II

(Ikke-lovgivningsmæssige retsakter)

FORORDNINGER

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2023/203

af 27. oktober 2022

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2018/1139 for så vidt angår krav til styring af informationssikkerhedsrisici med potentiel indvirkning på flyvesikkerheden gældende for de organisationer, der er omfattet af Kommissionens forordning (EU) nr. 1321/2014, (EU) nr. 965/2012, (EU) nr. 1178/2011 og (EU) 2015/340 samt af Kommissionens gennemførelsesforordning (EU) 2017/373 og (EU) 2021/664, og for de kompetente myndigheder, der er omfattet af Kommissionens forordning (EU) nr. 748/2012, (EU) nr. 1321/2014, (EU) nr. 965/2012, (EU) nr. 1178/2011, (EU) 2015/340 og (EU) nr. 139/2014 og af Kommissionens gennemførelsesforordning (EU) 2017/373 og (EU) 2021/664, og om ændring af Kommissionens forordning (EU) nr. 1178/2011, (EU) nr. 748/2012, (EU) nr. 965/2012, (EU) nr. 139/2014, (EU) nr. 1321/2014 og (EU) 2015/340 og af Kommissionens gennemførelsesforordning (EU) 2017/373 og (EU) 2021/664

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2018/1139 af 4. juli 2018 om fælles regler for civil luftfart og oprettelse af Den Europæiske Unions Luftfartssikkerhedsagentur og om ændring af forordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 og direktiv 2014/30/EU og 2014/53/EU og om ophævelse af (EF) nr. 552/2004 og (EF) nr. 216/2008 og Rådets forordning (EØF) nr. 3922/91 ([1]), særlig artikel 17, stk. 1, litra b), artikel 27, stk. 1, litra a), artikel 31, stk. 1, litra b), artikel 43, stk. 1, litra b), artikel 53, stk. 1, litra a), og artikel 62, stk. 15, litra c), og

ud fra følgende betragtninger:

(1) I overensstemmelse med de væsentlige krav i punkt 3.1, litra b), i bilag II til forordning (EU) 2018/1139 skal organisationer til sikring af vedvarende luftdygtighed og vedligeholdelsesorganisationer indføre og vedligeholde et styringssystem for at styre sikkerhedsrisici.

(2) Desuden skal organisationer, der uddanner piloter, organisationer, der uddanner kabinebesætninger, flyvemedicinske centre for flyvende personale og operatører af flyvesimulatortræningsanordninger i overensstemmelse med de væsentlige krav i punkt 3.3, litra b), og punkt 5, litra b), i bilag IV til forordning (EU) 2018/1139, indføre og vedligeholde et styringssystem for at styre sikkerhedsrisici.

(3) Desuden skal luftfartsforetagender i overensstemmelse med de væsentlige krav i punkt 8.1, litra c), i bilag V til forordning (EU) 2018/1139 indføre og vedligeholde et styringssystem for at styre sikkerhedsrisici.

(4) Desuden skal udøvere af lufttrafikstyrings- og luftfartstjenester, U-space-tjenesteudøvere, eneudøvere af fælles informationstjenester, uddannelsesorganisationer og flyvemedicinske centre for flyveledere i overensstemmelse med de væsentlige krav i punkt 5.1, litra c), og punkt 5.4, litra b), i bilag VIII til forordning (EU) 2018/1139 indføre og vedligeholde et styringssystem for at styre sikkerhedsrisici.

([1]) EUT L 212 af 22.8.2018, s. 1.

(5) Disse sikkerhedsrisici kan stamme fra forskellige kilder, f.eks. konstruktions- og vedligeholdelsesfejl, forhold vedrørende menneskelig ydeevne, miljøtrusler og trusler mod informationssikkerheden. Derfor bør der i forbindelse med de styringssystemer, der er indført af Den Europæiske Unions Luftfartssikkerhedsagentur (»agenturet«) og de nationale kompetente myndigheder og organisationer, der er omhandlet i betragtningerne ovenfor, ikke alene tages hensyn til sikkerhedsrisici som følge af tilfældige begivenheder, men også sikkerhedsrisici som følge af trusler mod informationssikkerheden, hvor eksisterende mangler kan udnyttes af personer med ondsindet hensigt. Disse informationssikkerhedsrisici er i konstant stigning i det civile luftfartsmiljø, da de nuværende informationssystemer bliver stadig mere indbyrdes forbundne og i stigende grad bliver mål for ondsindede aktører.

(6) De risici, der er forbundet med disse informationssystemer, er ikke begrænset til potentielle cyberangreb, men omfatter også trusler, som kan påvirke processer og procedurer samt menneskers ydeevne.

(7) Et betydeligt antal organisationer anvender allerede internationale standarder såsom ISO 27001 for at håndtere sikkerheden i forbindelse med digital information og data. I disse standarder tages der måske ikke fuldt ud højde for alle de særlige forhold, der gælder for den civile luftfart. Der bør derfor fastsættes krav til styring af informationssikkerhedsrisici med potentiel indvirkning på flyvesikkerheden.

(8) Det er vigtigt, at disse krav dækker alle luftfartsområder og deres grænseflader, da luftfart er et stærkt sammenkoblet system af systemer. De bør derfor finde anvendelse på alle de organisationer og kompetente myndigheder, der er omfattet af Kommissionens forordning (EU) nr. 748/2012 ([2]), (EU) nr. 1321/2014 ([3]), (EU) nr. 965/2012 ([4]), (EU) nr. 1178/2011 ([5]), (EU) 2015/340 ([6]), (EU) nr. 139/2014 ([7]) og Kommissionens gennemførelsesforordning (EU) 2021/664 ([8]), herunder også de organisationer og kompetente myndigheder, som allerede skal have et styringssystem i overensstemmelse med gældende EU-lovgivning om flyvesikkerhed. Nogle organisationer bør dog udelukkes fra denne forordnings anvendelsesområde for at sikre passende proportionalitet i forhold til de lavere informationssikkerhedsrisici, de udgør for luftfartssystemet.

(9) Kravene i denne forordning bør garantere en konsekvent gennemførelse på alle luftfartsområder, samtidig med at de får minimal indvirkning på den EU-lovgivning for flyvesikkerheden, der allerede finder anvendelse på disse områder.

([2]) Kommissionens forordning (EU) nr. 748/2012 af 3. august 2012 om gennemførelsesbestemmelser for luftdygtigheds- og miljøcertificering af luftfartøjer og hermed forbundet materiel, dele og apparatur og for certificering af konstruktions- og produktionsorganisationer (EUT L 224 af 21.8.2012, s. 1).

([3]) Kommissionens forordning (EU) nr. 1321/2014 af 26. november 2014 om vedvarende luftdygtighed af luftfartøjer og luftfartøjsmateriel, -dele og -apparatur og om godkendelse af organisationer og personale, der deltager i disse opgaver (EUT L 362 af 17.12.2014, s. 1).

([4]) Kommissionens forordning (EU) nr. 965/2012 af 5. oktober 2012 om fastsættelse af tekniske krav og administrative procedurer for flyveoperationer i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 216/2008 (EUT L 296 af 25.10.2012, s. 1).

([5]) Kommissionens forordning (EU) nr. 1178/2011 af 3. november 2011 om fastsættelse af tekniske krav og administrative procedurer for flyvebesætninger i civil luftfart i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 216/2008 (EUT L 311 af 25.11.2011, s. 1).

([6]) Kommissionens forordning (EU) 2015/340 af 20. februar 2015 om fastsættelse af tekniske krav og administrative procedurer for flyveledercertifikater i medfør af Europa-Parlamentets og Rådets forordning (EF) nr. 216/2008 og om ændring af Kommissionens gennemførelsesforordning (EU) nr. 923/2012 og om ophævelse af Kommissionens forordning (EU) nr. 805/2011 (EUT L 63 af 6.3.2015, s. 1).

([7]) Kommissionens forordning (EU) nr. 139/2014 af 12. februar 2014 om fastsættelse af krav og administrative procedurer for flyvepladser i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 216/2008 (EUT L 44 af 14.2.2014, s. 1).

([8]) Kommissionens gennemførelsesforordning (EU) 2021/664 af 22. april 2021 om et regelsæt for U-space (EUT L 139 af 23.4.2021, s. 161).

(10) Kravene i denne forordning bør ikke berøre kravene til informationssikkerhed og cybersikkerhed i punkt 1.7 i bilaget til Kommissionens gennemførelsesforordning (EU) 2015/1998 ([9]) og i artikel 14 i Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 ([10]).

(11) Sikkerhedskravene i artikel 33-43 i afsnit V »Programmets sikkerhed« i Europa-Parlamentets og Rådets forordning (EU) 2021/696 ([11]) anses for at være ækvivalente med kravene i nærværende forordning med undtagelse af punkt IS.I.OR.230 i bilag II til nærværende forordning, som bør overholdes.

(12) For at skabe retssikkerhed bør fortolkningen af begrebet »informationssikkerhed« som defineret i denne forordning, der afspejler dets gængse anvendelse inden for civil luftfart på globalt plan, anses for at være i overensstemmelse med begrebet »sikkerhed i net- og informationssystemer« som defineret i artikel 4, nr. 2), i direktiv (EU) 2016/1148. Den definition på informationssikkerhed, der anvendes i denne forordning, bør ikke fortolkes som værende forskellig fra definitionen på sikkerheden i net- og informationssystemer i direktiv (EU) 2016/1148.

(13) For at undgå overlappende retlige krav i de tilfælde, hvor organisationer omfattet af denne forordning allerede er underlagt sikkerhedskrav i henhold til EU-retsakter som omhandlet i betragtning (10) og 11, der i praksis svarer til bestemmelserne i denne forordning, bør opfyldelsen af nævnte sikkerhedskrav anses for at udgøre opfyldelse af kravene i denne forordning.

(14) Organisationer, der er omfattet af denne forordning, og som allerede er underlagt sikkerhedskrav i henhold til gennemførelsesforordning (EU) 2015/1998 eller forordning (EU) 2021/696, eller begge, bør også opfylde kravene i bilag II (del IS.I.OR.230 »Ekstern indberetningsordning for informationssikkerhed«) til nærværende forordning, da ingen af de to forordninger indeholder bestemmelser vedrørende ekstern indberetning af informationssikkerhedshændelser.

(15) For fuldstændighedens skyld bør forordning (EU) nr. 1178/2011, (EU) nr. 748/2012, (EU) nr. 965/2012, (EU) nr. 139/2014, (EU) nr. 1321/2014, (EU) 2015/340 og gennemførelsesforordning (EU) 2017/373 ([12]) og (EU) 2021/664 ændres for at indføre de krav til systemer til styring af informationssikkerheden, der er fastsat i denne forordning, sammen med de styringssystemer, der er fastsat heri, og for at fastsætte kravene til kompetente myndigheders tilsyn med organisationer, der gennemfører ovennævnte krav til styring af informationssikkerheden.

(16) For at give organisationerne tilstrækkelig tid til at sikre overholdelse af de nye regler og procedurer bør denne forordning finde anvendelse tre år efter dens ikrafttræden med undtagelse af luftfartstjenesteudøveren for den europæiske geostationære navigations-overlay-tjeneste (EGNOS) som defineret i gennemførelsesforordning (EU) 2017/373, hvor nærværende forordning på grund af den igangværende sikkerhedsgodkendelse af Egnossystemet og -tjenesterne i overensstemmelse med forordning (EU) 2021/696 bør finde anvendelse fra den 1. januar 2026.

(17) Kravene i denne forordning er baseret på udtalelse nr. 03/2021 ([13]) afgivet af agenturet i overensstemmelse med artikel 75, stk. 2, litra b) og c), og artikel 76, stk. 1, i forordning (EU) 2018/1139.

([9]) Kommissionens gennemførelsesforordning (EU) 2015/1998 af 5. november 2015 om detaljerede foranstaltninger til gennemførelse af de fælles grundlæggende normer for luftfartssikkerhed (EUT L 299 af 14.11.2015, s. 1).

([10]) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

([11]) Europa-Parlamentets og Rådets forordning (EU) 2021/696 af 28. april 2021 om oprettelse af Unionens rumprogram og Den Europæiske Unions Agentur for Rumprogrammet og om ophævelse af forordning (EU) nr. 912/2010, (EU) nr. 1285/2013 og (EU) nr. 377/2014 og afgørelse nr. 541/2014/EU (EUT L 170 af 12.5.2021, s. 69).

([12]) Kommissionens gennemførelsesforordning (EU) 2017/373 af 1. marts 2017 om fastsættelse af fælles krav til udøvere af lufttrafikstyrings- og luftfartstjenester og andre lufttrafikstyringsnetfunktioner og tilsynet med disse udøvere, om ophævelse af forordning (EF) nr. 482/2008, gennemførelsesforordning (EU) nr. 1034/2011, (EU) nr. 1035/2011 og (EU) 2016/1377 og om ændring af forordning (EU) nr. 677/2011 (EUT L 62 af 8.3.2017, s. 1).

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

(18) Kravene i denne forordning er i overensstemmelse med udtalelse fra det udvalg med hensyn til anvendelsen af fælles sikkerhedsregler for civil luftfart, der er nedsat ved artikel 127 i forordning (EU) 2018/1139 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Genstand

I denne forordning fastsættes de krav, som organisationerne og de kompetente myndigheder skal opfylde med henblik på:

a) at afdække og styre informationssikkerhedsrisici med potentiel indvirkning på flyvesikkerheden, som kan påvirke informations- og kommunikationsteknologisystemer og data, der anvendes til civile luftfartsformål

b) at opdage informationssikkerhedsbegivenheder og indkredse dem, der anses for at være informationssikkerhedshændelser med potentiel indvirkning på flyvesikkerheden

c) at reagere på disse informationssikkerhedshændelser og komme på fode igen.

Artikel 2

Anvendelsesområde

1. Denne forordning finder anvendelse på følgende organisationer:

a) vedligeholdelsesorganisationer, der er omfattet af sektion A i bilag II (del-145) til forordning (EU) nr. 1321/2014, bortset fra de organisationer, der udelukkende beskæftiger sig med vedligeholdelse af luftfartøjer i overensstemmelse med bilag Vb (del-ML) til forordning (EU) nr. 1321/2014

b) organisationer til sikring af vedvarende luftdygtighed (CAMO), der er omfattet af sektion A i bilag Vc (del-CAMO) til forordning (EU) nr. 1321/2014, bortset fra de organisationer, der udelukkende beskæftiger sig med sikring af vedvarende luftdygtighed af luftfartøjer i overensstemmelse med bilag Vb (del-ML) til forordning (EU) nr. 1321/2014

c) luftfartsforetagender, der er omfattet af bilag III (del-ORO) til forordning (EU) nr. 965/2012, bortset fra de luftfartsforetagender, der udelukkende beskæftiger sig med drift af følgende:

   i) et ELA2-luftfartøj som defineret i artikel 1, nr. 2), litra j), i forordning (EU) nr. 748/2012

   ii) enmotorede, propeldrevne flyvemaskiner med en maksimal passagersædekonfiguration for operation på fem eller derunder, der ikke er klassificeret som et komplekst motordrevet luftfartøj, som starter og lander på samme flyveplads eller driftssted, og som opererer efter visuelflyvereglerne (VFR) om dagen

   iii) enmotorede helikoptere med en maksimal passagersædekonfiguration for operation på fem eller derunder, der ikke er klassificeret som et komplekst motordrevet luftfartøj, som starter og lander på samme flyveplads eller driftssted, og som opererer efter VFR om dagen.

d) godkendte træningsorganisationer (ATO'er), der er omfattet af bilag VII (del-ORA) til forordning (EU) nr. 1178/2011, bortset fra de organisationer, der udelukkende beskæftiger sig med uddannelsesaktiviteter målrettet ELA2-luftfartøjer som defineret i artikel 1, nr. 2), litra j), i forordning (EU) nr. 748/2012, eller som udelukkende beskæftiger sig med teoretisk uddannelse

e) flyvemedicinske centre for flyvende personale, der er omfattet af bilag VII (del-ORA) til forordning (EU) nr. 1178/2011

f) operatører af flyvesimulatortræningsanordninger (FSTD'er), der er omfattet af bilag VII (del-ORA) til forordning (EU) nr. 1178/2011, bortset fra de operatører, der udelukkende beskæftiger sig med drift af FSTD'er målrettet ELA2-luftfartøjer som defineret i artikel 1, nr. 2), litra j), i forordning (EU) nr. 748/2012

g) flyvelederuddannelsesorganisationer (ATCO TO'er) og ATCO-flyvemedicinske centre, der er omfattet af bilag III (del ATCO.OR) til forordning (EU) 2015/340

h) organisationer, der er omfattet af bilag III (del-ATM/ANS.OR) til gennemførelsesforordning (EU) 2017/373, undtagen følgende tjenesteudøvere:

i) luftfartstjenesteudøvere med et begrænset certifikat i overensstemmelse med punkt ATM/ANS.OR.A.010 i nævnte bilag

ii) udøvere af flyveinformationstjenester, som har afgivet erklæring om deres aktiviteter i overensstemmelse med punkt ATM/ANS.OR.A.015 i nævnte bilag

i) U-space-tjenesteudøvere og eneudøvere af fælles informationstjenester, der er omfattet af gennemførelsesforordning (EU) 2021/664.

2. Denne forordning finder anvendelse på de kompetente myndigheder, herunder Den Europæiske Unions Luftfartssikkerhedsagentur (»agenturet«), der er omhandlet i artikel 6 i denne forordning og i artikel 5 i Kommissionens delegerede forordning (EU) 2022/1645 ([14]).

3. Denne forordning finder også anvendelse på den kompetente myndighed, der er ansvarlig for at udstede, forlænge, ændre, inddrage eller tilbagekalde luftfartøjsvedligeholdelsescertifikater i overensstemmelse med bilag III (del-66) til forordning (EU) nr. 1321/2014.

4. Denne forordning berører ikke kravene til informationssikkerhed og cybersikkerhed i punkt 1.7 i bilaget til gennemførelsesforordning (EU) 2015/1998 og i artikel 14 i direktiv (EU) 2016/1148.

Artikel 3

Definitioner

I denne forordning forstås ved:

1) »informationssikkerhed«: bevarelse af net- og informationssystemers fortrolighed, integritet, autenticitet og tilgængelighed

2) »informationssikkerhedsbegivenhed«: en påvist hændelse i en system-, tjeneste- eller nettilstand, der tyder på et muligt brud på informationssikkerhedspolitikken eller svigt i informationssikkerhedskontrollen, eller en tidligere ukendt situation, der kan være relevant for informationssikkerheden

3) »hændelse«: enhver begivenhed, der har en faktisk negativ indvirkning på sikkerheden i net- og informationssystemer som defineret i artikel 4, nr. 7), i direktiv (EU) 2016/1148

4) »informationssikkerhedsrisiko«: risikoen for organisatoriske operationer inden for civil luftfart, aktiver, personer og andre organisationer som følge af en mulig informationssikkerhedsbegivenhed. Informationssikkerhedsrisici er forbundet med risikoen for, at trusler vil udnytte sårbarheder i et informationsaktiv eller en gruppe af informationsaktiver

([14]) Kommissionens delegerede forordning (EU) 2022/1645 af 14. juli 2022 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2018/1139 for så vidt angår krav til styring af informationssikkerhedsrisici med potentiel indvirkning på luftfartssikkerheden gældende for de organisationer, der er omfattet af Kommissionens forordning (EU) nr. 748/2012 og (EU) nr. 139/2014, og om ændring af Kommissionens forordning (EU) nr. 748/2012 og (EU) nr. 139/2014 (EUT L 248 af 26.9.2022, s. 18).

5) »trussel«: en potentiel krænkelse af informationssikkerheden, som findes, hvor der er en enhed, omstændighed, handling eller begivenhed, der kan forårsage skade

6) »sårbarhed«: en fejl eller svaghed i et aktiv eller et system, procedurer, konstruktion, gennemførelse eller informationssikkerhedsforanstaltninger, der kan udnyttes og resulterer i en overtrædelse af informationssikkerhedspolitikken.

Artikel 4

Krav til organisationer og kompetente myndigheder

1. De organisationer, der er omhandlet i artikel 2, stk. 1, skal opfylde kravene i bilag II (del-IS.I.OR) til nærværende forordning.

2. De kompetente myndigheder, der er omhandlet i artikel 2, stk. 2 og 3, skal opfylde kravene i bilag I (del-IS.AR) til nærværende forordning.

Artikel 5

Krav i henhold til andre EU-retsakter

1. Opfylder en organisation nævnt i artikel 2, stk. 1, sikkerhedskrav, som er fastsat i overensstemmelse med artikel 14 i direktiv (EU) 2016/1148, og som er ækvivalente med kravene i nærværende forordning, anses opfyldelsen af nævnte krav for at udgøre opfyldelse af kravene i nærværende forordning.

2. Når en organisation som omhandlet i artikel 2, stk. 1, er en operatør eller en enhed som omhandlet i de nationale sikkerhedsprogrammer for civil luftfart, som medlemsstaterne har udarbejdet i overensstemmelse med artikel 10 i Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 ([15]), skal cybersikkerhedskravene i punkt 1.7 i bilaget til gennemførelsesforordning (EU) 2015/1998 anses for at være ækvivalente med kravene i nærværende forordning med undtagelse af punkt IS.I.OR.230 i bilag II til nærværende forordning, som skal overholdes i dettes ordlyd.

3. Når en organisation som omhandlet i artikel 2, stk. 1, er luftfartstjenesteudøveren for den europæiske geostationære navigations-overlay-tjeneste (EGNOS) som omhandlet i forordning (EU) 2021/696, anses sikkerhedskravene i artikel 33-43 i afsnit V i den forordning for at være ækvivalente med kravene i nærværende forordning med undtagelse af punkt IS.I.OR.230 i bilag II til nærværende forordning, som skal overholdes i dettes ordlyd.

4. Kommissionen kan efter høring af det agentur og den samarbejdsgruppe, der er omhandlet i artikel 11 i direktiv (EU) 2016/1148, udstede retningslinjer for vurdering af ækvivalensen af kravene i denne forordning og i direktiv (EU) 2016/1148.

Artikel 6

Kompetent myndighed

1. Uden at det griber ind i de opgaver, der er tildelt Komitéen for Sikkerhedsgodkendelse som omhandlet i artikel 36 i forordning (EU) 2021/696, skal den myndighed, der er ansvarlig for at attestere og føre tilsyn med overholdelsen af denne forordning:

a) for organisationer omhandlet i artikel 2, stk. 1, litra a), være den kompetente myndighed, der er udpeget i overensstemmelse med bilag II (del-145) til forordning (EU) nr. 1321/2014

b) for organisationer omhandlet i artikel 2, stk. 1, litra b), være den kompetente myndighed, der er udpeget i overensstemmelse med bilag Vc (del-CAMO) til forordning (EU) nr. 1321/2014

([15]) Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 af 11. marts 2008 om fælles bestemmelser om sikkerhed (security) inden for civil luftfart og om ophævelse af forordning (EF) nr. 2320/2002 (EUT L 97 af 9.4.2008, s. 72).

c) for organisationer omhandlet i artikel 2, stk. 1, litra c), være den kompetente myndighed, der er udpeget i overensstemmelse med bilag III (del-ORO) til forordning (EU) nr. 965/2012

d) for organisationer omhandlet i artikel 2, stk. 1, litra d)-f), være den kompetente myndighed, der er udpeget i overensstemmelse med bilag VII (del-ORA) til forordning (EU) nr. 1178/2011

e) for organisationer omhandlet i artikel 2, stk. 1, litra g), være den kompetente myndighed, der er udpeget i overensstemmelse med artikel 6, stk. 2, i forordning (EU) 2015/340

f) for organisationer omhandlet i artikel 2, stk. 1, litra h), være den kompetente myndighed, der er udpeget i overensstemmelse med artikel 4, stk. 1, i gennemførelsesforordning (EU) 2017/373

g) for organisationer omhandlet i artikel 2, stk. 1, litra i), være den kompetente myndighed, der er udpeget i overensstemmelse med artikel 14, stk. 1, eller artikel 14, stk. 2, alt efter hvad der er relevant, i gennemførelsesforordning (EU) 2021/664.

2. Medlemsstaterne kan med henblik på denne forordning udpege en uafhængig og selvstændig enhed til at varetage den tildelte rolle og de tildelte ansvarsområder for de kompetente myndigheder, der er omhandlet i stk. 1. I så tilfælde skal der træffes koordineringsforanstaltninger mellem nævnte enhed og de kompetente myndigheder, der er omhandlet i stk. 1, for at sikre et effektivt tilsyn med alle de krav, som organisationen skal opfylde.

3. Agenturet samarbejder i fuld overensstemmelse med de gældende regler om fortrolighed, beskyttelse af personoplysninger og beskyttelse af klassificerede oplysninger med Den Europæiske Unions Agentur for Rumprogrammet (EUSPA) og med Komitéen for Sikkerhedsgodkendelse omhandlet i artikel 36 i forordning (EU) 2021/696 for at sikre et effektivt tilsyn med de krav, der gælder for luftfartstjenesteudøveren for EGNOS.

Artikel 7

Fremsendelse af relevante oplysninger til de kompetente NIS-myndigheder

De kompetente myndigheder i henhold til denne forordning informerer uden unødigt ophold det centrale kontaktpunkt, der er udpeget i overensstemmelse med artikel 8 i direktiv (EU) 2016/1148, om alle relevante oplysninger medtaget i de indberetninger, der indgives i henhold til punkt IS.I.OR.230 i bilag II til nærværende forordning og punkt IS.D.OR.230 i bilag I til delegeret forordning (EU) 2022/1645 af operatører af væsentlige tjenester, der er angivet i overensstemmelse med artikel 5 i direktiv (EU) 2016/1148.

Artikel 8

Ændring af forordning (EU) nr. 1178/2011

Bilag VI (del-ARA) og bilag VII (del-ORA) til forordning (EU) nr. 1178/2011 ændres som angivet i bilag III til nærværende forordning.

Artikel 9

Ændring af forordning (EU) nr. 748/2012

Bilag I (del 21) til forordning (EU) nr. 748/2012 ændres som angivet i bilag IV til nærværende forordning.

Artikel 10

Ændring af forordning (EU) nr. 965/2012

Bilag II (del-ARO) og bilag III (del-ORO) til forordning (EU) nr. 965/2012 ændres som angivet i bilag V til nærværende forordning.

Artikel 11

Ændring af forordning (EU) nr. 139/2014

Bilag II (del-ADR.AR) til forordning (EU) nr. 139/2014 ændres som angivet i bilag VI til nærværende forordning.

Artikel 12

Ændring af forordning (EU) nr. 1321/2014

Bilag II (del-145), bilag III (del-66) og bilag Vc (del-CAMO) til forordning (EU) nr. 1321/2014 ændres som angivet i bilag VII til nærværende forordning.

Artikel 13

Ændring af forordning (EU) 2015/340

Bilag II (del-ATCO.AR) og bilag III (del-ATCO.OR) til forordning (EU) 2015/340 ændres som angivet i bilag VIII til nærværende forordning.

Artikel 14

Ændring af gennemførelsesforordning (EU) 2017/373

Bilag II (del-ATM/ANS.AR) og bilag III (del-ATM/ANS.OR) til gennemførelsesforordning (EU) 2017/373 ændres som angivet i bilag IX til nærværende forordning.

Artikel 15

Ændring af gennemførelsesforordning (EU) 2021/664

I gennemførelsesforordning (EU) 2021/664 foretages følgende ændringer:

1) Artikel 15, stk. 1, litra f), affattes således:

»f) gennemføre og opretholde et sikkerhedsstyringssystem i overensstemmelse med punkt ATM/ANS.OR.D.010 i subpart D i bilag III til gennemførelsesforordning (EU) 2017/373 og et system til styring af informationssikkerhed i overensstemmelse med bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203.«

2) I artikel 18 tilføjes følgende litra l):

»l) oprette, gennemføre og opretholde et system til styring af informationssikkerhed i overensstemmelse med bilag I (del-IS.AR) til gennemførelsesforordning (EU) 2023/203.«

Artikel 16

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Den finder anvendelse fra 22. februar 2026.

For så vidt angår luftfartstjenesteudøveren for EGNOS, der er omfattet af gennemførelsesforordning (EU) 2017/373, finder den dog anvendelse fra den 1. januar 2026.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 27. oktober 2022.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG I

INFORMATIONSSIKKERHED — MYNDIGHEDSKRAV

[DEL-IS.AR]

IS.AR.100 Anvendelsesområde

IS.AR.200 System til styring af informationssikkerhed (ISMS)

IS.AR.205 Vurdering af informationssikkerhedsrisici

IS.AR.210 Håndtering af informationssikkerhedsrisici

IS.AR.215 Informationssikkerhedshændelser — opdagelse, reaktion og genopretning

IS.AR.220 Indgåelse af kontrakter om aktiviteter i forbindelse med styring af informationssikkerhed

IS.AR.225 Personalekrav

IS.AR.230 Registrering

IS.AR.235 Vedvarende forbedring

IS.AR.100 Anvendelsesområde

I denne del fastsættes de krav til styring, som de kompetente myndigheder, der er omhandlet i artikel 2, stk. 2, i denne forordning, skal opfylde.

De krav, som de kompetente myndigheder skal opfylde i forbindelse med udførelsen af deres certificerings-, tilsyns- og håndhævelsesaktiviteter, er fastsat i de forordninger, der er omhandlet i artikel 2, stk. 1, i nærværende forordning og i artikel 2 i delegeret forordning (EU) 2022/1645.

IS.AR.200 System til styring af informationssikkerhed (ISMS)

a) For at nå de mål, der er fastsat i artikel 1, skal den kompetente myndighed oprette, gennemføre og opretholde et system til styring af informationssikkerhed (ISMS), som sikrer, at den kompetente myndighed:

1) fastlægger en politik for informationssikkerhed og fastlægger den kompetente myndigheds overordnede principper med hensyn til informationssikkerhedsrisicis potentielle indvirkning på flyvesikkerheden

2) indkredser og gennemgår informationssikkerhedsrisici i overensstemmelse med punkt IS.AR.205

3) udarbejder og gennemfører foranstaltninger til håndtering af informationssikkerhedsrisici i overensstemmelse med punkt IS.AR.210

4) udarbejder og gennemfører, i overensstemmelse med punkt IS.AR.215, de foranstaltninger, der er nødvendige for at opdage informationssikkerhedsbegivenheder, finder frem til dem, der betragtes som hændelser med en potentiel indvirkning på flyvesikkerheden, og sørger for reaktion på disse informationssikkerhedshændelser og efterfølgende genopretning

5) opfylder kravene i punkt IS.AR.220, når der indgås kontrakter med andre organisationer om en hvilken som helst del af de aktiviteter, der er beskrevet i punkt IS.AR.200

6) opfylder personalekravene i punkt IS.AR.225

7) opfylder registreringskravene i punkt IS.AR.230

8) overvåger sin egen organisations opfyldelse af kravene i denne forordning og giver feedback om resultaterne til den person, der er omhandlet i punkt IS.AR.225, litra a), for at sikre en effektiv gennemførelse af afhjælpende foranstaltninger

9) beskytter fortroligheden af alle oplysninger, som den kompetente myndighed kan have vedrørende organisationer, der er underlagt dens tilsyn, og oplysninger, som modtages gennem organisationens eksterne rapporteringsordninger, der er oprettet i overensstemmelse med punkt IS.I.OR.230 i bilag II (del-IS.I.OR) til nærværende forordning og punkt IS.D.OR.230 i bilaget (del-IS.D.OR) til delegeret forordning (EU) 2022/1645

10) underretter agenturet om ændringer, der påvirker den kompetente myndigheds evne til at udføre sine opgaver og varetage sit ansvar som defineret i denne forordning

11) definerer og gennemfører procedurer for deling, hvor det er relevant og på en praktisk og rettidig måde, af relevante oplysninger for at bistå andre kompetente myndigheder og agenturer samt organisationer, der er omfattet af denne forordning, med at foretage effektive vurderinger af sikkerhedsrisici i forbindelse med deres aktiviteter.

b) For kontinuerligt at opfylde de i artikel 1 nævnte krav skal den kompetente myndighed gennemføre en løbende forbedringsproces i overensstemmelse med punkt IS.AR.235.

c) Den kompetente myndighed skal dokumentere alle centrale processer, procedurer, roller og ansvarsområder, der er nødvendige for at overholde punkt IS.AR.200, litra a), og fastlægge en procedure for ændring af denne dokumentation.

d) De processer, procedurer, roller og ansvarsområder, som den kompetente myndighed har fastlagt med henblik på at overholde punkt IS.AR.200, litra a), skal stemme overens med karakteren og kompleksiteten af den kompetente myndigheds aktiviteter på grundlag af en vurdering af de informationssikkerhedsrisici, der er forbundet med disse aktiviteter, og kan integreres i andre eksisterende styringssystemer, som den kompetente myndighed allerede har indført.

IS.AR.205 Vurdering af informationssikkerhedsrisici

a) Den kompetente myndighed skal afdække alle elementer i sin egen organisation, som kan være udsat for informationssikkerhedsrisici. Dette skal omfatte:

1) den kompetente myndigheds aktiviteter, faciliteter og ressourcer samt de tjenester, som den kompetente myndighed udøver, yder, modtager eller vedligeholder

2) det udstyr og de systemer, data og oplysninger, som bidrager til funktionen af de elementer, der er nævnt i nr. 1)

b) Den kompetente myndighed skal angive de grænseflader, som dens egen organisation har med andre organisationer, og som kan medføre gensidig eksponering for informationssikkerhedsrisici.

c) For så vidt angår de elementer og grænseflader, der er omhandlet i litra a) og b), skal den kompetente myndighed angive de informationssikkerhedsrisici, som kan have en potentiel indvirkning på flyvesikkerheden.

For hver angivet risiko skal den kompetente myndighed:

1) tildele et risikoniveau i henhold til en foruddefineret klassifikation fastsat af den kompetente myndighed

2) knytte hver risiko og dens niveau til det tilsvarende element eller den tilsvarende grænseflade, der er identificeret i overensstemmelse med litra a) og b).

Der skal i forbindelse med den foruddefinerede klassificering, der er omhandlet i nr. 1), tages hensyn til trusselsscenariets potentielle opståen og alvoren af de sikkerhedsmæssige konsekvenser heraf. Gennem denne klassificering og under hensyntagen til, hvorvidt den kompetente myndighed har en struktureret og repeterbar risikostyringsprocedure for operationer, skal den kompetente myndighed kunne fastslå, hvorvidt risikoen er acceptabel eller skal behandles i overensstemmelse med punkt IS.AR.210.

For at lette den gensidige sammenlignelighed af risikovurderinger skal der ved tildelingen af risikoniveauet i henhold til nr. 1) tages hensyn til relevante oplysninger, der er indhentet i samarbejde med de organisationer, der er omhandlet i litra b).

d) Den kompetente myndighed skal gennemgå og ajourføre den risikovurdering, der udføres i overensstemmelse med litra a), b) og c), i følgende tilfælde:

1) der er sket en ændring i de elementer, der er genstand for informationssikkerhedsrisici

2) der er sket en ændring i grænsefladerne mellem den kompetente myndigheds organisation og andre organisationer eller i de risici, der meddeles af andre organisationer

3) der er sket en ændring i den information eller viden, der bruges til identifikation, analyse og klassificering af risici

4) der er høstet erfaring fra analysen af informationssikkerhedshændelser.

IS.AR.210 Håndtering af informationssikkerhedsrisici

a) Den kompetente myndighed skal udvikle foranstaltninger til håndtering af de uacceptable risici, der angives i overensstemmelse med punkt IS.AR.205, gennemføre dem rettidigt og kontrollere deres fortsatte effektivitet. Disse foranstaltninger skal gøre det muligt for den kompetente myndighed at:

1) udøve kontrol over de omstændigheder, der bidrager til, at trusselsscenariet rent faktisk opstår

2) mindske de konsekvenser for flyvesikkerheden, der er forbundet med trusselsscenariets opståen

3) undgå risiciene.

Disse foranstaltninger må ikke medføre nye potentielle uacceptable risici for flyvesikkerheden.

b) Den person, der er omhandlet i punkt IS.AR.225, litra a), og andet berørt personale i den kompetente myndighed skal orienteres om resultatet af den risikovurdering, der udføres i overensstemmelse med punkt IS.AR.205, de tilsvarende trusselsscenarier og de foranstaltninger, der skal gennemføres.

Den kompetente myndighed skal også underrette organisationer, som den har en grænseflade med, jf. punkt IS.AR.205, litra b), om enhver risiko, der deles af den kompetente myndighed og organisationen.

IS.AR.215 Informationssikkerhedshændelser — opdagelse, reaktion og genopretning

a) Baseret på resultatet af den risikovurdering, der udføres i overensstemmelse med punkt IS.AR.205, og resultatet af den risikohåndtering, der udføres i overensstemmelse med punkt IS.AR.210, skal den kompetente myndighed gennemføre foranstaltninger for at opdage begivenheder, der potentielt kan bevirke, at der opstår uacceptable risici, og som kan have en potentiel indvirkning på flyvesikkerheden. Disse opdagelsesforanstaltninger skal gøre det muligt for den kompetente myndighed at:

1) opdage afvigelser fra forudbestemte funktionelle præstationsreferencescenarier

2) udløse advarsler for at aktivere passende reaktionsforanstaltninger i tilfælde af afvigelser.

b) Den kompetente myndighed skal gennemføre foranstaltninger som reaktion på enhver omstændighed i forbindelse med en begivenhed i overensstemmelse med litra a), som kan udvikle sig eller har udviklet sig til en informationssikkerhedshændelse. Disse reaktionsforanstaltninger skal gøre det muligt for den kompetente myndighed at:

1) indlede en reaktion fra sin egen organisation på de advarsler, der er omhandlet i litra a), nr. 2), ved at aktivere foruddefinerede ressourcer og fremgangsmåder

2) begrænse spredningen af et angreb og undgå, at et trusselsscenarie bliver til virkelighed

3) kontrollere svigttilstanden for de berørte elementer, der er omhandlet i punkt IS.AR.205, litra a).

c) Den kompetente myndighed skal gennemføre foranstaltninger med henblik på genopretning efter informationssikkerhedshændelser, herunder om nødvendigt nødforanstaltninger. Disse genopretningsforanstaltninger skal gøre det muligt for den kompetente myndighed at:

1) fjerne den omstændighed, der forårsagede hændelsen, eller begrænse den til et acceptabelt niveau

2) genetablere en sikker tilstand for de berørte elementer, der er omhandlet i punkt IS.AR.205, litra a), inden for en genopretningstid, der i forvejen er fastlagt af dens egen organisation.

IS.AR.220 Indgåelse af kontrakter om aktiviteter i forbindelse med styring af informationssikkerhed

Den kompetente myndighed skal sikre at, når der indgås kontrakt om enhver del af aktiviteterne i punkt IS.AR.200 med andre organisationer, opfylder disse aktiviteter kravene i denne forordning, og den organisation, med hvilken der er indgået kontrakt, arbejder under organisationens tilsyn. Den kompetente myndighed skal sikre, at de risici, der er forbundet med de udliciterede aktiviteter, håndteres hensigtsmæssigt.

IS.AR.225 Personalekrav

Den kompetente myndighed skal:

a) have en person, som har bemyndigelse til at etablere og vedligeholde de organisationsstrukturer, politikker, processer og procedurer, der er nødvendige for at gennemføre nærværende forordning.

Denne person skal:

1) have bemyndigelse til at få fuld adgang til de ressourcer, der er nødvendige for, at den kompetente myndighed kan udføre alle de opgaver, der kræves i henhold til denne forordning

2) være i besiddelse af den delegation af beføjelser, der nødvendig for at udføre de tildelte opgaver

b) have en procedure for at sikre, at den har tilstrækkeligt personale i tjeneste til at udføre de aktiviteter, der er omfattet af dette bilag

c) have en procedure for at sikre, at det personale, der er omhandlet i litra b), har de nødvendige kompetencer til at udføre deres opgaver

d) have en procedure for at sikre, at personalet anerkender det ansvar, der er forbundet med de tildelte roller og opgaver

e) sikre, at identiteten og troværdigheden af det personale, som har adgang til informationssystemer og data, der er omfattet af kravene i denne forordning, er behørigt fastlagt.

IS.AR.230 Registrering

a) Den kompetente myndighed skal føre dokumentation for sine aktiviteter inden for styring af informationssikkerhed

1) Den kompetente myndighed skal sikre, at følgende dokumentation arkiveres og kan spores:

i) kontrakter for aktiviteter, jf. punkt IS.AR.200, litra a), nr. 5)

ii) dokumentation for centrale procedurer, jf. punkt IS.AR.200, litra d)

iii) dokumentation for de risici, der er angivet i risikovurderingen, jf. punkt IS.AR.205, sammen med de tilknyttede foranstaltninger til håndtering af risiciene, jf. punkt IS.AR.210

iv) dokumentation for informationssikkerhedsbegivenheder, der eventuelt skal revurderes for at afsløre uopdagede informationssikkerhedshændelser eller -sårbarheder.

2) Dokumentationen i nr. 1), i), skal opbevares i mindst fem år efter, at kontrakten er blevet ændret eller afsluttet.

3) Dokumentationen i nr. 1), ii) og iii), skal opbevares i mindst fem år.

4) Dokumentationen i nr. 1), iv), skal opbevares, indtil disse informationssikkerhedsbegivenheder er blevet revurderet i overensstemmelse med den hyppighed, der er defineret i en procedure, som den kompetente myndighed har fastsat.

b) den kompetente myndighed skal føre dokumentation for kvalifikationer og erfaring hos sit eget personale, der er involveret i aktiviteter inden for styring af informationssikkerhed

1) Dokumentationen for personalets kvalifikationer og erfaring opbevares, så længe personen arbejder for den kompetente myndighed og i mindst tre år efter, at personen har fratrådt den kompetente myndighed.

2) De ansatte skal på deres anmodning have adgang til deres personlige oplysninger. Endvidere skal den kompetente myndighed efter anmodning forsyne personalet med en udskrift af deres personlige oplysninger, når de fratræder den kompetente myndighed.

c) Formatet for dokumentationen specificeres i den kompetente myndigheds procedurer.

d) Dokumentationen skal lagres på en måde, der sikrer beskyttelse mod skade, forandringer og tyveri, idet oplysningerne identificeres, når det er nødvendigt, i henhold til deres sikkerhedsklassificeringsniveau. Den kompetente myndighed skal sikre, at dokumentationen lagres på en måde, der sikrer integritet, ægthed og autoriseret adgang.

IS.AR.235 Vedvarende forbedring

a) Den kompetente myndighed skal ved hjælp af passende resultatindikatorer vurdere effektiviteten og modenheden af sin egen ISMS. Vurderingen skal udføres med en forudbestemt hyppighed, som den kompetente myndighed har fastsat, eller efter en informationssikkerhedshændelse.

b) Hvis der konstateres mangler efter den vurdering, der foretages i henhold til litra a), skal den kompetente myndighed træffe de nødvendige udbedrende foranstaltninger for at sikre, at ISMS fortsat opfylder de gældende krav og bevarer informationssikkerhedsrisiciene på et acceptabelt niveau. Desuden skal den kompetente myndighed revurdere de elementer i ISMS, som påvirkes af de vedtagne foranstaltninger.

BILAG II

INFORMATIONSSIKKERHED — ORGANISATIONSKRAV

[DEL-IS.I.OR]

IS.I.OR.100 Anvendelsesområde

IS.I.OR.200 System til styring af informationssikkerhed (ISMS)

IS.I.OR.205 Vurdering af informationssikkerhedsrisici

IS.I.OR.210 Håndtering af informationssikkerhedsrisici

IS.I.OR.215 Intern indberetningsordning for informationssikkerhed

IS.I.OR.220 Informationssikkerhedshændelser — opdagelse, reaktion og genopretning

IS.I.OR.225 Reaktion på anmærkninger meddelt af den kompetente myndighed

IS.I.OR.230 Ekstern indberetningsordning for informationssikkerhed

IS.I.OR.235 Indgåelse af kontrakter om aktiviteter i forbindelse med styring af informationssikkerhed

IS.I.OR.240 Personalekrav

IS.I.OR.245 Registrering

IS.I.OR.250 Håndbog til styring af informationssikkerhed (ISMM)

IS.I.OR.255 Ændring af systemet til styring af informationssikkerhed

IS.I.OR.260 Vedvarende forbedring

IS.I.OR.100 Anvendelsesområde

I denne del fastsættes de krav, som de organisationer, der er omhandlet i artikel 2, stk. 1, i denne forordning, skal opfylde.

IS.I.OR.200 System til styring af informationssikkerhed (ISMS)

a) For at nå de mål, der er fastsat i artikel 1, skal organisationen oprette, gennemføre og opretholde et system til styring af informationssikkerhed (ISMS), som sikrer, at organisationen:

   1) fastlægger en politik for informationssikkerhed og fastlægger organisationens overordnede principper med hensyn til informationssikkerhedsrisicis potentielle indvirkning på flyvesikkerheden

   2) indkredser og gennemgår informationssikkerhedsrisici i overensstemmelse med punkt IS.I.OR.205

   3) udarbejder og gennemfører foranstaltninger til håndtering af informationssikkerhedsrisici i overensstemmelse med punkt IS.I.OR.210

   4) indfører en intern indberetningsordning for informationssikkerhed i overensstemmelse med punkt IS.I.OR.215

   5) udarbejder og gennemfører, i overensstemmelse med punkt IS.I.OR.220, de foranstaltninger, der er nødvendige for at opdage informationssikkerhedsbegivenheder, finder frem til de begivenheder, der betragtes som hændelser med en potentiel indvirkning på flyvesikkerheden, bortset fra når det er tilladt i henhold til punkt IS.I.OR.205, litra e), og sørger for reaktion på disse informationssikkerhedshændelser og efterfølgende genopretning

6) gennemfører de foranstaltninger, som den kompetente myndighed har givet meddelelse om, som en omgående reaktion på en informationssikkerhedshændelse eller -sårbarhed med indvirkning på flyvesikkerheden

7) træffer passende foranstaltninger i overensstemmelse med punkt IS.I.OR.225 for at følge op på de anmærkninger, som den kompetente myndighed har meddelt

8) indfører en ekstern indberetningsordning i overensstemmelse med punkt IS.I.OR.230 med henblik på at sætte den kompetente myndighed i stand til at træffe passende foranstaltninger

9) opfylder kravene i punkt IS.I.OR.235, når der indgås kontrakter med andre organisationer om en hvilken som helst del af de aktiviteter, der er omhandlet i punkt IS.I.OR.200

10) opfylder personalekravene i punkt IS.I.OR.240

11) opfylder registreringskravene i punkt IS.I.OR.245

12) overvåger organisationens opfyldelse af kravene i denne forordning og giver feedback om resultaterne til den teknisk/økonomisk ansvarlige person for at sikre en effektiv gennemførelse af afhjælpende foranstaltninger

13) beskytter, uden at dette berører gældende krav om indberetning af hændelser, fortroligheden af alle oplysninger, som organisationen måtte have modtaget fra andre organisationer, i henhold til deres følsomhedsgrad.

b) For kontinuerligt at opfylde de i artikel 1 nævnte krav skal organisationen gennemføre en løbende forbedringsproces i overensstemmelse med punkt IS.I.OR.260.

c) Organisationen skal i overensstemmelse med punkt IS.I.OR.250 dokumentere alle centrale processer, procedurer, roller og ansvarsområder, der er nødvendige for at overholde punkt IS.I.OR.200, litra a), og skal fastlægge en procedure for ændring af denne dokumentation. Ændringer af disse processer, procedurer, roller og ansvarsområder skal forvaltes i overensstemmelse med punkt IS.I.OR.255.

d) De processer, procedurer, roller og ansvarsområder, som organisationen har fastlagt med henblik på at overholde punkt IS.I.OR.200, litra a), skal stemme overens med karakteren og kompleksiteten af organisationens aktiviteter på grundlag af en vurdering af de informationssikkerhedsrisici, der er forbundet med disse aktiviteter, og kan integreres i andre eksisterende styringssystemer, som organisationen allerede har indført.

e) Uden at det berører forpligtelsen til at opfylde indberetningskravene i forordning (EU) nr. 376/2014 og kravene i punkt IS.I.OR.200, litra a), nr. 13), kan organisationen godkendes af den kompetente myndighed til ikke at gennemføre de krav, der er omhandlet i litra a)-d), og de relaterede krav i punkt IS.I.OR.205 til IS.I.OR.260, hvis den over for myndigheden godtgør, at dens aktiviteter, faciliteter og ressourcer samt de tjenester, den opererer, udøver, modtager og vedligeholder, ikke udgør nogen informationssikkerhedsrisiko med potentiel indvirkning på flyvesikkerheden, hverken for sig selv eller for andre organisationer. Godkendelsen skal baseres på en dokumenteret vurdering af informationssikkerhedsrisici, der er udført af organisationen eller en tredjepart i overensstemmelse med punkt IS.I.OR.205 og gennemgået og godkendt af dens kompetente myndighed.

Godkendelsens fortsatte gyldighed vil blive gennemgået af den kompetente myndighed efter den gældende cyklus for evaluering af tilsynet, og når der gennemføres ændringer i organisationens arbejdsområde.

IS.I.OR.205 Vurdering af informationssikkerhedsrisici

a) Organisationen skal klarlægge alle dens elementer, som kan være udsat for informationssikkerhedsrisici. Dette skal omfatte:

1) organisationens aktiviteter, faciliteter og ressourcer samt de tjenester, som organisationen opererer, udøver, modtager eller vedligeholder

2) det udstyr og de systemer, de data og de oplysninger, som bidrager til funktionen af de elementer, der er nævnt i nr. 1).

b) Organisationen skal identificere de grænseflader, den har med andre organisationer, og som kan medføre gensidig eksponering for informationssikkerhedsrisici.

c) Med hensyn til de elementer og grænseflader, der er omhandlet i litra a) og b), skal organisationen angive de informationssikkerhedsrisici, som kan have en potentiel indvirkning på flyvesikkerheden. For hver identificeret risiko skal organisationen:

1) tildele et risikoniveau i henhold til en foruddefineret klassifikation fastsat af organisationen

2) knytte hver risiko og dens niveau til det tilsvarende element eller den tilsvarende grænseflade, der er identificeret i overensstemmelse med litra a) og b).

Der skal i forbindelse med den foruddefinerede klassificering, der er omhandlet i nr. 1), tages hensyn til trusselsscenariets potentielle opståen og alvoren af de sikkerhedsmæssige konsekvenser heraf. På grundlag af denne klassificering og under hensyntagen til, hvorvidt organisationen har en struktureret og repeterbar risikostyringsprocedure for operationer, skal organisationen kunne fastslå, hvorvidt risikoen er acceptabel eller skal behandles i overensstemmelse med punkt IS.I.OR.210.

For at lette den gensidige sammenlignelighed af risikovurderinger skal der ved tildelingen af risikoniveauet i henhold til nr. 1) tages hensyn til relevante oplysninger, der er indhentet i samarbejde med de organisationer, der er omhandlet i litra b).

d) Organisationen skal gennemgå og ajourføre den risikovurdering, der udføres i overensstemmelse med litra a), b) og, alt efter hvad der er relevant, litra c) eller e), i følgende situationer:

1) der er sket en ændring i de elementer, der er genstand for informationssikkerhedsrisici

2) der er sket en ændring i grænsefladerne mellem organisationen og andre organisationer eller i de risici, der meddeles af andre organisationer

3) der er sket en ændring i den information eller viden, der bruges til identifikation, analyse og klassificering af risici

4) der er høstet erfaring fra analysen af informationssikkerhedshændelser.

e) Uanset litra c) erstatter de organisationer, der skal overholde subpart C i bilag III (del-ATM/ANS.OR) til gennemførelsesforordning (EU) 2017/373, analysen af indvirkningen på flyvesikkerheden med en analyse af indvirkningen på deres tjenester i henhold til den understøttende sikkerhedsvurdering, der kræves i punkt ATM/ANS.OR.C.005. Denne understøttende sikkerhedsvurdering stilles til rådighed for de lufttrafiktjenesteudøvere, som de udøver tjenester til, og disse lufttrafiktjenesteudøvere er ansvarlige for at evaluere indvirkningen på flyvesikkerheden.

IS.I.OR.210 Håndtering af informationssikkerhedsrisici

a) Organisationen skal udvikle foranstaltninger til håndtering af de uacceptable risici, der afdækkes i overensstemmelse med punkt IS.I.OR.205, gennemføre dem rettidigt og kontrollere deres fortsatte effektivitet. Disse foranstaltninger skal gøre det muligt for organisationen at:

1) udøve kontrol over de omstændigheder, der bidrager til, at trusselsscenariet rent faktisk opstår

2) mindske de konsekvenser for flyvesikkerheden, der er forbundet med trusselsscenariets opståen

3) undgå risiciene.

Disse foranstaltninger må ikke medføre nye potentielle uacceptable risici for flyvesikkerheden.

b) Den person, der er omhandlet i punkt IS.I.OR.240, litra a) og b), og andet berørt personale i organisationen skal orienteres om resultatet af den risikovurdering, der udføres i overensstemmelse med punkt IS.I.OR.205, de tilsvarende trusselsscenarier og de foranstaltninger, der skal gennemføres.

Organisationen skal også underrette organisationer, som den har en grænseflade med, jf. punkt IS.I.OR.205, litra b), om enhver risiko, der deles af begge organisationer.

IS.I.OR.215 Intern indberetningsordning for informationssikkerhed

a) Organisationen skal etablere en intern indberetningsordning for at muliggøre indsamling og evaluering af informationssikkerhedsbegivenheder, herunder begivenheder der skal indberettes i henhold til punkt IS.I.OR.230.

b) Denne ordning og den proces, der er omhandlet i punkt IS.I.OR.220, skal gøre det muligt for organisationen at:

1) fastlægge, hvilke af de begivenheder der indberettes i henhold til litra a), der anses som informationssikkerhedshændelser eller -sårbarheder med en potentiel indvirkning på flyvesikkerheden

2) afdække årsagerne til og de faktorer, der medvirker til de informationssikkerhedshændelser og -sårbarheder, der fastlægges i overensstemmelse med nr. 1), og håndtere dem som led i proceduren for styring af informationssikkerhedsrisici i overensstemmelse med punkt IS.I.OR.205 og IS.I.OR.220

3) sikre en evaluering af alle kendte og relevante oplysninger vedrørende de informationssikkerhedshændelser og -sårbarheder, der fastlægges i overensstemmelse med nr. 1)

4) sikre indførelsen af en metode til intern distribution af oplysningerne, hvis det er nødvendigt.

c) Enhver organisation, med hvilken der er indgået kontrakt, og som kan udsætte organisationen for informationssikkerhedsrisici med potentiel indvirkning på flyvesikkerheden, skal pålægges at indberette informationssikkerhedsbegivenheder til organisationen. Disse indberetninger indsendes i henhold til de procedurer, der er fastsat i de specifikke kontraktlige ordninger, og evalueres i overensstemmelse med litra b).

d) Organisationen skal arbejde sammen om undersøgelser med enhver anden organisation, der yder et væsentligt bidrag til informationssikkerheden for sine egne aktiviteter.

e) Organisationen kan integrere denne indberetningsordning med andre indberetningsordninger, som den allerede har indført.

IS.I.OR.220 Informationssikkerhedshændelser — opdagelse, reaktion og genopretning

a) Baseret på resultatet af den risikovurdering, der udføres i overensstemmelse med punkt IS.I.OR.205, og resultatet af den risikohåndtering, der udføres i overensstemmelse med punkt IS.I.OR.210, skal organisationen gennemføre foranstaltninger for at opdage hændelser og sårbarheder, der potentielt kan bevirke, at der opstår uacceptable risici, og som kan have en potentiel indvirkning på flyvesikkerheden. Disse opdagelsesforanstaltninger skal gøre det muligt for organisationen at:

1) opdage afvigelser fra forudbestemte funktionelle præstationsreferencescenarier

2) udløse advarsler for at aktivere passende reaktionsforanstaltninger i tilfælde af afvigelser.

b) Organisationen skal gennemføre foranstaltninger som reaktion på enhver omstændighed i forbindelse med en begivenhed i overensstemmelse med litra a), som kan udvikle sig eller har udviklet sig til en informationssikkerhedshændelse. Disse reaktionsforanstaltninger skal gøre det muligt for organisationen at:

1) indlede en reaktionen på de advarsler, der er omhandlet i litra a), nr. 2), ved at aktivere foruddefinerede ressourcer og fremgangsmåder

2) begrænse spredningen af et angreb og undgå, at et trusselsscenarie bliver til virkelighed

3) kontrollere svigttilstanden for de berørte elementer, der er omhandlet i punkt IS.I.OR.205, litra a).

c) Organisationen skal gennemføre foranstaltninger med henblik på genopretning efter informationssikkerhedshændelser, herunder om nødvendigt nødforanstaltninger. Disse genopretningsforanstaltninger skal gøre det muligt for organisationen at:

1) fjerne den omstændighed, der forårsagede hændelsen, eller begrænse den til et acceptabelt niveau

2) opnå en sikker tilstand for de berørte elementer, der er omhandlet i punkt IS.I.OR.205, litra a), inden for en genopretningstid, der i forvejen er fastlagt af organisationen.

IS.I.OR.225 Reaktion på anmærkninger meddelt af den kompetente myndighed

a) Efter modtagelsen af meddelelsen om anmærkninger, som den kompetente myndighed har forelagt, skal organisationen:

1) påvise den eller de bagvedliggende årsager til samt medvirkende faktorer, som ligger til grund for den manglende overensstemmelse

2) fastlægge en plan for afhjælpende foranstaltninger

3) påvise, at den manglende overensstemmelse er afhjulpet til den kompetente myndigheds tilfredshed.

b) Foranstaltningerne som omhandlet i litra a) skal træffes inden for den frist, der er aftalt med den pågældende kompetente myndighed.

IS.I.OR.230 Ekstern indberetningsordning for informationssikkerhed

a) Organisationen skal indføre et indberetningssystem for informationssikkerhed, der opfylder kravene i forordning (EU) nr. 376/2014 og i dennes delegerede retsakter og gennemførelsesretsakter, hvis nævnte forordning finder anvendelse på organisationen.

b) Uden at det berører forpligtelserne i henhold til forordning (EU) nr. 376/2014, skal organisationen sikre, at enhver informationssikkerhedshændelse eller -sårbarhed, der kan udgøre en væsentlig risiko for flyvesikkerheden, indberettes til dens kompetente myndighed. Derudover gælder følgende:

1) Hvor en sådan hændelse eller sårbarhed påvirker et luftfartøj eller et dermed forbundet system eller en dermed forbundet komponent, skal organisationen også indberette hændelsen eller sårbarheden til indehaveren af konstruktionsgodkendelsen

2) Hvor en sådan hændelse eller sårbarhed påvirker et system eller dele heraf, der anvendes af organisationen, skal organisationen indberette hændelsen eller sårbarheden til den organisation, der er ansvarlig for konstruktionen af systemet eller komponenten.

c) Organisationen skal indberette de omstændigheder, der er omhandlet i litra b), som følger:

1) der skal foretages en underretning til den kompetente myndighed og, hvis det er relevant, til indehaveren af konstruktionsgodkendelsen eller til den organisation, der er ansvarlig for systemets eller komponentens konstruktion, så snart organisationen har fået kendskab til omstændigheden

2) der skal forelægges en rapport for den kompetente myndighed og, hvis det er relevant, for indehaveren af konstruktionsgodkendelsen eller for den organisation, der er ansvarlig for systemets eller komponentens konstruktion, hurtigst muligt, men ikke senere end 72 timer fra det tidspunkt, hvor organisationen har fået kendskab til omstændigheden, medmindre særlige omstændigheder forhindrer dette.

Rapporten skal udarbejdes i den form, der er fastlagt af den kompetente myndighed, og skal indeholde alle de relevante oplysninger om den omstændighed, som organisationen er bekendt med

3) der skal forelægges en opfølgningsrapport for den kompetente myndighed og, hvis det er relevant, for indehaveren af konstruktionsgodkendelsen eller for den organisation, der er ansvarlig for systemets eller komponentens konstruktion, med oplysninger om de foranstaltninger, som organisationen har truffet eller agter at træffe for at forebygge lignende informationssikkerhedshændelser i fremtiden.

Den opfølgende rapport skal forelægges, så snart disse foranstaltninger er identificeret, og skal udarbejdes i den form, der er fastlagt af den kompetente myndighed.

IS.I.OR.235 Indgåelse af kontrakter om aktiviteter i forbindelse med styring af informationssikkerhed

a) Organisationen skal sikre, at når der er indgået kontrakt om enhver del af aktiviteterne i punkt IS.I.OR.200 med andre organisationer, opfylder disse aktiviteter kravene i denne forordning, og at den organisation, med hvilken der er indgået kontrakt, arbejder under organisationens tilsyn. Organisationen skal sikre, at de risici, der er forbundet med de udliciterede aktiviteter, håndteres hensigtsmæssigt.

b) Organisationen skal sikre, at den kompetente myndighed efter anmodning kan få adgang til den organisation, med hvilken der er indgået kontrakt, for at fastlægge, om de gældende krav i denne forordning fortsat er opfyldt.

IS.I.OR.240 Personalekrav

a) Organisationens teknisk/økonomisk ansvarlige person, som er udpeget i overensstemmelse med forordning (EU) nr. 1321/2014, (EU) nr. 965/2012, (EU) nr. 1178/2011, (EU) 2015/340, gennemførelsesforordning (EU) 2017/373 eller gennemførelsesforordning (EU) 2021/664, alt efter hvad der er relevant, jf. artikel 2, stk. 1, i denne forordning, skal have organisationens bemyndigelse til at sikre, at alle de aktiviteter, der kræves i henhold til denne forordning, kan finansieres og udføres. Denne person skal:

1) sikre, at alle nødvendige ressourcer er til rådighed for at opfylde kravene i denne forordning

2) fastlægge og fremme den informationssikkerhedspolitik, der er angivet i punkt IS.I.OR.200, litra a), nr. 1)

3) udvise en grundlæggende forståelse af denne forordning.

b) Den teknisk/økonomisk ansvarlige person skal udpege en person eller en gruppe af personer for at sikre, at organisationen opfylder kravene i denne forordning, og skal definere omfanget af deres beføjelser. Denne person eller gruppe af personer skal rapportere direkte til den teknisk/økonomisk ansvarlige person og skal have den nødvendige viden, baggrund og erfaring til at varetage sit ansvar. Det skal fastlægges i procedurerne, hvem der er stedfortræder for en given person i tilfælde af, at denne person er fraværende i længere tid.

c) Den teknisk/økonomisk ansvarlige person skal udpege en person eller en gruppe af personer med ansvar for at forvalte den overvågningsfunktion, der er angivet i punkt IS.I.OR.200, litra a), nr. 12).

d) Når organisationen deler organisationsstrukturer, politikker, processer og procedurer for informationssikkerhed med andre organisationer eller med områder af deres egen organisation, som ikke er omfattet af godkendelsen eller erklæringen, kan den teknisk/økonomisk ansvarlige person uddelegere sine aktiviteter til en fælles ansvarlig person.

I et sådant tilfælde skal der træffes koordineringsforanstaltninger mellem organisationens teknisk/økonomisk ansvarlige person og den fælles ansvarlige person for at sikre tilstrækkelig integration af styringen af informationssikkerheden i organisationen.

e) Den teknisk/økonomisk ansvarlige person eller den fælles ansvarlige person, der er omhandlet i litra d), skal have organisationens bemyndigelse til at etablere og vedligeholde de organisationsstrukturer, politikker, processer og procedurer, der er nødvendige for at gennemføre punkt IS.I.OR.200.

f) Organisationen skal indføre en procedure for at sikre, at den har tilstrækkeligt personale i tjeneste til at udføre de aktiviteter, der er omfattet af dette bilag.

g) Organisationen skal indføre en procedure for at sikre, at det personale, der er omhandlet i litra f), har de nødvendige kompetencer til at udføre deres opgaver.

h) Organisationen skal indføre en procedure for at sikre, at personalet anerkender det ansvar, der er forbundet med de tildelte roller og opgaver.

i) Organisationen skal sikre, at identiteten og troværdigheden af det personale, som har adgang til informationssystemer og data, der er omfattet af kravene i denne forordning, er behørigt fastlagt.

IS.I.OR.245 Registrering

a) *Organisationen skal føre dokumentation for sine aktiviteter inden for styring af informationssikkerhed*

1) Organisationen skal sikre, at følgende dokumentation arkiveres og kan spores:

i) enhver godkendelse, der er modtaget, og enhver tilknyttet vurdering af informationssikkerhedsrisici i overensstemmelse med punkt IS.I.OR.200, litra e)

ii) kontrakter for aktiviteter, jf. punkt IS.I.OR.200, litra a), nr. 9)

iii) dokumentation for centrale procedurer, jf. punkt IS.I.OR.200, litra d)

iv) dokumentation for de risici, der er kortlagt i risikovurderingen, jf. punkt IS.I.OR.205, sammen med de tilknyttede foranstaltninger til håndtering af risiciene, jf. punkt IS.I.OR.210

v) dokumentation for informationssikkerhedshændelser og -sårbarheder, der er indberettet i overensstemmelse med indberetningsordningerne, jf. punkt IS.I.OR.215 og IS.I.OR.230

vi) dokumentation for de informationssikkerhedsbegivenheder, der eventuelt skal revurderes for at afsløre uopdagede informationssikkerhedshændelser eller -sårbarheder.

2) Dokumentationen i nr. 1), i), skal opbevares i mindst fem år efter udløbet af godkendelsens gyldighedsperiode.

3) Dokumentationen i nr. 1), ii), skal opbevares i mindst fem år efter, at kontrakten er blevet ændret eller afsluttet.

4) Dokumentationen i nr. 1), iii), iv) og v), skal opbevares i mindst fem år.

5) Dokumentationen i nr. 1), vi), skal opbevares, indtil disse informationssikkerhedsbegivenheder er blevet revurderet i overensstemmelse med den hyppighed, der er defineret i en procedure, som organisationen har fastsat.

b) *Organisationen skal føre dokumentation for kvalifikationer og erfaring hos sit eget personale, der er involveret i aktiviteter inden for styring af informationssikkerhed*

1) Dokumentationen for personalets kvalifikationer og erfaring skal opbevares, så længe personen arbejder for organisationen og i mindst tre år efter, at personen har fratrådt organisationen.

2) De ansatte skal på deres anmodning have adgang til deres personlige oplysninger. Endvidere skal organisationen efter anmodning forsyne personalet med en udskrift af deres personlige oplysninger, når de fratræder organisationen.

c) Formatet for dokumentationen specificeres i organisationens procedurer.

d) Dokumentationen skal lagres på en måde, der sikrer beskyttelse mod skade, forandringer og tyveri, idet oplysningerne identificeres, når det er nødvendigt, i henhold til deres sikkerhedsklassificeringsniveau. Organisationen skal sikre, at dokumentationen lagres på en måde, der sikrer integritet, ægthed og autoriseret adgang.

IS.I.OR.250 Håndbog til styring af informationssikkerhed (ISMM)

a) Organisationen skal stille en håndbog til styring af informationssikkerhed (ISMM) til rådighed for den kompetente myndighed og, hvis det er relevant, alle dertil knyttede håndbøger og procedurer, der indeholder:

1) en erklæring, der er underskrevet af den teknisk/økonomisk ansvarlige person, hvori det bekræftes, at organisationen til enhver tid vil arbejde i overensstemmelse med dette bilag og med ISMM. Hvis den teknisk/økonomisk ansvarlige person ikke er organisationens administrerende direktør, skal en sådan administrerende direktør kontrasignere erklæringen

2) stillingsbetegnelse, navn, opgaver, ansvarlighed, ansvarsområder og bemyndigelser for den eller de personer, der er defineret i punkt IS.I.OR.240, litra b) og c)

3) stillingsbetegnelse, navn, opgaver, ansvarlighed, ansvarsområder og bemyndigelse for den fælles ansvarlige person defineret i punkt IS.I.OR.240, litra d), hvis det er relevant

4) organisationens informationssikkerhedspolitik som omhandlet i punkt IS.I.OR.200, litra a), nr. 1)

5) en generel beskrivelse af antallet af personalemedlemmer og disses kategorier og af det system, der er indført for at planlægge disponibiliteten af det personale, der kræves i henhold til punkt IS.I.OR.240

6) stillingsbetegnelse, navn, opgaver, ansvarlighed, ansvarsområder og bemyndigelser for de centrale personer, der har ansvaret for gennemførelsen af punkt IS.I.OR.200, herunder den eller de personer, der har ansvaret for overvågningsfunktionen, jf. punkt IS.I.OR.200, litra a), nr. 12)

7) en organisationsplan, der viser de tilknyttede ansvarligheds- og ansvarskæder for de personer, der er omhandlet i nr. 2) og 6)

8) beskrivelsen af den interne indberetningsordning, jf. punkt IS.I.OR.215

9) procedurerne for, hvordan organisationen sikrer overensstemmelse med denne del og især:

i) den i punkt IS.I.OR.200, litra c), omhandlede dokumentation

ii) de procedurer, der definerer, hvordan organisationen skal kontrollere udliciterede aktiviteter som omhandlet i punkt IS.I.OR.200, litra a), nr. 9)

iii) ISMM-ændringsproceduren som omhandlet i litra c)

10) oplysningerne om de på nuværende tidspunkt godkendte alternative måder for overensstemmelse.

b) Den kompetente myndighed godkender og opbevarer en kopi af den første udstedelse af den pågældende ISMM. ISMM skal ændres i det nødvendige omfang for at forblive en ajourført beskrivelse af organisationens ISMS. En kopi af alle ændringer af ISMM'en skal sendes til den kompetente myndighed.

c) Ændringer af ISMM skal forvaltes efter en procedure, der fastlægges af organisationen. Ændringer, der ikke er omfattet af denne procedure, og ændringer i forbindelse med de ændringer, der er omhandlet i punkt IS.I.OR.255, litra b), skal godkendes af den kompetente myndighed.

d) Organisationen kan integrere ISMM'en i andre redegørelser eller håndbøger, den er i besiddelse af, forudsat at der er en klar krydshenvisning, der angiver, hvilke dele af redegørelsen eller håndbogen der svarer til de forskellige krav i dette bilag.

IS.I.OR.255 Ændring af systemet til styring af informationssikkerhed

a) Ændringer af ISMS kan håndteres og formidles til den kompetente myndighed efter en procedure, der er udviklet af organisationen. Denne procedure skal godkendes af den kompetente myndighed.

b) For ændringer af ISMS, der ikke er omfattet af proceduren i litra a), skal organisationen ansøge om og opnå en godkendelse udstedt af den kompetente myndighed.

Hvad angår disse ændringer:

1) ansøgningen skal indgives, før en sådan ændring foretages, for at gøre det muligt for den kompetente myndighed at fastslå den fortsatte overensstemmelse med denne forordning og om nødvendigt ændre organisationens certifikat og de betingelser for godkendelse, som er knyttet til det

2) organisationen skal stille alle oplysninger til rådighed for den kompetente myndighed, som denne ønsker for at evaluere ændringen

3) ændringen må først gennemføres efter, at den kompetente myndigheds formelle godkendelse er modtaget

4) Organisationen skal drives i overensstemmelse med de betingelser, som den kompetente myndighed foreskriver, under gennemførelsen af sådanne ændringer.

IS.I.OR.260 Vedvarende forbedring

a) Organisationen skal ved hjælp af passende resultatindikatorer vurdere effektiviteten og modenheden af ISMS. Denne vurdering skal foretages med en hyppighed, som organisationen på forhånd har fastsat, eller efter en informationssikkerhedshændelse.

b) Hvis der konstateres mangler efter den vurdering, der foretages i henhold til litra a), skal organisationen træffe de nødvendige udbedrende foranstaltninger for at sikre, at ISMS fortsat opfylder de gældende krav og bevarer informationssikkerhedsrisiciene på et acceptabelt niveau. Desuden skal organisationen revurdere de elementer i ISMS, som påvirkes af de vedtagne foranstaltninger.

BILAG III

I bilag VI (del-ARA) og bilag VII (del-ORA) til forordning (EU) nr. 1178/2011 foretages følgende ændringer:

(1) I bilag VI (del-ARA) foretages følgende ændringer:

a) I punkt ARA.GEN.125 tilføjes følgende litra c):

»c) Medlemsstatens kompetente myndighed forelægger så hurtigt som muligt agenturet alle sikkerhedsrelevante oplysninger, der er uddraget af de indberetninger om informationssikkerhed, som den har modtaget i henhold til punkt IS.I.OR.230 i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203.«

b) Følgende indsættes som punkt ARA.GEN.135A efter punkt ARA.GEN.135:

»**ARA.GEN.135A Omgående reaktion på en informationssikkerhedshændelse eller -sårbarhed med indvirkning på flyvesikkerheden**

a) Den kompetente myndighed gennemfører et system til behørig indsamling, analyse og formidling af oplysninger om informationssikkerhedshændelser og -sårbarheder med potentiel indvirkning på flyvesikkerheden, som indberettes af organisationer. Dette gøres koordineret med andre relevante myndigheder med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten for at øge koordineringen og kompatibiliteten mellem indberetningsordninger.

b) Agenturet indfører et system til på passende vis at analysere alle relevante oplysninger, der er væsentlige for sikkerheden, som er modtages i overensstemmelse med punkt ARA.GEN.125, litra c), og giver uden unødigt ophold medlemsstaterne og Kommissionen alle de oplysninger, herunder henstillinger eller afhjælpende foranstaltninger, der skal iværksættes, som de skal bruge for at reagere rettidigt på en informationssikkerhedshændelse eller -sårbarhed med potentiel indvirkning på flyvesikkerheden, som involverer materiel, dele og apparatur, ikkefastmonteret udstyr samt personer eller organisationer, der er underlagt forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil.

c) Efter modtagelse af de oplysninger, der er omhandlet i litra a) og b), skal den kompetente myndighed iværksætte passende foranstaltninger for at afhjælpe de potentielle virkninger på flyvesikkerheden af informationssikkerhedshændelsen eller -sårbarheden.

d) Foranstaltninger, der iværksættes i henhold til litra c), skal omgående meddeles alle personer eller organisationer, som skal overholde dem i henhold til forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil. Medlemsstatens kompetente myndighed underretter også agenturet om disse foranstaltninger og, når der kræves en kombineret indsats, de andre berørte medlemsstaters kompetente myndigheder.«

c) I punkt ARA.GEN.200 tilføjes følgende litra e):

»e) Det styringssystem, der oprettes og opretholdes af den kompetente myndighed, skal ud over kravene i litra a) være i overensstemmelse med bilag I (del-IS-AR) til gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

d) I ARA.GEN.205 foretages følgende ændringer:

i) Overskriften affattes således:

»**ARA.GEN.205 Tildeling af opgaver**«

ii) Følgende litra c) tilføjes:

»c) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt ORA.GEN.200A kan den kompetente myndighed tildele opgaver til kvalificerede enheder i overensstemmelse med litra a) eller til enhver relevant myndighed med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten. Ved tildelingen af opgaver sikrer den kompetente myndighed, at:

1) alle aspekter vedrørende flyvesikkerhed koordineres og tages i betragtning af den kvalificerede enhed eller den relevante myndighed

2) resultaterne af de certificerings- og tilsynsaktiviteter, der udføres af den kvalificerede enhed eller den relevante myndighed, integreres i organisationens samlede certificerings- og tilsynsdokumenter

3) dens eget system til styring af sikkerhed, der er oprettet i overensstemmelse med punkt ARA.GEN.200, litra e), omfatter alle certificeringsopgaver og løbende tilsynsopgaver, der udføres på dens vegne.«

e) I punkt ARA.GEN.300 tilføjes følgende litra g):

»g) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt ORA.GEN.200A skal den kompetente myndighed ud over at overholde litra a)-f) gennemgå enhver tilladelse, der er givet i henhold til punkt IS.I.OR.200, litra e), i nærværende forordning eller punkt IS.D.OR.200, litra e), i delegeret forordning (EU) 2022/1645 efter den gældende cyklus for evaluering af tilsynet, og når der gennemføres ændringer i organisationens arbejdsområde.«

f) Følgende indsættes som punkt ARA.GEN.330A efter punkt ARA.GEN.330:

»**ARA.GEN.330A Ændring af systemet til styring af informationssikkerhed**

a) Med hensyn til de ændringer, der styres og meddeles den kompetente myndighed i overensstemmelse med proceduren i punkt IS.I.OR.255, litra a), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203, medtager den kompetente myndighed gennemgangen af sådanne ændringer i sit løbende tilsyn i overensstemmelse med principperne i punkt ARA.GEN.300. Hvis der konstateres manglende overholdelse af kravene, skal den kompetente myndighed underrette organisationen herom, anmode om yderligere ændringer og handle i overensstemmelse med punkt ARA.GEN.350.

b) Med hensyn til andre ændringer, der kræver en ansøgning om godkendelse i overensstemmelse med punkt IS.I.OR.255, litra b), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203:

1) når den kompetente myndighed modtager ansøgningen om ændringen, kontrollerer den, at organisationen opfylder de gældende krav, før godkendelsen udstedes

2) den kompetente myndighed fastsætter de betingelser, under hvilke organisationen kan operere under gennemførelsen af ændringen

3) hvis den kompetente myndighed finder det godtgjort, at organisationen opfylder de gældende krav, godkender myndigheden ændringen.«

(2) I bilag VII (del-ORA) foretages følgende ændringer:

Følgende indsættes som punkt ORA.GEN.200A efter punkt ORA.GEN.200:

»**ORA.GEN.200A System til styring af informationssikkerhed**

Organisationen skal ud over det styringssystem, der kræves i punkt ORA.GEN.200, oprette, gennemføre og opretholde et system til styring af informationssikkerhed i overensstemmelse med gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

BILAG IV

I bilag I (del 21) til forordning (EU) nr. 748/2012 foretages følgende ændringer:

(1) I indholdsfortegnelsen foretages følgende ændringer:

(a) Følgende overskrift indsættes efter overskriften 21.B.20:

»21.B.20A Omgående reaktion på en informationssikkerhedshændelse eller sårbarhed med indvirkning på flyvesikkerheden«

(b) Overskriften til punkt 21.B.30 affattes således:

»21.B.30 Tildeling af opgaver«

(c) Følgende overskrift indsættes efter overskriften 21.B.240:

»21.B.240A Ændring af systemet til styring af informationssikkerhed«

(d) Følgende overskrift indsættes efter overskriften 21.B.435:

»21.B.435A Ændring af systemet til styring af informationssikkerhed«

(2) I punkt 21.B.15 tilføjes følgende litra c):

»c) Medlemsstatens kompetente myndighed forelægger så hurtigt som muligt agenturet alle sikkerhedsrelevante oplysninger, der er uddraget af de indberetninger om informationssikkerhed, som den har modtaget i henhold til punkt IS.D.OR.230 i bilaget (del-IS.D.OR) til delegeret forordning (EU) 2022/1645.«

(3) Følgende indsættes som punkt 21.B.20A efter punkt 21.B.20:

»21.B.20A Omgående reaktion på en informationssikkerhedshændelse eller sårbarhed med indvirkning på flyvesikkerheden

a) Den kompetente myndighed gennemfører et system til behørig indsamling, analyse og formidling af oplysninger om informationssikkerhedshændelser og sårbarheder med potentiel indvirkning på flyvesikkerheden, som indberettes af organisationer. Dette gøres koordineret med andre relevante myndigheder med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten for at øge koordineringen og kompatibiliteten mellem indberetningsordninger.

b) Agenturet indfører et system til på passende vis at analysere alle relevante oplysninger, der er væsentlige for sikkerheden, som modtages i overensstemmelse med punkt 21.B.15, litra c), og giver uden unødigt ophold medlemsstaterne og Kommissionen alle de oplysninger, herunder henstillinger eller afhjælpende foranstaltninger, der skal iværksættes, som de skal bruge for at reagere rettidigt på en informationssikkerhedshændelse eller -sårbarhed med potentiel indvirkning på flyvesikkerheden, som involverer materiel, dele og apparatur, ikkefastmonteret udstyr samt personer eller organisationer, der er underlagt forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil.

c) Efter modtagelse af de oplysninger, der er omhandlet i litra a) og b), skal den kompetente myndighed iværksætte passende foranstaltninger for at afhjælpe de potentielle virkninger på flyvesikkerheden af informationssikkerhedshændelsen eller sårbarheden.

d) Foranstaltninger, der iværksættes i henhold til litra c), skal omgående meddeles alle personer eller organisationer, som skal overholde dem i henhold til forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil. Medlemsstatens kompetente myndighed underretter også agenturet om disse foranstaltninger og, når der kræves en kombineret indsats, de andre berørte medlemsstaters kompetente myndigheder.«

(4) I punkt 21.B.25 tilføjes følgende litra e):

»e) Det styringssystem, der oprettes og opretholdes af den kompetente myndighed, skal ud over kravene i litra a) være i overensstemmelse med bilag I (del-IS-AR) til gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

(5) I 21.B.30 foretages følgende ændringer:

(a) Overskriften affattes således:

»21.B.30 Tildeling af opgaver«

(b) Følgende litra c) tilføjes:

»c) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt 21.A.139A og 21.A.239A kan den kompetente myndighed tildele opgaver til kvalificerede enheder i overensstemmelse med litra a) eller til enhver relevant myndighed med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten. Ved tildelingen af opgaver sikrer den kompetente myndighed, at:

1) alle aspekter vedrørende flyvesikkerhed koordineres og tages i betragtning af den kvalificerede enhed eller den relevante myndighed

2) resultaterne af de certificerings- og tilsynsaktiviteter, der udføres af den kvalificerede enhed eller den relevante myndighed, integreres i organisationens samlede certificerings- og tilsynsdokumenter

3) dens eget system til styring af sikkerhed, der er oprettet i overensstemmelse med punkt 21.B.25, litra e), omfatter alle certificeringsopgaver og løbende tilsynsopgaver, der udføres på dens vegne.«

(6) I punkt 21.B.221 tilføjes følgende litra g):

»g) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt 21.A.139A skal den kompetente myndighed ud over at overholde litra a)-f) gennemgå enhver godkendelse, der er givet i henhold til punkt IS.I.OR.200, litra e), i nærværende forordning eller punkt IS.D.OR.200, litra e), i delegeret forordning (EU) 2022/1645 efter den gældende cyklus for evaluering af tilsynet, og når der gennemføres ændringer i organisationens arbejdsområde.«

(7) Følgende indsættes som punkt 21.B.240A efter punkt 21.B.240:

»**21.B.240A Ændring af systemet til styring af informationssikkerhed**

a) Med hensyn til de ændringer, der styres og meddeles den kompetente myndighed i overensstemmelse med proceduren i punkt IS.D.OR.255, litra a), i bilaget (del-IS.D.OR) til delegeret forordning (EU) 2022/1645, medtager den kompetente myndighed gennemgangen af sådanne ændringer i sit løbende tilsyn i overensstemmelse med principperne i punkt 21.B.221. Hvis der konstateres manglende overholdelse af kravene, skal den kompetente myndighed underrette organisationen herom, anmode om yderligere ændringer og handle i overensstemmelse med punkt 21.B.225.

b) Med hensyn til andre ændringer, der kræver en ansøgning om godkendelse i overensstemmelse med punkt IS.D.OR.255, litra b), i bilaget (del-IS.D.OR) til delegeret forordning (EU) 2022/1645:

1) når den kompetente myndighed modtager ansøgningen om ændringen, kontrollerer den, at organisationen opfylder de gældende krav, før godkendelsen udstedes

2) den kompetente myndighed fastsætter de betingelser, under hvilke organisationen kan operere under gennemførelsen af ændringen

3) hvis den kompetente myndighed finder det godtgjort, at organisationen opfylder de gældende krav, godkender myndigheden ændringen.«

(8) I punkt 21.B.431 tilføjes følgende litra d):

»d) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt 21.A.239A skal den kompetente myndighed ud over at overholde litra a)-c) overholde følgende principper:

1) den kompetente myndighed skal gennemgå grænsefladerne og de dermed forbundne risici, der angives i overensstemmelse med punkt IS.D.OR.205, litra b), i bilaget (del-IS.D.OR) til delegeret forordning (EU) 2022/1645 af hver organisation, der er underlagt dens tilsyn

2) hvis der konstateres uoverensstemmelser i de gensidige grænseflader og de dermed forbundne risici, der angives af forskellige organisationer, skal den kompetente myndighed gennemgå dem med de berørte organisationer og om nødvendigt tage passende resultater op med henblik på at sikre gennemførelsen af afhjælpende foranstaltninger

3) hvis den dokumentation, der gennemgås i henhold til punkt 2), viser, at der er betydelige risici forbundet med grænsefladerne med de organisationer, der er underlagt tilsyn af en anden kompetent myndighed i samme medlemsstat, skal disse oplysninger videregives til den tilsvarende kompetent myndighed.«

(9) Følgende indsættes som punkt 21.B.435A efter punkt 21.B.435:

»**21.B.435A Ændring af systemet til styring af informationssikkerhed**

a) Med hensyn til de ændringer, der styres og meddeles den kompetente myndighed i overensstemmelse med proceduren i punkt IS.D.OR.255, litra a), i bilaget (del-IS.D.OR) til delegeret forordning (EU) 2022/1645, medtager den kompetente myndighed gennemgangen af sådanne ændringer i sit løbende tilsyn i overensstemmelse med principperne i punkt 21.B.431. Hvis der konstateres manglende overholdelse af kravene, skal den kompetente myndighed underrette organisationen herom, anmode om yderligere ændringer og handle i overensstemmelse med punkt 21.B.433.

b) Med hensyn til andre ændringer, der kræver en ansøgning om godkendelse i overensstemmelse med punkt IS.D.OR.255, litra b), i bilaget (del-IS.D.OR) til delegeret forordning (EU) 2022/1645:

1) når den kompetente myndighed modtager ansøgningen om ændringen, kontrollerer den, at organisationen opfylder de gældende krav, før godkendelsen udstedes

2) den kompetente myndighed fastsætter de betingelser, under hvilke organisationen kan operere under gennemførelsen af ændringen

3) hvis den kompetente myndighed finder det godtgjort, at organisationen opfylder de gældende krav, godkender myndigheden ændringen.«

BILAG V

I bilag II (del-ARO) og bilag III (del-ORO) til forordning (EU) nr. 965/2012 foretages følgende ændringer:

(1) I bilag II (del-ARO) foretages følgende ændringer:

a) I punkt ARO.GEN.125 tilføjes følgende litra c):

»c) Medlemsstatens kompetente myndighed forelægger så hurtigt som muligt agenturet alle sikkerhedsrelevante oplysninger, der er uddraget af de indberetninger om informationssikkerhed, som den har modtaget i henhold til punkt IS.I.OR.230 i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203.«

b) Følgende indsættes som punkt ARO.GEN.135A efter punkt ARO.GEN.135:

»**ARO.GEN.135A Omgående reaktion på en informationssikkerhedshændelse eller -sårbarhed med indvirkning på flyvesikkerheden**

a) Den kompetente myndighed gennemfører et system til behørig indsamling, analyse og formidling af oplysninger om informationssikkerhedshændelser og -sårbarheder med potentiel indvirkning på flyvesikkerheden, som indberettes af organisationer. Dette gøres koordineret med andre relevante myndigheder med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten for at øge koordineringen og kompatibiliteten mellem indberetningsordninger.

b) Agenturet indfører et system til på passende vis at analysere alle relevante oplysninger, der er væsentlige for sikkerheden, som er modtages i overensstemmelse med punkt ARO.GEN.125, litra c), og giver uden unødigt ophold medlemsstaterne og Kommissionen alle de oplysninger, herunder henstillinger eller afhjælpende foranstaltninger, der skal iværksættes, som de skal bruge for at reagere rettidigt på en informationssikkerhedshændelse eller -sårbarhed med potentiel indvirkning på flyvesikkerheden, som involverer materiel, dele og apparatur, ikkefastmonteret udstyr samt personer eller organisationer, der er underlagt forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil.

c) Efter modtagelse af de oplysninger, der er omhandlet i litra a) og b), skal den kompetente myndighed iværksætte passende foranstaltninger for at afhjælpe de potentielle virkninger på flyvesikkerheden af informationssikkerhedshændelsen eller -sårbarheden.

d) Foranstaltninger, der iværksættes i henhold til litra c), skal omgående meddeles alle personer eller organisationer, som skal overholde dem i henhold til forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil. Medlemsstatens kompetente myndighed underretter også agenturet om disse foranstaltninger og, når der kræves en kombineret indsats, de andre berørte medlemsstaters kompetente myndigheder.«

c) I punkt ARO.GEN.200 tilføjes følgende litra e):

»e) Det styringssystem, der oprettes og opretholdes af den kompetente myndighed, skal ud over kravene i litra a) være i overensstemmelse med bilag I (del-IS-AR) til gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

d) I ARO.GEN.205 foretages følgende ændringer:

i) Overskriften affattes således:

»**ARO.GEN.205 Tildeling af opgaver**«

ii) Følgende litra c) tilføjes:

»c) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt ORO.GEN.200A kan den kompetente myndighed tildele opgaver til kvalificerede enheder i overensstemmelse med litra a) eller til enhver relevant myndighed med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten. Ved tildelingen af opgaver sikrer den kompetente myndighed, at:

1) alle aspekter vedrørende flyvesikkerhed koordineres og tages i betragtning af den kvalificerede enhed eller den relevante myndighed

2) resultaterne af de certificerings- og tilsynsaktiviteter, der udføres af den kvalificerede enhed eller den relevante myndighed, integreres i organisationens samlede certificerings- og tilsynsdokumenter

3) dens eget system til styring af sikkerhed, der er oprettet i overensstemmelse med punkt ARO.GEN.200, litra e), omfatter alle certificeringsopgaver og løbende tilsynsopgaver, der udføres på dens vegne.«

e) I punkt ARO.GEN.300 tilføjes følgende litra g):

»g) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt ORO.GEN.200A skal den kompetente myndighed ud over at overholde litra a)-f) gennemgå enhver tilladelse, der er givet i henhold til punkt IS.I.OR.200, litra e), i nærværende forordning eller punkt IS.D.OR.200, litra e), i delegeret forordning (EU) 2022/1645 efter den gældende cyklus for evaluering af tilsynet, og når der gennemføres ændringer i organisationens arbejdsområde.«

f) Følgende indsættes som punkt ARO.GEN.330A efter punkt ARO.GEN.330:

»**ARO.GEN.330A Ændring af systemet til styring af informationssikkerhed**

a) Med hensyn til de ændringer, der styres og meddeles den kompetente myndighed i overensstemmelse med proceduren i punkt IS.I.OR.255, litra a), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203, medtager den kompetente myndighed gennemgangen af sådanne ændringer i sit løbende tilsyn i overensstemmelse med principperne i punkt ARO.GEN.300. Hvis der konstateres manglende overholdelse af kravene, skal den kompetente myndighed underrette organisationen herom, anmode om yderligere ændringer og handle i overensstemmelse med punkt ARO.GEN.350.

b) Med hensyn til andre ændringer, der kræver en ansøgning om godkendelse i overensstemmelse med punkt IS.I.OR.255, litra b), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203:

1) når den kompetente myndighed modtager ansøgningen om ændringen, kontrollerer den, at organisationen opfylder de gældende krav, før godkendelsen udstedes

2) den kompetente myndighed fastsætter de betingelser, under hvilke organisationen kan operere under gennemførelsen af ændringen

3) hvis den kompetente myndighed finder det godtgjort, at organisationen opfylder de gældende krav, godkender myndigheden ændringen.«

(2) I bilag III (del-ORO) foretages følgende ændringer:

Følgende indsættes som punkt ORO.GEN.200A efter punkt ORO.GEN.200:

»**ORO.GEN.200A System til styring af informationssikkerhed**

Operatøren skal ud over det styringssystem, der kræves i punkt ORO.GEN.200, oprette, gennemføre og opretholde et system til styring af informationssikkerhed i overensstemmelse med gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

BILAG VI

I bilag II (del-ADR.AR) til forordning (EU) nr. 139/2014 foretages følgende ændringer:

(1) I punkt ADR.AR.A.025 tilføjes følgende litra c):

»c) Medlemsstatens kompetente myndighed forelægger så hurtigt som muligt agenturet alle sikkerhedsrelevante oplysninger, der er uddraget af de indberetninger om informationssikkerhed, som den har modtaget i henhold til punkt IS.D.OR.230 i bilaget (del-IS.D.OR) til delegeret forordning (EU) 2022/1645.«

(2) Følgende indsættes som punkt ADR.AR.A.030A efter punkt ADR.AR.A.030:

»**ADR.AR.A.030A Omgående reaktion på en informationssikkerhedshændelse eller -sårbarhed med indvirkning på flyvesikkerheden**

a) Den kompetente myndighed gennemfører et system til behørig indsamling, analyse og formidling af oplysninger om informationssikkerhedshændelser og -sårbarheder med potentiel indvirkning på flyvesikkerheden, som indberettes af organisationer. Dette gøres koordineret med andre relevante myndigheder med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten for at øge koordineringen og kompatibiliteten mellem indberetningsordninger.

b) Agenturet indfører et system til på passende vis at analysere alle relevante oplysninger, der er væsentlige for sikkerheden, som er modtages i overensstemmelse med punkt ADR.AR.A.025, litra c), og giver uden unødigt ophold medlemsstaterne og Kommissionen alle de oplysninger, herunder henstillinger eller afhjælpende foranstaltninger, der skal iværksættes, som de skal bruge for at reagere rettidigt på en informationssikkerhedshændelse eller -sårbarhed med potentiel indvirkning på flyvesikkerheden, som involverer materiel, dele og apparatur, ikkefastmonteret udstyr samt personer eller organisationer, der er underlagt forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil.

c) Efter modtagelse af de oplysninger, der er omhandlet i litra a) og b), skal den kompetente myndighed iværksætte passende foranstaltninger for at afhjælpe de potentielle virkninger på flyvesikkerheden af informationssikkerhedshændelsen eller -sårbarheden.

d) Foranstaltninger, der iværksættes i henhold til litra c), skal omgående meddeles alle personer eller organisationer, som skal overholde dem i henhold til forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil. Medlemsstatens kompetente myndighed underretter også agenturet om disse foranstaltninger og, når der kræves en kombineret indsats, de andre berørte medlemsstaters kompetente myndigheder.«

(3) I punkt ADR.AR.B.005 tilføjes følgende litra d):

»d) Det styringssystem, der oprettes og opretholdes af den kompetente myndighed, skal ud over kravene i litra a) være i overensstemmelse med bilag I (del-IS-AR) til gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

(4) I ADR.AR.B.010 foretages følgende ændringer:

i) Overskriften affattes således:

»**ADR.AR.B.010 Tildeling af opgaver**«

ii) Følgende litra c) tilføjes:

»c) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt ADR.OR.D.005A kan den kompetente myndighed tildele opgaver til kvalificerede enheder i overensstemmelse med litra a) eller til enhver relevant myndighed med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten. Ved tildelingen af opgaver sikrer den kompetente myndighed, at:

1) alle aspekter vedrørende flyvesikkerhed koordineres og tages i betragtning af den kvalificerede enhed eller den relevante myndighed

2) resultaterne af de certificerings- og tilsynsaktiviteter, der udføres af den kvalificerede enhed eller den relevante myndighed, integreres i organisationens samlede certificerings- og tilsynsdokumenter

3) dens eget system til styring af sikkerhed, der er oprettet i overensstemmelse med punkt ADR.AR.B.005, litra e), omfatter alle certificeringsopgaver og løbende tilsynsopgaver, der udføres på dens vegne.«

(5) I punkt ADR.AR.C.005 indsættes følgende litra f):

»f) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt ADR.OR.D.005A skal den kompetente myndighed ud over at overholde litra a)-e) gennemgå enhver tilladelse, der er givet i henhold til punkt IS.I.OR.200, litra e), i nærværende forordning eller punkt IS.D.OR.200, litra e), i delegeret forordning (EU) 2022/1645 efter den gældende cyklus for evaluering af tilsynet, og når der gennemføres ændringer i organisationens arbejdsområde.«

(6) Følgende indsættes som punkt ADR.AR.C.040A efter punkt ADR.AR.C.040:

»**ADR.AR.C.040A Ændring af systemet til styring af informationssikkerhed**

a) Med hensyn til de ændringer, der styres og meddeles den kompetente myndighed i overensstemmelse med proceduren i punkt IS.D.OR.255, litra a), i bilaget (del-IS.D.OR) til delegeret forordning (EU) 2022/1645, medtager den kompetente myndighed gennemgangen af sådanne ændringer i sit løbende tilsyn i overensstemmelse med principperne i punkt ADR.AR.C.005. Hvis der konstateres manglende overholdelse af kravene, skal den kompetente myndighed underrette organisationen herom, anmode om yderligere ændringer og handle i overensstemmelse med punkt ADR.AR.C.055.

b) Med hensyn til andre ændringer, der kræver en ansøgning om godkendelse i overensstemmelse med punkt IS.D.OR.255, litra b), i bilaget (del-IS.D.OR) til delegeret forordning (EU) 2022/1645:

1) når den kompetente myndighed modtager ansøgningen om ændringen, kontrollerer den, at organisationen opfylder de gældende krav, før godkendelsen udstedes

2) den kompetente myndighed fastsætter de betingelser, under hvilke organisationen kan operere under gennemførelsen af ændringen

3) hvis den kompetente myndighed finder det godtgjort, at organisationen opfylder de gældende krav, godkender myndigheden ændringen.«

BILAG VII

I bilag II (del-145), bilag III (del-66) og bilag Vc (del-CAMO) til forordning (EU) nr. 1321/2014 foretages følgende ændringer:

(1) I bilag II (del-145) foretages følgende ændringer:

(a) I indholdsfortegnelsen foretages følgende ændringer:

i) Følgende overskrift indsættes efter overskriften 145.A.200:

»145.A.200A System til styring af informationssikkerhed«

ii) Følgende overskrift indsættes efter overskriften 145.B.135:

»145.B.135A Omgående reaktion på en informationssikkerhedshændelse eller sårbarhed med indvirkning på flyvesikkerheden«

iii) Overskriften til punkt 145.B.205 affattes således:

»145.B.205 Tildeling af opgaver«

iv) Følgende overskrift indsættes efter overskriften 145.B.330:

»145.B.330A Ændring af systemet til styring af informationssikkerhed«

(b) Følgende indsættes som punkt 145.A.200A efter punkt 145.A.200:

»145.A.200A **System til styring af informationssikkerhed**

Vedligeholdelsesorganisationen skal ud over det styringssystem, der kræves i punkt 145.A.200, oprette, gennemføre og opretholde et system til styring af informationssikkerhed i overensstemmelse med gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

(c) I punkt 145.B.125 tilføjes følgende litra c):

»c) Medlemsstatens kompetente myndighed forelægger så hurtigt som muligt agenturet alle sikkerhedsrelevante oplysninger, der er uddraget af de indberetninger om informationssikkerhed, som den har modtaget i henhold til punkt IS.I.OR.230 i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203.«

(d) Følgende indsættes som punkt 145.B.135A efter punkt 145.B.135:

»145.B.135A **Omgående reaktion på en informationssikkerhedshændelse eller sårbarhed med indvirkning på flyvesikkerheden**

a) Den kompetente myndighed gennemfører et system til behørig indsamling, analyse og formidling af oplysninger om informationssikkerhedshændelser og sårbarheder med potentiel indvirkning på flyvesikkerheden, som indberettes af organisationer. Dette gøres koordineret med andre relevante myndigheder med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten for at øge koordineringen og kompatibiliteten mellem indberetningsordninger.

b) Agenturet indfører et system til på passende vis at analysere alle relevante oplysninger, der er væsentlige for sikkerheden, som modtages i overensstemmelse med punkt 145.B.125, litra c), og giver uden unødigt ophold medlemsstaterne og Kommissionen alle de oplysninger, herunder henstillinger eller afhjælpende foranstaltninger, der skal iværksættes, som de skal bruge for at reagere rettidigt på en informationssikkerhedshændelse eller -sårbarhed med potentiel indvirkning på flyvesikkerheden, som involverer materiel, dele og apparatur, ikkefastmonteret udstyr samt personer eller organisationer, der er underlagt forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil.

c) Efter modtagelse af de oplysninger, der er omhandlet i litra a) og b), skal den kompetente myndighed iværksætte passende foranstaltninger for at afhjælpe de potentielle virkninger på flyvesikkerheden af informationssikkerhedshændelsen eller sårbarheden.

d) Foranstaltninger, der iværksættes i henhold til litra c), skal omgående meddeles alle personer eller organisationer, som skal overholde dem i henhold til forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil. Medlemsstatens kompetente myndighed underretter også agenturet om disse foranstaltninger og, når der kræves en kombineret indsats, de andre berørte medlemsstaters kompetente myndigheder.«

(e) I punkt 145.B.200 tilføjes følgende litra e):

»e) Det styringssystem, der oprettes og opretholdes af den kompetente myndighed, skal ud over kravene i litra a) være i overensstemmelse med bilag I (del-IS-AR) til gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

(f) I punkt 145.B.205 foretages følgende ændringer:

i) Overskriften affattes således:

»145.B.205 **Tildeling af opgaver**«

ii) Følgende litra c) tilføjes:

»c) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt 145.A.200A kan den kompetente myndighed tildele opgaver til kvalificerede enheder i overensstemmelse med litra a) eller til enhver relevant myndighed med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten. Ved tildelingen af opgaver sikrer den kompetente myndighed, at:

1) alle aspekter vedrørende flyvesikkerhed koordineres og tages i betragtning af den kvalificerede enhed eller den relevante myndighed

2) resultaterne af de certificerings- og tilsynsaktiviteter, der udføres af den kvalificerede enhed eller den relevante myndighed, integreres i organisationens samlede certificerings- og tilsynsdokumenter

3) dens eget system til styring af sikkerhed, der er oprettet i overensstemmelse med punkt 145.B.200, litra e), omfatter alle certificeringsopgaver og løbende tilsynsopgaver, der udføres på dens vegne.«

(g) I punkt 145.B.300 tilføjes følgende litra g):

»g) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt 145.A.200A skal den kompetente myndighed ud over at overholde litra a)-f) gennemgå enhver godkendelse, der er givet i henhold til punkt IS.I.OR.200, litra e), i nærværende forordning eller punkt IS.D.OR.200, litra e), i delegeret forordning (EU) 2022/1645 efter den gældende cyklus for evaluering af tilsynet, og når der gennemføres ændringer i organisationens arbejdsområde.«

(h) Følgende indsættes som punkt 145.B.330A efter punkt 145.B.330:

»145.B.330A **Ændring af systemet til styring af informationssikkerhed**

a) Med hensyn til de ændringer, der styres og meddeles den kompetente myndighed i overensstemmelse med proceduren i punkt IS.I.OR.255, litra a), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203, medtager den kompetente myndighed gennemgangen af sådanne ændringer i sit løbende tilsyn i overensstemmelse med principperne i punkt 145.B.300. Hvis der konstateres manglende overholdelse af kravene, skal den kompetente myndighed underrette organisationen herom, anmode om yderligere ændringer og handle i overensstemmelse med punkt 145.B.350.

b) Med hensyn til andre ændringer, der kræver en ansøgning om godkendelse i overensstemmelse med punkt IS.I.OR.255, litra b), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203:

1) når den kompetente myndighed modtager ansøgningen om ændringen, kontrollerer den, at organisationen opfylder de gældende krav, før godkendelsen udstedes

2) den kompetente myndighed fastsætter de betingelser, under hvilke organisationen kan operere under gennemførelsen af ændringen

3) hvis den kompetente myndighed finder det godtgjort, at organisationen opfylder de gældende krav, godkender myndigheden ændringen.«

(2) I bilag III (del-66) foretages følgende ændringer:

a) I indholdsfortegnelsen indsættes følgende overskrift efter overskriften 66.B.10:

»66.B.15 System til styring af informationssikkerhed«

b) Følgende indsættes som punkt 66.B.15 efter punkt 66.B.10:

»66.B.15 **System til styring af informationssikkerhed**

Den kompetente myndighed skal oprette, gennemføre og opretholde et system til styring af informationssikkerhed i overensstemmelse med bilag I (del-IS.AR) til gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

(3) I bilag Vc (del-CAMO) foretages følgende ændringer:

a) I indholdsfortegnelsen foretages følgende ændringer:

i) Følgende overskrift indsættes efter overskriften CAMO.A.200:

»CAMO.A.200A System til styring af informationssikkerhed«

ii) Følgende overskrift indsættes efter overskriften CAMO.B.135:

»CAMO.B.135A Omgående reaktion på en informationssikkerhedshændelse eller -sårbarhed med indvirkning på flyvesikkerheden«

iii) Overskriften til punkt CAMO.B.205 affattes således:

»CAMO.B.205 Tildeling af opgaver«

iv) Følgende overskrift indsættes efter overskriften CAMO.B.330:

»CAMO.B.330A Ændring af systemet til styring af informationssikkerhed«

b) Følgende indsættes som punkt CAMO.A.200A efter punkt CAMO.A.200:

»CAMO.A.200A **System til styring af informationssikkerhed**

Organisationen skal ud over det styringssystem, der kræves i punkt CAMO.A.200, oprette, gennemføre og opretholde et system til styring af informationssikkerhed i overensstemmelse med gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

c) I punkt CAMO.B.125 tilføjes følgende litra c):

»c) Medlemsstatens kompetente myndighed forelægger så hurtigt som muligt agenturet alle sikkerhedsrelevante oplysninger, der er uddraget af de indberetninger om informationssikkerhed, som den har modtaget i henhold til punkt IS.I.OR.230 i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203.«

d) Følgende indsættes som punkt CAMO.B.135A efter punkt CAMO.B.135:

»CAMO.B.135A **Omgående reaktion på en informationssikkerhedshændelse eller -sårbarhed med indvirkning på flyvesikkerheden**

a) Den kompetente myndighed gennemfører et system til behørig indsamling, analyse og formidling af oplysninger om informationssikkerhedshændelser og -sårbarheder med potentiel indvirkning på flyvesikkerheden, som indberettes af organisationer. Dette gøres koordineret med andre relevante myndigheder med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten for at øge koordineringen og kompatibiliteten mellem indberetningsordninger.

b) Agenturet indfører et system til på passende vis at analysere alle relevante oplysninger, der er væsentlige for sikkerheden, som er modtages i overensstemmelse med punkt CAMO.B.125, litra c), og giver uden unødigt ophold medlemsstaterne og Kommissionen alle de oplysninger, herunder henstillinger eller afhjælpende foranstaltninger, der skal iværksættes, som de skal bruge for at reagere rettidigt på en informationssikkerhedshændelse eller -sårbarhed med potentiel indvirkning på flyvesikkerheden, som involverer materiel, dele og apparatur, ikkefastmonteret udstyr samt personer eller organisationer, der er underlagt forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil.

c) Efter modtagelse af de oplysninger, der er omhandlet i litra a) og b), skal den kompetente myndighed iværksætte passende foranstaltninger for at afhjælpe de potentielle virkninger på flyvesikkerheden af informationssikkerhedshændelsen eller -sårbarheden.

d) Foranstaltninger, der iværksættes i henhold til litra c), skal omgående meddeles alle personer eller organisationer, som skal overholde dem i henhold til forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil. Medlemsstatens kompetente myndighed underretter også agenturet om disse foranstaltninger og, når der kræves en kombineret indsats, de andre berørte medlemsstaters kompetente myndigheder.«

e) I punkt CAMO.B.200 tilføjes følgende litra e):

»e) Det styringssystem, der oprettes og opretholdes af den kompetente myndighed, skal ud over kravene i litra a) være i overensstemmelse med bilag I (del-IS-AR) til gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

f) I CAMO.B.205 foretages følgende ændringer:

i) Overskriften affattes således:

»CAMO.B.205 **Tildeling af opgaver**«

ii) Følgende litra c) tilføjes:

»c) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt CAMO.A.200A kan den kompetente myndighed tildele opgaver til kvalificerede enheder i overensstemmelse med litra a) eller til enhver relevant myndighed med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten. Ved tildelingen af opgaver sikrer den kompetente myndighed, at:

1) alle aspekter vedrørende flyvesikkerhed koordineres og tages i betragtning af den kvalificerede enhed eller den relevante myndighed

2) resultaterne af de certificerings- og tilsynsaktiviteter, der udføres af den kvalificerede enhed eller den relevante myndighed, integreres i organisationens samlede certificerings- og tilsynsdokumenter

3) dens eget system til styring af sikkerhed, der er oprettet i overensstemmelse med punkt CAMO.B.200, litra e), omfatter alle certificeringsopgaver og løbende tilsynsopgaver, der udføres på dens vegne.«

g) I punkt CAMO.B.300 tilføjes følgende litra g):

»g) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt CAMO.A.200A skal den kompetente myndighed ud over at overholde litra a)-f) gennemgå enhver tilladelse, der er givet i henhold til punkt IS.I.OR.200, litra e), i nærværende forordning eller punkt IS.D.OR.200, litra e), i delegeret forordning (EU) 2022/1645 efter den gældende cyklus for evaluering af tilsynet, og når der gennemføres ændringer i organisationens arbejdsområde.«

h) Følgende indsættes som punkt CAMO.B.330A efter punkt CAMO.B.330:

»CAMO.B.330A **Ændring af systemet til styring af informationssikkerhed**

a) Med hensyn til de ændringer, der styres og meddeles den kompetente myndighed i overensstemmelse med proceduren i punkt IS.I.OR.255, litra a), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203, medtager den kompetente myndighed gennemgangen af sådanne ændringer i sit løbende tilsyn i overensstemmelse med principperne i punkt CAMO.B.300. Hvis der konstateres manglende overholdelse af kravene, skal den kompetente myndighed underrette organisationen herom, anmode om yderligere ændringer og handle i overensstemmelse med punkt CAMO.B.350.

b) Med hensyn til andre ændringer, der kræver en ansøgning om godkendelse i overensstemmelse med punkt IS.I.OR.255, litra b), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203:

1) når den kompetente myndighed modtager ansøgningen om ændringen, kontrollerer den, at organisationen opfylder de gældende krav, før godkendelsen udstedes

2) den kompetente myndighed fastsætter de betingelser, under hvilke organisationen kan operere under gennemførelsen af ændringen

3) hvis den kompetente myndighed finder det godtgjort, at organisationen opfylder de gældende krav, godkender myndigheden ændringen.«

BILAG VIII

I bilag II (del-ATCO.AR) og bilag III (del-ATCO.OR) til forordning (EU) 2015/340 foretages følgende ændringer:

(1) I bilag II (del-ATCO.AR) foretages følgende ændringer:

a) I punkt ATCO.AR.A.020 tilføjes følgende litra c):

»c) Medlemsstatens kompetente myndighed forelægger så hurtigt som muligt agenturet alle sikkerhedsrelevante oplysninger, der er uddraget af de indberetninger om informationssikkerhed, som den har modtaget i henhold til punkt IS.I.OR.230 i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203.«

b) Følgende indsættes som punkt ATCO.AR.A.025A efter punkt ATCO.AR.A.025:

»**ATCO.AR.A.025A Omgående reaktion på en informationssikkerhedshændelse eller -sårbarhed med indvirkning på flyvesikkerheden**

a) Den kompetente myndighed gennemfører et system til behørig indsamling, analyse og formidling af oplysninger om informationssikkerhedshændelser og -sårbarheder med potentiel indvirkning på flyvesikkerheden, som indberettes af organisationer. Dette gøres koordineret med andre relevante myndigheder med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten for at øge koordineringen og kompatibiliteten mellem indberetningsordninger.

b) Agenturet indfører et system til på passende vis at analysere alle relevante oplysninger, der er væsentlige for sikkerheden, som er modtages i overensstemmelse med punkt ATCO.AR.A.020 og giver uden unødigt ophold medlemsstaterne og Kommissionen alle de oplysninger, herunder henstillinger eller afhjælpende foranstaltninger, der skal iværksættes, som de skal bruge for at reagere rettidigt på en informationssikkerhedshændelse eller -sårbarhed med potentiel indvirkning på flyvesikkerheden, som involverer materiel, dele og apparatur, ikkefastmonteret udstyr samt personer eller organisationer, der er underlagt forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil.

c) Efter modtagelse af de oplysninger, der er omhandlet i litra a) og b), skal den kompetente myndighed iværksætte passende foranstaltninger for at afhjælpe de potentielle virkninger på flyvesikkerheden af informationssikkerhedshændelsen eller -sårbarheden.

d) Foranstaltninger, der iværksættes i henhold til litra c), skal omgående meddeles alle personer eller organisationer, som skal overholde dem i henhold til forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil. Medlemsstatens kompetente myndighed underretter også agenturet om disse foranstaltninger og, når der kræves en kombineret indsats, de andre berørte medlemsstaters kompetente myndigheder.«

c) I punkt ATCO.AR.B.001 tilføjes følgende litra e):

»e) Det styringssystem, der oprettes og opretholdes af den kompetente myndighed, skal ud over kravene i litra a) være i overensstemmelse med bilag I (del-IS-AR) til gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

d) I ATCO.AR.B.005 foretages følgende ændringer:

i) Overskriften affattes således:

»**ATCO.AR.B.005 Tildeling af opgaver**«

ii) Følgende litra c) tilføjes:

»c) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt ATCO.OR.C.001A kan den kompetente myndighed tildele opgaver til kvalificerede enheder i overensstemmelse med litra a) eller til enhver relevant myndighed med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten. Ved tildelingen af opgaver sikrer den kompetente myndighed, at:

1) alle aspekter vedrørende flyvesikkerhed koordineres og tages i betragtning af den kvalificerede enhed eller den relevante myndighed

2) resultaterne af de certificerings- og tilsynsaktiviteter, der udføres af den kvalificerede enhed eller den relevante myndighed, integreres i organisationens samlede certificerings- og tilsynsdokumenter

3) dens eget system til styring af sikkerhed, der er oprettet i overensstemmelse med punkt ATCO.AR.B.001, litra e), omfatter alle certificeringsopgaver og løbende tilsynsopgaver, der udføres på dens vegne.«

e) I punkt ATCO.AR.C.001 indsættes følgende litra f):

»f) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt ATCO.OR.C.001A skal den kompetente myndighed ud over at overholde litra a)-e) gennemgå enhver tilladelse, der er givet i henhold til punkt IS.I.OR.200, litra e), i nærværende forordning eller punkt IS.D.OR.200, litra e), i delegeret forordning (EU) 2022/1645 efter den gældende cyklus for evaluering af tilsynet, og når der gennemføres ændringer i organisationens arbejdsområde.«

f) Følgende indsættes som punkt ATCO.AR.E.010A efter punkt ATCO.AR.E.010:

»**ATCO.AR.E.010A Ændring af systemet til styring af informationssikkerhed**

a) Med hensyn til de ændringer, der styres og meddeles den kompetente myndighed i overensstemmelse med proceduren i punkt IS.I.OR.255, litra a), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203, medtager den kompetente myndighed gennemgangen af sådanne ændringer i sit løbende tilsyn i overensstemmelse med principperne i punkt ATCO.AR.C.001. Hvis der konstateres manglende overholdelse af kravene, skal den kompetente myndighed underrette organisationen herom, anmode om yderligere ændringer og handle i overensstemmelse med punkt ATCO.AR.C.010.

b) Med hensyn til andre ændringer, der kræver en ansøgning om godkendelse i overensstemmelse med punkt IS.I.OR.255, litra b), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203:

1) når den kompetente myndighed modtager ansøgningen om ændringen, kontrollerer den, at organisationen opfylder de gældende krav, før godkendelsen udstedes

2) den kompetente myndighed fastsætter de betingelser, under hvilke organisationen kan operere under gennemførelsen af ændringen

3) hvis den kompetente myndighed finder det godtgjort, at organisationen opfylder de gældende krav, godkender myndigheden ændringen.«

(2) I bilag III (del-ATCO.OR) foretages følgende ændringer:

Følgende indsættes som punkt ATCO.OR.C.001A efter punkt ATCO.OR.C.001:

»**ATCO.OR.C.001A System til styring af informationssikkerhed**

Uddannelsesorganisationen skal ud over det styringssystem, der kræves i punkt ATCO.OR.C.001, oprette, gennemføre og opretholde et system til styring af informationssikkerhed i overensstemmelse med gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

BILAG IX

I bilag II (del-ATM/ANS.AR) og bilag III (del-ATM/ANS.OR) til gennemførelsesforordning (EU) 2017/373 foretages følgende ændringer:

(1) I bilag II (del-ATM/ANS.AR) foretages følgende ændringer:

a) I punkt ATM/ANS.AR.A.020 tilføjes følgende litra c):

»c) Medlemsstatens kompetente myndighed forelægger så hurtigt som muligt agenturet alle sikkerhedsrelevante oplysninger, der er uddraget af de indberetninger om informationssikkerhed, som den har modtaget i henhold til punkt IS.I.OR.230 i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203.«

b) Følgende indsættes som punkt ATM/ANS.AR.A.025A efter punkt ATM/ANS.AR.A.025:

»**ATM/ANS.AR.A.025A Omgående reaktion på en informationssikkerhedshændelse eller -sårbarhed med indvirkning på flyvesikkerheden**

a) Den kompetente myndighed gennemfører et system til behørig indsamling, analyse og formidling af oplysninger om informationssikkerhedshændelser og -sårbarheder med potentiel indvirkning på flyvesikkerheden, som indberettes af organisationer. Dette gøres koordineret med andre relevante myndigheder med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten for at øge koordineringen og kompatibiliteten mellem indberetningsordninger.

b) Agenturet indfører et system til på passende vis at analysere alle relevante oplysninger, der er væsentlige for sikkerheden, som er modtages i overensstemmelse med punkt ATM/ANS.AR.A.020, litra c), og giver uden unødigt ophold medlemsstaterne og Kommissionen alle de oplysninger, herunder henstillinger eller afhjælpende foranstaltninger, der skal iværksættes, som de skal bruge for at reagere rettidigt på en informationssikkerhedshændelse eller -sårbarhed med potentiel indvirkning på flyvesikkerheden, som involverer materiel, dele og apparatur, ikkefastmonteret udstyr samt personer eller organisationer, der er underlagt forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil.

c) Efter modtagelse af de oplysninger, der er omhandlet i litra a) og b), skal den kompetente myndighed iværksætte passende foranstaltninger for at afhjælpe de potentielle virkninger på flyvesikkerheden af informationssikkerhedshændelsen eller -sårbarheden.

d) Foranstaltninger, der iværksættes i henhold til litra c), skal omgående meddeles alle personer eller organisationer, som skal overholde dem i henhold til forordning (EU) 2018/1139 samt delegerede retsakter og gennemførelsesretsakter hertil. Medlemsstatens kompetente myndighed underretter også agenturet om disse foranstaltninger og, når der kræves en kombineret indsats, de andre berørte medlemsstaters kompetente myndigheder.«

c) I punkt ATM/ANS.AR.B.001 tilføjes følgende litra e):

»e) Det styringssystem, der oprettes og opretholdes af den kompetente myndighed, skal ud over kravene i litra a) være i overensstemmelse med bilag I (del-IS.AR) til gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

d) I punkt ATM/ANS.AR.B.005 foretages følgende ændringer:

i) Overskriften affattes således:

»**ATM/ANS.AR.B.005 Tildeling af opgaver**«

ii) Følgende litra c) tilføjes:

»c) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt ATM/ANS.OR.B.005A kan den kompetente myndighed tildele opgaver til kvalificerede enheder i overensstemmelse med litra a) eller til enhver relevant myndighed med ansvar for informationssikkerhed eller cybersikkerhed i medlemsstaten. Ved tildelingen af opgaver sikrer den kompetente myndighed, at:

1) alle aspekter vedrørende flyvesikkerhed koordineres og tages i betragtning af den kvalificerede enhed eller den relevante myndighed

2) resultaterne af de certificerings- og tilsynsaktiviteter, der udføres af den kvalificerede enhed eller den relevante myndighed, integreres i organisationens samlede certificerings- og tilsynsdokumenter

3) dens eget system til styring af sikkerhed, der er oprettet i overensstemmelse med punkt ATM/ANS.AR.B.001, litra e), omfatter alle certificeringsopgaver og løbende tilsynsopgaver, der udføres på dens vegne.«

e) I punkt ATM/ANS.AR.C.010 tilføjes følgende litra d):

»d) Med hensyn til certificering af og tilsyn med organisationens overholdelse af punkt ATM/ANS.OR.B.005A skal den kompetente myndighed ud over at overholde litra a)-c) gennemgå enhver tilladelse, der er givet i henhold til punkt IS.I.OR.200, litra e), i nærværende forordning eller punkt IS.D.OR.200, litra e), i delegeret forordning (EU) 2022/1645 efter den gældende cyklus for evaluering af tilsynet, og når der gennemføres ændringer i organisationens arbejdsområde.«

f) Følgende indsættes som punkt ATM/ANS.AR.C.025A efter punkt ATM/ANS.AR.C.025:

»**ATM/ANS.AR.C.025A Ændring af systemet til styring af informationssikkerhed**

a) Med hensyn til de ændringer, der styres og meddeles den kompetente myndighed i overensstemmelse med proceduren i punkt IS.I.OR.255, litra a), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203, medtager den kompetente myndighed gennemgangen af sådanne ændringer i sit løbende tilsyn i overensstemmelse med principperne i punkt ATM/ANS.AR.C.010. Hvis der konstateres manglende overholdelse af kravene, skal den kompetente myndighed underrette organisationen herom, anmode om yderligere ændringer og handle i overensstemmelse med punkt ATM/ANS.AR.C.050.

b) Med hensyn til andre ændringer, der kræver en ansøgning om godkendelse i overensstemmelse med punkt IS.I.OR.255, litra b), i bilag II (del-IS.I.OR) til gennemførelsesforordning (EU) 2023/203:

1) når den kompetente myndighed modtager ansøgningen om ændringen, kontrollerer den, at organisationen opfylder de gældende krav, før godkendelsen udstedes

2) den kompetente myndighed fastsætter de betingelser, under hvilke organisationen kan operere under gennemførelsen af ændringen

3) hvis den kompetente myndighed finder det godtgjort, at organisationen opfylder de gældende krav, godkender myndigheden ændringen.«

(2) I bilag III (del-ATM/ANS.OR) foretages følgende ændringer:

a) Følgende indsættes som punkt ATM/ANS.OR.B.005A efter punkt ATM/ANS.OR.B.005:

»**ATM/ANS.OR.B.005A System til styring af informationssikkerhed**

Tjenesteudøveren skal ud over det styringssystem, der kræves i punkt ATM/ANS.OR.B.005, oprette, gennemføre og opretholde et system til styring af informationssikkerhed i overensstemmelse med gennemførelsesforordning (EU) 2023/203 for at sikre en korrekt styring af informationssikkerhedsrisici, som kan have indvirkning på flyvesikkerheden.«

b) Punkt ATM/ANS.OR.D.010 affattes således:

»**ATM/ANS.OR.D.010 Luftfartssikkerhedsstyring (security)**

a) Udøvere af luftfartstjenester og lufttrafikregulering og netforvalteren skal som en integrerende del af deres styringssystem, jf. punkt ATM/ANS.OR.B.005, oprette et luftfartssikkerhedsstyringssystem for at tilgodese:

1) deres faciliteters og personales sikkerhed med henblik på at forhindre ulovlig indgriben i udøvelsen af tjenesterne

2) sikkerheden af de operative data, som de modtager, frembringer eller på anden måde anvender, således at adgangen dertil strengt begrænses til dem, der er bemyndiget dertil.

b) Luftfartssikkerhedsstyringssystemet skal omfatte:

1) processer og procedurer for vurdering og reduktion af sikkerhedsrisici, overvågning og forbedring af sikkerheden, sikkerhedsundersøgelser og videreformidling af indhøstede erfaringer

2) midler til påvisning, overvågning og opdagelse af brud på sikkerhedsbeskyttelsen og varsling af personalet ved hjælp af passende sikkerhedsalarmer

3) midler til at holde virkningerne af brud på luftfartssikkerheden under kontrol og til at fastlægge udbedrende foranstaltninger og risikoreducerende procedurer for at forhindre gentagelse.

c) Udøvere af luftfartstjenester og lufttrafikregulering og netforvalteren skal, når der er grundlag herfor, sørge for sikkerhedsgodkendelse af deres personale samt for koordination med de relevante civile og militære myndigheder med henblik på at tilgodese deres faciliteters, personales og datas sikkerhed.

d) De aspekter, der er relateret til informationssikkerhed, skal styres i overensstemmelse med punkt ATM/ANS.OR.B.005A.«