagálás a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre**

a) Az illetékes hatóság létrehoz egy rendszert a szervezetek által jelentett, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensekkel és sebezhetőségekkel kapcsolatos információk megfelelő szintű gyűjtésére, elemzésére és terjesztésére. Ezt az adott tagállam minden más érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságával egyeztetve kell végrehajtani a jelentéstételi rendszerek közötti nagyobb összhang és összeegyeztethetőség érdekében.

b) Az Ügynökségnek létre kell hoznia egy rendszert az ARA.GEN.125. c) pont szerint kapott, a repülésbiztonság szempontjából lényeges információk megfelelő szintű elemzésére, és haladéktalanul tájékoztatnia kell mindenről – ideértve az ajánlásokat és a végrehajtandó kiigazító intézkedéseket – a tagállamokat és a Bizottságot annak érdekében, hogy azok időben megoldást találhassanak az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak hatálya alá eső termékeket, alkatrészeket, fel nem szerelt berendezéseket, személyeket és szervezeteket érintő, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensre és sebezhetőségre.

c) Az a) és b) pontban említett információk kézhezvétele után az illetékes hatóságnak meg kell tennie a szükséges intézkedéseket az információbiztonsági incidens vagy sebezhetőség repülésbiztonságra potenciálisan hatásának elhárítására.

d) A c) pont szerinti intézkedésekről haladéktalanul értesíteni kell minden olyan személyt és szervezetet, akinek/amelynek az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak értelmében teljesítenie kell ezeket az intézkedéseket. Az illetékes tagállami hatóságnak értesítenie kell az intézkedésekről az Ügynökséget is, valamint ha közös fellépésre van szükség, akkor a többi érintett tagállam illetékes hatóságát is.";

c) az ARA.GEN.200. pont a következő e) alponttal egészül ki:

„e) Az illetékes hatóság által létrehozott és fenntartott irányítási rendszernek az a) pontban foglalt követelményeken felül az (EU) 2023/203 végrehajtási rendelet I. mellékletében (IS.AR rész) foglalt rendelkezéseknek is meg kell felelnie a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében.";

d) az ARA.GEN.205. pont a következőképpen módosul:

i. a cím helyébe a következő szöveg lép:

„**ARA.GEN.205. Feladatok átruházása**";

ii. a szöveg a következő c) alponttal egészül ki:

„c) Az ORA.GEN.200A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság feladatokat ruházhat át az a) pont szerinti minősített szervezetekre vagy az adott tagállam érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságára. A feladatok átruházásakor az illetékes hatóságnak gondoskodnia kell az alábbiakról:

1. a minősített szervezet vagy az érintett hatóság minden repülésbiztonsági szempontot összehangol és figyelembe vesz;

2. a minősített szervezet vagy érintett hatóság által végzett tanúsítási és felügyeleti tevékenységek eredményeit a szervezet általános tanúsítási és felügyeleti irataiban rögzítik;

3. az ARA.GEN.200. e) pont szerint létrehozott saját információbiztonsági irányítási rendszere kiterjed a nevében végrehajtott valamennyi tanúsítási és folyamatos felügyelet feladatra.";

e) az ARA.GEN.300. pont a következő g) alponttal egészül ki:

„g) Az ORA.GEN.200A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság az a)–f) pont teljesítésén felül az e rendelet IS.I.OR.200. e) pontja vagy az (EU) 2022/1645 felhatalmazáson alapuló rendelet IS.D.OR.200. e) pontja alapján adott jóváhagyást is felülvizsgálja az alkalmazandó felügyeleti ellenőrzési ciklust követően, valamint minden olyan esetben, amikor a szervezet tevékenységi körében változtatásokat hajtanak végre.";

f) a szöveg az ARA.GEN.330. pont után a következő ARA.GEN.330A. ponttal egészül ki:

„ARA.GEN.330A. Az információbiztonsági irányítási rendszer változásai

a) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR. rész) IS.I.OR.255. a) pontja szerint kezelt és az illetékes hatóságnak bejelentett változtatások esetében az illetékes hatóságnak az ARA.GEN.300. pontban meghatározott elvekkel összhangban ki kell terjesztenie a folyamatos felügyeletet a szóban forgó változtatások felülvizsgálatára. Amennyiben meg nem felelést állapít meg, az illetékes hatóság értesíti erről a szervezetet, további változtatásokat kér, és az ARA.GEN.350. pont szerint jár el.

b) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR. rész) IS.I.OR.255. b) pontja szerint jóváhagyás iránti kérelmet igénylő egyéb változtatások esetében:

1. a változtatásra vonatkozó kérelem kézhezvételekor az illetékes hatóság a jóváhagyás megadása előtt ellenőrzi, hogy az adott szervezet teljesíti-e a vonatkozó követelményeket;

2. az illetékes hatóság meghatározza, hogy a szervezet milyen feltételek mellett működhet a változtatás végrehajtásának ideje alatt;

3. miután meggyőződött arról, hogy a szervezet teljesíti a vonatkozó követelményeket, az illetékes hatóság jóváhagyja a változtatást."

2. A VII. melléklet (ORA rész) a következőképpen módosul:

A szöveg az ORA.GEN.200. pont után a következő ORA.GEN.200A. ponttal egészül ki:

„ORA.GEN.200A, Információbiztonsági irányítási rendszer

Az ORA.GEN.200. pontban említett irányítási rendszeren kívül a szervezet az (EU) 2023/203 végrehajtási rendelet felhatalmazáson alapuló rendeletnek megfelelően létrehoz, alkalmaz és fenntart egy információbiztonsági irányítási rendszert a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében."

IV. MELLÉKLET

A 748/2012/EU rendelet I. melléklete (21. rész) a következőképpen módosul:

1. a tartalomjegyzék a következőképpen módosul:

   a) a szöveg a 21.B.20. cím után a következő címmel egészül ki:

   „21.B.20A. Azonnali reagálás a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre”;

   b) a 21.B.30. pont címének helyébe a következő szöveg lép:

   „21.B.30. Feladatok átruházása”;

   c) a szöveg a 21.B.240. cím után a következő címmel egészül ki:

   „21.B.240A. Az információbiztonsági irányítási rendszer változásai”;

   d) a szöveg a 21.B.435. cím után a következő címmel egészül ki:

   „21.B.435A. Az információbiztonsági irányítási rendszer változásai”;

2. A 21.B.15. pont a következő c) alponttal egészül ki:

   „c) Az illetékes tagállami hatóságnak a lehető leghamarabb közölnie kell az Ügynökséggel az általa kapott, az (EU) 2022/1645 felhatalmazáson alapuló rendelet mellékletének (IS.D.OR rész) IS.D.OR.230. pontja szerinti információbiztonsági jelentésekben szereplő, a repülésbiztonság szempontjából jelentős információkat.”

3. A szöveg a 21.B.20. pont után a következő 21.B.20A. ponttal egészül ki:

„21.B.20A. Azonnali reagálás a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre

a) Az illetékes hatóság létrehoz egy rendszert a szervezetek által jelentett, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensekkel és sebezhetőségekkel kapcsolatos információk megfelelő szintű gyűjtésére, elemzésére és terjesztésére. Ezt az adott tagállam minden más érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságával egyeztetve kell végrehajtani a jelentéstételi rendszerek közötti nagyobb összhang és összeegyeztethetőség érdekében.

b) Az Ügynökségnek létre kell hoznia egy rendszert a 21.B.15. c) pont szerint kapott, a repülésbiztonság szempontjából lényeges információk megfelelő szintű elemzésére, és haladéktalanul tájékoztatnia kell mindenről – ideértve az ajánlásokat és a végrehajtandó kiigazító intézkedéseket – a tagállamokat és a Bizottságot annak érdekében, hogy azok időben megoldást találhassanak az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak hatálya alá eső termékeket, alkatrészeket, fel nem szerelt berendezéseket, személyeket és szervezeteket érintő, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensre és sebezhetőségre.

c) Az a) és b) pontban említett információk kézhezvétele után az illetékes hatóságnak meg kell tennie a szükséges intézkedéseket az információbiztonsági incidens vagy sebezhetőség repülésbiztonságra gyakorolt potenciális hatásának elhárítására.

d) A c) pont szerinti intézkedésekről haladéktalanul értesíteni kell minden olyan személyt és szervezetet, akinek/amelynek az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak értelmében teljesítenie kell ezeket az intézkedéseket. Az illetékes tagállami hatóságnak értesítenie kell az intézkedésekről az Ügynökséget is, valamint ha közös fellépésre van szükség, akkor a többi érintett tagállam illetékes hatóságát is.”

4. A 21.B.25. pont a következő e) alponttal egészül ki:

   „e) Az illetékes hatóság által létrehozott és fenntartott irányítási rendszernek az a) pontban foglalt követelményeken felül az (EU) 2023/203 végrehajtási rendelet I. mellékletében (IS.AR rész) foglalt rendelkezéseknek is meg kell felelnie a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében.”

5. A 21.B.30. pont a következőképpen módosul:

a) a cím helyébe a következő szöveg lép:

„21.B.30. Feladatok átruházása”;

b) a szöveg a következő c) alponttal egészül ki:

„c) A 21.A.139A. és a 21.A.239A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság feladatokat ruházhat át az a) pont szerinti minősített szervezetekre vagy az adott tagállam érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságára. A feladatok átruházásakor az illetékes hatóságnak gondoskodnia kell az alábbiakról:

1. a minősített szervezet vagy az érintett hatóság minden repülésbiztonsági szempontot összehangol és figyelembe vesz;

2. a minősített szervezet vagy érintett hatóság által végzett tanúsítási és felügyeleti tevékenységek eredményeit a szervezet általános tanúsítási és felügyeleti irataiban rögzítik;

3. a 21.B.25. e) pont szerint létrehozott saját információbiztonsági irányítási rendszere kiterjed a nevében végrehajtott valamennyi tanúsítási és folyamatos felügyelet feladatra.”

6. A 21.B.221. pont a következő g) alponttal egészül ki:

„g) A 21.A.139A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság az a)–f) pont teljesítésén felül az e rendelet IS.I.OR.200. e) pontja vagy az (EU) 2022/1645 felhatalmazáson alapuló rendelet IS.D.OR.200. e) pontja alapján adott jóváhagyást is felülvizsgálja az alkalmazandó felügyeleti ellenőrzési ciklust követően, valamint minden olyan esetben, amikor a szervezet tevékenységi körében változtatásokat hajtanak végre.”

7. A szöveg a 21.B.240. pont után a következő 21.B.240A. ponttal egészül ki:

„**21.B.240A. Az információbiztonsági irányítási rendszer változásai**

a) Az (EU) 2022/1645 felhatalmazáson alapuló rendelet mellékletének (IS.D.OR rész) IS.D.OR.255. a) pontja szerint kezelt és az illetékes hatóságnak bejelentett változtatások esetében az illetékes hatóságnak a 21.B.221. pontban meghatározott elvekkel összhangban ki kell terjesztenie a folyamatos felügyeletet a szóban forgó változtatások felülvizsgálatára. Amennyiben meg nem felelést állapít meg, az illetékes hatóság értesíti erről a szervezetet, további változtatásokat kér, és a 21.B.225. pont szerint jár el.

b) Az (EU) 2022/1645 felhatalmazáson alapuló rendelet mellékletének (IS.D.OR rész) IS.D.OR.255. b) pontja szerint jóváhagyás iránti kérelmet igénylő egyéb változtatások esetében:

1. a változtatásra vonatkozó kérelem kézhezvételekor az illetékes hatóság a jóváhagyás megadása előtt ellenőrzi, hogy az adott szervezet teljesíti-e a vonatkozó követelményeket;

2. az illetékes hatóság meghatározza, hogy a szervezet milyen feltételek mellett működhet a változtatás végrehajtásának ideje alatt;

3. miután meggyőződött arról, hogy a szervezet teljesíti a vonatkozó követelményeket, az illetékes hatóság jóváhagyja a változtatást.”

8. A 21.B.431. pont a következő d) alponttal egészül ki:

„d) A 21.A.239A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóságnak az a)–c) pont teljesítésén felül az alábbi elveknek kell megfelelnie:

1. az illetékes hatóság felülvizsgálja a felügyelete alatt álló egyes szervezetek által az (EU) 2022/1645 felhatalmazáson alapuló rendelet mellékletének (IS.D.OR rész) IS.D.OR.205. b) pontja szerint azonosított kapcsolódási pontokat és a hozzájuk kapcsolódó kockázatokat;

2. ha a különböző szervezetek által azonosított kölcsönös kapcsolódási pontok és a hozzájuk kapcsolódó kockázatok között eltérések állapíthatók meg, az illetékes hatóság felülvizsgálja őket az érintett szervezetekkel, és szükség esetén, és megfelelő megállapításokat fogalmaz meg korrekciós intézkedések végrehajtása érdekében;

3. ha a dokumentáció 2. pont szerinti felülvizsgálatából kiderül, hogy az ugyanazon tagállamok belüli különböző illetékes hatóságok felügyelete alatt álló szervezetekkel való kapcsolódási pontokhoz jelentős kockázatok kapcsolódnak, ezt az információt közölni kell a megfelelő illetékes hatósággal.”

9. A szöveg a 21.B.435. pont után a következő 21.B.435A. ponttal egészül ki:

„**21.B.435A. Az információbiztonsági irányítási rendszer változásai**

a) Az (EU) 2022/1645 felhatalmazáson alapuló rendelet mellékletének (IS.D.OR rész) IS.D.OR.255. a) pontja szerint kezelt és az illetékes hatóságnak bejelentett változtatások esetében az illetékes hatóságnak a 21.B.431. pontban meghatározott elvekkel összhangban ki kell terjesztenie a folyamatos felügyeletet a szóban forgó változtatások felülvizsgálatára. Amennyiben meg nem felelést állapít meg, az illetékes hatóság értesíti erről a szervezetet, további változtatásokat kér, és a 21.B.433. pont szerint jár el.

b) Az (EU) 2022/1645 felhatalmazáson alapuló rendelet mellékletének (IS.D.OR rész) IS.D.OR.255. b) pontja szerint jóváhagyás iránti kérelmet igénylő egyéb változtatások esetében:

1. a változtatásra vonatkozó kérelem kézhezvételekor az illetékes hatóság a jóváhagyás megadása előtt ellenőrzi, hogy az adott szervezet teljesíti-e a vonatkozó követelményeket;

2. az illetékes hatóság meghatározza, hogy a szervezet milyen feltételek mellett működhet a változtatás végrehajtásának ideje alatt;

3. miután meggyőződött arról, hogy a szervezet teljesíti a vonatkozó követelményeket, az illetékes hatóság jóváhagyja a változtatást.”

V. MELLÉKLET

A 965/2012/EU rendelet II. (ARO rész) és III. melléklete (ORO rész) a következőképpen módosul:

1. A II. melléklet (ARO rész) a következőképpen módosul:

a) az ARO.GEN.125. pont a következő c) alponttal egészül ki:

„c) Az illetékes tagállami hatóságnak a lehető leghamarabb közölnie kell az Ügynökséggel az általa kapott, az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR rész) IS.I.OR.230. pontja szerinti információbiztonsági jelentésekben szereplő, a repülésbiztonság szempontjából jelentős információkat.";

b) a szöveg az ARO.GEN.135. pont után a következő ARO.GEN.135A. ponttal egészül ki:

„**ARO.GEN.135A. Azonnali reagálás a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre**

a) Az illetékes hatóság létrehoz egy rendszert a szervezetek által jelentett, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensekkel és sebezhetőségekkel kapcsolatos információk megfelelő szintű gyűjtésére, elemzésére és terjesztésére. Ezt az adott tagállam minden más érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságával egyeztetve kell végrehajtani a jelentéstételi rendszerek közötti nagyobb összhang és összeegyeztethetőség érdekében.

b) Az Ügynökségnek létre kell hoznia egy rendszert az ARO.GEN.125. c) pont szerint kapott, a repülésbiztonság szempontjából lényeges információk megfelelő szintű elemzésére, és haladéktalanul tájékoztatnia kell mindenről – ideértve az ajánlásokat és a végrehajtandó kiigazító intézkedéseket – a tagállamokat és a Bizottságot annak érdekében, hogy azok időben megoldást találhassanak az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak hatálya alá eső termékeket, alkatrészeket, fel nem szerelt berendezéseket, személyeket és szervezeteket érintő, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensre és sebezhetőségre.

c) Az a) és b) pontban említett információk kézhezvétele után az illetékes hatóságnak meg kell tennie a szükséges intézkedéseket az információbiztonsági incidens vagy sebezhetőség repülésbiztonságra potenciálisan hatásának elhárítására.

d) A c) pont szerinti intézkedésekről haladéktalanul értesíteni kell minden olyan személyt és szervezetet, akinek/amelynek az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak értelmében teljesítenie kell ezeket az intézkedéseket. Az illetékes tagállami hatóságnak értesítenie kell az intézkedésekről az Ügynökséget is, valamint ha közös fellépésre van szükség, akkor a többi érintett tagállam illetékes hatóságát is.";

c) az ARO.GEN.200. pont a következő e) alponttal egészül ki:

„e) Az illetékes hatóság által létrehozott és fenntartott irányítási rendszernek az a) pontban foglalt követelményeken felül az (EU) 2023/203 végrehajtási rendelet I. mellékletében (IS.AR rész) foglalt rendelkezéseknek is meg kell felelnie a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében.";

d) az ARO.GEN.205. pont a következőképpen módosul:

i. a cím helyébe a következő szöveg lép:

„**ARO.GEN.205. Feladatok átruházása**";

ii. a szöveg a következő c) alponttal egészül ki:

„c) Az ORO.GEN.200A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság feladatokat ruházhat át az a) pont szerinti minősített szervezetekre vagy az adott tagállam érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságára. A feladatok átruházásakor az illetékes hatóságnak gondoskodnia kell az alábbiakról:

1. a minősített szervezet vagy az érintett hatóság minden repülésbiztonsági szempontot összehangol és figyelembe vesz;

2. a minősített szervezet vagy érintett hatóság által végzett tanúsítási és felügyeleti tevékenységek eredményeit a szervezet általános tanúsítási és felügyeleti irataiban rögzítik;

3. az ARO.GEN.200. e) pont szerint létrehozott saját információbiztonsági irányítási rendszere kiterjed a nevében végrehajtott valamennyi tanúsítási és folyamatos felügyelet feladatra.";

e) az ARO.GEN.300. pont a következő g) alponttal egészül ki:

„g) Az ORO.GEN.200A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság az a)–f) pont teljesítésén felül az e rendelet IS.I.OR.200. e) pontja vagy az (EU) 2022/1645 felhatalmazáson alapuló rendelet IS.D.OR.200. e) pontja alapján adott jóváhagyást is felülvizsgálja az alkalmazandó felügyeleti ellenőrzési ciklust követően, valamint minden olyan esetben, amikor a szervezet tevékenységi körében változtatásokat hajtanak végre.";

f) az ARO.GEN.330. pont után a következő ARO.GEN.330A. ponttal egészül ki:

„**ARO.GEN.330A. Az információbiztonsági irányítási rendszer változásai**

a) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR. rész) IS.I.OR.255. a) pontja szerint kezelt és az illetékes hatóságnak bejelentett változtatások esetében az illetékes hatóságnak az ARO.GEN.300. pontban meghatározott elvekkel összhangban ki kell terjesztenie a folyamatos felügyeletet a szóban forgó változtatások felülvizsgálatára. Amennyiben meg nem felelést állapít meg, az illetékes hatóság értesíti erről a szervezetet, további változtatásokat kér, és az ARO.GEN.350. pont szerint jár el.

b) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR. rész) IS.I.OR.255. b) pontja szerint jóváhagyás iránti kérelmet igénylő egyéb változtatások esetében:

1. a változtatásra vonatkozó kérelem kézhezvételekor az illetékes hatóság a jóváhagyás megadása előtt ellenőrzi, hogy az adott szervezet teljesíti-e a vonatkozó követelményeket;

2. az illetékes hatóság meghatározza, hogy a szervezet milyen feltételek mellett működhet a változtatás végrehajtásának ideje alatt;

3. miután meggyőződött arról, hogy a szervezet teljesíti a vonatkozó követelményeket, az illetékes hatóság jóváhagyja a változtatást."

2. A III. melléklet (ORO rész) a következőképpen módosul:

a szöveg az ORO.GEN.200. pont után a következő ORO.GEN.200A. ponttal egészül ki:

„**ORO.GEN.200A, Információbiztonsági irányítási rendszer**

Az ORO.GEN.200. pontban említett irányítási rendszeren kívül az üzemeltető az (EU) 2023/203 végrehajtási rendelet felhatalmazáson alapuló rendeletnek megfelelően létrehoz, alkalmaz és fenntart egy információbiztonsági irányítási rendszert a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében."

VI. MELLÉKLET

A 139/2014/EU rendelet II. melléklete (ADR.AR. rész) a következőképpen módosul:

1. Az ADR.AR.A.025. pont a következő c) alponttal egészül ki:

„c) Az illetékes tagállami hatóságnak a lehető leghamarabb közölnie kell az Ügynökséggel az általa kapott, az (EU) 2022/1645 felhatalmazáson alapuló rendelet mellékletének (IS.D.OR rész) IS.D.OR.230. pontja szerinti információbiztonsági jelentésekben szereplő, a repülésbiztonság szempontjából jelentős információkat.”

2. A szöveg az ADR.AR.A.030. pont után a következő ADR.AR.A.030A. ponttal egészül ki:

„**ADR.AR.A.030A. Azonnali reagálás a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre**

a) Az illetékes hatóság létrehoz egy rendszert a szervezetek által jelentett, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensekkel és sebezhetőségekkel kapcsolatos információk megfelelő szintű gyűjtésére, elemzésére és terjesztésére. Ezt az adott tagállam minden más érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságával egyeztetve kell végrehajtani a jelentéstételi rendszerek közötti nagyobb összhang és összeegyeztethetőség érdekében.

b) Az Ügynökségnek létre kell hoznia egy rendszert az ADR.AR.A.025. c) pont szerint kapott, a repülésbiztonság szempontjából lényeges információk megfelelő szintű elemzésére, és haladéktalanul tájékoztatnia kell mindenről – ideértve az ajánlásokat és a végrehajtandó kiigazító intézkedéseket – a tagállamokat és a Bizottságot annak érdekében, hogy azok időben megoldást találhassanak az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak hatálya alá eső termékeket, alkatrészeket, fel nem szerelt berendezéseket, személyeket és szervezeteket érintő, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensre és sebezhetőségre.

c) Az a) és b) pontban említett információk kézhezvétele után az illetékes hatóságnak meg kell tennie a szükséges intézkedéseket az információbiztonsági incidens vagy sebezhetőség repülésbiztonságra potenciálisan hatásának elhárítására.

d) A c) pont szerinti intézkedésekről haladéktalanul értesíteni kell minden olyan személyt és szervezetet, akinek/amelynek az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak értelmében teljesítenie kell ezeket az intézkedéseket. Az illetékes tagállami hatóságnak értesítenie kell az intézkedésekről az Ügynökséget is, valamint ha közös fellépésre van szükség, akkor a többi érintett tagállam illetékes hatóságát is.”

3. Az ADR.AR.B.005. pont a következő d) alponttal egészül ki:

„d) Az illetékes hatóság által létrehozott és fenntartott irányítási rendszernek az a) pontban foglalt követelményeken felül az (EU) 2023/203 végrehajtási rendelet I. mellékletében (IS.AR rész) foglalt rendelkezéseknek is meg kell felelnie a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében.”

4. Az ADR.AR.B.010. pont a következőképpen módosul:

i. a cím helyébe a következő szöveg lép:

„**ADR.AR.B.010. Feladatok átruházása**”;

ii. a szöveg a következő c) alponttal egészül ki:

„c) Az ADR.OR.D.005A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság feladatokat ruházhat át az a) pont szerinti minősített szervezetekre vagy az adott tagállam érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságára. A feladatok átruházásakor az illetékes hatóságnak gondoskodnia kell az alábbiakról:

1. a minősített szervezet vagy az érintett hatóság minden repülésbiztonsági szempontot összehangol és figyelembe vesz;

2. a minősített szervezet vagy érintett hatóság által végzett tanúsítási és felügyeleti tevékenységek eredményeit a szervezet általános tanúsítási és felügyeleti irataiban rögzítik;

3. az ADR.AR.B.005. e) pont szerint létrehozott saját információbiztonsági irányítási rendszere kiterjed a nevében végrehajtott valamennyi tanúsítási és folyamatos felügyelet feladatra."

5. Az ADR.AR.C.005. pont a következő f) alponttal egészül ki:

„f) Az ADR.OR.D.005A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság az a)–e) pont teljesítésén felül az e rendelet IS.I.OR.200. e) pontja vagy az (EU) 2022/1645 felhatalmazáson alapuló rendelet IS.D.OR.200. e) pontja alapján adott jóváhagyást is felülvizsgálja az alkalmazandó felügyeleti ellenőrzési ciklust követően, valamint minden olyan esetben, amikor a szervezet tevékenységi körében változtatásokat hajtanak végre."

6. A szöveg az ADR.AR.C.040. pont után a következő ADR.AR.C.040A. ponttal egészül ki:

„**ADR.AR.C.040A. Az információbiztonsági irányítási rendszer változásai**

a) Az (EU) 2022/1645 felhatalmazáson alapuló rendelet mellékletének (IS.D.OR rész) IS.D.OR.255. a) pontja szerint kezelt és az illetékes hatóságnak bejelentett változtatások esetében az illetékes hatóságnak az ADR.AR.C.005. pontban meghatározott elvekkel összhangban ki kell terjesztenie a folyamatos felügyeletet a szóban forgó változtatások felülvizsgálatára. Amennyiben meg nem felelést állapít meg, az illetékes hatóság értesíti erről a szervezetet, további változtatásokat kér, és az ADR.AR.C.055. pont szerint jár el.

b) Az (EU) 2022/1645 felhatalmazáson alapuló rendelet mellékletének (IS.D.OR rész) IS.D.OR.255. b) pontja szerint jóváhagyás iránti kérelmet igénylő egyéb változtatások esetében:

1. a változtatásra vonatkozó kérelem kézhezvételekor az illetékes hatóság a jóváhagyás megadása előtt ellenőrzi, hogy az adott szervezet teljesíti-e a vonatkozó követelményeket;

2. az illetékes hatóság meghatározza, hogy a szervezet milyen feltételek mellett működhet a változtatás végrehajtásának ideje alatt;

3. miután meggyőződött arról, hogy a szervezet teljesíti a vonatkozó követelményeket, az illetékes hatóság jóváhagyja a változtatást."

VII. MELLÉKLET

Az 1321/2014/EU rendelet II. (145. rész), III. (66. rész) és Vc. melléklete (CAMO rész) a következőképpen módosul:

1. A II. melléklet (145. rész) a következőképpen módosul:

a) a tartalomjegyzék a következőképpen módosul:

i. a szöveg a 145.A.200. cím után a következő címmel egészül ki:

„145.A.200A. Információbiztonsági irányítási rendszer”;

ii. a szöveg a 145.B.135. cím után a következő címmel egészül ki:

„145.B.135A. Azonnali reagálás a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre”;

iii. a 145.B.205. pont címének helyébe a következő szöveg lép:

„145.B.205. Feladatok átruházása”;

iv. a szöveg a 145.B.330. cím után a következő címmel egészül ki:

„145.B.330A. Az információbiztonsági irányítási rendszer változásai”;

b) a szöveg a 145.A.200. pont után a következő 145.A.200A. ponttal egészül ki:

„145.A.200A. **Információbiztonsági irányítási rendszer**

A 145.A.200. pontban említett irányítási rendszeren kívül a karbantartó szervezet az (EU) 2023/203 végrehajtási rendeletnek megfelelően létrehoz, alkalmaz és fenntart egy információbiztonsági irányítási rendszert a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében.”;

c) a 145.B.125. pont a következő c) alponttal egészül ki:

„c) Az illetékes tagállami hatóságnak a lehető leghamarabb közölnie kell az Ügynökséggel az általa kapott, az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR rész) IS.I.OR.230. pontja szerinti információbiztonsági jelentésekben szereplő, a repülésbiztonság szempontjából jelentős információkat.”;

d) a szöveg a 145.B.135. pont után a következő 145.B.135A. ponttal egészül ki:

„145.B.135A. **Azonnali reagálás a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre**

a) Az illetékes hatóság létrehoz egy rendszert a szervezetek által jelentett, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensekkel és sebezhetőségekkel kapcsolatos információk megfelelő szintű gyűjtésére, elemzésére és terjesztésére. Ezt az adott tagállam minden más érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságával egyeztetve kell végrehajtani a jelentéstételi rendszerek közötti nagyobb összhang és összeegyeztethetőség érdekében.

b) Az Ügynökségnek létre kell hoznia egy rendszert a 145.B.125. c) pont szerint kapott, a repülésbiztonság szempontjából lényeges információk megfelelő szintű elemzésére, és haladéktalanul tájékoztatnia kell mindenről – ideértve az ajánlásokat és a végrehajtandó kiigazító intézkedéseket – a tagállamokat és a Bizottságot annak érdekében, hogy azok időben megoldást találhassanak az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak hatálya alá eső termékeket, alkatrészeket, fel nem szerelt berendezéseket, személyeket és szervezeteket érintő, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensre és sebezhetőségre.

c) Az a) és b) pontban említett információk kézhezvétele után az illetékes hatóságnak meg kell tennie a szükséges intézkedéseket az információbiztonsági incidens vagy sebezhetőség repülésbiztonságra gyakorolt potenciális hatásának elhárítására.

d) A c) pont szerinti intézkedésekről haladéktalanul értesíteni kell minden olyan személyt és szervezetet, akinek/amelynek az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak értelmében teljesítenie kell ezeket az intézkedéseket. Az illetékes tagállami hatóságnak értesítenie kell az intézkedésekről az Ügynökséget is, valamint ha közös fellépésre van szükség, akkor a többi érintett tagállam illetékes hatóságát is.";

e) a 145.B.200. pont a következő e) alponttal egészül ki:

„e) Az illetékes hatóság által létrehozott és fenntartott irányítási rendszernek az a) pontban foglalt követelményeken felül az (EU) 2023/203 végrehajtási rendelet I. mellékletében (IS.AR rész) foglalt rendelkezéseknek is meg kell felelnie a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében.";

f) a 145.B.205. pont a következőképpen módosul:

i. a cím helyébe a következő szöveg lép:

„145.B.205. **Feladatok átruházása**";

ii. a szöveg a következő c) alponttal egészül ki:

„c) A 145.A.200A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság feladatokat ruházhat át az a) pont szerinti minősített szervezetekre vagy az adott tagállam érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságára. A feladatok átruházásakor az illetékes hatóságnak gondoskodnia kell az alábbiakról:

1. a minősített szervezet vagy az érintett hatóság minden repülésbiztonsági szempontot összehangol és figyelembe vesz;

2. a minősített szervezet vagy érintett hatóság által végzett tanúsítási és felügyeleti tevékenységek eredményeit a szervezet általános tanúsítási és felügyeleti irataiban rögzítik;

3. a 145.B.200. e) pont szerint létrehozott saját információbiztonsági irányítási rendszere kiterjed a nevében végrehajtott valamennyi tanúsítási és folyamatos felügyelet feladatra.";

g) a 145.B.300 pont a következő g) alponttal egészül ki:

„g) A 145.A.200A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság az a)–f) pont teljesítésén felül az e rendelet IS.I.OR.200. e) pontja vagy az (EU) 2022/1645 felhatalmazáson alapuló rendelet IS.D.OR.200. e) pontja alapján adott jóváhagyást is felülvizsgálja az alkalmazandó felügyeleti ellenőrzési ciklust követően, valamint minden olyan esetben, amikor a szervezet tevékenységi körében változtatásokat hajtanak végre.";

h) a szöveg a 145.B.330. pont után a következő 145.B.330A. ponttal egészül ki:

„145.B.330A. **Az információbiztonsági irányítási rendszer változásai**

a) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR rész) IS.I.OR.255. a) pontja szerint kezelt és az illetékes hatóságnak bejelentett változtatások esetében az illetékes hatóságnak a 145.B.300. pontban meghatározott elvekkel összhangban ki kell terjesztenie a folyamatos felügyeletet a szóban forgó változtatások felülvizsgálatára. Amennyiben meg nem felelést állapít meg, az illetékes hatóság értesíti erről a szervezetet, további változtatásokat kér, és a 145.B.350. pont szerint jár el.

b) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR rész) IS.I.OR.255. b) pontja szerint jóváhagyás iránti kérelmet igénylő egyéb változtatások esetében:

1. a változtatásra vonatkozó kérelem kézhezvételekor az illetékes hatóság a jóváhagyás megadása előtt ellenőrzi, hogy az adott szervezet teljesíti-e a vonatkozó követelményeket;

2. az illetékes hatóság meghatározza, hogy a szervezet milyen feltételek mellett működhet a változtatás végrehajtásának ideje alatt;

3. miután meggyőződött arról, hogy a szervezet teljesíti a vonatkozó követelményeket, az illetékes hatóság jóváhagyja a változtatást."

2. A III. melléklet (66. rész) a következőképpen módosul:

a) a tartalomjegyzék a 66.B.10. cím után a következő címmel egészül ki:

„66.B.15. Információbiztonsági irányítási rendszer";

b) a szöveg a 66.B.10. pont után a következő 66.B.15. ponttal egészül ki:

„66.B.15. **Információbiztonsági irányítási rendszer**

Az illetékes hatóság az (EU) 2023/203 végrehajtási rendelet I. mellékletének (IS.AR. rész) megfelelően létrehoz, alkalmaz és fenntart egy információbiztonsági irányítási rendszert a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében."

3. Az Vc. melléklet (CAMO rész) a következőképpen módosul:

a) a tartalomjegyzék a következőképpen módosul:

i. a szöveg a CAMO.A.200. cím után a következő címmel egészül ki:

„CAMO.A.200A. Információbiztonsági irányítási rendszer";

ii. a szöveg a CAMO.B.135. cím után a következő címmel egészül ki:

„CAMO.B.135A. Azonnali reagálás a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre";

iii. a CAMO.B.205. pont helyébe a következő szöveg lép:

„CAMO.B.205. Feladatok átruházása";

iv. a szöveg a CAMO.B.330. cím után a következő címmel egészül ki:

„CAMO.B.330A. Az információbiztonsági irányítási rendszer változásai";

b) a szöveg a CAMO.A.200. pont után a következő CAMO.A.200A. ponttal egészül ki:

„CAMO.A.200A. **Információbiztonsági irányítási rendszer**

A CAMO.A.200. pontban említett irányítási rendszeren kívül a szervezet az (EU) 2023/203 végrehajtási rendelet felhatalmazáson alapuló rendeletnek megfelelően létrehoz, alkalmaz és fenntart egy információbiztonsági irányítási rendszert a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében.";

c) a CAMO.B.125. pont a következő c) alponttal egészül ki:

„c) Az illetékes tagállami hatóságnak a lehető leghamarabb közölnie kell az Ügynökséggel az általa kapott, az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR rész) IS.I.OR.230. pontja szerinti információbiztonsági jelentésekben szereplő, a repülésbiztonság szempontjából jelentős információkat.";

d) a szöveg a CAMO.B.135. pont után a következő CAMO.B.135A. ponttal egészül ki:

„CAMO.B.135A. **Azonnali reagálás a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre**

a) Az illetékes hatóság létrehoz egy rendszert a szervezetek által jelentett, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensekkel és sebezhetőségekkel kapcsolatos információk megfelelő szintű gyűjtésére, elemzésére és terjesztésére. Ezt az adott tagállam minden más érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságával egyeztetve kell végrehajtani a jelentéstételi rendszerek közötti nagyobb összhang és összeegyeztethetőség érdekében.

b) Az Ügynökségnek létre kell hoznia egy rendszert a CAMO.B.125. c) pont szerint kapott, a repülésbiztonság szempontjából lényeges információk megfelelő szintű elemzésére, és haladéktalanul tájékoztatnia kell mindenről – ideértve az ajánlásokat és a végrehajtandó kiigazító intézkedéseket – a tagállamokat és a Bizottságot annak érdekében, hogy azok időben megoldást találhassanak az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak hatálya alá eső termékeket, alkatrészeket, fel nem szerelt berendezéseket, személyeket és szervezeteket érintő, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensre és sebezhetőségre.

c) Az a) és b) pontban említett információk kézhezvétele után az illetékes hatóságnak meg kell tennie a szükséges intézkedéseket az információbiztonsági incidens vagy sebezhetőség repülésbiztonságra potenciálisan hatásának elhárítására.

d) A c) pont szerinti intézkedésekről haladéktalanul értesíteni kell minden olyan személyt és szervezetet, akinek/amelynek az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak értelmében teljesítenie kell ezeket az intézkedéseket. Az illetékes tagállami hatóságnak értesítenie kell az intézkedésekről az Ügynökséget is, valamint ha közös fellépésre van szükség, akkor a többi érintett tagállam illetékes hatóságát is.";

e) a CAMO.B.200. pont a következő e) alponttal egészül ki:

„e) Az illetékes hatóság által létrehozott és fenntartott irányítási rendszernek az a) pontban foglalt követelményeken felül az (EU) 2023/203 végrehajtási rendelet I. mellékletében (IS.AR rész) foglalt rendelkezéseknek is meg kell felelnie a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében.";

f) a CAMO.B.205. pont a következőképpen módosul:

i. a cím helyébe a következő szöveg lép:

„CAMO.B.205. **Feladatok átruházása**";

ii. a szöveg a következő c) alponttal egészül ki:

„c) A CAMO.A.200A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság feladatokat ruházhat át az a) pont szerinti minősített szervezetekre vagy az adott tagállam érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságára. A feladatok átruházásakor az illetékes hatóságnak gondoskodnia kell az alábbiakról:

1. a minősített szervezet vagy az érintett hatóság minden repülésbiztonsági szempontot összehangol és figyelembe vesz;

2. a minősített szervezet vagy érintett hatóság által végzett tanúsítási és felügyeleti tevékenységek eredményeit a szervezet általános tanúsítási és felügyeleti irataiban rögzítik;

3. a CAMO.B.200. e) pont szerint létrehozott saját információbiztonsági irányítási rendszere kiterjed a nevében végrehajtott valamennyi tanúsítási és folyamatos felügyelet feladatra.";

g) a CAMO.B.300. pont a következő g) alponttal egészül ki:

„g) A CAMO.A.200A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság az a)–f) pont teljesítésén felül az e rendelet IS.I.OR.200. e) pontja vagy az (EU) 2022/1645 felhatalmazáson alapuló rendelet IS.D.OR.200. e) pontja alapján adott jóváhagyást is felülvizsgálja az alkalmazandó felügyeleti ellenőrzési ciklust követően, valamint minden olyan esetben, amikor a szervezet tevékenységi körében változtatásokat hajtanak végre.";

h) a szöveg a CAMO.B.330. pont után a következő CAMO.B.330A. ponttal egészül ki:

„CAMO.B.330A. **Az információbiztonsági irányítási rendszer változásai**

a) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR. rész) IS.I.OR.255. a) pontja szerint kezelt és az illetékes hatóságnak bejelentett változtatások esetében az illetékes hatóságnak a CAMO.B.300. pontban meghatározott elvekkel összhangban ki kell terjesztenie a folyamatos felügyeletet a szóban forgó változtatások felülvizsgálatára. Amennyiben meg nem felelést állapít meg, az illetékes hatóság értesíti erről a szervezetet, további változtatásokat kér, és a CAMO.B.350. pont szerint jár el.

b) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR. rész) IS.I.OR.255. b) pontja szerint jóváhagyás iránti kérelmet igénylő egyéb változtatások esetében:

1. a változtatásra vonatkozó kérelem kézhezvételekor az illetékes hatóság a jóváhagyás megadása előtt ellenőrzi, hogy az adott szervezet teljesíti-e a vonatkozó követelményeket;

2. az illetékes hatóság meghatározza, hogy a szervezet milyen feltételek mellett működhet a változtatás végrehajtásának ideje alatt;

3. miután meggyőződött arról, hogy a szervezet teljesíti a vonatkozó követelményeket, az illetékes hatóság jóváhagyja a változtatást."

VIII. MELLÉKLET

Az (EU) 2015/340 rendelet II. (ATCO.AR rész) és III. melléklete (ATCO.OR. rész) az alábbiak szerint módosul:

1. A II. melléklet (ATCO.AR rész) a következőképpen módosul:

a) az ATCO.AR.A.020. pont a következő c) alponttal egészül ki:

„c) Az illetékes tagállami hatóságnak a lehető leghamarabb közölnie kell az Ügynökséggel az általa kapott, az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR rész) IS.I.OR.230. pontja szerinti információbiztonsági jelentésekben szereplő, a repülésbiztonság szempontjából jelentős információkat.”;

b) a szöveg az ATCO.AR.A.025. pont után a következő ATCO.AR.A.025A. ponttal egészül ki:

„**ATCO.AR.A.025A. Azonnali reagálás a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre**

a) Az illetékes hatóság létrehoz egy rendszert a szervezetek által jelentett, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensekkel és sebezhetőségekkel kapcsolatos információk megfelelő szintű gyűjtésére, elemzésére és terjesztésére. Ezt az adott tagállam minden más érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságával egyeztetve kell végrehajtani a jelentéstételi rendszerek közötti nagyobb összhang és összeegyeztethetőség érdekében.

b) Az Ügynökségnek létre kell hoznia egy rendszert az ATCO.AR.A.020. pont szerint kapott, a repülésbiztonság szempontjából lényeges információk megfelelő szintű elemzésére, és haladéktalanul tájékoztatnia kell mindenről – ideértve az ajánlásokat és a végrehajtandó kiigazító intézkedéseket – a tagállamokat és a Bizottságot annak érdekében, hogy azok időben megoldást találhassanak az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak hatálya alá eső termékeket, alkatrészeket, fel nem szerelt berendezéseket, személyeket és szervezeteket érintő, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensre és sebezhetőségre.

c) Az a) és b) pontban említett információk kézhezvétele után az illetékes hatóságnak meg kell tennie a szükséges intézkedéseket az információbiztonsági incidens vagy sebezhetőség repülésbiztonságra potenciálisan hatásának elhárítására.

d) A c) pont szerinti intézkedésekről haladéktalanul értesíteni kell minden olyan személyt és szervezetet, akinek/amelynek az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak értelmében teljesítenie kell ezeket az intézkedéseket. Az illetékes tagállami hatóságnak értesítenie kell az intézkedésekről az Ügynökséget is, valamint ha közös fellépésre van szükség, akkor a többi érintett tagállam illetékes hatóságát is.”;

c) az ATCO.AR.B.001. pont a következő e) alponttal egészül ki:

„e) Az illetékes hatóság által létrehozott és fenntartott irányítási rendszernek az a) pontban foglalt követelményeken felül az (EU) 2023/203 végrehajtási rendelet I. mellékletében (IS.AR rész) foglalt rendelkezéseknek is meg kell felelnie a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében.”;

d) az ATCO.AR.B.005. pont a következőképpen módosul:

i. a cím helyébe a következő szöveg lép:

„**ATCO.AR.B.005. Feladatok átruházása**”;

ii. a szöveg a következő c) alponttal egészül ki:

„c) Az ATCO.OR.C.001A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság feladatokat ruházhat át az a) pont szerinti minősített szervezetekre vagy az adott tagállam érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságára. A feladatok átruházásakor az illetékes hatóságnak gondoskodnia kell az alábbiakról:

1. a minősített szervezet vagy az érintett hatóság minden repülésbiztonsági szempontot összehangol és figyelembe vesz;

2. a minősített szervezet vagy érintett hatóság által végzett tanúsítási és felügyeleti tevékenységek eredményeit a szervezet általános tanúsítási és felügyeleti irataiban rögzítik;

3. az ATCO.AR.B.001. e) pont szerint létrehozott saját információbiztonsági irányítási rendszere kiterjed a nevében végrehajtott valamennyi tanúsítási és folyamatos felügyelet feladatra.";

e) az ATCO.AR.C.001. pont a következő f) alponttal egészül ki:

„f) Az ATCO.OR.C.001A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság az a)–e) pont teljesítésén felül az e rendelet IS.I.OR.200. e) pontja vagy az (EU) 2022/1645 felhatalmazáson alapuló rendelet IS.D.OR.200. e) pontja alapján adott jóváhagyást is felülvizsgálja az alkalmazandó felügyeleti ellenőrzési ciklust követően, valamint minden olyan esetben, amikor a szervezet tevékenységi körében változtatásokat hajtanak végre.";

f) a szöveg az ATCO.AR.E.010. pont után a következő ATCO.AR.E.010A. ponttal egészül ki:

„**ATCO.AR.E.010A. Az információbiztonsági irányítási rendszer változásai**

a) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR. rész) IS.I.OR.255. a) pontja szerint kezelt és az illetékes hatóságnak bejelentett változtatások esetében az illetékes hatóságnak az ATCO.AR.C.001. pontban meghatározott elvekkel összhangban ki kell terjesztenie a folyamatos felügyeletet a szóban forgó változtatások felülvizsgálatára. Amennyiben meg nem felelést állapít meg, az illetékes hatóság értesíti erről a szervezetet, további változtatásokat kér, és az ATCO.AR.C.010. pont szerint jár el.

b) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR. rész) IS.I.OR.255. b) pontja szerint jóváhagyás iránti kérelmet igénylő egyéb változtatások esetében:

1. a változtatásra vonatkozó kérelem kézhezvételekor az illetékes hatóság a jóváhagyás megadása előtt ellenőrzi, hogy az adott szervezet teljesíti-e a vonatkozó követelményeket;

2. az illetékes hatóság meghatározza, hogy a szervezet milyen feltételek mellett működhet a változtatás végrehajtásának ideje alatt;

3. miután meggyőződött arról, hogy a szervezet teljesíti a vonatkozó követelményeket, az illetékes hatóság jóváhagyja a változtatást."

2. A III. melléklet (ATCO.OR rész) a következőképpen módosul:

A szöveg az ATCO.OR.C.001. pont után a következő ATCO.OR.C.001A. ponttal egészül ki:

„**ATCO.OR.C.001A, Információbiztonsági irányítási rendszer**

Az ATCO.OR.C.001. pontban említett irányítási rendszeren kívül a képzési szervezet az (EU) 2023/203 végrehajtási rendelet felhatalmazáson alapuló rendeletnek megfelelően létrehoz, alkalmaz és fenntart egy információbiztonsági irányítási rendszert a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében."

IX. MELLÉKLET

Az (EU) 2017/373 végrehajtási rendelet II. (ATM/ANS.AR rész) és III. melléklete (ATM/ANS.OR rész) az alábbiak szerint módosul:

1. A II. melléklet (ATM/ANS.AR rész) a következőképpen módosul:

a) az ATM/ANS.AR.A.020. pont a következő c) alponttal egészül ki:

„c) Az illetékes tagállami hatóságnak a lehető leghamarabb közölnie kell az Ügynökséggel az általa kapott, az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR rész) IS.I.OR.230. pontja szerinti információbiztonsági jelentésekben szereplő, a repülésbiztonság szempontjából jelentős információkat.";

b) a szöveg az ATM/ANS.AR.A.025. pont után a következő ATM/ANS.AR.A.025A. ponttal egészül ki:

„**ATM/ANS.AR.A.025A. Azonnali reagálás a repülésbiztonságra hatást gyakorló információbiztonsági incidensre vagy sebezhetőségre**

a) Az illetékes hatóság létrehoz egy rendszert a szervezetek által jelentett, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensekkel és sebezhetőségekkel kapcsolatos információk megfelelő szintű gyűjtésére, elemzésére és terjesztésére. Ezt az adott tagállam minden más érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságával egyeztetve kell végrehajtani a jelentéstételi rendszerek közötti nagyobb összhang és összeegyeztethetőség érdekében.

b) Az Ügynökségnek létre kell hoznia egy rendszert az ATM/ANS.AR.A.020. c) pont szerint kapott, a repülésbiztonság szempontjából lényeges információk megfelelő szintű elemzésére, és haladéktalanul tájékoztatnia kell mindenről – ideértve az ajánlásokat és a végrehajtandó kiigazító intézkedéseket – a tagállamokat és a Bizottságot annak érdekében, hogy azok időben megoldást találhassanak az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak hatálya alá eső termékeket, alkatrészeket, fel nem szerelt berendezéseket, személyeket és szervezeteket érintő, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidensre és sebezhetőségre.

c) Az a) és b) pontban említett információk kézhezvétele után az illetékes hatóságnak meg kell tennie a szükséges intézkedéseket az információbiztonsági incidens vagy sebezhetőség repülésbiztonságra potenciálisan hatásának elhárítására.

d) A c) pont szerinti intézkedésekről haladéktalanul értesíteni kell minden olyan személyt és szervezetet, akinek/amelynek az (EU) 2018/1139 rendeletnek és annak felhatalmazáson alapuló és végrehajtási jogi aktusainak értelmében teljesítenie kell ezeket az intézkedéseket. Az illetékes tagállami hatóságnak értesítenie kell az intézkedésekről az Ügynökséget is, valamint ha közös fellépésre van szükség, akkor a többi érintett tagállam illetékes hatóságát is.";

c) az ATM/ANS.AR.B.001. pont a következő e) ponttal egészül ki:

„e) Az illetékes hatóság által létrehozott és fenntartott irányítási rendszernek az a) pontban foglalt követelményeken felül az (EU) 2023/203 végrehajtási rendelet I. mellékletében (IS.AR rész) foglalt rendelkezéseknek is meg kell felelnie a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében.";

d) az ATM/ANS.AR.B.005. pont a következőképpen módosul:

i. a cím helyébe a következő szöveg lép:

„**ATM/ANS.AR.B.005. Feladatok átruházása**";

ii. a szöveg a következő c) alponttal egészül ki:

„c) Az ATM/ANS.OR.B.005A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság feladatokat ruházhat át az a) pont szerinti minősített szervezetekre vagy az adott tagállam érintett, információbiztonságért vagy kiberbiztonságért felelős hatóságára. A feladatok átruházásakor az illetékes hatóságnak gondoskodnia kell az alábbiakról:

1. a minősített szervezet vagy az érintett hatóság minden repülésbiztonsági szempontot összehangol és figyelembe vesz;

2. a minősített szervezet vagy érintett hatóság által végzett tanúsítási és felügyeleti tevékenységek eredményeit a szervezet általános tanúsítási és felügyeleti irataiban rögzítik;

3. az ATM/ANS.AR.B.001. e) pont szerint létrehozott saját információbiztonsági irányítási rendszere kiterjed a nevében végrehajtott valamennyi tanúsítási és folyamatos felügyelet feladatra.";

e) az ATM/ANS.AR.C.010. pont a következő d) alponttal egészül ki:

„d) Az ANS.OR.B.005A. pont szervezet általi teljesítésének tanúsításával és felügyeletével összefüggésben az illetékes hatóság az a)–c) pont teljesítésén felül az e rendelet IS.I.OR.200. e) pontja vagy az (EU) 2022/1645 felhatalmazáson alapuló rendelet IS.D.OR.200. e) pontja alapján adott jóváhagyást is felülvizsgálja az alkalmazandó felügyeleti ellenőrzési ciklust követően, valamint minden olyan esetben, amikor a szervezet tevékenységi körében változtatásokat hajtanak végre.";

f) a szöveg az ATM/ANS.AR.C.025. pont után a következő ATM/ANS.AR.C.025A. ponttal egészül ki:

„**ATM/ANS.AR.C.025A. Az információbiztonsági irányítási rendszer változásai**

a) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR. rész) IS.I.OR.255. a) pontja szerint kezelt és az illetékes hatóságnak bejelentett változtatások esetében az illetékes hatóságnak az ATM/ANS.AR.C.010. pontban meghatározott elvekkel összhangban ki kell terjesztenie a folyamatos felügyeletet a szóban forgó változtatások felülvizsgálatára. Amennyiben meg nem felelést állapít meg, az illetékes hatóság értesíti erről a szervezetet, további változtatásokat kér, és az ATM/ANS.AR.C.050. pont szerint jár el.

b) Az (EU) 2023/203 végrehajtási rendelet II. mellékletének (IS.I.OR. rész) IS.I.OR.255. b) pontja szerint jóváhagyás iránti kérelmet igénylő egyéb változtatások esetében:

1. a változtatásra vonatkozó kérelem kézhezvételekor az illetékes hatóság a jóváhagyás megadása előtt ellenőrzi, hogy az adott szervezet teljesíti-e a vonatkozó követelményeket;

2. az illetékes hatóság meghatározza, hogy a szervezet milyen feltételek mellett működhet a változtatás végrehajtásának ideje alatt;

3. miután meggyőződött arról, hogy a szervezet teljesíti a vonatkozó követelményeket, az illetékes hatóság jóváhagyja a változtatást."

2. A III. melléklet (ATM/ANS.OR rész) a következőképpen módosul:

a) a szöveg az ATM/ANS.OR.B.005. pont után a következő ATM/ANS.OR.B.005A. ponttal egészül ki:

„**ATM/ANS.OR.B.005. Információbiztonsági irányítási rendszer**

Az ATM/ANS.OR.B.005. pontban említett irányítási rendszeren kívül a szolgáltató az (EU) 2023/203 végrehajtási rendelet felhatalmazáson alapuló rendeletnek megfelelően létrehoz, alkalmaz és fenntart egy információbiztonsági irányítási rendszert a repülésbiztonságot esetlegesen befolyásoló információbiztonsági kockázatok megfelelő kezelésének biztosítása érdekében.";

b) az ATM/ANS.OR.D.010. pont helyébe a következő szöveg lép:

„**ATM/ANS.OR.D.010. Védelmi irányítás**

a) A léginavigációs szolgatok, a légiforgalmiáramlás-szervezést végző szolgáltatók és a hálózatirányító az ATM/ANS.OR.B.005. pontban előírt irányítási rendszerük szerves részeként védelmi irányítási rendszert hoznak létre, hogy biztosítsák:

1. létesítményeik és személyzetük biztonságát a szolgáltatásnyújtásba való jogellenes beavatkozás megakadályozása érdekében;

2. a kapott, előállított vagy egyéb módon felhasznált működési adatok védelmét annak érdekében, hogy azokhoz csak engedéllyel rendelkezők férhessenek hozzá.

b) A védelemirányítási rendszer meghatározza:

1. a védelmi kockázat elemzésével és csökkentésével, a biztonság nyomon követésével és javításával, a biztonsági vizsgálatokkal és a tanulságok terjesztésével kapcsolatos folyamatokat és eljárásokat;

2. a biztonsági előírások megszegésének feltárására, figyelésére és észlelésére és a személyzet megfelelő biztonsági figyelmeztetésekkel történő riasztására szolgáló eszközöket;

3. a biztonsági rések hatásainak csökkentését és az újbóli bekövetkezést megelőző javító intézkedések és kockázatcsökkentő eljárások azonosítását célzó eszközöket.

c) A léginavigációs szolgálatok, a légiforgalmiáramlás-szervezést végző szolgáltatók és a hálózatirányító szükség esetén biztosítják a személyzet védelmi ellenőrzését, és a létesítmények, a személyzet és az adatok védelmének biztosítása érdekében egyeztetnek az illetékes polgári és katonai szervekkel.

d) Az információbiztonsághoz kapcsolódó szempontokat az ATM/ANS.OR.B.005A. pontban foglaltak szerint kell kezelni.”