II

(Niet-wetgevingshandelingen)

VERORDENINGEN

UITVOERINGSVERORDENING (EU) 2023/203 VAN DE COMMISSIE

van 27 oktober 2022

tot vaststelling van regels voor de toepassing van Verordening (EU) 2018/1139 van het Europees Parlement en de Raad, wat betreft de eisen voor het beheer van risico's op het gebied van informatiebeveiliging met mogelijke gevolgen voor de veiligheid van de luchtvaart voor organisaties waarop de Verordeningen (EU) nr. 1321/2014, (EU) nr. 965/2012, (EU) nr. 1178/2011 en (EU) 2015/340 van de Commissie en de Uitvoeringsverordeningen (EU) 2017/373 en (EU) 2021/664 van de Commissie van toepassing zijn en voor bevoegde autoriteiten waarop de Verordeningen (EU) nr. 748/2012, (EU) nr. 1321/2014, (EU) nr. 965/2012, (EU) nr. 1178/2011, (EU) 2015/340 en (EU) nr. 139/2014 van de Commissie en de Uitvoeringsverordeningen (EU) 2017/373 en (EU) 2021/664 van de Commissie van toepassing zijn, en tot wijziging van de Verordeningen (EU) nr. 1178/2011, (EU) nr. 748/2012, (EU) nr. 965/2012, (EU) nr. 139/2014, (EU) nr. 1321/2014 en (EU) 2015/340 van de Commissie en Uitvoeringsverordeningen (EU) 2017/373 en (EU) 2021/664 van de Commissie

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2018/1139 van het Europees Parlement en de Raad van 4 juli 2018 inzake gemeenschappelijke regels op het gebied van burgerluchtvaart en tot oprichting van een Agentschap van de Europese Unie voor de veiligheid van de luchtvaart, en tot wijziging van de Verordeningen (EG) nr. 2111/2005, (EG) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 en de Richtlijnen 2014/30/EU en 2014/53/EU van het Europees Parlement en de Raad, en tot intrekking van de Verordeningen (EG) nr. 552/2004 en (EG) nr. 216/2008 van het Europees Parlement en de Raad en Verordening (EEG) nr. 3922/91 van de Raad [1], en met name artikel 17, lid 1, punt b), artikel 27, lid 1, punt a), artikel 31, lid 1, punt b), artikel 43, lid 1, punt b), artikel 53, lid 1, punt a) en artikel 62, lid 15, punt c),

Overwegende hetgeen volgt:

(1) Overeenkomstig de essentiële eisen van bijlage II, punt 3.1, b), van Verordening (EU) 2018/1139 moeten organisaties voor het beheer van de permanente luchtwaardigheid en onderhoudsorganisaties een beheersysteem opzetten en onderhouden om veiligheidsrisico's te beheren.

(2) Bovendien moeten, overeenkomstig de essentiële eisen van bijlage IV, punt 3.3, b), en punt 5, b), van Verordening (EU) 2018/1139, organisaties voor de opleiding van piloten, organisaties voor de opleiding van cabinepersoneel, luchtvaartgeneeskundige centra voor vliegend personeel en exploitanten van vluchtnabootsers een beheersysteem toepassen en onderhouden om veiligheidsrisico's te beheren.

(3) Overeenkomstig de essentiële eisen van bijlage V, punt 8.1, c), van Verordening (EU) 2018/1139 moeten luchtvaartuigexploitanten een beheersysteem opzetten en onderhouden om veiligheidsrisico's te beheren.

(4) Overeenkomstig de essentiële eisen van bijlage VIII, punt 5.1, c), en punt 5.4, b), van Verordening (EU) 2018/1139 moeten verleners van luchtverkeersbeheers- en luchtvaartnavigatiediensten, U-spacedienstverleners en aanbieders van gemeenschappelijke informatiediensten, en opleidingsorganisaties en luchtvaartgeneeskundige centra voor luchtverkeersleiders een beheersysteem invoeren en onderhouden om veiligheidsrisico's te beheren.

[1] PB L 212 van 22.8.2018, blz. 1.

(5) Die veiligheidsrisico's kunnen ontstaan om verschillende redenen, zoals ontwerp- en onderhoudsgebreken, aspecten van menselijke prestaties, milieubedreigingen en bedreigingen voor de informatiebeveiliging. De beheersystemen die worden toegepast door het Agentschap van de Europese Unie voor de veiligheid van de luchtvaart ("het Agentschap") en de in bovenstaande overwegingen bedoelde nationale bevoegde autoriteiten en organisaties moeten daarom niet alleen rekening houden met veiligheidsrisico's die voortvloeien uit toevallige gebeurtenissen, maar ook met veiligheidsrisico's die voortvloeien uit bedreigingen voor de informatiebeveiliging waarbij bestaande tekortkomingen kunnen worden uitgebuit door personen met slechte bedoelingen. Die risico's voor de informatiebeveiliging in de burgerluchtvaart nemen voortdurend toe omdat de actuele informatiesystemen steeds meer met elkaar verweven zijn en steeds vaker het doelwit worden van kwaadwillige actoren.

(6) De risico's in verband met die informatiesystemen blijven niet beperkt tot mogelijke aanvallen op de cyberruimte, maar omvatten ook bedreigingen die van invloed kunnen zijn op processen en procedures en op de prestaties van mensen.

(7) Een aanzienlijk aantal organisaties maakt reeds gebruik van internationale normen, zoals ISO 27001, om digitale informatie en gegevens te beveiligen. Het is mogelijk dat die normen niet volledig beantwoorden aan alle specifieke kenmerken van de burgerluchtvaart. Het is dan ook passend eisen in te voeren voor het beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.

(8) Het is van essentieel belang dat deze eisen betrekking hebben op alle luchtvaartdomeinen en hun interfaces aangezien de luchtvaart een sterk onderling verweven systeem is. Daarom moeten zij van toepassing zijn op alle organisaties en bevoegde autoriteiten waarop Verordeningen (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]) van de Commissie en Uitvoeringsverordening (EU) 2021/664 ([8]) van de Commissie van toepassing zijn, met inbegrip van die organisaties en bevoegde autoriteiten die reeds over een beheersysteem moeten beschikken overeenkomstig de bestaande wetgeving van de Unie inzake de veiligheid van de luchtvaart. Sommige organisaties moeten echter van het toepassingsgebied van deze verordening worden uitgesloten omdat ze lagere informatiebeveiligingsrisico's inhouden voor het luchtvaartsysteem.

(9) De in deze verordening vastgestelde eisen moeten consequent worden toegepast op alle luchtvaartdomeinen en tegelijkertijd zo weinig mogelijk gevolgen hebben voor de luchtvaartveiligheidswetgeving van de Unie die reeds van toepassing is op deze domeinen.

([2]) Verordening (EU) nr. 748/2012 van de Commissie van 3 augustus 2012 tot vaststelling van uitvoeringsvoorschriften inzake de luchtwaardigheid en milieucertificering van luchtvaartuigen en aanverwante producten, onderdelen en uitrustingsstukken, alsmede voor de certificering van ontwerp- en productieorganisaties (PB L 224 van 21.8.2012, blz. 1).

([3]) Verordening (EU) nr. 1321/2014 van de Commissie van 26 november 2014 betreffende de permanente luchtwaardigheid van luchtvaartuigen en luchtvaartproducten, -onderdelen en -uitrustingsstukken, en betreffende de goedkeuring van bij voornoemde taken betrokken organisaties en personen (PB L 362 van 17.12.2014, blz. 1).

([4]) Verordening (EU) nr. 965/2012 van de Commissie van 5 oktober 2012 tot vaststelling van technische eisen en administratieve procedures voor vluchtuitvoering, overeenkomstig Verordening (EG) nr. 216/2008 van het Europees Parlement en de Raad (PB L 296 van 25.10.2012, blz. 1).

([5]) Verordening (EU) nr. 1178/2011 van de Commissie van 3 november 2011 tot vaststelling van technische eisen en administratieve procedures met betrekking tot de bemanning van burgerluchtvaartuigen, overeenkomstig Verordening (EG) nr. 216/2008 van het Europees Parlement en de Raad (PB L 311 van 25.11.2011, blz. 1).

([6]) Verordening (EU) 2015/340 van de Commissie van 20 februari 2015 tot vaststelling van technische eisen en administratieve procedures met betrekking tot vergunningen en certificaten van luchtverkeersleiders overeenkomstig Verordening (EG) nr. 216/2008 van het Europees Parlement en de Raad, tot wijziging van Uitvoeringsverordening (EU) nr. 923/2012 van de Commissie en tot intrekking van Verordening (EU) nr. 805/2011 van de Commissie (PB L 63 van 6.3.2015, blz. 1).

([7]) Verordening (EU) nr. 139/2014 van de Commissie van 12 februari 2014 tot vaststelling van eisen en administratieve procedures met betrekking tot luchtvaartterreinen, overeenkomstig Verordening (EG) nr. 216/2008 van het Europees Parlement en de Raad (PB L 44 van 14.2.2014, blz. 1).

([8]) Uitvoeringsverordening (EU) 2021/664 van de Commissie van 22 april 2021 inzake een regelgevingskader voor U-space (PB L 139van 23.4.2021, blz. 161).

(10) De in deze verordening vastgestelde eisen mogen geen afbreuk doen aan de eisen inzake informatiebeveiliging en cyberbeveiliging die zijn vastgesteld in punt 1.7 van de bijlage bij Uitvoeringsverordening (EU) 2015/1998 van de Commissie ([9]) en in artikel 14 van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad ([10]).

(11) De beveiligingsvoorschriften van de artikelen 33 tot en met 43 van titel V "Beveiliging van het programma" van Verordening (EU) 2021/696 van het Europees Parlement en de Raad ([11]) worden beschouwd als gelijkwaardig aan de voorschriften van deze verordening, behalve wat punt IS.I.OR.230 van bijlage II bij deze verordening betreft, waaraan moet worden voldaan.

(12) Om rechtszekerheid te verschaffen, moet de interpretatie van de term "informatiebeveiliging" zoals gedefinieerd in deze verordening, die het gemeenschappelijke gebruik ervan in de mondiale burgerluchtvaart weerspiegelt, worden geacht in overeenstemming te zijn met die van de term "beveiliging van netwerk- en informatiesystemen" zoals gedefinieerd in artikel 4, lid 2, van Richtlijn (EU) 2016/1148. De definitie van informatiebeveiliging die in deze verordening wordt gebruikt, mag niet worden geïnterpreteerd als een afwijking van de definitie van beveiliging van netwerk- en informatiesystemen in Richtlijn (EU) 2016/1148.

(13) Indien onder deze verordening vallende organisaties reeds onderworpen zijn aan beveiligingseisen die voortvloeien uit in de overwegingen (10) en (11) bedoelde rechtshandelingen van de Unie die qua werking gelijkwaardig zijn aan de in deze verordening vastgestelde voorschriften, moet de naleving van die beveiligingseisen worden beschouwd als naleving van de in deze verordening vastgestelde eisen, teneinde verdubbeling van wettelijke voorschriften te vermijden.

(14) Onder deze verordening vallende organisaties die reeds onderworpen zijn aan beveiligingseisen die voortvloeien uit Uitvoeringsverordening (EU) 2015/1998 of Verordening (EU) 2021/696, of beide, moeten ook voldoen aan de eisen van bijlage II (Deel IS.I.OR.230 "Regeling voor de externe rapportering van informatiebeveiligingsincidenten") van de onderhavige verordening aangezien geen van beide verordeningen bepalingen bevat die betrekking hebben op de externe rapportering van informatiebeveiligingsincidenten.

(15) Volledigheidshalve moeten de Verordeningen (EU) nr. 1178/2011, (EU) nr. 748/2012, (EU) nr. 965/2012, (EU) nr. 139/2014, (EU) nr. 1321/2014, (EU) 2015/340 en Uitvoeringsverordeningen (EU) 2017/373 ([12]) en (EU) 2021/664 worden gewijzigd om er de in de onderhavige verordening voorgeschreven vereisten voor het beheer van informatiebeveiliging in op te nemen, samen met de daarin beschreven beheersystemen, en om de verplichtingen van de bevoegde autoriteiten vast te stellen met betrekking tot het toezicht op organisaties die de bovengenoemde vereisten inzake informatiebeveiligingsbeheer uitvoeren.

(16) Om organisaties voldoende tijd te geven om de naleving van de nieuwe regels en procedures te waarborgen, moet deze verordening 3 jaar na de inwerkingtreding ervan van toepassing worden, behalve voor de verlener van luchtvaartnavigatiediensten van de European Geostationary Navigation Overlay Service (EGNOS), zoals gedefinieerd in Uitvoeringsverordening (EU) 2017/373. Wegens de lopende veiligheidsaccreditatie van het systeem en de diensten van EGNOS, overeenkomstig Verordening (EU) 2021/696, moet de onderhavige verordening met ingang van 1 januari 2026 van toepassing worden op verlener van EGNOS-luchtvaartnavigatiediensten.

(17) De in deze verordening vastgestelde eisen zijn gebaseerd op Advies nr. 03/2021 ([13]), dat door het Agentschap is uitgebracht overeenkomstig artikel 75, lid 2, punten b) en c), en artikel 76, lid 1, van Verordening (EU) 2018/1139.

([9]) Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart (PB L 299 van 14.11.2015, blz. 1).

([10]) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

([11]) Verordening (EU) 2021/696 van het Europees Parlement en de Raad van 28 april 2021 tot vaststelling van het ruimtevaartprogramma van de Unie, tot oprichting van het Agentschap van de Europese Unie voor het ruimtevaartprogramma en tot intrekking van de Verordeningen (EU) nr. 912/2010, (EU) nr. 1285/2013 en (EU) nr. 377/2014 en Besluit nr. 541/2014/EU (PB L 170 van 12.5.2021, blz. 69).

([12]) Uitvoeringsverordening (EU) 2017/373 van de Commissie van 1 maart 2017 tot vaststelling van de gemeenschappelijke eisen voor verleners van luchtverkeersbeheers-/luchtvaartnavigatiediensten en andere netwerkfuncties voor luchtverkeersbeheer en het toezicht daarop, en tot intrekking van Verordening (EG) nr. 482/2008, Uitvoeringsverordeningen (EU) nr. 1034/2011, (EU) nr. 1035/2011 en (EU) 2016/1377 en tot wijziging van Verordening (EU) nr. 677/2011 (PB L 62 van 8.3.2017, blz. 1).

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

(18) De in deze verordening vastgestelde eisen zijn in overeenstemming met het advies van het bij artikel 127 van Verordening (EU) 2018/1139 ingestelde Comité voor de toepassing van gemeenschappelijke veiligheidsvoorschriften op het gebied van de burgerluchtvaart,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Onderwerp

In deze verordening worden de eisen vastgesteld waaraan de organisaties en bevoegde autoriteiten moeten voldoen met het oog op:

a) de identificatie en het beheer van risico's op het gebied van informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart en van invloed kunnen zijn op informatie- en communicatietechnologiesystemen en gegevens die voor burgerluchtvaartdoeleinden worden gebruikt;

b) de opsporing van informatiebeveiligingsvoorvallen en de identificatie van de voorvallen die worden beschouwd als informatiebeveiligingsincidenten die gevolgen kunnen hebben voor de veiligheid van de luchtvaart;

c) de reactie op en het herstel van dergelijke incidenten op het gebied van informatiebeveiliging.

Artikel 2

Toepassingsgebied

1. Deze verordening is van toepassing op de volgende organisaties:

a) onderhoudsorganisaties die vallen onder sectie A van bijlage II (deel-145) bij Verordening (EU) nr. 1321/2014, met uitzondering van organisaties die uitsluitend betrokken zijn bij het onderhoud van luchtvaartuigen overeenkomstig bijlage V ter (deel-ML) bij Verordening (EU) nr. 1321/2014;

b) organisaties voor het beheer van de permanente luchtwaardigheid (CAMO's) die vallen onder sectie A van bijlage V quater (deel-CAMO) bij Verordening (EU) nr. 1321/2014, met uitzondering van organisaties die uitsluitend betrokken zijn bij het beheer van de permanente luchtwaardigheid van luchtvaartuigen overeenkomstig bijlage V ter (deel-ML) bij Verordening (EU) nr. 1321/2014;

c) luchtvaartexploitanten die vallen onder bijlage III (deel-ORO) bij Verordening (EU) nr. 965/2012, met uitzondering van exploitanten die uitsluitend betrokken zijn bij de exploitatie van:

   i) ELA 2-luchtvaartuigen als gedefinieerd in artikel 1, lid 2, punt j), van Verordening (EU) nr. 748/2012;

   ii) eenmotorige propellervliegtuigen met een maximale operationele passagiersconfiguratie van hoogstens 5 die niet zijn geclassificeerd als complexe motoraangedreven luchtvaartuigen, wanneer zij opstijgen en landen op hetzelfde luchtvaartterrein of dezelfde vluchtuitvoeringslocatie en vluchten uitvoeren volgens zichtvliegvoorschriften (VFR) overdag;

   iii) eenmotorige helikopters met een maximale operationele passagiersconfiguratie van hoogstens 5 die niet zijn geclassificeerd als complexe motoraangedreven luchtvaartuigen, wanneer zij opstijgen en landen op hetzelfde luchtvaartterrein of dezelfde vluchtuitvoeringslocatie en vluchten uitvoeren volgens VFR-regels overdag.

d) erkende opleidingsorganisaties (ATO's) die vallen onder bijlage VII (deel-ORA) bij Verordening (EU) nr. 1178/2011, met uitzondering van organisaties die uitsluitend betrokken zijn bij opleidingsactiviteiten voor ELA2-luchtvaartuigen zoals gedefinieerd in artikel 1, lid 2, punt j), van Verordening (EU) nr. 748/2012, of die uitsluitend betrokken zijn bij theoretische opleiding;

e) luchtvaartgeneeskundige centra voor vliegend personeel die vallen onder bijlage VII (deel-ORA) bij Verordening (EU) nr. 1178/2011;

f) exploitanten van vluchtnabootsers (FSTD) die vallen onder bijlage VII (deel-ORA) bij Verordening (EU) nr. 1178/2011, met uitzondering van exploitanten die uitsluitend betrokken zijn bij de exploitatie van FSTD's voor ELA2-luchtvaartuigen zoals gedefinieerd in artikel 1, lid 2, punt j), van Verordening (EU) nr. 748/2012;

g) organisaties voor de opleiding van luchtverkeersleiders (ATCO TO's) en luchtvaartgeneeskundige centra voor luchtverkeersleiders die vallen onder bijlage III (deel ATCO.OR) bij Verordening (EU) 2015/340;

h) organisaties die vallen onder bijlage III (deel-ATM/ANS.OR) bij Uitvoeringsverordening (EU) 2017/373, met uitzondering van de volgende dienstverleners:

i) verleners van luchtvaartnavigatiediensten die houder zijn van een beperkt certificaat overeenkomstig ATM/ANS.OR.A.010 van die bijlage;

ii) verleners van vluchtinformatiediensten die hun activiteiten verklaren overeenkomstig ATM/ANS.OR.A.015 van die bijlage;

i) U-spacedienstverleners en enige verleners van gemeenschappelijke informatiediensten die onder Uitvoeringsverordening (EU) 2021/664 vallen.

2. Deze verordening is van toepassing op de bevoegde autoriteiten, met inbegrip van het Agentschap van de Europese Unie voor de veiligheid van de luchtvaart ("het Agentschap"), als bedoeld in artikel 6 van deze verordening en in artikel 5 van Gedelegeerde Verordening (EU) 2022/1645 van de Commissie ([14]).

3. Deze verordening is ook van toepassing op de bevoegde autoriteit die verantwoordelijk is voor de afgifte, voortzetting, wijziging, opschorting of intrekking van bevoegdheidsbewijzen voor onderhoud van luchtvaartuigen overeenkomstig bijlage III (deel-66) bij Verordening (EU) nr. 1321/2014.

4. Deze verordening doet geen afbreuk aan de eisen inzake informatiebeveiliging en cyberbeveiliging die zijn vastgesteld in punt 1.7 van de bijlage bij Uitvoeringsverordening (EU) 2015/1998 en in artikel 14 van Richtlijn (EU) 2016/1148.

Artikel 3

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

1) "informatiebeveiliging": de instandhouding van de vertrouwelijkheid, integriteit, authenticiteit en beschikbaarheid van netwerk- en informatiesystemen;

2) "informatiebeveiligingsvoorval": een vastgestelde toestand van een systeem, dienst of netwerk die wijst op een mogelijke inbreuk op het informatiebeveiligingsbeleid of een storing van de informatiebeveiligingscontroles, of een voorheen onbekende situatie die relevant kan zijn voor de informatiebeveiliging;

3) "incident": elke gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen, zoals gedefinieerd in artikel 4, lid 7, van Richtlijn (EU) 2016/1148;

4) "informatiebeveiligingsrisico": het risico voor organisatorische burgerluchtvaartactiviteiten, activa, individuen en andere organisaties als gevolg van het potentieel van een informatiebeveiligingsvoorval. Informatiebeveiligingsrisico's houden verband met de mogelijkheid dat bedreigingen misbruik maken van kwetsbaarheden van een informatiebron of groep van informatieactiva;

([14]) Gedelegeerde Verordening (EU) 2022/1645 van de Commissie van 14 juli 2022 tot vaststelling van regels voor de toepassing van Verordening (EU) 2018/1139 van het Europees Parlement en de Raad, wat betreft eisen voor het beheer van risico's voor de informatiebeveiliging met mogelijke gevolgen voor de luchtvaartveiligheid voor organisaties die onder Verordeningen (EU) nr. 748/2012 en (EU) nr. 139/2014 van de Commissie vallen en tot wijziging van Verordeningen (EU) nr. 748/2012 en (EU) nr. 139/2014 van de Commissie (PB L 248 van 26.9.2022, blz. 18).

5) "bedreiging": een potentiële inbreuk op de informatiebeveiliging die bestaat wanneer er sprake is van een entiteit, omstandigheid, actie of gebeurtenis die schade kan veroorzaken;

6) "kwetsbaarheid": een tekortkoming of zwak punt in een activum, systeem, procedure, ontwerp of toepassing, of informatiebeveiligingsmaatregelen die kunnen worden misbruikt en leiden tot een inbreuk op of schending van het informatiebeveiligingsbeleid.

Artikel 4

Eisen voor organisaties en bevoegde autoriteiten

1. De in artikel 2, lid 1, bedoelde organisaties moeten voldoen aan de eisen van bijlage II (deel-IS.I.OR) bij deze verordening.

2. De in artikel 2, leden 2 en 3, bedoelde bevoegde autoriteiten moeten voldoen aan de eisen van bijlage I (deel-IS.AR) bij deze verordening.

Artikel 5

Eisen die voortvloeien uit andere wetgeving van de Unie

1. Wanneer een in artikel 2, lid 1, bedoelde organisatie voldoet aan de overeenkomstig artikel 14 van Richtlijn (EU) 2016/1148 vastgestelde beveiligingseisen die gelijkwaardig zijn aan de in deze verordening vastgestelde eisen, wordt de naleving van die beveiligingseisen beschouwd als naleving van de in deze verordening vastgestelde eisen.

2. Wanneer een in artikel 2, lid 1, bedoelde organisatie een exploitant of entiteit is als bedoeld in de overeenkomstig artikel 10 van Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad ([15]) opgestelde nationale programma's voor de beveiliging van de burgerluchtvaart van de lidstaten, worden de cyberbeveiligingseisen in punt 1.7 van de bijlage bij Uitvoeringsverordening (EU) 2015/1998 als gelijkwaardig beschouwd aan de in deze verordening vastgestelde eisen, behalve wat punt IS.I.OR.230 van bijlage II bij deze verordening betreft, waaraan als zodanig moet worden voldaan.

3. Wanneer de in artikel 2, lid 1, bedoelde organisatie de verlener van luchtvaartnavigatiediensten van de in Verordening (EU) 2021/696 bedoelde European Geostationary Navigation Overlay Service (EGNOS) is, worden de beveiligingsvoorschriften van titel V, artikelen 33 tot en met 43, van die verordening geacht gelijkwaardig te zijn aan de in deze verordening vastgestelde eisen, behalve wat betreft punt IS.I.OR.230 van bijlage II bij deze verordening, waaraan als zodanig moet worden voldaan.

4. Na raadpleging van het Agentschap en de in artikel 11 van Richtlijn (EU) 2016/1148 bedoelde samenwerkingsgroep kan de Commissie richtsnoeren uitvaardigen voor de beoordeling van de gelijkwaardigheid van de in deze verordening en Richtlijn (EU) 2016/1148 vastgestelde eisen.

Artikel 6

Bevoegde autoriteit

1. Onverminderd de taken die zijn toevertrouwd aan de Raad voor de beveiligingshomologatie als bedoeld in artikel 36 van Verordening (EU) 2021/696, is de autoriteit die verantwoordelijk is voor de certificering van en het toezicht op de naleving van deze verordening:

a) met betrekking tot de in artikel 2, lid 1, punt a), bedoelde organisaties, de bevoegde autoriteit die is aangewezen overeenkomstig bijlage II (deel-145) bij Verordening (EU) nr. 1321/2014;

b) met betrekking tot de in artikel 2, lid 1, punt b), bedoelde organisaties, de bevoegde autoriteit die is aangewezen overeenkomstig bijlage V quater (deel-CAMO) bij Verordening (EU) nr. 1321/2014;

([15]) Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van Verordening (EG) nr. 2320/2002 (PB L 97 van 9.4.2008, blz. 72).

c) met betrekking tot de in artikel 2, lid 1, punt c), bedoelde organisaties, de bevoegde autoriteit die is aangewezen overeenkomstig bijlage III (deel-ORO) bij Verordening (EU) nr. 965/2012;

d) met betrekking tot de in artikel 2, lid 1, punten d), e) en f), bedoelde organisaties, de bevoegde autoriteit die is aangewezen overeenkomstig bijlage VII (deel-ORA) bij Verordening (EU) nr. 1178/2011;

e) met betrekking tot de in artikel 2, lid 1, punt g), bedoelde organisaties, de bevoegde autoriteit die is aangewezen overeenkomstig artikel 6, lid 2, van Verordening (EU) 2015/340;

f) met betrekking tot de in artikel 2, lid 1, punt h), bedoelde organisaties, de bevoegde autoriteit die is aangewezen overeenkomstig artikel 4, lid 1, van Uitvoeringsverordening (EU) 2017/373 van de Commissie;

g) met betrekking tot de in artikel 2, lid 1, punt i), bedoelde organisaties, de bevoegde autoriteit die is aangewezen overeenkomstig artikel 14, lid 1, of artikel 14, lid 2, van Uitvoeringsverordening (EU) 2021/664, al naargelang van toepassing.

2. Met het oog op de toepassing van deze verordening mogen de lidstaten een onafhankelijke en zelfstandige entiteit aanwijzen die de rol en verantwoordelijkheden opneemt van de in lid 1 bedoelde bevoegde autoriteit. In dat geval worden maatregelen getroffen voor coördinatie tussen die entiteit en de in lid 1 bedoelde bevoegde autoriteiten, teneinde te garanderen dat de organisatie doeltreffend toezicht houdt op alle eisen waaraan moet worden voldaan.

3. Het Agentschap werkt, met volledige inachtneming van de toepasselijke regels inzake geheimhouding, bescherming van persoonsgegevens en bescherming van gerubriceerde informatie, samen met het Agentschap van de Europese Unie voor het ruimtevaartprogramma (EUSPA) en de in artikel 36 van Verordening (EU) 2021/696 bedoelde raad voor beveiligingshomologatie om te zorgen voor doeltreffend toezicht op de eisen die van toepassing zijn op de verlener van EGNOS-luchtvaartnavigatiediensten.

Artikel 7

Indiening van relevante informatie bij bevoegde autoriteiten inzake de beveiliging van netwerk- en informatiesystemen

De uit hoofde van deze verordening bevoegde autoriteiten stellen het overeenkomstig artikel 8 van Richtlijn (EU) 2016/1148 aangewezen centrale contactpunt onverwijld in kennis van alle relevante informatie die is opgenomen in kennisgevingen die overeenkomstig punt IS.I.OR.230 van bijlage II bij deze verordening en punt IS.D.OR.230 van bijlage I bij Gedelegeerde Verordening 2022/1645 zijn ingediend door aanbieders van essentiële diensten die zijn geïdentificeerd overeenkomstig artikel 5 van Richtlijn (EU) 2016/1148.

Artikel 8

Wijziging van Verordening (EU) nr. 1178/2011

Bijlagen VI (deel-ARA) en VII (deel-ORA) bij Verordening (EU) nr. 1178/2011 worden gewijzigd overeenkomstig bijlage III bij deze verordening.

Artikel 9

Wijziging van Verordening (EU) nr. 748/2012

Bijlage I (deel 21) bij Verordening (EU) nr. 748/2012 wordt gewijzigd overeenkomstig bijlage IV bij deze verordening.

Artikel 10

Wijziging van Verordening (EU) nr. 965/2012

Bijlagen II (deel-ARO) en III (deel-ORO) bij Verordening (EU) nr. 965/2012 worden gewijzigd overeenkomstig bijlage V bij deze verordening.

Artikel 11

Wijziging van Verordening (EU) nr. 139/2014

Bijlage II (deel-ADR.AR) bij Verordening (EU) nr. 139/2014 wordt gewijzigd overeenkomstig bijlage VI bij deze verordening.

Artikel 12

Wijziging van Verordening (EU) nr. 1321/2014

Bijlagen II (deel-145), III (deel-66) en V quater (deel-CAMO) bij Verordening (EU) nr. 1321/2014 worden gewijzigd overeenkomstig bijlage VII bij deze verordening.

Artikel 13

Wijziging van Verordening (EU) 2015/340

Bijlagen II (deel-ATCO.AR) en III (deel-ATCO.OR) bij Verordening (EU) 2015/340 worden gewijzigd overeenkomstig bijlage VIII bij deze verordening.

Artikel 14

Wijziging van Uitvoeringsverordening (EU) 2017/373

Bijlagen II (deel-ATM/ANS.AR) en III (deel-ATM/ANS.OR) bij Uitvoeringsverordening (EU) 2017/373 worden gewijzigd overeenkomstig bijlage IX bij deze verordening.

Artikel 15

Wijziging van Uitvoeringsverordening (EU) 2021/664

Uitvoeringsverordening (EU) 2021/664 wordt als volgt gewijzigd:

1) In artikel 15, lid 1, wordt punt f) vervangen door:

"f) een beveiligingsbeheersysteem overeenkomstig ATM/ANS.OR.D.010 van subdeel D van bijlage III bij Uitvoeringsverordening (EU) 2017/373 en een beheersysteem voor informatiebeveiliging overeenkomstig bijlage II (deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203 toepassen en onderhouden.".

2) Aan artikel 18 wordt het volgende punt l) toegevoegd:

"l) een beheersysteem voor informatiebeveiliging opzetten, toepassen en onderhouden overeenkomstig bijlage I (deel-IS.AR) bij Uitvoeringsverordening (EU) 2023/203.".

Artikel 16

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Zij is van toepassing met ingang van 22 februari 2026.

Wat de onder Uitvoeringsverordening (EU) 2017/373 vallende verlener van EGNOS-luchtvaartnavigatiediensten betreft, is deze echter van toepassing met ingang van 1 januari 2026.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 27 oktober 2022.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE I

INFORMATIEBEVEILIGING — EISEN VOOR DE AUTORITEIT

[DEEL-IS.AR]

IS.AR.100 Toepassingsgebied

IS.AR.200 Beheersysteem voor informatiebeveiliging

IS.AR.205 Beoordeling van risico's voor de informatiebeveiliging

IS.AR.210 Behandeling van risico's voor de informatiebeveiliging

IS.AR.215 Informatiebeveiligingsincidenten — opsporing, reactie en herstel

IS.AR.220 Uitbesteding van activiteiten op het gebied van informatiebeveiligingsbeheer

IS.AR.225 Personeelsvoorschriften

IS.AR.230 Bijhouden van gegevens

IS.AR.235 Permanente verbetering

IS.AR.100 Toepassingsgebied

In dit deel worden de beheerseisen vastgesteld waaraan de in artikel 2, lid 2, van deze verordening bedoelde bevoegde autoriteiten moeten voldoen.

De eisen waaraan die bevoegde autoriteiten moeten voldoen voor de uitvoering van hun certificerings-, toezichts- en handhavingsactiviteiten zijn opgenomen in de in artikel 2, lid 1, van deze verordening en in artikel 2 van Gedelegeerde Verordening (EU) 2022/1645 bedoelde verordeningen.

IS.AR.200 Beheersysteem voor informatiebeveiliging

a) Om de in artikel 1 uiteengezette doelstellingen te verwezenlijken, ontwikkelt, implementeert en onderhoudt de bevoegde autoriteit een beheersysteem voor informatiebeveiliging, dat waarborgt dat de bevoegde autoriteit:

1) een beleid inzake informatiebeveiliging vaststelt, waarin de algemene beginselen van de bevoegde autoriteit met betrekking tot de mogelijke gevolgen van informatiebeveiligingsrisico's voor de veiligheid van de luchtvaart worden uiteengezet;

2) informatiebeveiligingsrisico's vaststelt en beoordeelt overeenkomstig IS.AR.205;

3) maatregelen voor de behandeling van informatiebeveiligingsrisico's definieert en uitvoert overeenkomstig IS.AR.210;

4) overeenkomstig IS.AR.215 de maatregelen vaststelt en toepast die nodig zijn om informatiebeveiligingsvoorvallen op te sporen, om te bepalen welke daarvan worden beschouwd als informatiebeveiligingsincidenten met potentiële gevolgen voor de luchtvaartveiligheid en om te reageren op en te herstellen van dergelijke informatiebeveiligingsincidenten;

5) voldoet aan de eisen van IS.AR.220 bij het uitbesteden van een deel van de in IS.AR.200 beschreven activiteiten aan andere organisaties;

6) voldoet aan de personeelseisen die zijn vastgesteld in IS.AR.225;

7) voldoet aan de eisen inzake het bijhouden van gegevens die zijn vastgesteld in IS.AR.230;

8) erop toeziet dat zijn eigen organisatie voldoet aan de vereisten van deze verordening en de in IS.AR.225, punt a), bedoelde persoon feedback over bevindingen geeft om ervoor te zorgen dat corrigerende maatregelen doeltreffend worden uitgevoerd;

9) de vertrouwelijkheid beschermt van alle informatie die de bevoegde autoriteit kan hebben met betrekking tot organisaties die onder haar toezicht staan en de informatie die is ontvangen via de externe rapportagesystemen van de organisatie die zijn vastgesteld overeenkomstig IS.I.OR.230 van bijlage II (Deel-IS.I.OR) bij deze verordening en IS.D.OR.230 van de bijlage (Deel-IS.D.OR) bij Gedelegeerde Verordening (EU) 2022/1645;

10) het Agentschap in kennis stelt van wijzigingen die van invloed zijn op het vermogen van de bevoegde autoriteit om haar taken uit te voeren en zich te kwijten van haar verantwoordelijkheden zoals gedefinieerd in deze verordening;

11) procedures vaststelt en uitvoert om, waar passend en op een praktische en tijdige manier, relevante informatie te delen om andere bevoegde autoriteiten en agentschappen, alsmede organisaties die onder deze verordening vallen, bij te staan bij het uitvoeren van doeltreffende veiligheidsrisicobeoordelingen met betrekking tot hun activiteiten.

b) Om blijvend te voldoen aan de in artikel 1 vermelde eisen, voert de bevoegde autoriteit een continu verbeteringsproces uit overeenkomstig IS.AR.235.

c) De bevoegde autoriteit documenteert alle belangrijke processen, procedures, rollen en verantwoordelijkheden die vereist zijn om te voldoen aan IS.AR.200, a), en stelt een procedure vast voor het wijzigen van die documentatie.

d) De processen, procedures, rollen en verantwoordelijkheden die door de bevoegde autoriteit zijn vastgesteld om te voldoen aan IS.AR.200, punt a), moeten overeenstemmen met de aard en complexiteit van haar activiteiten, op basis van een beoordeling van de aan die activiteiten inherente risico's voor de informatiebeveiliging, en mogen worden geïntegreerd in andere bestaande beheersystemen die reeds door de bevoegde autoriteit worden toegepast.

IS.AR.205 Beoordeling van risico's voor de informatiebeveiliging

a) De bevoegde autoriteit identificeert alle elementen van haar eigen organisatie die aan risico's voor de informatiebeveiliging kunnen worden blootgesteld. Dit omvat:

1) de activiteiten, faciliteiten en middelen van de bevoegde autoriteit en de diensten die de bevoegde autoriteit exploiteert, verleent, ontvangt of onderhoudt;

2) de apparatuur, systemen, gegevens en informatie die bijdragen tot de werking van de in punt 1) bedoelde elementen.

b) De bevoegde autoriteit identificeert de interfaces die haar eigen organisatie heeft met andere organisaties en die kunnen leiden tot wederzijdse blootstelling aan informatiebeveiligingsrisico's.

c) Met betrekking tot de in de punten a) en b) vermelde elementen en interfaces identificeert de bevoegde autoriteit de informatiebeveiligingsrisico's die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.

Voor elk geïdentificeerd risico moet de bevoegde autoriteit:

1) een risiconiveau toekennen op basis van een classificatie die zij vooraf heeft opgesteld;

2) elk risico en het niveau ervan koppelen aan het overeenkomstige element of de overeenkomstige interface, zoals vastgesteld overeenkomstig de punten a) en b).

De in punt 1) bedoelde vooraf opgestelde classificatie houdt rekening met de mogelijkheid dat het dreigingsscenario zich voordoet en met de ernst van de gevolgen daarvan voor de veiligheid. Aan de hand van die classificatie en rekening houdend met de vraag of de bevoegde autoriteit beschikt over een gestructureerd en herhaalbaar proces voor het beheer van de risico's van haar activiteiten, moet de bevoegde autoriteit in staat zijn te bepalen of het risico aanvaardbaar is of moet worden behandeld overeenkomstig IS.AR.210.

Om risicobeoordelingen gemakkelijker te kunnen vergelijken, moet bij de toekenning van het risiconiveau overeenkomstig punt 1) rekening worden gehouden met relevante informatie die in overleg met de in punt b) bedoelde organisaties is verkregen.

d) De bevoegde autoriteit evalueert en actualiseert de overeenkomstig de punten a), b) en c) uitgevoerde risicobeoordeling in elk van de volgende gevallen:

1) er is een wijziging in de elementen die onderhevig zijn aan informatiebeveiligingsrisico's;

2) er is een wijziging in de interfaces tussen de organisatie van de bevoegde autoriteit en andere organisaties, of in de risico's die door de andere organisaties zijn meegedeeld;

3) er is een wijziging in de informatie of kennis die gebruikt is voor de identificatie, analyse en classificatie van risico's;

4) er zijn lessen getrokken uit de analyse van informatiebeveiligingsincidenten.

IS.AR.210 Behandeling van risico's voor de informatiebeveiliging

a) De bevoegde autoriteit ontwikkelt maatregelen om onaanvaardbare risico's aan te pakken die overeenkomstig IS.AR.205 zijn vastgesteld, voert deze maatregelen tijdig uit en controleert de blijvende doeltreffendheid ervan. Die maatregelen moeten de bevoegde autoriteit in staat stellen om:

1) controle uit te oefenen op de omstandigheden die ertoe bijdragen dat het dreigingsscenario zich effectief voordoet;

2) de gevolgen van het dreigingsscenario voor de veiligheid van de luchtvaart te beperken;

3) de risico's te vermijden.

Deze maatregelen mogen niet leiden tot nieuwe potentiële onaanvaardbare risico's voor de veiligheid van de luchtvaart.

b) De in IS.AR.225, punt a), bedoelde persoon en andere betrokken personeelsleden van de bevoegde autoriteit worden in kennis gesteld van de resultaten van de overeenkomstig IS.AR.205 uitgevoerde risicobeoordeling, de overeenkomstige dreigingsscenario's en de uit te voeren maatregelen.

De bevoegde autoriteit stelt de organisaties waarmee zij een interface heeft overeenkomstig IS.AR.205, b), eveneens in kennis van elk risico dat wordt gedeeld door de bevoegde autoriteit en de organisatie.

IS.AR.215 Informatiebeveiligingsincidenten — opsporing, reactie en herstel

a) Op basis van de resultaten van de overeenkomstig IS.AR.205 en IS.AR.210 uitgevoerde risicobeoordeling en risicobehandeling, past de bevoegde autoriteit maatregelen toe om voorvallen op te sporen die erop wijzen dat zich onaanvaardbare risico's kunnen voordoen die potentiële gevolgen kunnen hebben voor de veiligheid van de luchtvaart. Die opsporingsmaatregelen moeten de bevoegde autoriteit in staat stellen om:

1) afwijkingen van vooraf bepaalde referentiescenario's voor functionele prestaties vast te stellen;

2) waarschuwingen te geven om passende responsmaatregelen te activeren in geval van een afwijking.

b) De bevoegde autoriteit past maatregelen toe om te reageren op overeenkomstig punt a) vastgestelde voorvalsomstandigheden die zich kunnen ontwikkelen of hebben ontwikkeld tot een informatiebeveiligingsincident. Die responsmaatregelen moeten de bevoegde autoriteit in staat stellen om:

1) haar eigen organisatie te laten reageren op de in punt a), 2), bedoelde waarschuwingen door vooraf gedefinieerde middelen en acties te activeren;

2) de verspreiding van een aanval in te dammen en te voorkomen dat het dreigingsscenario volledig werkelijkheid wordt;

3) de faalwijze van de in IS.AR.205, a), gedefinieerde getroffen elementen te controleren.

c) De bevoegde autoriteit voert maatregelen uit die gericht zijn op herstel van informatiebeveiligingsincidenten, met inbegrip van noodmaatregelen, indien nodig. Die herstelmaatregelen moeten de bevoegde autoriteit in staat stellen om:

1) de omstandigheid die het incident heeft veroorzaakt, weg te nemen of tot een aanvaardbaar niveau te beperken;

2) opnieuw een veilige toestand te bereiken van de in IS.AR.205, a), gedefinieerde getroffen elementen, binnen een vooraf door haar eigen organisatie vastgestelde hersteltijd.

IS.AR.220 Uitbesteding van activiteiten op het gebied van informatiebeveiligingsbeheer

De bevoegde autoriteit ziet erop toe dat bij het uitbesteden van een deel van de in IS.AR.200 bedoelde activiteiten aan andere organisaties, de uitbestede activiteiten voldoen aan de eisen van deze verordening en dat de gecontracteerde organisatie onder haar toezicht werkt. De bevoegde autoriteit zorgt ervoor dat de risico's in verband met de uitbestede activiteiten op passende wijze worden beheerd.

IS.AR.225 Personeelsvoorschriften

De bevoegde autoriteit moet:

a) beschikken over een persoon die bevoegd is om de organisatorische structuren, beleidslijnen, processen en procedures vast te stellen en in stand te houden die nodig zijn voor de uitvoering van deze verordening.

Deze persoon moet:

1) de bevoegdheid hebben om volledige toegang te krijgen tot de middelen die de bevoegde autoriteit nodig heeft om alle bij deze verordening voorgeschreven taken uit te voeren;

2) beschikken over de bevoegdheidsdelegatie die nodig is om de toegewezen taken uit te voeren;

b) beschikken over een proces om ervoor te zorgen dat zij over voldoende personeel beschikt om de onder deze bijlage vallende activiteiten uit te voeren;

c) beschikken over een proces om ervoor te zorgen dat het in punt b) bedoelde personeel over de nodige bekwaamheid beschikt om zijn taken uit te voeren;

d) beschikken over een proces om ervoor te zorgen dat het personeel de aan de toegewezen rollen en taken verbonden verantwoordelijkheden erkent;

e) ervoor zorgen dat de identiteit en betrouwbaarheid van het personeel dat toegang heeft tot informatiesystemen en gegevens waarop de eisen van deze verordening van toepassing zijn, op passende wijze worden vastgesteld.

IS.AR.230 Bijhouden van gegevens

a) De bevoegde autoriteit houdt gegevens bij over haar activiteiten op het gebied van informatiebeveiligingsbeheer.

1) De bevoegde autoriteit zorgt ervoor dat de volgende gegevens worden gearchiveerd en traceerbaar zijn:

i) contracten voor de in IS.AR.200, a), 5), bedoelde activiteiten;

ii) gegevens over de in IS.AR.200, d), bedoelde cruciale processen;

iii) gegevens over de risico's die zijn vastgesteld tijdens de in IS.AR.205 bedoelde risicobeoordeling, samen met de in IS.AR.210 bedoelde maatregelen voor het behandelen van die risico's;

iv) gegevens over informatiebeveiligingsvoorvallen die mogelijk opnieuw moeten worden beoordeeld om onopgespoorde informatiebeveiligingsincidenten of kwetsbaarheden te ontdekken.

2) De in punt 1), i), bedoelde gegevens worden bewaard gedurende minstens 5 jaar nadat het contract is gewijzigd of beëindigd.

3) De in punt 1), ii) en iii), bedoelde gegevens worden minstens 5 jaar bewaard.

4) De in punt 1), iv), bedoelde gegevens worden bewaard totdat die informatiebeveiligingsvoorvallen opnieuw zijn beoordeeld overeenkomstig een frequentie die is vastgesteld in een door de bevoegde autoriteit opgestelde procedure.

b) De bevoegde autoriteit houdt gegevens bij over de kwalificaties en ervaring van haar eigen personeel dat betrokken is bij activiteiten op het gebied van informatiebeveiligingsbeheer.

1) De gegevens over de kwalificaties en ervaring van het personeel moeten worden bewaard zolang de persoon in kwestie voor de bevoegde autoriteit werkt, en gedurende minstens 3 jaar nadat hij de bevoegde autoriteit heeft verlaten.

2) Indien personeelsleden daarom verzoeken, moeten zij toegang krijgen tot hun persoonlijke gegevens. Wanneer zij de bevoegde autoriteit verlaten, moet de bevoegde autoriteit hen, op verzoek, een kopie geven van hun individuele gegevens.

c) De vorm waarin de gegevens worden geregistreerd, wordt gespecificeerd in de procedures van de bevoegde autoriteit.

d) De gegevens worden zodanig opgeslagen dat zij beschermd zijn tegen schade, wijziging en diefstal, waarbij de informatie, indien vereist, wordt geïdentificeerd volgens rubriceringsniveau. De bevoegde autoriteit zorgt ervoor dat de gegevens worden opgeslagen met behulp van middelen die de integriteit, authenticiteit en geautoriseerde toegang waarborgen.

IS.AR.235 Permanente verbetering

a) De bevoegde autoriteit beoordeelt aan de hand van passende prestatie-indicatoren de doeltreffendheid en maturiteit van het beheersysteem voor informatiebeveiliging. De beoordeling wordt uitgevoerd op basis van een vooraf door de bevoegde autoriteit vastgestelde kalender of na een informatiebeveiligingsincident.

b) Als na de overeenkomstig punt a) uitgevoerde beoordeling tekortkomingen worden vastgesteld, neemt de bevoegde autoriteit de nodige verbeteringsmaatregelen om te garanderen dat het beheersysteem voor informatiebeveiliging blijft voldoen aan de toepasselijke eisen en de informatiebeveiligingsrisico's op een aanvaardbaar niveau handhaaft. De bevoegde autoriteit zal de elementen van het beheersysteem voor informatiebeveiliging die onder de vastgestelde maatregelen vallen, opnieuw beoordelen.

BIJLAGE II

INFORMATIEBEVEILIGING — VEREISTEN VOOR DE ORGANISATIE

[DEEL-IS.I.OR]

IS.I.OR.100 Toepassingsgebied

IS.I.OR.200 Beheersysteem voor informatiebeveiliging

IS.I.OR.205 Beoordeling van risico's voor de informatiebeveiliging

IS.I.OR.210 Behandeling van risico's voor de informatiebeveiliging

IS.I.OR.215 Regeling voor interne rapportage over informatiebeveiliging

IS.I.OR.220 Informatiebeveiligingsincidenten — opsporing, reactie en herstel

IS.I.OR.225 Reactie op door de bevoegde autoriteit gemelde bevindingen

IS.I.OR.230 Regeling voor externe rapportage over informatiebeveiliging

IS.I.OR.235 Uitbesteding van activiteiten op het gebied van informatiebeveiligingsbeheer

IS.I.OR.240 Personeelsvoorschriften

IS.I.OR.245 Bijhouden van gegevens

IS.I.OR.250 Handboek informatiebeveiligingsbeheer

IS.I.OR.255 Wijzigingen van het beheersysteem voor informatiebeveiliging

IS.I.OR.260 Permanente verbetering

IS.I.OR.100 Toepassingsgebied

In dit deel worden de eisen vastgesteld waaraan de in artikel 2, lid 1, van deze verordening bedoelde organisaties moeten voldoen.

IS.I.OR.200 Beheersysteem voor informatiebeveiliging

a) Om de in artikel 1 uiteengezette doelstellingen te verwezenlijken, ontwikkelt, implementeert en onderhoudt de organisatie een beheersysteem voor informatiebeveiliging, dat waarborgt dat de organisatie:

   1) een beleid inzake informatiebeveiliging vaststelt, waarin de algemene beginselen van de organisatie met betrekking tot de mogelijke gevolgen van informatiebeveiligingsrisico's voor de veiligheid van de luchtvaart worden uiteengezet;

   2) informatiebeveiligingsrisico's vaststelt en beoordeelt overeenkomstig IS.I.OR.205;

   3) maatregelen voor de behandeling van informatiebeveiligingsrisico's definieert en uitvoert overeenkomstig IS.I.OR.210;

   4) een regeling voor interne rapportage over informatiebeveiliging toepast overeenkomstig IS.I.OR.215;

   5) overeenkomstig IS.I.OR.220 de maatregelen vaststelt en toepast die nodig zijn om informatiebeveiligingsvoorvallen op te sporen, om te bepalen welke daarvan worden beschouwd als informatiebeveiligingsincidenten met potentiële gevolgen voor de luchtvaartveiligheid, met uitzondering van de voorvallen die zijn toegestaan uit hoofde van IS.I.OR.205, e), en om te reageren op en te herstellen van dergelijke informatiebeveiligingsincidenten;

6) de maatregelen uitvoert die door de bevoegde autoriteit zijn gemeld als een onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart;

7) passende maatregelen neemt, overeenkomstig IS.I.OR.225, om de door de bevoegde autoriteit gemelde bevindingen aan te pakken;

8) een extern rapportagesysteem toepast, overeenkomstig IS.I.OR.230, om de bevoegde autoriteit in staat te stellen passende maatregelen te nemen;

9) voldoet aan de eisen van IS.I.OR.235 bij het uitbesteden van een deel van de in IS.I.OR.200 bedoelde activiteiten aan andere organisaties;

10) voldoet aan de personeelseisen die zijn vastgesteld in IS.I.OR.240;

11) voldoet aan de eisen inzake het bijhouden van gegevens die zijn vastgesteld in IS.I.OR.245;

12) erop toeziet dat de organisatie voldoet aan de vereisten van deze verordening en aan de verantwoordelijke manager feedback geeft over bevindingen om ervoor te zorgen dat corrigerende maatregelen doeltreffend worden uitgevoerd;

13) onverminderd de toepasselijke vereisten inzake rapportage van incidenten, de vertrouwelijkheid beschermt van alle informatie die de organisatie heeft ontvangen van andere organisaties, volgens het niveau van vertrouwelijkheid.

b) Om blijvend te voldoen aan de in artikel 1 vermelde eisen, voert de organisatie een continu verbeteringsproces uit overeenkomstig IS.I.OR.260.

c) Overeenkomstig IS.I.OR.250 documenteert de organisatie alle belangrijke processen, procedures, rollen en verantwoordelijkheden die vereist zijn om te voldoen aan IS.I.OR.200, a), en stelt zij een procedure vast voor het wijzigen van die documentatie. Wijzigingen van die processen, procedures, rollen en verantwoordelijkheden worden beheerd overeenkomstig IS.I.OR.255.

d) De processen, procedures, rollen en verantwoordelijkheden die door de organisatie zijn vastgesteld om te voldoen aan punt IS.I.OR.200, a), moeten overeenstemmen met de aard en complexiteit van haar activiteiten, op basis van een beoordeling van de aan die activiteiten inherente risico's voor de informatiebeveiliging, en mogen worden geïntegreerd in andere bestaande beheersystemen die reeds door de organisatie worden toegepast.

e) Onverminderd de verplichting om te voldoen aan de rapportagevereisten van Verordening (EU) nr. 376/2014 en de eisen van IS.I.OR.200, a), 13), kan de organisatie toestemming krijgen van de bevoegde autoriteit om de in de punten a) tot en met d) bedoelde eisen en de daarmee verband houdende eisen van IS.I.OR.205 tot en met IS.I.OR.260 niet toe te passen, als zij tot tevredenheid van die autoriteit aantoont dat haar activiteiten, faciliteiten en middelen, alsook de diensten die zij exploiteert, verleent, ontvangt en onderhoudt, geen informatiebeveiligingsrisico's met mogelijke gevolgen voor de veiligheid van de luchtvaart inhouden, noch voor haarzelf, noch voor andere organisaties. De toestemming wordt gebaseerd op een gedocumenteerde beoordeling van de informatiebeveiligingsrisico's die door de organisatie of door een derde partij wordt uitgevoerd overeenkomstig IS.I.OR.205 en door haar bevoegde autoriteit wordt beoordeeld en goedgekeurd.

De blijvende geldigheid van die toestemming zal door de bevoegde autoriteit worden beoordeeld na de toepasselijke auditcyclus en telkens wanneer wijzigingen worden doorgevoerd in het toepassingsgebied van de werkzaamheden van de organisatie.

IS.I.OR.205 Beoordeling van risico's voor de informatiebeveiliging

a) De organisatie identificeert al haar elementen die kunnen worden blootgesteld aan informatiebeveiligingsrisico's, waaronder:

1) de activiteiten, faciliteiten en middelen van de organisatie, en de diensten die de organisatie exploiteert, verleent, ontvangt of onderhoudt;

2) de apparatuur, systemen, gegevens en informatie die bijdragen tot de werking van de in punt 1) vermelde elementen.

b) De organisatie identificeert de interfaces die zij heeft met andere organisaties en die kunnen leiden tot wederzijdse blootstelling aan informatiebeveiligingsrisico's.

c) Met betrekking tot de in de punten a) en b) vermelde elementen en interfaces identificeert de organisatie de informatiebeveiligingsrisico's die gevolgen kunnen hebben voor de veiligheid van de luchtvaart. Voor elk geïdentificeerd risico moet de organisatie:

1) een risiconiveau toekennen op basis van een classificatie die zij vooraf heeft opgesteld;

2) elk risico en het niveau ervan koppelen aan het overeenkomstige element of de overeenkomstige interface, zoals vastgesteld overeenkomstig de punten a) en b).

De in punt 1) bedoelde vooraf opgestelde classificatie houdt rekening met de mogelijkheid dat het dreigingsscenario zich voordoet en met de ernst van de gevolgen daarvan voor de veiligheid. Op basis van die classificatie en rekening houdend met de vraag of de organisatie beschikt over een gestructureerd en aanvaardbaar proces voor het beheer van de risico's van haar activiteiten, moet de organisatie in staat zijn te bepalen of het risico aanvaardbaar is of moet worden behandeld overeenkomstig IS.I.OR.210.

Om risicobeoordelingen gemakkelijker te kunnen vergelijken, moet bij de toekenning van het risiconiveau overeenkomstig punt 1) rekening worden gehouden met relevante informatie die in overleg met de in punt b) bedoelde organisaties is verkregen.

d) De organisatie evalueert en actualiseert de overeenkomstig de punten a), b) en, indien van toepassing, c) of e), uitgevoerde risicobeoordeling in elk van de volgende situaties:

1) er is een wijziging in de elementen die onderhevig zijn aan informatiebeveiligingsrisico's;

2) er is een wijziging in de interfaces tussen de organisatie en andere organisaties, of in de risico's die door de andere organisaties zijn meegedeeld;

3) er is een wijziging in de informatie of kennis die gebruikt is voor de identificatie, analyse en classificatie van risico's;

4) er zijn lessen getrokken uit de analyse van informatiebeveiligingsincidenten.

e) In afwijking van punt c) vervangen organisaties die moeten voldoen aan subdeel C van bijlage III (Deel-ATM/ANS.OR) bij Uitvoeringsverordening (EU) 2017/373 de analyse van het effect op de luchtvaartveiligheid door een analyse van het effect op hun diensten, overeenkomstig de veiligheidsondersteunende beoordeling die vereist is op grond van ATM/ANS.OR.C.005. Deze veiligheidsondersteunende beoordeling wordt ter beschikking gesteld van de verleners van luchtverkeersdiensten aan wie zij diensten verlenen en die verleners van luchtverkeersdiensten zijn verantwoordelijk voor de beoordeling van de gevolgen voor de veiligheid van de luchtvaart.

IS.I.OR.210 Behandeling van risico's voor de informatiebeveiliging

a) De organisatie ontwikkelt maatregelen om onaanvaardbare risico's aan te pakken die overeenkomstig IS.I.OR.205 zijn vastgesteld, voert deze maatregelen tijdig uit en controleert de blijvende doeltreffendheid ervan. Die maatregelen moeten de organisatie in staat stellen om:

1) controle uit te oefenen op de omstandigheden die ertoe bijdragen dat het dreigingsscenario zich effectief voordoet;

2) de gevolgen van het dreigingsscenario voor de veiligheid van de luchtvaart te beperken;

3) de risico's te vermijden.

Deze maatregelen mogen niet leiden tot nieuwe potentiële onaanvaardbare risico's voor de veiligheid van de luchtvaart.

b) De in IS.I.OR.240, a) en b), bedoelde persoon en andere betrokken personeelsleden van de organisatie worden in kennis gesteld van de resultaten van de overeenkomstig IS.I.OR.205 uitgevoerde risicobeoordeling, de overeenkomstige dreigingsscenario's en de uit te voeren maatregelen.

De organisatie stelt de organisaties waarmee zij een interface heeft overeenkomstig IS.I.OR.205, b), eveneens in kennis van elk risico dat door beide organisaties wordt gedeeld.

IS.I.OR.215 Regeling voor interne rapportage over informatiebeveiliging

a) De organisatie zet een interne rapportageregeling op om het mogelijk te maken informatiebeveiligingsvoorvallen te verzamelen en te beoordelen, met inbegrip van die welke overeenkomstig IS.I.OR.230 moeten worden gerapporteerd.

b) Die regeling en het in IS.I.OR.220 bedoelde proces moeten de organisatie in staat stellen om:

1) te bepalen welke van de overeenkomstig punt a) gemelde gebeurtenissen moeten worden beschouwd als informatiebeveiligingsincidenten of kwetsbaarheden met potentiële gevolgen voor de veiligheid van de luchtvaart;

2) de oorzaken van en de factoren die bijdragen tot de overeenkomstig punt 1) vastgestelde incidenten en kwetsbaarheden te bepalen en aan te pakken in het kader van het proces voor het beheer van risico's voor de informatiebeveiliging, overeenkomstig IS.I.OR.205 en IS.I.OR.220;

3) erop toe te zien dat een evaluatie wordt uitgevoerd van alle bekende relevante informatie met betrekking tot de overeenkomstig punt 1) vastgestelde informatiebeveiligingsincidenten en kwetsbaarheden;

4) erop toe te zien dat een methode ten uitvoer wordt gelegd om de informatie indien nodig intern te verspreiden.

c) Elke gecontracteerde organisatie die de organisatie kan blootstellen aan informatiebeveiligingsrisico's met potentiële gevolgen voor de veiligheid van de luchtvaart moet informatiebeveiligingsvoorvallen melden aan de organisatie. Deze meldingen worden ingediend volgens de procedures die in de specifieke contractuele regelingen zijn vastgesteld en worden geëvalueerd overeenkomstig punt b).

d) De organisatie pleegt overleg over onderzoeken met elke andere organisatie die een belangrijke bijdrage levert aan de informatiebeveiliging van haar eigen activiteiten.

e) De organisatie mag dat rapportagesysteem integreren in andere rapportagesystemen die zij reeds toepast.

IS.I.OR.220 Informatiebeveiligingsincidenten — opsporing, reactie en herstel

a) Op basis van de resultaten van de overeenkomstig IS.I.OR.205 en IS.I.OR.210 uitgevoerde risicobeoordeling en risicobehandeling, past de organisatie maatregelen toe om incidenten en kwetsbaarheden op te sporen die erop wijzen dat zich onaanvaardbare risico's kunnen voordoen die potentiële gevolgen kunnen hebben voor de veiligheid van de luchtvaart. Die opsporingsmaatregelen moeten de organisatie in staat stellen om:

1) afwijkingen van vooraf bepaalde referentiescenario's voor functionele prestaties vast te stellen;

2) waarschuwingen te geven om passende responsmaatregelen te activeren in geval van een afwijking.

b) De organisatie past maatregelen toe om te reageren op overeenkomstig punt a) vastgestelde voorvalsomstandigheden die zich kunnen ontwikkelen of hebben ontwikkeld tot een informatiebeveiligingsincident. Die responsmaatregelen moeten de organisatie in staat stellen om:

1) te reageren op de in punt a), 2), bedoelde waarschuwingen door vooraf gedefinieerde middelen en acties te activeren;

2) de verspreiding van een aanval in te dammen en te voorkomen dat het dreigingsscenario volledig werkelijkheid wordt;

3) de faalwijze van de in IS.I.OR.205, a), gedefinieerde getroffen elementen te controleren.

c) De organisatie voert maatregelen uit die gericht zijn op herstel van informatiebeveiligingsincidenten, met inbegrip van noodmaatregelen, indien nodig. Die herstelmaatregelen moeten de organisatie in staat stellen om:

1) de omstandigheid die het incident heeft veroorzaakt, weg te nemen of tot een aanvaardbaar niveau te beperken;

2) een veilige toestand te bereiken van de in IS.I.OR.205, a), gedefinieerde getroffen elementen, binnen een vooraf door de organisatie vastgestelde hersteltijd.

IS.I.OR.225 Reactie op door de bevoegde autoriteit gemelde bevindingen

a) Na ontvangst van de door de bevoegde autoriteit ingediende kennisgeving van bevindingen, moet de organisatie:

1) de fundamentele oorzaak of oorzaken van het geval van niet-naleving identificeren, alsook de factoren die ertoe hebben bijgedragen;

2) een corrigerend actieplan opstellen;

3) tot voldoening van de bevoegde autoriteit aantonen dat de niet-naleving is gecorrigeerd.

b) De in punt a) vermelde acties worden uitgevoerd binnen de met de bevoegde autoriteit overeengekomen termijn.

IS.I.OR.230 Regeling voor externe rapportage over informatiebeveiliging

a) De organisatie past een systeem voor informatiebeveiligingsmeldingen toe dat overeenstemt met de in Verordening (EU) nr. 376/2014 en de gedelegeerde en uitvoeringshandelingen daarvan vastgestelde eisen, als die verordening op de organisatie van toepassing is.

b) Onverminderd de verplichtingen van Verordening (EU) nr. 376/2014 ziet de organisatie erop toe dat alle incidenten of kwetsbaarheden op het gebied van informatiebeveiliging die een aanzienlijk risico voor de veiligheid van de luchtvaart kunnen vormen, aan hun bevoegde autoriteit worden gemeld. Bovendien:

1) als een incident of kwetsbaarheid gevolgen heeft voor een luchtvaartuig of bijbehorende systemen of componenten, moet de organisatie dit ook melden aan de houder van de ontwerpgoedkeuring;

2) als een incident of kwetsbaarheid gevolgen heeft voor door de organisatie gebruikte systemen of onderdelen, moet de organisatie dit melden aan de organisatie die verantwoordelijk is voor het ontwerp van het systeem of onderdeel.

c) De organisatie rapporteert de in punt b) bedoelde omstandigheden als volgt:

1) zodra de organisatie weet krijgt van de omstandigheid, wordt een kennisgeving ingediend bij de bevoegde autoriteit en, indien van toepassing, de houder van de ontwerpgoedkeuring of de organisatie die verantwoordelijk is voor het ontwerp van het systeem of onderdeel;

2) zo snel mogelijk, maar uiterlijk 72 uur na het tijdstip waarop de organisatie weet heeft gekregen van de omstandigheid, tenzij uitzonderlijke omstandigheden dit verhinderen, wordt een verslag ingediend bij de bevoegde autoriteit en, indien van toepassing, de houder van de ontwerpgoedkeuring of de organisatie die verantwoordelijk is voor het ontwerp van het systeem of onderdeel.

Het verslag wordt opgesteld in de door de bevoegde autoriteit bepaalde vorm en bevat alle relevante informatie over de omstandigheid waar de organisatie weet van heeft;

3) er wordt een follow-upverslag ingediend bij de bevoegde autoriteit en, indien van toepassing, de houder van de ontwerpgoedkeuring of de organisatie die verantwoordelijk is voor het ontwerp van het systeem of onderdeel, met nadere informatie over de acties die de organisatie heeft genomen of voornemens is te nemen om van het incident te herstellen en de acties die zij voornemens is te nemen om soortgelijke informatiebeveiligingsincidenten in de toekomst te voorkomen.

Het follow-upverslag wordt ingediend zodra deze maatregelen zijn vastgesteld, en wordt opgesteld in de door de bevoegde autoriteit vastgestelde vorm.

IS.I.OR.235 Uitbesteding van activiteiten op het gebied van informatiebeveiligingsbeheer

a) De organisatie ziet erop toe dat bij het uitbesteden van een deel van de in IS.I.OR.200 bedoelde activiteiten aan andere organisaties, de uitbestede activiteiten voldoen aan de eisen van deze verordening en dat de gecontracteerde organisatie onder haar toezicht werkt. De organisatie zorgt ervoor dat de risico's in verband met de uitbestede activiteiten op passende wijze worden beheerd.

b) De organisatie ziet erop toe dat de bevoegde autoriteit op verzoek toegang krijgt tot de gecontracteerde organisatie om na te gaan of zij blijvend de in deze verordening vastgestelde toepasselijke eisen naleeft.

IS.I.OR.240 Personeelsvoorschriften

a) De verantwoordelijke manager van de organisatie die is aangewezen overeenkomstig Verordeningen (EU) nr. 1321/2014, (EU) nr. 965/2012, (EU) nr. 1178/2011 en (EU) 2015/340, Uitvoeringsverordening (EU) 2017/373 of Uitvoeringsverordening (EU) 2021/664, als bedoeld in artikel 2, lid 1, van deze verordening, heeft binnen de organisatie de bevoegdheid om ervoor te zorgen dat alle krachtens deze verordening vereiste activiteiten kunnen worden gefinancierd en uitgevoerd. Die persoon moet:

1) ervoor zorgen dat alle nodige middelen beschikbaar zijn om aan de voorschriften van deze verordening te voldoen;

2) het in IS.I.OR.200, a), 1), bedoelde informatiebeveiligingsbeleid vaststellen en bevorderen;

3) blijk te geven van een fundamenteel begrip van deze verordening.

b) De verantwoordelijke manager benoemt een persoon of een groep personen die ervoor moet zorgen dat de organisatie voldoet aan de eisen van deze verordening, en stelt de reikwijdte van hun bevoegdheden vast. Die persoon of groep personen brengt rechtstreeks verslag uit aan de verantwoordelijke manager en beschikt over de nodige kennis, achtergrond en ervaring om zich van zijn verantwoordelijkheden te kwijten. Voorts wordt ook vastgesteld wie bij langdurige afwezigheid van een bepaalde persoon als plaatsvervanger optreedt.

c) De verantwoordelijke manager benoemt een persoon of een groep personen die verantwoordelijk is voor het beheer van de in IS.I.OR.200, a), 12), bedoelde functie voor toezicht op de naleving.

d) Als de organisatie organisatorische structuren, beleidslijnen, processen en procedures voor informatiebeveiliging deelt met andere organisaties of met afdelingen van de eigen organisatie die niet onder de goedkeuring of verklaring vallen, mag de verantwoordelijke manager zijn activiteiten delegeren aan een gemeenschappelijke verantwoordelijke persoon.

In dat geval worden coördinatiemaatregelen vastgesteld tussen de verantwoordelijke manager en de gemeenschappelijke verantwoordelijke persoon om de passende integratie van het informatiebeveiligingsbeheer in de organisatie te waarborgen.

e) De verantwoordelijke manager of de in punt d) bedoelde gemeenschappelijke verantwoordelijke persoon, is binnen de organisatie bevoegd voor de vaststelling en instandhouding van de organisatorische structuren, het beleid en de processen en procedures die nodig zijn voor de uitvoering van IS.I.OR.200.

f) De organisatie beschikt over een proces om ervoor te zorgen dat zij over voldoende personeel beschikt om de onder deze bijlage vallende activiteiten uit te voeren.

g) De organisatie beschikt over een proces om ervoor te zorgen dat het in punt f) bedoelde personeel over de nodige bekwaamheid beschikt om zijn taken uit te voeren.

h) De organisatie beschikt over een proces om ervoor te zorgen dat het personeel de aan de toegewezen rollen en taken verbonden verantwoordelijkheden erkent.

i) De organisatie zorgt ervoor dat de identiteit en betrouwbaarheid van het personeel dat toegang heeft tot informatiesystemen en gegevens waarop de eisen van deze verordening van toepassing zijn, op passende wijze worden vastgesteld.

IS.I.OR.245 Bijhouden van gegevens

a) *De organisatie houdt gegevens bij over haar activiteiten op het gebied van informatiebeveiligingsbeheer.*

1) De organisatie zorgt ervoor dat de volgende gegevens worden gearchiveerd en traceerbaar zijn:

i) alle ontvangen goedkeuringen en eventuele bijbehorende beoordelingen van de informatiebeveiligingsrisico's overeenkomstig IS.I.OR.200, e);

ii) contracten voor de in IS.I.OR.200, a), 9), bedoelde activiteiten;

iii) gegevens over de in IS.I.OR.200, d), bedoelde cruciale processen;

iv) gegevens over de risico's die zijn vastgesteld tijdens de in IS.I.OR.205 bedoelde risicobeoordeling, samen met de in IS.I.OR.210 bedoelde maatregelen voor het behandelen van die risico's;

v) gegevens over informatiebeveiligingsincidenten en kwetsbaarheden die gerapporteerd zijn overeenkomstig de in IS.I.OR.215 en IS.I.OR.230 bedoelde rapportageregelingen;

vi) gegevens over informatiebeveiligingsvoorvallen die mogelijk opnieuw moeten worden beoordeeld om onopgespoorde informatiebeveiligingsincidenten of kwetsbaarheden te ontdekken.

2) De in punt 1), i), bedoelde gegevens worden bewaard gedurende minstens 5 jaar nadat de geldigheid van de goedkeuring is verstreken.

3) De in punt 1), ii), bedoelde gegevens worden bewaard gedurende minstens 5 jaar nadat het contract is gewijzigd of beëindigd.

4) De in punt 1), iii), iv) en v), bedoelde gegevens worden minstens 5 jaar bewaard.

5) De in punt 1), vi), bedoelde gegevens worden bewaard totdat die informatiebeveiligingsvoorvallen opnieuw zijn beoordeeld overeenkomstig een frequentie die is vastgesteld in een door de organisatie opgestelde procedure.

b) *De organisatie houdt gegevens bij over de kwalificaties en ervaring van haar eigen personeel dat betrokken is bij activiteiten op het gebied van informatiebeveiligingsbeheer.*

1) De gegevens over de kwalificaties en ervaring van het personeel worden bewaard zolang de persoon in kwestie voor de organisatie werkt, en gedurende minstens 3 jaar nadat hij de organisatie heeft verlaten.

2) Indien personeelsleden daarom verzoeken, moeten zij toegang krijgen tot hun persoonlijke gegevens. Wanneer zij de organisatie verlaten, moet de organisatie hen, op verzoek, een kopie geven van hun individuele gegevens.

c) De vorm van de gegevens wordt gespecificeerd in de procedures van de organisatie.

d) De gegevens worden zodanig opgeslagen dat zij beschermd zijn tegen schade, wijziging en diefstal, waarbij de informatie, indien vereist, wordt geïdentificeerd volgens rubriceringsniveau. De organisatie zorgt ervoor dat de gegevens worden opgeslagen met behulp van middelen die de integriteit, authenticiteit en geautoriseerde toegang waarborgen.

IS.I.OR.250 Handboek informatiebeveiligingsbeheer

a) De organisatie verstrekt de bevoegde autoriteit een handboek informatiebeveiligingsbeheer en, indien van toepassing, alle bijbehorende handleidingen en procedures, die het volgende bevatten:

1) een door de verantwoordelijke manager ondertekende verklaring waarbij wordt bevestigd dat de organisatie te allen tijde haar werkzaamheden zal verrichten in overeenstemming met deze bijlage en het handboek informatiebeveiligingsbeheer; Indien de verantwoordelijke manager niet de chief executive officer (CEO) van de organisatie is, moet de CEO de verklaring medeondertekenen;

2) de titel(s), na(a)m(en), taken, aansprakelijkheden, verantwoordelijkheden en bevoegdheden van de in IS.I.OR.240, b) en c), bedoelde persoon of personen;

3) de titel, naam, taken, aansprakelijkheden, verantwoordelijkheden en bevoegdheid van de in IS.I.OR.240, d), bedoelde gemeenschappelijke verantwoordelijke persoon, indien van toepassing;

4) het informatiebeveiligingsbeleid van de organisatie, zoals bedoeld in IS.I.OR.200, a), 1);

5) een algemene beschrijving van het aantal en de categorieën personeelsleden en van het systeem om de beschikbaarheid van personeel te plannen, zoals vereist bij IS.I.OR.240;

6) de titel(s), na(a)m(en), taken, aansprakelijkheden, verantwoordelijkheden en bevoegdheden van de belangrijkste personen die verantwoordelijk zijn voor de uitvoering van IS.I.OR.200, met inbegrip van de persoon of personen die verantwoordelijk is (zijn) voor de in IS.I.OR.200, a), 12), bedoelde functie toezicht op de naleving;

7) een organisatieschema met de bijbehorende aansprakelijkheids- en verantwoordelijkheidsketens voor de in de punten 2) en 6) bedoelde personen;

8) de beschrijving van het in IS.I.OR.215 bedoelde interne rapportagesysteem;

9) de procedures waarin gespecificeerd is hoe de organisatie de naleving van dit deel waarborgt, en met name:

i) de in IS.I.OR.200, punt c), bedoelde documentatie;

ii) de procedures die bepalen hoe de organisatie de in IS.I.OR.200, a), 9), bedoelde gecontracteerde activiteiten controleert;

iii) de procedure voor de wijziging van het in punt c) bedoelde handboek informatiebeveiligingsbeheer;

10) de bijzonderheden van de op dit moment goedgekeurde alternatieve wijzen van naleving.

b) De eerste uitgave van het handboek informatiebeveiligingsbeheer wordt goedgekeurd en een kopie ervan wordt bewaard door de bevoegde autoriteit. Het handboek informatiebeveiligingsbeheer dient zo nodig te worden gewijzigd om een actuele beschrijving van het beheersysteem voor informatiebeveiliging van de organisatie te blijven bieden. Een kopie van eventuele wijzigingen van het handboek informatiebeveiligingsbeheer wordt verstrekt aan de bevoegde autoriteit.

c) Wijzigingen van het handboek informatiebeveiligingsbeheer worden beheerd volgens een door de organisatie vastgestelde procedure. Alle wijzigingen die buiten het toepassingsgebied van deze procedure vallen en alle amendementen van de in IS.I.OR.255, b), bedoelde wijzigingen moeten worden goedgekeurd door de bevoegde autoriteit.

d) De organisatie mag het handboek informatiebeveiligingsbeheer integreren met andere managementhandboeken of handleidingen, voor zover er een duidelijke kruisverwijzing is die aangeeft welke delen van het managementhandboek of de handleiding overeenstemmen met de verschillende eisen van deze bijlage.

IS.I.OR.255 Wijzigingen van het beheersysteem voor informatiebeveiliging

a) Wijzigingen van het beheersysteem voor informatiebeveiliging worden beheerd en meegedeeld aan de bevoegde autoriteit volgens een door de organisatie ontwikkelde procedure. Deze procedure moet worden goedgekeurd door de bevoegde autoriteit.

b) Voor wijzigingen van het beheersysteem voor informatiebeveiliging die niet onder de in punt a) bedoelde procedure vallen, moet de organisatie bij de bevoegde autoriteit een goedkeuring aanvragen en verkrijgen.

Wat deze wijzigingen betreft:

1) wordt de aanvraag ingediend alvorens een dergelijke wijziging wordt doorgevoerd, zodat de bevoegde autoriteit kan bepalen of er nog altijd wordt voldaan aan deze verordening en zo nodig het certificaat van de organisatie en de bijbehorende voorwaarden van de goedkeuring kan aanpassen;

2) verstrekt de organisatie aan de bevoegde autoriteit alle informatie die zij vraagt om de wijziging te evalueren;

3) worden ze pas doorgevoerd na ontvangst van een formele goedkeuring door de bevoegde autoriteit;

4) werkt de organisatie tijdens de uitvoering van dergelijke wijzigingen onder de door de bevoegde autoriteit voorgeschreven voorwaarden.

IS.I.OR.260 Permanente verbetering

a) De organisatie beoordeelt aan de hand van passende prestatie-indicatoren de doeltreffendheid en maturiteit van het beheersysteem voor informatiebeveiliging. Die beoordeling wordt uitgevoerd op basis van een vooraf door de organisatie vastgestelde kalender of na een informatiebeveiligingsincident.

b) Als na de overeenkomstig punt a) uitgevoerde beoordeling tekortkomingen worden vastgesteld, neemt de organisatie de nodige verbeteringsmaatregelen om te garanderen dat het beheersysteem voor informatiebeveiliging blijft voldoen aan de toepasselijke eisen en de informatiebeveiligingsrisico's op een aanvaardbaar niveau handhaaft. De organisatie zal de elementen van het beheersysteem voor informatiebeveiliging die onder de vastgestelde maatregelen vallen, opnieuw beoordelen.

BIJLAGE III

Bijlagen VI (deel-ARA) en VII (deel-ORA) bij Verordening (EU) nr. 1178/2011 worden als volgt gewijzigd:

1) Bijlage VI (deel-ARA) wordt als volgt gewijzigd:

a) aan ARA.GEN.125 wordt het volgende punt c) toegevoegd:

"c) De bevoegde autoriteit van de lidstaat verstrekt het Agentschap zo spoedig mogelijk veiligheidsrelevante informatie die afkomstig is van de informatiebeveiligingsrapporten die zij heeft ontvangen overeenkomstig punt IS.I.OR.230 van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203";

b) na punt ARA.GEN.135 wordt het volgende punt ARA.GEN.135A ingevoegd:

"**ARA.GEN.135A Onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart**

a) De bevoegde autoriteit past een systeem toe voor het op passende wijze verzamelen, analyseren en verspreiden van informatie over incidenten en kwetsbaarheden op het gebied van informatiebeveiliging met mogelijke gevolgen voor de veiligheid van de luchtvaart die door organisaties worden gemeld. Dit gebeurt in coördinatie met alle andere relevante autoriteiten die binnen de lidstaat verantwoordelijk zijn voor informatiebeveiliging of cyberbeveiliging om de coördinatie en compatibiliteit van meldingsregelingen te verbeteren.

b) Het Agentschap voert een systeem in om alle veiligheidsrelevante informatie die is ontvangen overeenkomstig ARA.GEN.125, punt c), op passende wijze te analyseren en verstrekt de lidstaten en de Commissie zonder onnodige vertraging alle informatie, met inbegrip van aanbevelingen of te nemen corrigerende maatregelen, die zij nodig hebben om tijdig te kunnen reageren op een informatiebeveiligingsincident of kwetsbaarheid met mogelijke gevolgen voor de luchtvaartveiligheid met betrekking tot producten, onderdelen, niet-geïnstalleerde apparatuur, personen of organisaties die onder Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan vallen.

c) Na ontvangst van de in de punten a) en b) bedoelde informatie neemt de bevoegde autoriteit passende maatregelen om de mogelijke gevolgen van het informatiebeveiligingsincident of de kwetsbaarheid voor de veiligheid van de luchtvaart aan te pakken.

d) Overeenkomstig punt c) genomen maatregelen moeten onmiddellijk ter kennis worden gebracht van alle personen of organisaties die daaraan moeten voldoen krachtens Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan. De bevoegde autoriteit van de lidstaat stelt ook het Agentschap in kennis van deze maatregelen, alsmede de bevoegde autoriteiten van de andere betrokken lidstaten in zoverre gecombineerd optreden vereist is.";

c) aan ARA.GEN.200 wordt het volgende punt e) toegevoegd:

"e) Naast de eisen van punt a) moet het door de bevoegde autoriteit opgezette en onderhouden beheersysteem voldoen aan bijlage I (Deel-IS.AR) bij Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.";

d) ARA.GEN.205 wordt als volgt gewijzigd:

i) de titel wordt vervangen door:

"**ARA.GEN.205 Toewijzing van taken**";

ii) het volgende punt c) wordt toegevoegd:

"c) Met betrekking tot de certificering van en het toezicht op de naleving van ORA.GEN.200A door de organisatie kan de bevoegde autoriteit taken toewijzen aan gekwalificeerde entiteiten overeenkomstig punt a) of aan elke relevante autoriteit die verantwoordelijk is voor informatiebeveiliging of cyberbeveiliging in de lidstaat. Bij het toewijzen van deze taken zorgt de bevoegde autoriteit ervoor dat:

1) alle aspecten in verband met luchtvaartveiligheid worden gecoördineerd en in aanmerking genomen door de gekwalificeerde entiteit of de relevante autoriteit;

2) de resultaten van de certificerings- en toezichtsactiviteiten die door de gekwalificeerde entiteit of de relevante autoriteit worden uitgevoerd, zijn opgenomen in de algemene certificerings- en toezichtsdossiers van de organisatie;

3) haar eigen beheersysteem voor informatiebeveiliging, dat is opgezet overeenkomstig ARA.GEN.200, punt e), alle taken op het gebied van certificering en permanent toezicht die namens haar worden uitgevoerd, bestrijkt.";

e) aan ARA.GEN.300 wordt het volgende punt g) toegevoegd:

"g) Met betrekking tot de certificering van en het toezicht op de naleving van ORA.GEN.200A door de organisatie evalueert de bevoegde autoriteit, naast de punten a) tot en met f), elke goedkeuring die is verleend uit hoofde van IS.I.OR.200, punt e), van deze verordening of IS.D.OR.200, punt e), van Gedelegeerde Verordening (EU) 2022/1645 na de toepasselijke auditcyclus en telkens wanneer wijzigingen worden doorgevoerd in de reikwijdte van de werkzaamheden van de organisatie.";

f) na ARA.GEN.330 wordt ARA.GEN.330A ingevoegd:

"**ARA.GEN.330A Wijzigingen van het beheersysteem voor informatiebeveiliging**

a) Met betrekking tot wijzigingen die worden beheerd en meegedeeld aan de bevoegde autoriteit overeenkomstig de procedure van IS.I.OR.255, punt a), van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203, neemt de bevoegde autoriteit de beoordeling van deze wijzigingen op in haar permanente toezicht overeenkomstig de beginselen van punt ARA.GEN.300. Wanneer een geval van niet-naleving wordt vastgesteld, stelt de bevoegde autoriteit de organisatie daarvan in kennis, vraagt zij verdere wijzigingen en handelt zij overeenkomstig ARA.GEN.350.

b) Met betrekking tot andere wijzigingen waarvoor een erkenningsaanvraag vereist is overeenkomstig IS.I.OR.255, punt b), van bijlage II (deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203:

1) controleert de bevoegde autoriteit, bij ontvangst van de wijzigingsaanvraag, of de organisatie aan de toepasselijke eisen voldoet alvorens de erkenning af te geven;

2) stelt de bevoegde autoriteit de voorwaarden vast waaronder de organisatie tijdens de uitvoering van de wijziging haar activiteiten mag uitvoeren;

3) keurt de bevoegde autoriteit de wijziging goed als zij ervan overtuigd is dat de organisatie voldoet aan de toepasselijke eisen.".

2) Bijlage VII (deel-ORA) wordt als volgt gewijzigd:

na ORA.GEN.200 wordt ORA.GEN.200A ingevoegd:

"**ORA.GEN.200A Beheersysteem voor informatiebeveiliging**

Naast het bij punt ORA.GEN.200 vereiste beheersysteem moet de organisatie een beheersysteem voor informatiebeveiliging opzetten, toepassen en onderhouden overeenkomstig Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.".

BIJLAGE IV

Bijlage I (deel 21) bij Verordening (EU) nr. 748/2012 wordt als volgt gewijzigd:

1) De inhoudsopgave wordt als volgt gewijzigd:

a) na 21.B.20 wordt de volgende titel ingevoegd:

"21.B.20A Onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart";

b) de titel van 21.B.30 wordt vervangen door:

"21.B.30 Toewijzing van taken";

c) na 21.B.240 wordt de volgende titel ingevoegd:

"21.B.240A Wijzigingen van het beheersysteem voor informatiebeveiliging";

d) na 21.B.435 wordt de volgende titel ingevoegd:

"21.B.435A Wijzigingen van het beheersysteem voor informatiebeveiliging".

2) Aan 21.B.15 wordt het volgende punt c) toegevoegd:

"c) De bevoegde autoriteit van de lidstaat verstrekt het Agentschap zo spoedig mogelijk veiligheidsrelevante informatie die afkomstig is van de informatiebeveiligingsrapporten die zij heeft ontvangen overeenkomstig punt IS.D.OR.230 van de bijlage (Deel-IS.D.OR) bij Gedelegeerde Verordening (EU) 2022/1645.".

3) Na 21.B.20 wordt 21.B.20A ingevoegd:

"21.B.20A Onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart

a) De bevoegde autoriteit past een systeem toe voor het op passende wijze verzamelen, analyseren en verspreiden van informatie over incidenten en kwetsbaarheden op het gebied van informatiebeveiliging met mogelijke gevolgen voor de veiligheid van de luchtvaart die door organisaties worden gemeld. Dit gebeurt in coördinatie met alle andere relevante autoriteiten die binnen de lidstaat verantwoordelijk zijn voor informatiebeveiliging of cyberbeveiliging om de coördinatie en compatibiliteit van meldingsregelingen te verbeteren.

b) Het Agentschap voert een systeem in om alle veiligheidsrelevante informatie die is ontvangen overeenkomstig 21.B.15, punt c), op passende wijze te analyseren en verstrekt de lidstaten en de Commissie zonder onnodige vertraging alle informatie, met inbegrip van aanbevelingen of te nemen corrigerende maatregelen, die zij nodig hebben om tijdig te kunnen reageren op een informatiebeveiligingsincident of kwetsbaarheid met mogelijke gevolgen voor de luchtvaartveiligheid met betrekking tot producten, onderdelen, niet-geïnstalleerde apparatuur, personen of organisaties die onder Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan vallen.

c) Na ontvangst van de in de punten a) en b) bedoelde informatie neemt de bevoegde autoriteit passende maatregelen om de mogelijke gevolgen van het informatiebeveiligingsincident of de kwetsbaarheid voor de veiligheid van de luchtvaart aan te pakken.

d) Overeenkomstig punt c) genomen maatregelen moeten onmiddellijk ter kennis worden gebracht van alle personen of organisaties die daaraan moeten voldoen krachtens Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan. De bevoegde autoriteit van de lidstaat stelt ook het Agentschap in kennis van deze maatregelen, alsmede de bevoegde autoriteiten van de andere betrokken lidstaten in zoverre gecombineerd optreden vereist is.".

4) Aan 21.B.25 wordt het volgende punt e) toegevoegd:

"e) Naast de eisen van punt a) moet het door de bevoegde autoriteit opgezette en onderhouden beheersysteem voldoen aan bijlage I (Deel-IS.AR) bij Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.".

5) 21.B.30 wordt als volgt gewijzigd:

a) de titel wordt vervangen door:

“21.B.30 Toewijzing van taken”;

b) het volgende punt c) wordt toegevoegd:

“c) Voor de certificering van en het toezicht op de naleving van 21.A.139A en 21.A.239A door de organisatie kan de bevoegde autoriteit taken toewijzen aan gekwalificeerde entiteiten overeenkomstig punt a) of aan elke relevante autoriteit die verantwoordelijk is voor informatiebeveiliging of cyberbeveiliging in de lidstaat. Bij het toewijzen van deze taken zorgt de bevoegde autoriteit ervoor dat:

1) alle aspecten in verband met luchtvaartveiligheid worden gecoördineerd en in aanmerking genomen door de gekwalificeerdeentiteit of de relevante autoriteit;

2) de resultaten van de certificerings- en toezichtsactiviteiten die door de gekwalificeerde entiteit of de relevante autoriteit worden uitgevoerd, zijn opgenomen in de algemene certificerings- en toezichtsdossiers van de organisatie;

3) haar eigen beheersysteem voor informatiebeveiliging, dat is opgezet overeenkomstig 21.B.25, punt e), alle taken op het gebied van certificering en permanent toezicht die namens haar worden uitgevoerd, bestrijkt.”.

6) Aan 21.B.221 wordt het volgende punt g) toegevoegd:

“g) Met betrekking tot de certificering van en het toezicht op de naleving van 21.A.139A door de organisatie evalueert de bevoegde autoriteit, naast de punten a) tot en met f), elke goedkeuring die is verleend uit hoofde van IS.I.OR.200, punt e), van deze verordening of IS.D.OR.200, punt e), van Gedelegeerde Verordening (EU) 2022/1645 na de toepasselijke auditcyclus en telkens wanneer wijzigingen worden doorgevoerd in de reikwijdte van de werkzaamheden van de organisatie.”.

7) Na 21.B.240 wordt 21.B.240A ingevoegd:

“**21.B.240A Wijzigingen van het beheersysteem voor informatiebeveiliging**

a) Voor wijzigingen die worden beheerd en meegedeeld aan de bevoegde autoriteit overeenkomstig de procedure van IS.D.OR.255, punt a), van de bijlage (Deel-IS.D.OR) bij Gedelegeerde Verordening (EU) 2022/1645, neemt de bevoegde autoriteit de beoordeling van deze wijzigingen op in haar permanente toezicht overeenkomstig de beginselen van punt 21.B.221. Wanneer een geval van niet-naleving wordt vastgesteld, stelt de bevoegde autoriteit de organisatie daarvan in kennis, vraagt zij verdere wijzigingen en handelt zij overeenkomstig 21.B.225.

b) Met betrekking tot andere wijzigingen waarvoor een erkenningsaanvraag vereist is overeenkomstig IS.D.OR.255, punt b), van de bijlage (deel-IS.D.OR) bij Gedelegeerde Verordening (EU) 2022/1645:

1) controleert de bevoegde autoriteit, bij ontvangst van de wijzigingsaanvraag, of de organisatie aan de toepasselijke eisen voldoet alvorens de erkenning af te geven;

2) stelt de bevoegde autoriteit de voorwaarden vast waaronder de organisatie tijdens de uitvoering van de wijziging haar activiteiten mag uitvoeren;

3) keurt de bevoegde autoriteit de wijziging goed als zij ervan overtuigd is dat de organisatie voldoet aan de toepasselijke eisen.”.

8) Aan 21.B.431 wordt het volgende punt d) toegevoegd:

“d) Voor de certificering van en het toezicht op de naleving door de organisatie van punt 21.A.239A moet de bevoegde autoriteit niet alleen voldoen aan de punten a), b) en c), maar ook aan de volgende beginselen:

1) de bevoegde autoriteit beoordeelt de interfaces en de bijbehorende risico's die zijn vastgesteld overeenkomstig IS.D.OR.205, punt b), van de bijlage (Deel-IS.D.OR) bij Gedelegeerde Verordening (EU) 2022/1645 door elke organisatie die onder haar toezicht staat;

2) indien er discrepanties worden vastgesteld in de onderlinge interfaces en de daaraan verbonden risico's die door verschillende organisaties zijn vastgesteld, evalueert de bevoegde autoriteit deze samen met de betrokken organisaties en brengt zij, indien nodig, passende bevindingen uit om ervoor te zorgen dat corrigerende maatregelen worden uitgevoerd;

3) indien uit de overeenkomstig punt 2) onderzochte documentatie blijkt dat er significante risico's bestaan in verband met interfaces met organisaties die onder toezicht staan van een andere bevoegde autoriteit in dezelfde lidstaat, wordt deze informatie meegedeeld aan de overeenkomstige bevoegde autoriteit.".

9) Na 21.B.435 wordt 21.B.435A ingevoegd:

"**21.B.435A Wijzigingen van het beheersysteem voor informatiebeveiliging**

a) Voor wijzigingen die worden beheerd en meegedeeld aan de bevoegde autoriteit overeenkomstig de procedure van IS.D.OR.255, punt a), van de bijlage (Deel-IS.D.OR) bij Gedelegeerde Verordening (EU) 2022/1645, neemt de bevoegde autoriteit de beoordeling van deze wijzigingen op in haar permanente toezicht overeenkomstig de beginselen van punt 21.B.431. Wanneer een geval van niet-naleving wordt vastgesteld, stelt de bevoegde autoriteit de organisatie daarvan in kennis, vraagt zij verdere wijzigingen en handelt zij overeenkomstig 21.B.433.

b) Met betrekking tot andere wijzigingen waarvoor een erkenningsaanvraag vereist is overeenkomstig IS.D.OR.255, punt b), van de bijlage (deel-IS.D.OR) bij Gedelegeerde Verordening (EU) 2022/1645:

1) controleert de bevoegde autoriteit, bij ontvangst van de wijzigingsaanvraag, of de organisatie aan de toepasselijke eisen voldoet alvorens de erkenning af te geven;

2) stelt de bevoegde autoriteit de voorwaarden vast waaronder de organisatie tijdens de uitvoering van de wijziging haar activiteiten mag uitvoeren;

3) keurt de bevoegde autoriteit de wijziging goed als zij ervan overtuigd is dat de organisatie voldoet aan de toepasselijke eisen.".

BIJLAGE V

Bijlagen II (deel-ARO) en III (deel-ORO) bij Verordening (EU) nr. 965/2012 worden als volgt gewijzigd:

1) Bijlage II (deel-ARO) wordt als volgt gewijzigd:

a) aan ARO.GEN.125 wordt het volgende punt c) toegevoegd:

"c) De bevoegde autoriteit van de lidstaat verstrekt het Agentschap zo spoedig mogelijk veiligheidsrelevante informatie die afkomstig is van de informatiebeveiligingsrapporten die zij heeft ontvangen overeenkomstig punt IS.I.OR.230 van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203.";

b) na ARO.GEN.135 wordt ARO.GEN.135A ingevoegd:

"**ARO.GEN.135A Onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart**

a) De bevoegde autoriteit past een systeem toe voor het op passende wijze verzamelen, analyseren en verspreiden van informatie over incidenten en kwetsbaarheden op het gebied van informatiebeveiliging met mogelijke gevolgen voor de veiligheid van de luchtvaart die door organisaties worden gemeld. Dit gebeurt in coördinatie met alle andere relevante autoriteiten die binnen de lidstaat verantwoordelijk zijn voor informatiebeveiliging of cyberbeveiliging om de coördinatie en compatibiliteit van meldingsregelingen te verbeteren.

b) Het Agentschap voert een systeem in om alle veiligheidsrelevante informatie die is ontvangen overeenkomstig ARO.GEN.125, punt c), op passende wijze te analyseren en verstrekt de lidstaten en de Commissie zonder onnodige vertraging alle informatie, met inbegrip van aanbevelingen of te nemen corrigerende maatregelen, die zij nodig hebben om tijdig te kunnen reageren op een informatiebeveiligingsincident of kwetsbaarheid met mogelijke gevolgen voor de luchtvaartveiligheid met betrekking tot producten, onderdelen, niet-geïnstalleerde apparatuur, personen of organisaties die onder Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan vallen.

c) Na ontvangst van de in de punten a) en b) bedoelde informatie neemt de bevoegde autoriteit passende maatregelen om de mogelijke gevolgen van het informatiebeveiligingsincident of de kwetsbaarheid voor de veiligheid van de luchtvaart aan te pakken.

d) Overeenkomstig punt c) genomen maatregelen moeten onmiddellijk ter kennis worden gebracht van alle personen of organisaties die daaraan moeten voldoen krachtens Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan. De bevoegde autoriteit van de lidstaat stelt ook het Agentschap in kennis van deze maatregelen, alsmede de bevoegde autoriteiten van de andere betrokken lidstaten in zoverre gecombineerd optreden vereist is.";

c) aan ARO.GEN.200 wordt het volgende punt e) toegevoegd:

"e) Naast de eisen van punt a) moet het door de bevoegde autoriteit opgezette en onderhouden beheersysteem voldoen aan bijlage I (Deel-IS.AR) bij Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.";

d) ARO.GEN.205 wordt als volgt gewijzigd:

i) de titel wordt vervangen door:

"**ARO.GEN.205 Toewijzing van taken**";

ii) het volgende punt c) wordt toegevoegd:

"c) Voor de certificering van en het toezicht op de naleving van ORO.GEN.200A door de organisatie kan de bevoegde autoriteit taken toewijzen aan gekwalificeerde entiteiten overeenkomstig punt a) of aan elke relevante autoriteit die verantwoordelijk is voor informatiebeveiliging of cyberbeveiliging in de lidstaat. Bij het toewijzen van deze taken zorgt de bevoegde autoriteit ervoor dat:

1) alle aspecten in verband met luchtvaartveiligheid worden gecoördineerd en in aanmerking genomen door de gekwalificeerde entiteit of de relevante autoriteit;

2) de resultaten van de certificerings- en toezichtsactiviteiten die door de gekwalificeerde entiteit of de relevante autoriteit worden uitgevoerd, zijn opgenomen in de algemene certificerings- en toezichtsdossiers van de organisatie;

3) haar eigen beheersysteem voor informatiebeveiliging, dat is opgezet overeenkomstig ARO.GEN.200, punt e), alle taken op het gebied van certificering en permanent toezicht die namens haar worden uitgevoerd, bestrijkt.";

e) aan ARO.GEN.300 wordt het volgende punt g) toegevoegd:

"g) Met betrekking tot de certificering van en het toezicht op de naleving van ORO.GEN.200A door de organisatie evalueert de bevoegde autoriteit, naast de punten a) tot en met f), elke goedkeuring die is verleend uit hoofde van IS.I.OR.200, punt e), van deze verordening of IS.D.OR.200, punt e), van Gedelegeerde Verordening (EU) 2022/1645 na de toepasselijke auditcyclus en telkens wanneer wijzigingen worden doorgevoerd in de reikwijdte van de werkzaamheden van de organisatie.";

f) na ARO.GEN.330 wordt ARO.GEN.330A ingevoegd:

"**ARO.GEN.330A Wijzigingen van het beheersysteem voor informatiebeveiliging**

a) Voor wijzigingen die worden beheerd en meegedeeld aan de bevoegde autoriteit overeenkomstig de procedure van IS.I.OR.255, punt a), van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203, neemt de bevoegde autoriteit de beoordeling van deze wijzigingen op in haar permanente toezicht overeenkomstig de beginselen van punt ARO.GEN.300. Wanneer een geval van niet-naleving wordt vastgesteld, stelt de bevoegde autoriteit de organisatie daarvan in kennis, vraagt zij verdere wijzigingen en handelt zij overeenkomstig ARO.GEN.350.

b) Met betrekking tot andere wijzigingen waarvoor een erkenningsaanvraag vereist is overeenkomstig IS.I.OR.255, punt b), van bijlage II (deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203:

1) controleert de bevoegde autoriteit, bij ontvangst van de wijzigingsaanvraag, of de organisatie aan de toepasselijke eisen voldoet alvorens de erkenning af te geven;

2) stelt de bevoegde autoriteit de voorwaarden vast waaronder de organisatie tijdens de uitvoering van de wijziging haar activiteiten mag uitvoeren;

3) keurt de bevoegde autoriteit de wijziging goed als zij ervan overtuigd is dat de organisatie voldoet aan de toepasselijke eisen.".

2) Bijlage III (deel-ORO) wordt als volgt gewijzigd:

na ORO.GEN.200 wordt ORO.GEN.200A ingevoegd:

"**ORO.GEN.200A Beheersysteem voor informatiebeveiliging**

Naast het bij punt ORO.GEN.200 vereiste beheersysteem moet de organisatie een beheersysteem voor informatiebeveiliging opzetten, toepassen en onderhouden overeenkomstig Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.".

BIJLAGE VI

Bijlage II (Deel-ADR.AR) bij Verordening (EU) nr. 139/2014 wordt als volgt gewijzigd:

1) Aan ADR.AR.A.025 wordt het volgende punt c) toegevoegd:

"c) De bevoegde autoriteit van de lidstaat verstrekt het Agentschap zo spoedig mogelijk veiligheidsrelevante informatie die afkomstig is van de informatiebeveiligingsrapporten die zij heeft ontvangen overeenkomstig punt IS.D.OR.230 van de bijlage (Deel-IS.D.OR) bij Gedelegeerde Verordening (EU) 2022/1645.".

2) Na ADR.AR.A.030 wordt ADR.AR.A.030A ingevoegd:

"**ADR.AR.A.030A Onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart**

a) De bevoegde autoriteit past een systeem toe voor het op passende wijze verzamelen, analyseren en verspreiden van informatie over incidenten en kwetsbaarheden op het gebied van informatiebeveiliging met mogelijke gevolgen voor de veiligheid van de luchtvaart die door organisaties worden gemeld. Dit gebeurt in coördinatie met alle andere relevante autoriteiten die binnen de lidstaat verantwoordelijk zijn voor informatiebeveiliging of cyberbeveiliging om de coördinatie en compatibiliteit van meldingsregelingen te verbeteren.

b) Het Agentschap voert een systeem in om alle veiligheidsrelevante informatie die is ontvangen overeenkomstig ADR.AR.A.025, punt c), op passende wijze te analyseren en verstrekt de lidstaten en de Commissie zonder onnodige vertraging alle informatie, met inbegrip van aanbevelingen of te nemen corrigerende maatregelen, die zij nodig hebben om tijdig te kunnen reageren op een informatiebeveiligingsincident of kwetsbaarheid met mogelijke gevolgen voor de luchtvaartveiligheid met betrekking tot producten, onderdelen, niet-geïnstalleerde apparatuur, personen of organisaties die onder Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan vallen.

c) Na ontvangst van de in de punten a) en b) bedoelde informatie neemt de bevoegde autoriteit passende maatregelen om de mogelijke gevolgen van het informatiebeveiligingsincident of de kwetsbaarheid voor de veiligheid van de luchtvaart aan te pakken.

d) Overeenkomstig punt c) genomen maatregelen moeten onmiddellijk ter kennis worden gebracht van alle personen of organisaties die daaraan moeten voldoen krachtens Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan. De bevoegde autoriteit van de lidstaat stelt ook het Agentschap in kennis van deze maatregelen, alsmede de bevoegde autoriteiten van de andere betrokken lidstaten in zoverre gecombineerd optreden vereist is.".

3) Aan ADR.AR.B.005 wordt het volgende punt d) toegevoegd:

"d) Naast de eisen van punt a) moet het door de bevoegde autoriteit opgezette en onderhouden beheersysteem voldoen aan bijlage I (Deel-IS.AR) bij Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.".

4) ADR.AR.B.010 wordt als volgt gewijzigd:

i) de titel wordt vervangen door:

"**ADR.AR.B.010 Toewijzing van taken**";

ii) het volgende punt c) wordt toegevoegd:

"c) Met betrekking tot de certificering van en het toezicht op de naleving van ADR.OR.D.005A door de organisatie kan de bevoegde autoriteit taken toewijzen aan gekwalificeerde entiteiten overeenkomstig punt a) of aan elke relevante autoriteit die verantwoordelijk is voor informatiebeveiliging of cyberbeveiliging in de lidstaat. Bij het toewijzen van deze taken zorgt de bevoegde autoriteit ervoor dat:

1) alle aspecten in verband met luchtvaartveiligheid worden gecoördineerd en in aanmerking genomen door de gekwalificeerde entiteit of de relevante autoriteit;

2) de resultaten van de certificerings- en toezichtsactiviteiten die door de gekwalificeerde entiteit of de relevante autoriteit worden uitgevoerd, zijn opgenomen in de algemene certificerings- en toezichtsdossiers van de organisatie;

3) haar eigen beheersysteem voor informatiebeveiliging, dat is opgezet overeenkomstig ADR.AR.B.005, punt e), alle taken op het gebied van certificering en permanent toezicht die namens haar worden uitgevoerd, bestrijkt.".

5) Aan ADR.AR.C.005 wordt het volgende punt f) toegevoegd:

"f) Met betrekking tot de certificering van en het toezicht op de naleving van ADR.OR.D.005A door de organisatie evalueert de bevoegde autoriteit, naast de punten a) tot en met e), elke goedkeuring die is verleend uit hoofde van IS.I.OR.200, punt e), van deze verordening of IS.D.OR.200, punt e), van Gedelegeerde Verordening (EU) 2022/1645 na de toepasselijke auditcyclus en telkens wanneer wijzigingen worden doorgevoerd in de reikwijdte van de werkzaamheden van de organisatie.".

6) Na ADR.AR.C.040 wordt ADR.AR.C.040A ingevoegd:

"**ADR.AR.C.040A Wijzigingen van het beheersysteem voor informatiebeveiliging**

a) Met betrekking tot wijzigingen die worden beheerd en meegedeeld aan de bevoegde autoriteit overeenkomstig de procedure van IS.D.OR.255, punt a), van de bijlage (Deel-IS.D.OR) bij Gedelegeerde Verordening (EU) 2022/1645, neemt de bevoegde autoriteit de beoordeling van deze wijzigingen op in haar permanente toezicht overeenkomstig de beginselen van punt ADR.AR.C.005. Wanneer een geval van niet-naleving wordt vastgesteld, stelt de bevoegde autoriteit de organisatie daarvan in kennis, vraagt zij verdere wijzigingen en handelt zij overeenkomstig ADR.AR.C.055.

b) Met betrekking tot andere wijzigingen waarvoor een erkenningsaanvraag vereist is overeenkomstig IS.D.OR.255, punt b), van de bijlage (deel-IS.D.OR) bij Gedelegeerde Verordening (EU) 2022/1645:

1) controleert de bevoegde autoriteit, bij ontvangst van de wijzigingsaanvraag, of de organisatie aan de toepasselijke eisen voldoet alvorens de erkenning af te geven;

2) stelt de bevoegde autoriteit de voorwaarden vast waaronder de organisatie tijdens de uitvoering van de wijziging haar activiteiten mag uitvoeren;

3) keurt de bevoegde autoriteit de wijziging goed als zij ervan overtuigd is dat de organisatie voldoet aan de toepasselijke eisen.".

BIJLAGE VII

Bijlagen II (deel-145), III (deel-66) en V quater (deel-CAMO) bij Verordening (EU) nr. 1321/2014 worden als volgt gewijzigd:

1) Bijlage II (deel-145) wordt als volgt gewijzigd:

a) de inhoudsopgave wordt als volgt gewijzigd:

i) na 145.A.200 wordt de volgende titel ingevoegd:

"145.A.200A Beheersysteem voor informatiebeveiliging";

ii) na 145.B.135 wordt de volgende titel ingevoegd:

"145.B.135A Onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart";

iii) de titel van 145.B.205 wordt vervangen door:

"145.B.205 Toewijzing van taken";

iv) na 145.B.330 wordt de volgende titel ingevoegd:

"145.B.330A Wijzigingen van het beheersysteem voor informatiebeveiliging";

b) na 145.A.200 wordt 145.A.200A ingevoegd:

"145.A.200A **Beheersysteem voor informatiebeveiliging**

Naast het bij punt 145.A.200 vereiste beheersysteem moet de organisatie een beheersysteem voor informatiebeveiliging opzetten, toepassen en onderhouden overeenkomstig Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.";

c) aan 145.B.125 wordt het volgende punt c) toegevoegd:

"c) De bevoegde autoriteit van de lidstaat verstrekt het Agentschap zo spoedig mogelijk veiligheidsrelevante informatie die afkomstig is van de informatiebeveiligingsrapporten die zij heeft ontvangen overeenkomstig punt IS.I.OR.230 van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203";

d) na 145.B.135 wordt 145.B.135A ingevoegd:

"145.B.135A **Onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart**

a) De bevoegde autoriteit past een systeem toe voor het op passende wijze verzamelen, analyseren en verspreiden van informatie over incidenten en kwetsbaarheden op het gebied van informatiebeveiliging met mogelijke gevolgen voor de veiligheid van de luchtvaart die door organisaties worden gemeld. Dit gebeurt in coördinatie met alle andere relevante autoriteiten die binnen de lidstaat verantwoordelijk zijn voor informatiebeveiliging of cyberbeveiliging om de coördinatie en compatibiliteit van meldingsregelingen te verbeteren.

b) Het Agentschap voert een systeem in om alle veiligheidsrelevante informatie die is ontvangen overeenkomstig 145.B.125, punt c), op passende wijze te analyseren en verstrekt de lidstaten en de Commissie zonder onnodige vertraging alle informatie, met inbegrip van aanbevelingen of te nemen corrigerende maatregelen, die zij nodig hebben om tijdig te kunnen reageren op een informatiebeveiligingsincident of kwetsbaarheid met mogelijke gevolgen voor de luchtvaartveiligheid met betrekking tot producten, onderdelen, niet-geïnstalleerde apparatuur, personen of organisaties die onder Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan vallen.

c) Na ontvangst van de in de punten a) en b) bedoelde informatie neemt de bevoegde autoriteit passende maatregelen om de mogelijke gevolgen van het informatiebeveiligingsincident of de kwetsbaarheid voor de veiligheid van de luchtvaart aan te pakken.

d) Overeenkomstig punt c) genomen maatregelen moeten onmiddellijk ter kennis worden gebracht van alle personen of organisaties die daaraan moeten voldoen krachtens Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan. De bevoegde autoriteit van de lidstaat stelt ook het Agentschap in kennis van deze maatregelen, alsmede de bevoegde autoriteiten van de andere betrokken lidstaten in zoverre gecombineerd optreden vereist is.";

e) Aan 145.B.200 wordt het volgende punt e) toegevoegd:

"e) Naast de eisen van punt a) moet het door de bevoegde autoriteit opgezette en onderhouden beheersysteem voldoen aan bijlage I (Deel-IS.AR) bij Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.";

f) 145.B.205 wordt als volgt gewijzigd:

i) de titel wordt vervangen door:

"145.B.205 **Toewijzing van taken**";

ii) het volgende punt c) wordt toegevoegd:

"c) Voor de certificering van en het toezicht op de naleving van 145.A.200A door de organisatie kan de bevoegde autoriteit taken toewijzen aan gekwalificeerde entiteiten overeenkomstig punt a) of aan elke relevante autoriteit die verantwoordelijk is voor informatiebeveiliging of cyberbeveiliging in de lidstaat. Bij het toewijzen van deze taken zorgt de bevoegde autoriteit ervoor dat:

1) alle aspecten in verband met luchtvaartveiligheid worden gecoördineerd en in aanmerking genomen door de gekwalificeerde entiteit of de relevante autoriteit;

2) de resultaten van de certificerings- en toezichtsactiviteiten die door de gekwalificeerde entiteit of de relevante autoriteit worden uitgevoerd, zijn opgenomen in de algemene certificerings- en toezichtsdossiers van de organisatie;

3) haar eigen beheersysteem voor informatiebeveiliging, dat is opgezet overeenkomstig 145.B.200, punt e), alle taken op het gebied van certificering en permanent toezicht die namens haar worden uitgevoerd, bestrijkt.";

g) aan 145.B.300 wordt het volgende punt g) toegevoegd:

"g) Met betrekking tot de certificering van en het toezicht op de naleving van 145.A.200A door de organisatie evalueert de bevoegde autoriteit, naast de punten a) tot en met f), elke goedkeuring die is verleend uit hoofde van IS.I.OR.200, punt e), van deze verordening of IS.D.OR.200, punt e), van Gedelegeerde Verordening (EU) 2022/1645 na de toepasselijke auditcyclus en telkens wanneer wijzigingen worden doorgevoerd in de reikwijdte van de werkzaamheden van de organisatie.";

h) na 145.B.330 wordt 145.B.330A ingevoegd:

"145.B.330A **Wijzigingen van het beheersysteem voor informatiebeveiliging**

a) Voor wijzigingen die worden beheerd en meegedeeld aan de bevoegde autoriteit overeenkomstig de procedure van IS.I.OR.255, punt a), van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203, neemt de bevoegde autoriteit de beoordeling van deze wijzigingen op in haar permanente toezicht overeenkomstig de beginselen van punt 145.B.300. Wanneer een geval van niet-naleving wordt vastgesteld, stelt de bevoegde autoriteit de organisatie daarvan in kennis, vraagt zij verdere wijzigingen en handelt zij overeenkomstig 145.B.350.

b) Met betrekking tot andere wijzigingen waarvoor een erkenningsaanvraag vereist is overeenkomstig IS.I.OR.255, punt b), van bijlage II (deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203:

1) controleert de bevoegde autoriteit, bij ontvangst van de wijzigingsaanvraag, of de organisatie aan de toepasselijke eisen voldoet alvorens de erkenning af te geven;

2) stelt de bevoegde autoriteit de voorwaarden vast waaronder de organisatie tijdens de uitvoering van de wijziging haar activiteiten mag uitvoeren;

3) keurt de bevoegde autoriteit de wijziging goed als zij ervan overtuigd is dat de organisatie voldoet aan de toepasselijke eisen.";".

2) Bijlage III (deel-66) wordt als volgt gewijzigd:

a) na 66.B.10 wordt de volgende titel ingevoegd in de inhoudsopgave:

"66.B.15 Beheersysteem voor informatiebeveiliging";

b) na 66.B.10 wordt 66.B.15 ingevoegd:

"66.B.15 **Beheersysteem voor informatiebeveiliging**

De bevoegde autoriteit ontwikkelt, implementeert en onderhoudt een beheersysteem voor informatiebeveiliging overeenkomstig bijlage I (deel-IS.AR) bij Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.".

3) Bijlage V quater (deel-CAMO) wordt als volgt gewijzigd:

a) de inhoudsopgave wordt als volgt gewijzigd:

i) na CAMO.A.200 wordt de volgende titel ingevoegd:

"CAMO.A.200A Beheersysteem voor informatiebeveiliging";

ii) na CAMO.B.135 wordt de volgende titel ingevoegd:

"CAMO.B.135A Onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart";

iii) de titel van CAMO.B.205 wordt vervangen door:

"CAMO.B.205 Toewijzing van taken";

iv) na CAMO.B.330 wordt de volgende titel ingevoegd:

"CAMO.B.330A Wijzigingen van het beheersysteem voor informatiebeveiliging";

b) na CAMO.A.200 wordt CAMO.A.200A ingevoegd:

"CAMO.A.200A **Beheersysteem voor informatiebeveiliging**

Naast het bij punt CAMO.A.200 vereiste beheersysteem moet de organisatie een beheersysteem voor informatiebeveiliging opzetten, toepassen en onderhouden overeenkomstig Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.";

c) aan CAMO.B.125 wordt het volgende punt c) toegevoegd:

"c) De bevoegde autoriteit van de lidstaat verstrekt het Agentschap zo spoedig mogelijk veiligheidsrelevante informatie die afkomstig is van de informatiebeveiligingsrapporten die zij heeft ontvangen overeenkomstig punt IS.I.OR.230 van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203";

d) na CAMO.B.135 wordt CAMO.B.135A ingevoegd:

"CAMO.B.135A **Onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart**

a) De bevoegde autoriteit past een systeem toe voor het op passende wijze verzamelen, analyseren en verspreiden van informatie over incidenten en kwetsbaarheden op het gebied van informatiebeveiliging met mogelijke gevolgen voor de veiligheid van de luchtvaart die door organisaties worden gemeld. Dit gebeurt in coördinatie met alle andere relevante autoriteiten die binnen de lidstaat verantwoordelijk zijn voor informatiebeveiliging of cyberbeveiliging om de coördinatie en compatibiliteit van meldingsregelingen te verbeteren.

b) Het Agentschap voert een systeem in om alle veiligheidsrelevante informatie die is ontvangen overeenkomstig CAMO.B.125, punt c), op passende wijze te analyseren en verstrekt de lidstaten en de Commissie zonder onnodige vertraging alle informatie, met inbegrip van aanbevelingen of te nemen corrigerende maatregelen, die zij nodig hebben om tijdig te kunnen reageren op een informatiebeveiligingsincident of kwetsbaarheid met mogelijke gevolgen voor de luchtvaartveiligheid met betrekking tot producten, onderdelen, niet-geïnstalleerde apparatuur, personen of organisaties die onder Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan vallen.

c) Na ontvangst van de in de punten a) en b) bedoelde informatie neemt de bevoegde autoriteit passende maatregelen om de mogelijke gevolgen van het informatiebeveiligingsincident of de kwetsbaarheid voor de veiligheid van de luchtvaart aan te pakken.

d) Overeenkomstig punt c) genomen maatregelen moeten onmiddellijk ter kennis worden gebracht van alle personen of organisaties die daaraan moeten voldoen krachtens Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan. De bevoegde autoriteit van de lidstaat stelt ook het Agentschap in kennis van deze maatregelen, alsmede de andere betrokken lidstaten in zoverre gecombineerd optreden vereist is.";

e) aan CAMO.B.200 wordt het volgende punt e) toegevoegd:

"e) Naast de eisen van punt a) moet het door de bevoegde autoriteit opgezette en onderhouden beheersysteem voldoen aan bijlage I (Deel-IS.AR) bij Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.";

f) CAMO.B.205 wordt als volgt gewijzigd:

i) de titel wordt vervangen door:

"CAMO.B.205 **Toewijzing van taken**";

ii) het volgende punt c) wordt toegevoegd:

"c) Met betrekking tot de certificering van en het toezicht op de naleving van CAMO.A.200A door de organisatie kan de bevoegde autoriteit taken toewijzen aan gekwalificeerde entiteiten overeenkomstig punt a) of aan elke relevante autoriteit die verantwoordelijk is voor informatiebeveiliging of cyberbeveiliging in de lidstaat. Bij het toewijzen van deze taken zorgt de bevoegde autoriteit ervoor dat:

1) alle aspecten in verband met luchtvaartveiligheid worden gecoördineerd en in aanmerking genomen door de gekwalificeerde entiteit of de relevante autoriteit;

2) de resultaten van de certificerings- en toezichtsactiviteiten die door de gekwalificeerde entiteit of de relevante autoriteit worden uitgevoerd, zijn opgenomen in de algemene certificerings- en toezichtsdossiers van de organisatie;

3) haar eigen beheersysteem voor informatiebeveiliging, dat is opgezet overeenkomstig CAMO.B.200, punt e), alle taken op het gebied van certificering en permanent toezicht die namens haar worden uitgevoerd, bestrijkt.";

g) aan CAMO.B.300 wordt het volgende punt g) toegevoegd:

"g) Met betrekking tot de certificering van en het toezicht op de naleving van CAMO.A.200A door de organisatie evalueert de bevoegde autoriteit, naast de punten a) tot en met f), elke goedkeuring die is verleend uit hoofde van IS.I.OR.200, punt e), van deze verordening of IS.D.OR.200, punt e), van Gedelegeerde Verordening (EU) 2022/1645 na de toepasselijke auditcyclus en telkens wanneer wijzigingen worden doorgevoerd in de reikwijdte van de werkzaamheden van de organisatie.".

h) na CAMO.B.330 wordt CAMO.B.330A ingevoegd:

"CAMO.B.330A **Wijzigingen van het beheersysteem voor informatiebeveiliging**

a) Voor wijzigingen die worden beheerd en meegedeeld aan de bevoegde autoriteit overeenkomstig de procedure van IS.I.OR.255, punt a), van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203, neemt de bevoegde autoriteit de beoordeling van deze wijzigingen op in haar permanente toezicht overeenkomstig de beginselen van punt CAMO.B.300. Wanneer een geval van niet-naleving wordt vastgesteld, stelt de bevoegde autoriteit de organisatie daarvan in kennis, vraagt zij verdere wijzigingen en handelt zij overeenkomstig CAMO.B.350.

b) Met betrekking tot andere wijzigingen waarvoor een erkenningsaanvraag vereist is overeenkomstig IS.I.OR.255, punt b), van bijlage II (deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203:

1) controleert de bevoegde autoriteit, bij ontvangst van de wijzigingsaanvraag, of de organisatie aan de toepasselijke eisen voldoet alvorens de erkenning af te geven;

2) stelt de bevoegde autoriteit de voorwaarden vast waaronder de organisatie tijdens de uitvoering van de wijziging haar activiteiten mag uitvoeren;

3) keurt de bevoegde autoriteit de wijziging goed als zij ervan overtuigd is dat de organisatie voldoet aan de toepasselijke eisen.".

BIJLAGE VIII

Bijlagen II (deel-ATCO.AR) en III (deel-ATCO.OR) bij Verordening (EU) 2015/340 worden als volgt gewijzigd:

1) Bijlage II (deel-ATCO.AR) wordt als volgt gewijzigd:

a) aan ATCO.AR.A.020 wordt het volgende punt c) toegevoegd:

"c) De bevoegde autoriteit van de lidstaat verstrekt het Agentschap zo spoedig mogelijk veiligheidsrelevante informatie die afkomstig is van de informatiebeveiligingsrapporten die zij heeft ontvangen overeenkomstig punt IS.I.OR.230 van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203.";

b) na ATCO.AR.A.025 wordt ATCO.AR.A.025A ingevoegd:

"**ATCO.AR.A.025A Onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart**

a) De bevoegde autoriteit past een systeem toe voor het op passende wijze verzamelen, analyseren en verspreiden van informatie over incidenten en kwetsbaarheden op het gebied van informatiebeveiliging met mogelijke gevolgen voor de veiligheid van de luchtvaart die door organisaties worden gemeld. Dit gebeurt in coördinatie met alle andere relevante autoriteiten die binnen de lidstaat verantwoordelijk zijn voor informatiebeveiliging of cyberbeveiliging om de coördinatie en compatibiliteit van meldingsregelingen te verbeteren.

b) Het Agentschap voert een systeem in om alle veiligheidsrelevante informatie die is ontvangen overeenkomstig ATCO.AR.A.020, op passende wijze te analyseren en verstrekt de lidstaten en de Commissie zonder onnodige vertraging alle informatie, met inbegrip van aanbevelingen of te nemen corrigerende maatregelen, die zij nodig hebben om tijdig te kunnen reageren op een informatiebeveiligingsincident of kwetsbaarheid met mogelijke gevolgen voor de luchtvaartveiligheid met betrekking tot producten, onderdelen, niet-geïnstalleerde apparatuur, personen of organisaties die onder Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan vallen.

c) Na ontvangst van de in de punten a) en b) bedoelde informatie neemt de bevoegde autoriteit passende maatregelen om de mogelijke gevolgen van het informatiebeveiligingsincident of de kwetsbaarheid voor de veiligheid van de luchtvaart aan te pakken.

d) Overeenkomstig punt c) genomen maatregelen moeten onmiddellijk ter kennis worden gebracht van alle personen of organisaties die daaraan moeten voldoen krachtens Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan. De bevoegde autoriteit van de lidstaat stelt ook het Agentschap in kennis van deze maatregelen, alsmede de bevoegde autoriteiten van de andere betrokken lidstaten in zoverre gecombineerd optreden vereist is.";

c) aan ATCO.AR.B.001 wordt het volgende punt e) toegevoegd:

"e) Naast de eisen van punt a) moet het door de bevoegde autoriteit opgezette en onderhouden beheersysteem voldoen aan bijlage I (Deel-IS.AR) bij Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.";

d) ATCO.AR.B.005 wordt als volgt gewijzigd:

i) de titel wordt vervangen door:

"**ATCO.AR.B.005 Toewijzing van taken**";

ii) het volgende punt c) wordt toegevoegd:

"c) Met betrekking tot de certificering van en het toezicht op de naleving van ATCO.OR.C.001A door de organisatie kan de bevoegde autoriteit taken toewijzen aan gekwalificeerde entiteiten overeenkomstig punt a) of aan elke relevante autoriteit die verantwoordelijk is voor informatiebeveiliging of cyberbeveiliging in de lidstaat. Bij het toewijzen van deze taken zorgt de bevoegde autoriteit ervoor dat:

1) alle aspecten in verband met luchtvaartveiligheid worden gecoördineerd en in aanmerking genomen door de gekwalificeerde entiteit of de relevante autoriteit;

2) de resultaten van de certificerings- en toezichtsactiviteiten die door de gekwalificeerde entiteit of de relevante autoriteit worden uitgevoerd, zijn opgenomen in de algemene certificerings- en toezichtsdossiers van de organisatie;

3) haar eigen beheersysteem voor informatiebeveiliging, dat is opgezet overeenkomstig ATCO.AR.B.001, punt e), alle taken op het gebied van certificering en permanent toezicht die namens haar worden uitgevoerd, bestrijkt.";

e) aan ATCO.AR.C.001 wordt het volgende punt f) toegevoegd:

"f) Met betrekking tot de certificering van en het toezicht op de naleving van ATCO.OR.C.001A door de organisatie evalueert de bevoegde autoriteit, naast de punten a) tot en met e), elke goedkeuring die is verleend uit hoofde van IS.I.OR.200, punt e), van deze verordening of IS.D.OR.200, punt e), van Gedelegeerde Verordening (EU) 2022/1645 na de toepasselijke auditcyclus en telkens wanneer wijzigingen worden doorgevoerd in de reikwijdte van de werkzaamheden van de organisatie.";

f) na ATCO.AR.E.010 wordt ATCO.AR.E.010A ingevoegd:

"**ATCO.AR.E.010A Wijzigingen van het beheersysteem voor informatiebeveiliging**

a) Met betrekking tot wijzigingen die worden beheerd en meegedeeld aan de bevoegde autoriteit overeenkomstig de procedure van IS.I.OR.255, punt a), van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203, neemt de bevoegde autoriteit de beoordeling van deze wijzigingen op in haar permanente toezicht overeenkomstig de beginselen van punt ATCO.AR.C.001. Wanneer een geval van niet-naleving wordt vastgesteld, stelt de bevoegde autoriteit de organisatie daarvan in kennis, vraagt zij verdere wijzigingen en handelt zij overeenkomstig ATCO.AR.C.010.

b) Met betrekking tot andere wijzigingen waarvoor een erkenningsaanvraag vereist is overeenkomstig IS.I.OR.255, punt b), van bijlage II (deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203:

1) controleert de bevoegde autoriteit, bij ontvangst van de wijzigingsaanvraag, of de organisatie aan de toepasselijke eisen voldoet alvorens de erkenning af te geven;

2) stelt de bevoegde autoriteit de voorwaarden vast waaronder de organisatie tijdens de uitvoering van de wijziging haar activiteiten mag uitvoeren;

3) keurt de bevoegde autoriteit de wijziging goed als zij ervan overtuigd is dat de organisatie voldoet aan de toepasselijke eisen.".

2) Bijlage III (deel-ATCO.OR) wordt als volgt gewijzigd:

na ATCO.OR.C.001 wordt ATCO.OR.C.001A ingevoegd:

"**ATCO.OR.C.001A Beheersysteem voor informatiebeveiliging**

Naast het bij punt ATCO.OR.C.001 vereiste beheersysteem moet de opleidingsorganisatie een beheersysteem voor informatiebeveiliging opzetten, toepassen en onderhouden overeenkomstig Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.".

BIJLAGE IX

Bijlagen II (deel-ATM/ANS.AR) en III (deel-ATM/ANS.OR) bij Uitvoeringsverordening (EU) 2017/373 worden als volgt gewijzigd:

1) Bijlage II (deel-ATM/ANS.AR) wordt als volgt gewijzigd:

a) aan ATM/ANS.AR.A.020 wordt het volgende punt c) toegevoegd:

"c) De bevoegde autoriteit van de lidstaat verstrekt het Agentschap zo spoedig mogelijk veiligheidsrelevante informatie die afkomstig is van de informatiebeveiligingsrapporten die zij heeft ontvangen overeenkomstig punt IS.I.OR.230 van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203.";

b) na ATM/ANS.AR.A.025 wordt ATM/ANS.AR.A.025A ingevoegd:

"**ATM/ANS.AR.A.025A Onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart**

a) De bevoegde autoriteit past een systeem toe voor het op passende wijze verzamelen, analyseren en verspreiden van informatie over incidenten en kwetsbaarheden op het gebied van informatiebeveiliging met mogelijke gevolgen voor de veiligheid van de luchtvaart die door organisaties worden gemeld. Dit gebeurt in coördinatie met alle andere relevante autoriteiten die binnen de lidstaat verantwoordelijk zijn voor informatiebeveiliging of cyberbeveiliging om de coördinatie en compatibiliteit van meldingsregelingen te verbeteren.

b) Het Agentschap voert een systeem in om alle veiligheidsrelevante informatie die is ontvangen overeenkomstig ATM/ANS.AR.A.020, punt c), op passende wijze te analyseren en verstrekt de lidstaten en de Commissie zonder onnodige vertraging alle informatie, met inbegrip van aanbevelingen of te nemen corrigerende maatregelen, die zij nodig hebben om tijdig te kunnen reageren op een informatiebeveiligingsincident of kwetsbaarheid met mogelijke gevolgen voor de luchtvaartveiligheid met betrekking tot producten, onderdelen, niet-geïnstalleerde apparatuur, personen of organisaties die onder Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan vallen.

c) Na ontvangst van de in de punten a) en b) bedoelde informatie neemt de bevoegde autoriteit passende maatregelen om de mogelijke gevolgen van het informatiebeveiligingsincident of de kwetsbaarheid voor de veiligheid van de luchtvaart aan te pakken.

d) Overeenkomstig punt c) genomen maatregelen moeten onmiddellijk ter kennis worden gebracht van alle personen of organisaties die daaraan moeten voldoen krachtens Verordening (EU) 2018/1139 en de gedelegeerde en uitvoeringshandelingen daarvan. De bevoegde autoriteit van de lidstaat stelt ook het Agentschap in kennis van deze maatregelen, alsmede de bevoegde autoriteiten van de andere betrokken lidstaten in zoverre gecombineerd optreden vereist is.";

c) aan ATM/ANS.AR.B.001 wordt het volgende punt e) toegevoegd:

"e) Naast de eisen van punt a) moet het door de bevoegde autoriteit opgezette en onderhouden beheersysteem voldoen aan bijlage I (deel-IS.AR) bij Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.";

d) ATM/ANS.AR.B.005 wordt als volgt gewijzigd:

i) de titel wordt vervangen door:

"**ATM/ANS.AR.B.005 Toewijzing van taken**";

ii) het volgende punt c) wordt toegevoegd:

"c) Met betrekking tot de certificering van en het toezicht op de naleving van ATM/ANS.OR.B.005A door de organisatie kan de bevoegde autoriteit taken toewijzen aan gekwalificeerde entiteiten overeenkomstig punt a) of aan elke relevante autoriteit die verantwoordelijk is voor informatiebeveiliging of cyberbeveiliging in de lidstaat. Bij het toewijzen van deze taken zorgt de bevoegde autoriteit ervoor dat:

1) alle aspecten in verband met luchtvaartveiligheid worden gecoördineerd en in aanmerking genomen door de gekwalificeerde entiteit of de relevante autoriteit;

2) de resultaten van de certificerings- en toezichtsactiviteiten die door de gekwalificeerde entiteit of de relevante autoriteit worden uitgevoerd, zijn opgenomen in de algemene certificerings- en toezichtsdossiers van de organisatie;

3) haar eigen beheersysteem voor informatiebeveiliging, dat is opgezet overeenkomstig ATM/ANS.AR.B.001, punt e), alle taken op het gebied van certificering en permanent toezicht die namens haar worden uitgevoerd, bestrijkt.";

e) aan ATM/ANS.AR.C.010 wordt het volgende punt d) toegevoegd:

"d) Met betrekking tot de certificering van en het toezicht op de naleving van ATM/ANS.OR.B.005A door de organisatie evalueert de bevoegde autoriteit, naast de punten a), b) en c), elke goedkeuring die is verleend uit hoofde van IS.I.OR.200, punt e), van deze verordening of IS.D.OR.200, punt e), van Gedelegeerde Verordening (EU) 2022/1645 na de toepasselijke auditcyclus en telkens wanneer wijzigingen worden doorgevoerd in de reikwijdte van de werkzaamheden van de organisatie.";

f) na ATM/ANS.AR.C.025 wordt ATM/ANS.AR.C.025A ingevoegd:

"**ATM/ANS.AR.C.025A Wijzigingen van het beheersysteem voor informatiebeveiliging**

a) Voor wijzigingen die worden beheerd en meegedeeld aan de bevoegde autoriteit overeenkomstig de procedure van IS.I.OR.255, punt a), van bijlage II (Deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203, neemt de bevoegde autoriteit de beoordeling van deze wijzigingen op in haar permanente toezicht overeenkomstig de beginselen van punt ATM/ANS.AR.C.010. Wanneer een geval van niet-naleving wordt vastgesteld, stelt de bevoegde autoriteit de organisatie daarvan in kennis, vraagt zij verdere wijzigingen en handelt zij overeenkomstig ATM/ANS.AR.C.050.

b) Met betrekking tot andere wijzigingen waarvoor een erkenningsaanvraag vereist is overeenkomstig IS.I.OR.255, punt b), van bijlage II (deel-IS.I.OR) bij Uitvoeringsverordening (EU) 2023/203:

1) controleert de bevoegde autoriteit, bij ontvangst van de wijzigingsaanvraag, of de organisatie aan de toepasselijke eisen voldoet alvorens de erkenning af te geven;

2) stelt de bevoegde autoriteit de voorwaarden vast waaronder de organisatie tijdens de uitvoering van de wijziging haar activiteiten mag uitvoeren;

3) keurt de bevoegde autoriteit de wijziging goed als zij ervan overtuigd is dat de organisatie voldoet aan de toepasselijke eisen.".

2) Bijlage III (deel-ATM/ANS.OR) wordt als volgt gewijzigd:

a) na ATM/ANS.OR.B.005 wordt ATM/ANS.OR.B.005A ingevoegd:

"**ATM/ANS.OR.B.005A Beheersysteem voor informatiebeveiliging**

Naast het bij ATM/ANS.OR.B.005 vereiste beheersysteem moet de dienstverlener een beheersysteem voor informatiebeveiliging opzetten, toepassen en onderhouden overeenkomstig Uitvoeringsverordening (EU) 2023/203 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.";

b) ATM/ANS.OR.D.010 wordt vervangen door:

"**ATM/ANS.OR.D.010 Beheer van de beveiliging**

a) Verleners van luchtvaartnavigatiediensten en diensten voor het beheer van de luchtverkeersstromen en de Netwerkbeheerder stellen, als een integrerend onderdeel van hun beheersysteem zoals vereist bij punt ATM/ANS.OR.B.005, een systeem voor het beheer van de beveiliging vast teneinde:

1) de veiligheid van hun faciliteiten en personeel te verzekeren door onrechtmatige daden bij de dienstverlening te voorkomen;

2) de beveiliging van de door hen ontvangen, verschafte of op andere wijze gebruikte operationele gegevens te garanderen, zodat deze alleen voor bevoegden toegankelijk zijn.

b) In dit beveiligingsbeheersysteem moet het volgende worden vastgesteld:

1) het proces en de procedures voor de beoordeling en beperking van beveiligingsrisico's, het toezicht op en de verbetering van de beveiliging, de beoordeling van de beveiliging en de verspreiding van opgedane ervaringen;

2) de methoden die zijn ontworpen om lekken in de beveiliging te identificeren, te monitoren en op te sporen en het personeel op passende wijze te waarschuwen;

3) de methoden om de gevolgen van inbreuken op de beveiliging te controleren en om herstel- en schadebeperkingsprocedures vast te stellen teneinde herhaling te voorkomen.

c) Verleners van luchtvaartnavigatiediensten en diensten voor het beheer van de luchtverkeersstromen en de Netwerkbeheerder zorgen voor de beveiligingsklaring van hun personeel, voor zover van toepassing, en plegen overleg met de relevante civiele en militaire autoriteiten om de beveiliging van hun faciliteiten, personeel en gegevens te waarborgen.

d) De aspecten die verband houden met informatiebeveiliging worden beheerd overeenkomstig ATM/ANS.OR.B.005A.".