Europeiska unionens råd

Bryssel den 18 juli 2022
(OR. en)

11468/22

AVIATION 171
DELACT 120

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	14 juli 2022
till:	Rådets generalsekretariat
Komm. dok. nr:	C(2022) 4882 final
Ärende:	KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 14 juli 2022 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1139 vad gäller krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten för organisationer som omfattas av kommissionens förordningar (EU) nr 748/2012 och nr 139/2014, och om ändring av kommissionens förordningar (EU) nr 748/2012 och nr 139/2014

För delegationerna bifogas dokument – C(2022) 4882 final.

Bilaga: C(2022) 4882 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 14.7.2022
C(2022) 4882 final

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/…

av den 14.7.2022

om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1139 vad gäller krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten för organisationer som omfattas av kommissionens förordningar (EU) nr 748/2012 och nr 139/2014, och om ändring av kommissionens förordningar (EU) nr 748/2012 och nr 139/2014

MOTIVERING

1. BAKGRUND TILL DEN DELEGERADE AKTEN

Det nuvarande europeiska regelverket för flygsäkerhet innehåller en rad krav som syftar till att minska sannolikheten för att en olycka ska inträffa.

Denna kombination av krav gör att det inte bör uppstå farliga situationer som kan leda till en olycka eller ett allvarligt tillbud även om fel, misstag och/eller brister inträffar. Tanken är alltså att en olycka eller ett allvarligt tillbud endast skulle inträffa vid en osannolik slumpmässig händelse där flera brister inträffar samtidigt och av en ren slump samverkar med varandra.

Det råder dock oro om att man inte har fokuserat tillräckligt på att förebygga en situation där befintliga brister på olika områden avsiktligt fås att samverka och utnyttjas av personer med ont uppsåt, då det inte längre rör sig om en slumpmässig händelse. Risken för detta ökar hela tiden inom den civila luftfarten, då de nuvarande informationssystemen blir alltmer sammankopplade.

Därför är det nödvändigt att införa krav på hantering av informationssäkerhetsrisker som kan ha en potentiell inverkan på flygsäkerheten.

De bestämmelser som införs genom denna delegerade akt stärker de ledningssystem, rapporteringsprocesser och rapporteringsförfaranden som krävs enligt bilaga II ”Grundläggande krav för luftvärdighet” och bilaga VII ”Grundläggande krav för flygplatser” till förordning (EU) 2018/1139[1] för konstruktions- och tillverkningsorganisationer samt för flygplatsoperatörer och leverantörer av ledningstjänster för trafik på plattan.

2. SAMRÅD SOM FÖREGÅTT ANTAGANDET AV AKTEN

I enlighet med artikel 128.4 i förordning (EU) 2018/1139 ska kommissionen, innan den antar en delegerad akt, samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning. Utkastet till delegerad akt lades fram för expertgruppen för flygsäkerhet, där företrädare för medlemsstaterna deltar, vid dess möten den 17 februari och den 29 juni 2022. Denna delegerade akt grundar sig på Easas yttrande nr 03/2021, vars innehåll konsulterades offentligt genom meddelandet om föreslagen ändring NPA 2019-07 *Management of information security risks*[2] (RMT.0720), offentliggjort av Easa den 27 maj 2019.

3. DEN DELEGERADE AKTENS RÄTTSLIGA ASPEKTER

Genom artiklarna 19.1 och 39.1 i förordning (EU) 2018/1139 ges kommissionen befogenhet att anta delegerade akter i enlighet med artikel 128 i den förordningen, med närmare bestämmelser med avseende på organisationer som ansvarar för konstruktion och tillverkning av produkter, delar och utrustning som inte är fast installerad och med avseende på organisationer som ansvarar för drift av flygplatser och tillhandahållande av ledningstjänster för trafik på plattan.

---

1 Europaparlamentets och rådets förordning (EU) 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91 (EUT L 212, 22.8.2018, s. 1)(https://eur-lex.europa.eu/legal-content/SV/TXT/?qid=1535612134845&uri=CELEX:32018R1139).

2 https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-07

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/…

av den 14.7.2022

om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1139 vad gäller krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten för organisationer som omfattas av kommissionens förordningar (EU) nr 748/2012 och nr 139/2014, och om ändring av kommissionens förordningar (EU) nr 748/2012 och nr 139/2014

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91[3], särskilt artiklarna 19.1 g och 39.1 b, och

av följande skäl:

(1) I enlighet med de grundläggande kraven i punkt 3.1 b i bilaga II till förordning (EU) 2018/1139 ska konstruktions- och tillverkningsorganisationer införa och upprätthålla ett ledningssystem för att hantera säkerhetsrisker.

(2) I enlighet med de grundläggande kraven i punkterna 2.2.1 och 5.2 i bilaga VII till förordning (EU) 2018/1139 ska dessutom flygplatsoperatörer och organisationer som ansvarar för tillhandahållande av ledningstjänster för trafik på plattan införa och upprätthålla ett ledningssystem för att hantera säkerhetsrisker.

(3) De säkerhetsrisker som avses i skälen 1 och 2 kan härröra från olika källor, bland annat konstruktions- och underhållsbrister, aspekter som rör mänskliga prestationer, miljöhot och informationssäkerhetshot. De ledningssystem som införs av organisationerna i den mening som avses i skälen 1 och 2 bör därför inte bara beakta säkerhetsrisker som härrör från slumpmässiga händelser, utan även säkerhetsrisker som härrör från informationssäkerhetshot där befintliga brister kan utnyttjas av personer med ont uppsåt. Dessa informationssäkerhetsrisker ökar ständigt inom den civila luftfarten, då de nuvarande informationssystemen blir alltmer sammankopplade och i allt högre grad blir måltavlor för illvilliga aktörer.

(4) De risker som är förknippade med dessa informationssystem är inte begränsade till eventuella cyberangrepp, utan omfattar även hot som kan påverka processer och förfaranden samt människors prestationer.

(5) Ett betydande antal organisationer använder redan internationella standarder, såsom ISO 27001, för att hantera säkerheten för digital information och digitala data. Dessa standarder kanske inte fullt ut tar hänsyn till den civila luftfartens alla särdrag.

3 EUT L 212, 22.8.2018, s. 1..

(6) Därför är det lämpligt att fastställa krav för hanteringen av informationssäkerhetsrisker med en potentiell inverkan på flygsäkerheten.

(7) Det är viktigt att dessa krav omfattar de olika luftfartsområdena och deras gränssnitt, eftersom luftfarten är ett i hög grad sammanlänkat system av system. De bör därför gälla för alla organisationer som redan måste ha ett ledningssystem i enlighet med unionens befintliga lagstiftning om flygsäkerhet.

(8) De krav som fastställs i denna förordning bör tillämpas konsekvent inom alla luftfartsområden, samtidigt som de skapar en minimal inverkan på den unionslagstiftning om flygsäkerhet som redan är tillämplig på dessa områden.

(9) De krav som fastställs i denna förordning bör inte påverka de krav på informationssäkerhet och cybersäkerhet som anges i punkt 1.7 i bilagan till kommissionens genomförandeförordning (EU) 2015/1998[4] och i artikel 14 i Europaparlamentets och rådets direktiv (EU) 2016/1148[5].

(10) Den definition av informationssäkerhet som används i denna rättsakt bör inte tolkas som en avvikelse från den definition av säkerhet i nätverks- och informationssystem som fastställs i direktiv 2016/1148.

(11) När organisationer som omfattas av denna förordning redan omfattas av säkerhetskrav som följer av andra unionsakter som avses i skäl 9 och som till sin verkan är likvärdiga med bestämmelserna i denna förordning bör uppfyllelse av dessa säkerhetskrav, för att undvika dubblering av rättsliga krav, anses utgöra uppfyllelse av de krav som fastställs i denna förordning.

(12) Organisationer som omfattas av denna förordning och som redan omfattas av säkerhetskrav som följer av förordning (EU) 2015/1998 bör också uppfylla kraven i bilaga I (Del IS.D.OR.230 ”Externt rapporteringssystem för informationssäkerhet”) till denna förordning eftersom förordning (EU) 2015/1998 inte innehåller några bestämmelser om extern rapportering av informationssäkerhetsincidenter.

(13) Förordningarna (EU) nr 748/2012[6] och nr 139/2014[7] bör ändras för att upprätta en koppling mellan de ledningssystem som föreskrivs i de förordningar som förtecknas ovan och de krav på hantering av informationssäkerhet som föreskrivs i denna förordning.

(14) För att ge organisationerna tillräckligt med tid för att säkerställa efterlevnaden av de nya regler och förfaranden som införs genom denna förordning bör denna förordning tillämpas från och med tre år efter dagen för ikraftträdandet.

---

4 Kommissionens genomförandeförordning (EU) 2015/1998 av den 5 november 2015 om detaljerade bestämmelser för genomförande av de gemensamma grundläggande standarderna avseende luftfartsskydd (EUT L 299, 14.11.2015, s. 1).

5 Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

6 Kommissionens förordning (EU) nr 748/2012 av den 3 augusti 2012 om fastställande av tillämpningsföreskrifter för luftvärdighets- och miljöcertifiering av luftfartyg och tillhörande produkter, delar och anordningar samt för certifiering av konstruktions- och tillverkningsorganisationer.

7 Kommissionens förordning (EU) nr 139/2014 av den 12 februari 2014 om krav och administrativa rutiner för flygplatser enligt Europaparlamentets och rådets förordning (EG) nr 216/2008.

(15) De krav som fastställs i denna förordning grundar sig på yttrande nr 03/2021[8] som utfärdats av byrån i enlighet med artikel 75.2 b och c och artikel 76.1 i förordning (EU) 2018/1139.

(16) I enlighet med artikel 128.4 i förordning (EU) 2018/1139 samrådde kommissionen med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning[9].

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Innehåll

I denna förordning fastställs de krav som de organisationer som avses i artikel 2 ska uppfylla för att identifiera och hantera informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten vilka skulle kunna påverka informations- och kommunikationstekniksystem och data som används för civil luftfart och för att upptäcka informationssäkerhetshändelser och identifiera dem som anses vara informationssäkerhetsincidenter med potentiell inverkan på flygsäkerheten samt hantera dessa informationssäkerhetsincidenter, även när det gäller återställning efter dem.

Artikel 2

Tillämpningsområde

1. Denna förordning är tillämplig på följande organisationer:

(a) Tillverkningsorganisationer och konstruktionsorganisationer som omfattas av avsnitt A kapitlen G och J i bilaga I (Del 21) till förordning (EU) nr 748/2012, utom konstruktions- och tillverkningsorganisationer som enbart deltar i konstruktion och/eller tillverkning av ELA2-luftfartyg enligt definitionen i artikel 1.2 j i förordning (EU) nr 748/2012.

(b) Flygplatsoperatörer och leverantörer av ledningstjänster för trafik på plattan vilka omfattas av bilaga III ”Del om organisationskrav (Del-ADR.OR)” till förordning (EU) nr 139/2014[10].

2. Denna förordning påverkar inte de krav på informationssäkerhet och cybersäkerhet som anges i punkt 1.7 i bilagan till kommissionens genomförandeförordning (EU) 2015/1998[11] och i artikel 14 i Europaparlamentets och rådets direktiv (EU) 2016/1148[12].

---

8 https://www.easa.europa.eu/document-library/opinions

9 EUT L 123, 12.5.2016, s. 1.

10 Kommissionens förordning (EU) nr 139/2014 av den 12 februari 2014 om krav och administrativa rutiner för flygplatser enligt Europaparlamentets och rådets förordning (EG) nr 216/2008 (EUT L 44, 14.2.2014, s. 1).

11 Kommissionens genomförandeförordning (EU) 2015/1998 av den 5 november 2015 om detaljerade bestämmelser för genomförande av de gemensamma grundläggande standarderna avseende luftfartsskydd (EUT L 299, 14.11.2015, s. 1).

12 Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

(1) *informationssäkerhet*: bevarande av nätverks- och informationssystemens konfidentialitet, integritet, autenticitet och tillgänglighet.

(2) *informationssäkerhetshändelse*: ett konstaterat system-, tjänste- eller nätverkstillstånd som tyder på en möjlig överträdelse av informationssäkerhetspolicyn eller fel i informationssäkerhetskontrollerna, eller en tidigare okänd situation som kan vara relevant för informationssäkerhet.

(3) *incident*: varje händelse som inverkar negativt på säkerheten i nätverks- och informationssystem enligt definitionen i artikel 4.7 i direktiv (EU) 2016/1148.

(4) *informationssäkerhetsrisk*: risken för organisatorisk civil luftfartsverksamhet, tillgångar, personer och andra organisationer på grund av potentialen för en informationssäkerhetshändelse. Informationssäkerhetsrisker är förknippade med potentialen att hot kommer att utnyttja sårbarheter i en informationstillgång eller en grupp av informationstillgångar.

(5) *hot*: en potentiell kränkning av informationssäkerheten som föreligger när det finns en enhet, omständighet, handling eller händelse som skulle kunna orsaka skada.

(6) *sårbarhet*: en brist eller svaghet i en tillgång eller ett system, förfaranden, konstruktion, genomförande eller informationssäkerhetsåtgärder som skulle kunna utnyttjas och som leder till en överträdelse eller kränkning av informationssäkerhetspolicyn.

Artikel 4

Krav som följer av annan unionslagstiftning

1. När en organisation som avses i artikel 2 uppfyller sådana säkerhetskrav som fastställs i artikel 14 i Europaparlamentets och rådets direktiv (EU) 2016/1148 och som är likvärdiga med kraven i den här förordningen, ska uppfyllelse av dessa säkerhetskrav anses utgöra uppfyllelse av kraven i den här förordningen.

2. När en organisation som avses i artikel 2 är en operatör eller en verksamhetsutövare som avses i medlemsstaternas nationella säkerhetsprogram för civil luftfart vilket utarbetats i enlighet med artikel 10 i Europaparlamentets och rådets förordning (EG) nr 300/2008[13], anses cybersäkerhetskraven i punkt 1.7 i bilagan till genomförandeförordning (EU) 2015/1998 vara likvärdiga med kraven i den här förordningen, med undantag för kraven i punkt IS.D.OR.230 i bilagan till den här förordningen vilka ska uppfyllas.

3. Kommissionen får, efter samråd med Easa och den samarbetsgrupp som avses i artikel 11 i direktiv (EU) 2016/1148, utfärda riktlinjer för bedömningen av likvärdigheten av de krav som fastställs i denna förordning och i direktiv (EU) 2016/1148.

[13] Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).

Artikel 5

Behörig myndighet

1. Den myndighet som ansvarar för att certifiera och övervaka efterlevnaden av denna förordning ska vara

   (a) den behöriga myndighet som utsetts i enlighet med bilaga I (Del 21) till förordning (EU) nr 748/2012, när det gäller organisationer som avses i artikel 2 a,

   (b) den behöriga myndighet som utsetts i enlighet med bilaga III (Del-ADR.OR) till förordning (EU) nr 139/2014, när det gäller organisationer som avses i artikel 2 b.

2. Medlemsstaterna får för tillämpningen av denna förordning utse en oberoende och autonom enhet som ska fullgöra den roll och det ansvar som tilldelas de behöriga myndigheter som avses i punkt 1. I sådana fall ska samordningsåtgärder fastställas mellan den enheten och de behöriga myndigheter som avses i punkt 1 för att säkerställa en effektiv tillsyn av alla krav som organisationen ska uppfylla.

Artikel 6

Ändring av förordning (EU) nr 748/2012

Bilaga I (Del 21) till förordning (EU) nr 748/2012 ska ändras på följande sätt:

(1) Innehållsförteckningen ska ändras på följande sätt:

   (a) Följande rubrik ska införas efter rubrik 21.A.139:

   ”21.A.139A System för hantering av informationssäkerhet”.

   (b) Följande rubrik ska införas efter rubrik 21.A.239:

   ”21.A.239A System för hantering av informationssäkerhet”.

(2) Efter punkt 21.A.139 ska följande punkt införas som punkt 21.A.139A:

”21.A.139A System för hantering av informationssäkerhet

Utöver det ledningssystem för tillverkningsorganisationer som krävs enligt punkt 21.A.139 ska tillverkningsorganisationen inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med delegerad förordning (EU) 202X/XXXX *[Publikationsbyrån: inför hänvisning till denna delegerade förordning]* för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(3) Efter punkt 21.A.239 ska följande punkt införas som punkt 21.A.239A:

”21.A.239A System för hantering av informationssäkerhet

Utöver det ledningssystem för konstruktionsorganisationer som krävs enligt punkt 21.A.239 ska konstruktionsorganisationen inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med delegerad förordning (EU) 202X/XXXX *[Publikationsbyrån: inför hänvisning till denna delegerade förordning]* för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

Artikel 7

Ändring av förordning (EU) nr 139/2014

Bilaga III (Del-ADR.OR) till förordning (EU) nr 139/2014[14] ska ändras på följande sätt:

(1) Efter punkt ADR.OR.D.005 ska följande punkt införas som punkt ADR.OR.D.005A:

”ADR.OR.D.005A System för hantering av informationssäkerhet

Flygplatsoperatören ska inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med delegerad förordning (EU) 202X/XXXX *[Publikationsbyrån: inför hänvisning till denna delegerade förordning]* för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(2) Punkt ADR.OR.D.007 ska ersättas med följande:

”ADR.OR.D.007 Behandling av flygdata och flyginformation

(a) Som en del av sitt ledningssystem ska flygplatsoperatören införa och underhålla ett system för kvalitetsstyrning som omfattar

(1) dess verksamheter som avser flygdata,

(2) dess verksamhet för tillhandahållande av flyginformation.

(b) Som en del av sitt ledningssystem ska flygplatsoperatören inrätta ett skyddsledningssystem för att säkerställa skyddet mot obehörig åtkomst av operativa data som den tar emot, tar fram eller använder på annat sätt, så att endast de som är bemyndigade får åtkomst till dessa data.

(c) Skyddsledningssystemet ska fastställa

(1) förfaranden för bedömning och reducering av dataskyddsrisker, övervakning och höjning av skyddet, skyddsöversyn och spridning av erfarenheter,

(2) medel för att upptäcka brister i skyddet och för att varsko personalen på lämpligt sätt,

(3) medel för att kontrollera följderna av brister i skyddet och för att identifiera motåtgärder i syfte att förhindra en upprepning.

(d) Flygplatsoperatören ska säkerställa att dess personal har säkerhetsprövats när det gäller säkerhet för flygdata.

(e) De aspekter som rör informationssäkerhet ska hanteras i enlighet med punkt ADR.OR.D.005A.”

(3) Efter punkt ADR.OR.F.045 ska följande punkt införas som punkt ADR.OR.F.045A:

”ADR.OR.F.045A System för hantering av informationssäkerhet

Den organisation som ansvarar för tillhandahållande av ledningstjänster för trafik på plattan ska inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med delegerad förordning (EU) 202X/XXXX *[Publikationsbyrån: inför hänvisning*

---

14 Kommissionens förordning (EU) nr 139/2014 av den 12 februari 2014 om krav och administrativa rutiner för flygplatser enligt Europaparlamentets och rådets förordning (EG) nr 216/2008 (EUT L 44, 14.2.2014, s. 1).

till denna delegerade förordning] för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

Artikel 8

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med ***tre år*** *efter dagen för ikraftträdandet*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 14.7.2022

På kommissionens vägnar
Ordförande
Ursula VON DER LEYEN