II

(Rechtsakte ohne Gesetzescharakter)

VERORDNUNGEN

DURCHFÜHRUNGSVERORDNUNG (EU) 2023/203 DER KOMMISSION

vom 27. Oktober 2022

zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates hinsichtlich der Anforderungen an das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit für Organisationen, die unter die Verordnungen (EU) Nr. 1321/2014, (EU) Nr. 965/2012, (EU) Nr. 1178/2011, (EU) 2015/340 der Kommission, die Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission fallen, sowie für zuständige Behörden, die unter die Verordnungen (EU) Nr. 748/2012, (EU) Nr. 1321/2014, (EU) Nr. 965/2012, (EU) Nr. 1178/2011, (EU) 2015/340 und (EU) Nr. 139/2014 der Kommission und die Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission fallen, sowie zur Änderung der Verordnungen (EU) Nr. 1178/2011, (EU) Nr. 748/2012, (EU) Nr. 965/2012, (EU) Nr. 139/2014, (EU) Nr. 1321/2014, (EU) 2015/340 der Kommission und der Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr. 2111/2005, (EG) Nr. 1008/2008, (EU) Nr. 996/2010, (EU) Nr. 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates, und zur Aufhebung der Verordnungen (EG) Nr. 552/2004 und (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr. 3922/91 des Rates ([1]), insbesondere auf die Artikel 17 Absatz 1 Buchstabe b, Artikel 27 Absatz 1 Buchstabe a, Artikel 31 Absatz 1 Buchstabe b, Artikel 43 Absatz 1 Buchstabe b, Artikel 53 Absatz 1 Buchstabe a und Artikel 62 Absatz 15 Buchstabe c,

in Erwägung nachstehender Gründe:

(1) Gemäß den grundlegenden Anforderungen in Anhang II Nummer 3.1 Buchstabe b der Verordnung (EU) 2018/1139 müssen Organisationen zur Führung der Aufrechterhaltung der Lufttüchtigkeit und Instandhaltungsorganisationen für das Management von Sicherheitsrisiken ein Managementsystem einführen und aufrechterhalten.

(2) Gemäß den grundlegenden Anforderungen in Anhang IV Nummer 3.3 Buchstabe b und Nummer 5 Buchstabe b der Verordnung (EU) 2018/1139 müssen auch Ausbildungsorganisationen für Piloten, Ausbildungsorganisationen für Flugbegleiter, flugmedizinische Zentren für die Flugbesatzung und Betreiber von Flugsimulationsübungsgeräten für das Management von Sicherheitsrisiken ein Managementsystem einführen und aufrechterhalten.

(3) Zudem müssen gemäß den grundlegenden Anforderungen in Anhang V Nummer 8.1 Buchstabe c der Verordnung (EU) 2018/1139 Luftfahrtunternehmen für das Management von Sicherheitsrisiken ein Managementsystem einführen und aufrechterhalten.

(4) Außerdem müssen gemäß den grundlegenden Anforderungen in Anhang VIII Nummer 5.1 Buchstabe c und Nummer 5.4 Buchstabe b der Verordnung (EU) 2018/1139 Anbieter von Flugverkehrsmanagement- und Flugsicherungsdiensten, Anbieter von U-Space-Diensten und einzige Anbieter gemeinsamer Informationsdienste sowie Ausbildungsorganisationen und flugmedizinische Zentren für Fluglotsen für das Management von Sicherheitsrisiken ein Managementsystem einrichten und aufrechterhalten.

([1]) ABl. L 212 vom 22.8.2018, S. 1.

(5) Diese Sicherheitsrisiken können aus verschiedenen Quellen herrühren, darunter Anfälligkeiten in der Konstruktion oder bei der Instandhaltung, Aspekte der menschlichen Leistungsfähigkeit, Bedrohungen durch das Umfeld und Bedrohungen der Informationssicherheit. Daher sollten die von der Agentur der Europäischen Union für Flugsicherheit (im Folgenden die „Agentur“) eingerichteten Managementsysteme sowie die Managementsysteme, die von den in den Erwägungsgründen genannten nationalen zuständigen Behörden und Organisationen eingerichtet wurden, nicht nur Sicherheitsrisiken berücksichtigen, die sich aus zufälligen Ereignissen ergeben, sondern auch solche, die sich aus Bedrohungen der Informationssicherheit ergeben und bei denen bestehende Anfälligkeiten von Personen mit böswilliger Absicht ausgenutzt werden können. Diese Risiken für die Informationssicherheit nehmen in der Zivilluftfahrt ständig zu, da die derzeitigen Informationssysteme immer stärker vernetzt werden und immer häufiger zum Angriffsziel böswilliger Akteure werden.

(6) Die mit diesen Informationssystemen verbundenen Risiken beschränken sich nicht auf mögliche Angriffe auf den Cyberraum, sondern umfassen auch Bedrohungen, die Prozesse und Verfahren sowie die menschliche Leistungsfähigkeit beeinträchtigen können.

(7) Eine beträchtliche Anzahl von Organisationen wendet bereits internationale Normen wie ISO 27001 an, um die Sicherheit digitaler Informationen und Daten zu verbessern. Allerdings berücksichtigen diese Normen möglicherweise nicht alle Besonderheiten der Zivilluftfahrt. Daher sollten Anforderungen für das Management von sich potenziell auf die Flugsicherheit auswirkenden Informationssicherheitsrisiken eingeführt werden.

(8) Angesichts des hochgradig vernetzten Luftfahrtsystems kommt es darauf an, dass diese Anforderungen alle Bereiche der Luftfahrt und deren Schnittstellen abdecken. Daher sollten sie für alle Organisationen und zuständigen Behörden gelten, die unter die Verordnungen (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]) der Kommission und die Durchführungsverordnung (EU) 2021/664 ([8]) der Kommission fallen, sowie auch für die Organisationen, die bereits jetzt über ein Managementsystem im Einklang mit den geltenden Rechtsvorschriften der Union im Bereich der Flugsicherheit verfügen müssen. Einige Organisationen sollten jedoch zur Wahrung der Verhältnismäßigkeit vom Anwendungsbereich dieser Verordnung ausgenommen werden, da von ihnen nur geringe Informationssicherheitsrisiken für das Luftfahrtsystem ausgehen.

(9) Die in dieser Verordnung festgelegten Anforderungen sollten eine einheitliche Anwendung in allen Bereichen der Luftfahrt gewährleisten und sich dabei nur geringfügig auf die bereits für diese Bereiche geltenden Flugsicherheitsvorschriften der Union auswirken.

([2]) Verordnung (EU) Nr. 748/2012 der Kommission vom 3. August 2012 zur Festlegung der Durchführungsbestimmungen für die Erteilung von Lufttüchtigkeits- und Umweltzeugnissen für Luftfahrzeuge und zugehörige Produkte, Bau- und Ausrüstungsteile sowie für die Zulassung von Entwicklungs- und Herstellungsbetrieben (ABl. L 224 vom 21.8.2012, S. 1).

([3]) Verordnung (EU) Nr. 1321/2014 der Kommission vom 26. November 2014 über die Aufrechterhaltung der Lufttüchtigkeit von Luftfahrzeugen und luftfahrttechnischen Erzeugnissen, Teilen und Ausrüstungen und die Erteilung von Genehmigungen für Organisationen und Personen, die diese Tätigkeiten ausführen (ABl. L 362 vom 17.12.2014, S. 1).

([4]) Verordnung (EU) Nr. 965/2012 der Kommission vom 5. Oktober 2012 zur Festlegung technischer Vorschriften und von Verwaltungsverfahren in Bezug auf den Flugbetrieb gemäß der Verordnung (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates (ABl. L 296 vom 25.10.2012, S. 1).

([5]) Verordnung (EU) Nr. 1178/2011 der Kommission vom 3. November 2011 zur Festlegung technischer Vorschriften und von Verwaltungsverfahren in Bezug auf den Flugbetrieb gemäß der Verordnung (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates (ABl. L 311 vom 25.11.2011, S. 1).

([6]) Verordnung (EU) 2015/340 der Kommission vom 20. Februar 2015 zur Festlegung technischer Vorschriften und von Verwaltungsverfahren in Bezug auf Lizenzen und Bescheinigungen von Fluglotsen gemäß der Verordnung (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates, zur Änderung der Durchführungsverordnung (EU) Nr. 923/2012 der Kommission und zur Aufhebung der Verordnung (EU) Nr. 805/2011 der Kommission (ABl. L 63 vom 6.3.2015, S. 1).

([7]) Verordnung (EU) Nr. 139/2014 der Kommission vom 12. Februar 2014 zur Festlegung von Anforderungen und Verwaltungsverfahren in Bezug auf Flugplätze gemäß der Verordnung (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates (ABl. L 44 vom 14.2.2014, S. 1).

([8]) Durchführungsverordnung (EU) 2021/664 der Kommission vom 22. April 2021 über einen Rechtsrahmen für den U-Space (ABl. L 139 vom 23.4.2021, S. 161).

(10) Die in dieser Verordnung festgelegten Anforderungen sollten die in Nummer 1.7 des Anhangs der Durchführungsverordnung (EU) 2015/1998 der Kommission ([9]) und in Artikel 14 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([10]) festgelegten Anforderungen an die Informationssicherheit und die Cybersicherheit unberührt lassen.

(11) Die in Titel V „Sicherheit des Programms" Artikel 33 bis 43 der Verordnung (EU) 2021/696 des Europäischen Parlaments und des Rates ([11]) festgelegten Sicherheitsanforderungen gelten als gleichwertig mit den Anforderungen der vorliegenden Verordnung, mit Ausnahme von Punkt IS.I.OR.230 des Anhangs II dieser Verordnung, der eingehalten werden muss.

(12) Im Interesse der Rechtssicherheit sollte die Auslegung des in dieser Verordnung festgelegten Begriffs der „Informationssicherheit", wie er weltweit in der Zivilluftfahrt gebräuchlich ist, als mit der Auslegung des Begriffs „Sicherheit von Netz- und Informationssystemen", wie er in Artikel 4 Nummer 2 der Richtlinie (EU) 2016/1148 festgelegt ist, in Einklang stehend angesehen werden. Die für die Zwecke dieser Verordnung verwendete Definition der Informationssicherheit sollte nicht so ausgelegt werden, dass sie von der Begriffsbestimmung der Sicherheit von Netz- und Informationssystemen in der Richtlinie (EU) 2016/1148 abweicht.

(13) Um Überschneidungen bei den rechtlichen Anforderungen zu vermeiden, sollte in Fällen, in denen unter diese Verordnung fallende Organisationen bereits bestimmten Sicherheitsanforderungen unterliegen, die sich aus in den Erwägungsgründen 10 und 11 genannten Rechtsakten der Union ergeben und die in ihrer Wirkung den Bestimmungen dieser Verordnung gleichwertig sind, die Einhaltung jener Sicherheitsanforderungen als Erfüllung der in dieser Verordnung festgelegten Anforderungen gelten.

(14) Unter diese Verordnung fallende Organisationen, die bereits den Sicherheitsanforderungen der Durchführungsverordnung (EU) 2015/1998 oder der Verordnung (EU) 2021/696 oder beiden unterliegen, sollten auch die Anforderungen von Anhang II (Teil IS.I.OR.230 „Informationssicherheitssystem für externe Meldungen") dieser Verordnung erfüllen, da keine der beiden genannten Verordnungen Bestimmungen über die externe Meldung von Störungen der Informationssicherheit enthält.

(15) Der Vollständigkeit halber sollten die Verordnungen (EU) Nr. 1178/2011, (EU) Nr. 748/2012, (EU) Nr. 965/2012, (EU) Nr. 139/2014, (EU) Nr. 1321/2014, (EU) 2015/340 sowie die Durchführungsverordnungen (EU) 2017/373 ([12]) und (EU) 2021/664 dahingehend geändert werden, dass die in dieser Verordnung vorgeschriebenen Anforderungen an das Informationssicherheitsmanagementsystem zusammen mit den darin festgelegten Managementsystemen aufgenommen und die Anforderungen an die zuständigen Behörden hinsichtlich der Aufsicht über Organisationen, die die genannten Anforderungen an das Informationssicherheitsmanagement umsetzen, festgelegt werden.

(16) Damit die Organisationen ausreichend Zeit haben, um die Einhaltung der neuen Vorschriften und Verfahren sicherzustellen, sollte die Geltung dieser Verordnung drei Jahre nach ihrem Inkrafttreten beginnen. Ausgenommen hiervon sind die in der Durchführungsverordnung (EU) 2017/373 festgelegten Anbieter von Flugsicherungsdiensten für die Europäische Erweiterung des geostationären Navigationssystems (EGNOS), für die die Geltung aufgrund der laufenden Sicherheitsakkreditierung des EGNOS-Systems und der EGNOS-Dienste im Einklang mit der Verordnung (EU) 2021/696 ab dem 1. Januar 2026 beginnen sollte.

(17) Die in dieser Verordnung festgelegten Anforderungen beruhen auf der Stellungnahme Nr. 03/2021 ([13]), die von der Agentur gemäß Artikel 75 Absatz 2 Buchstaben b und c sowie Artikel 76 Absatz 1 der Verordnung (EU) 2018/1139 abgegeben wurde.

([9]) Durchführungsverordnung (EU) 2015/1998 der Kommission vom 5. November 2015 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit (ABl. L 299 vom 14.11.2015, S. 1).

([10]) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

([11]) Verordnung (EU) 2021/696 des Europäischen Parlaments und des Rates vom 28. April 2021 zur Einrichtung des Weltraumprogramms der Union und der Agentur der Europäischen Union für das Weltraumprogramm und zur Aufhebung der Verordnungen (EU) Nr. 912/2010, (EU) Nr. 1285/2013 und (EU) Nr. 377/2014 sowie des Beschlusses Nr. 541/2014/EU (ABl. L 170 vom 12.5.2021, S. 69).

([12]) Durchführungsverordnung (EU) 2017/373 der Kommission vom 1. März 2017 zur Festlegung gemeinsamer Anforderungen an Flugverkehrsmanagementanbieter und Anbieter von Flugsicherungsdiensten sowie sonstiger Funktionen des Flugverkehrsmanagementnetzes und die Aufsicht hierüber sowie zur Aufhebung der Verordnung (EG) Nr. 482/2008, der Durchführungsverordnungen (EU) Nr. 1034/2011, (EU) Nr. 1035/2011 und (EU) 2016/1377 und zur Änderung der Verordnung (EU) Nr. 677/2011 (ABl. L 62 vom 8.3.2017, S. 1).

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

(18) Die in dieser Verordnung festgelegten Anforderungen entsprechen der Stellungnahme des nach Artikel 127 der Verordnung (EU) 2018/1139 eingesetzten Ausschusses für die Anwendung der gemeinsamen Sicherheitsvorschriften für die Zivilluftfahrt —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Gegenstand

In dieser Verordnung werden die von den Organisationen und zuständigen Behörden zu erfüllenden Anforderungen festgelegt, und zwar im Hinblick auf

a) die Identifizierung und das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit, die für die Zwecke der Zivilluftfahrt eingesetzte Systeme und Daten der Informations- und Kommunikationstechnik beeinträchtigen könnten;

b) die Erkennung von Informationssicherheitsereignissen und die Identifizierung solcher Ereignisse, die als Störungen der Informationssicherheit mit potenziellen Auswirkungen auf die Flugsicherheit gelten;

c) die Reaktion auf solche Störungen der Informationssicherheit und die Wiederherstellung.

Artikel 2

Geltungsbereich

(1) Diese Verordnung gilt für folgende Organisationen:

a) Instandhaltungsorganisationen nach Anhang II (Teil-145) Abschnitt A der Verordnung (EU) Nr. 1321/2014, mit Ausnahme der Organisationen, die ausschließlich mit der Instandhaltung von Luftfahrzeugen nach Anhang Vb (Teil-ML) der Verordnung (EU) Nr. 1321/2014 befasst sind;

b) Organisationen zur Führung der Aufrechterhaltung der Lufttüchtigkeit (CAMO) nach Anhang Vc (Teil-CAMO) Abschnitt A der Verordnung (EU) Nr. 1321/2014, mit Ausnahme der Organisationen, die ausschließlich mit der Führung der Aufrechterhaltung der Lufttüchtigkeit von Luftfahrzeugen nach Anhang Vb (Teil-ML) der Verordnung (EU) Nr. 1321/2014 befasst sind;

c) Luftfahrtunternehmen nach Anhang III (Teil-ORO) der Verordnung (EU) Nr. 965/2012, mit Ausnahme der Organisationen, die ausschließlich mit dem Betrieb eines der folgenden Luftfahrzeuge befasst sind:

   i) ELA2-Luftfahrzeuge im Sinne des Artikels 1 Absatz 2 Buchstabe j der Verordnung (EU) Nr. 748/2012;

   ii) einmotorige Propellerflugzeuge mit einer höchstzulässigen betrieblichen Fluggastsitzkonfiguration von höchstens 5 Plätzen, die nicht als technisch komplizierte motorgetriebene Luftfahrzeuge eingestuft sind, wenn sie auf demselben Flugplatz oder Einsatzort starten und landen und nach Sichtflugregeln (VFR) am Tag betrieben werden;

   iii) einmotorige Hubschrauber mit einer höchstzulässigen betrieblichen Fluggastsitzkonfiguration von höchstens 5 Plätzen, die nicht als technisch komplizierte motorgetriebene Luftfahrzeuge eingestuft sind, wenn sie auf demselben Flugplatz oder Einsatzort starten und landen und nach Sichtflugregeln (VFR) am Tag betrieben werden;

d) zugelassene Ausbildungsorganisationen (ATO) nach Anhang VII (Teil-ORA) der Verordnung (EU) Nr. 1178/2011, mit Ausnahme der Organisationen, die ausschließlich mit Ausbildungsmaßnahmen für ELA2-Luftfahrzeuge im Sinne des Artikels 1 Absatz 2 Buchstabe j der Verordnung (EU) Nr. 748/2012 oder ausschließlich mit theoretischer Ausbildung befasst sind;

e) flugmedizinische Zentren für das fliegende Personal nach Anhang VII (Teil-ORA) der Verordnung (EU) Nr. 1178/2011;

f) Betreiber von Flugsimulationsübungsgeräten (FSTD) nach Anhang VII (Teil-ORA) der Verordnung (EU) Nr. 1178/2011, mit Ausnahme der Organisationen, die ausschließlich mit dem FSTD-Betrieb für ELA2-Luftfahrzeuge im Sinne des Artikels 1 Absatz 2 Buchstabe j der Verordnung (EU) Nr. 748/2012 oder ausschließlich mit theoretischer Ausbildung befasst sind;

g) Ausbildungsorganisationen (ATCO TO) und flugmedizinische Zentren für Fluglotsen nach Anhang III (Teil ATCO.OR) der Verordnung (EU) 2015/340;

h) Organisationen nach Anhang III (Teil-ATM/ANS.OR) der Durchführungsverordnung (EU) 2017/373, mit Ausnahme der folgenden Diensteanbieter:

i) Anbieter von Flugsicherungsdiensten, die Inhaber eines eingeschränkten Zeugnisses nach Punkt ATM/ANS.OR.A.010 jenes Anhangs sind;

ii) Anbieter von Fluginformationsdiensten, die eine Erklärung nach Punkt ATM/ANS.OR.A.015 jenes Anhangs abgeben;

i) Anbieter von U-Space-Diensten und einzige Anbieter gemeinsamer Informationsdienste nach Durchführungsverordnung (EU) 2021/664.

(2) Diese Verordnung gilt für die in Artikel 6 dieser Verordnung und in Artikel 5 der Delegierten Verordnung (EU) 2022/1645 der Kommission ([14]) genannten zuständigen Behörden, einschließlich der Agentur der Europäischen Union für Flugsicherheit (im Folgenden die „Agentur").

(3) Diese Verordnung gilt auch für die zuständige Behörde, die für die Erteilung, Aufrechterhaltung, Änderung, Aussetzung oder den Widerruf von Lizenzen für freigabeberechtigtes Personal nach Anhang III (Teil-66) der Verordnung (EU) Nr. 1321/2014 zuständig ist.

(4) Diese Verordnung lässt die in Nummer 1.7 des Anhangs der Durchführungsverordnung (EU) 2015/1998 und in Artikel 14 der Richtlinie (EU) 2016/1148 festgelegten Anforderungen an die Informationssicherheit und die Cybersicherheit unberührt.

Artikel 3

Begriffsbestimmungen

Für die Zwecke der vorliegenden Verordnung gelten folgende Begriffsbestimmungen:

1. „Informationssicherheit" (*information security*): die Wahrung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Netz- und Informationssystemen;

2. „Informationssicherheitsereignis" (*information security event*): ein identifizierter System-, Dienst- oder Netzzustand, der auf einen möglichen Verstoß gegen das Informationssicherheitskonzept oder ein Versagen von Informationssicherheitskontrollen oder auf eine bis dahin unbekannte Situation hinweist, die für die Informationssicherheit relevant sein kann;

3. „Störung" (*incident*): jedes Ereignis im Sinne des Artikels 4 Nummer 7 der Richtlinie (EU) 2016/1148, das sich tatsächlich nachteilig auf die Sicherheit von Netz- und Informationssystemen auswirkt;

4. „Informationssicherheitsrisiko" (*information security risk*): auf ein mögliches Informationssicherheitsereignis zurückzuführendes Risiko für die Organisation des Zivilluftfahrtbetriebs sowie für Vermögenswerte, Privatpersonen und andere Organisationen. Informationssicherheitsrisiken bergen das Potenzial, dass Schwachstellen eines Informationsbestands oder einer Gruppe von Informationsbeständen durch Bedrohungen ausgenutzt werden;

([14]) Delegierte Verordnung (EU) 2022/1645 der Kommission vom 14. Juli 2022 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates im Hinblick auf die Anforderungen an das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit für Organisationen, die unter die Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission fallen, und zur Änderung der Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission (ABl. L 248 vom 26.9.2022, S. 18).

5. „Bedrohung“ (*threat*): eine potenzielle Verletzung der Informationssicherheit, die vorliegt, wenn durch eine Einrichtung, einen Umstand, eine Handlung oder ein Ereignis ein Schaden verursacht werden könnte;

6. „Schwachstelle“ (*vulnerability*): eine Anfälligkeit oder eine Schwäche in einem Bestand oder System, in Verfahren, im Design, in der Umsetzung oder bei Maßnahmen zur Informationssicherheit, die ausgenutzt werden und zu einer Verletzung des Informationssicherheitskonzepts führen könnten.

Artikel 4

Anforderungen an Organisationen und zuständige Behörden

(1) Die in Artikel 2 Absatz 1 genannten Organisationen müssen die Anforderungen von Anhang II (Teil-IS.I.OR) dieser Verordnung erfüllen.

(2) Die in Artikel 2 Absätze 2 und 3 genannten zuständigen Behörden müssen die Anforderungen von Anhang I (Teil-IS.AR) dieser Verordnung erfüllen.

Artikel 5

Anforderungen, die sich aus anderen Rechtsvorschriften der Union ergeben

(1) Erfüllt eine in Artikel 2 Absatz 1 genannte Organisation Sicherheitsanforderungen, die in Artikel 14 der Richtlinie (EU) 2016/1148 festgelegt und den Anforderungen dieser Verordnung gleichwertig sind, so gilt die Einhaltung jener Sicherheitsanforderungen als Erfüllung der in dieser Verordnung festgelegten Anforderungen.

(2) Handelt es sich bei einer in Artikel 2 Absatz 1 genannten Organisation um einen Betreiber oder eine Stelle, auf die in den nationalen Luftsicherheitsprogrammen der Mitgliedstaaten nach Artikel 10 der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates ([15]) Bezug genommen wird, so gelten die in Nummer 1.7 des Anhangs der Durchführungsverordnung (EU) 2015/1998 festgelegten Cybersicherheitsanforderungen als gleichwertig mit den Anforderungen dieser Verordnung, mit Ausnahme von Punkt IS.I.OR.230 des Anhangs II dieser Verordnung, der als solcher eingehalten werden muss.

(3) Handelt es sich bei der in Artikel 2 Absatz 1 genannten Organisation um den Anbieter von Flugsicherungsdiensten der Europäischen Erweiterung des geostationären Navigationssystems (EGNOS) gemäß der Verordnung (EU) 2021/696, so gelten die Sicherheitsanforderungen nach Titel V Artikel 33 bis 43 jener Verordnung als gleichwertig mit den Anforderungen dieser Verordnung, mit Ausnahme von Anhang II Punkt IS.I.OR.230 dieser Verordnung, der als solcher eingehalten werden muss.

(4) Die Kommission kann nach Konsultation der Agentur und der in Artikel 11 der Richtlinie (EU) 2016/1148 genannten Kooperationsgruppe Leitlinien für die Bewertung der Gleichwertigkeit der in dieser Verordnung und der Richtlinie (EU) 2016/1148 festgelegten Anforderungen herausgeben.

Artikel 6

Zuständige Behörde

(1) Unbeschadet der der Sicherheitsakkreditierungsstelle (SAB) nach Artikel 36 der Verordnung (EU) 2021/696 übertragenen Aufgaben ist für die Bescheinigung und Überwachung der Einhaltung dieser Verordnung folgende Behörde zuständig:

a) In Bezug auf die in Artikel 2 Absatz 1 Buchstabe a genannten Organisationen die nach Anhang II (Teil-145) der Verordnung (EU) Nr. 1321/2014 benannte zuständige Behörde;

b) in Bezug auf die in Artikel 2 Absatz 1 Buchstabe b genannten Organisationen die nach Anhang Vc (Teil-CAMO) der Verordnung (EU) Nr. 1321/2014 benannte zuständige Behörde;

([15]) Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72).

c) in Bezug auf die in Artikel 2 Absatz 1 Buchstabe c genannten Organisationen die nach Anhang III (Teil-ORO) der Verordnung (EU) Nr. 965/2012 benannte zuständige Behörde;

d) in Bezug auf die in Artikel 2 Absatz 1 Buchstaben d bis f genannten Organisationen die nach Anhang VII (Teil-ORA) der Verordnung (EU) Nr. 1178/2011 benannte zuständige Behörde;

e) in Bezug auf die in Artikel 2 Absatz 1 Buchstabe g genannten Organisationen die nach Artikel 6 Absatz 2 der Verordnung (EU) 2015/340 benannte zuständige Behörde;

f) in Bezug auf die in Artikel 2 Absatz 1 Buchstabe h genannten Organisationen die nach Artikel 4 Absatz 1 der Durchführungsverordnung (EU) 2017/373 benannte zuständige Behörde;

g) in Bezug auf die in Artikel 2 Absatz 1 Buchstabe i genannten Organisationen die nach Artikel 14 Absatz 1 oder Absatz 2 der Durchführungsverordnung (EU) 2021/664 benannte zuständige Behörde.

(2) Die Mitgliedstaaten können für die Zwecke dieser Verordnung eine unabhängige und autonome Stelle benennen, die die zugewiesenen Aufgaben und Zuständigkeiten der in Absatz 1 genannten zuständigen Behörden wahrnimmt. In diesem Fall müssen zwischen dieser Stelle und den in Absatz 1 genannten zuständigen Behörden Koordinierungsmaßnahmen festgelegt werden, damit eine wirksame Aufsicht über alle von der Organisation zu erfüllenden Anforderungen gewährleistet ist.

(3) Zur Gewährleistung einer wirksamen Aufsicht über die für Anbieter von EGNOS-Flugsicherungsdiensten geltenden Anforderungen muss die Agentur unter uneingeschränkter Einhaltung der geltenden Vorschriften über die Geheimhaltung, den Schutz personenbezogener Daten und den Schutz von Verschlusssachen mit der Agentur der Europäischen Union für das Weltraumprogramm (EUSPA) und der in Artikel 36 der Verordnung (EU) 2021/696 genannten Sicherheitsakkreditierungsstelle zusammenarbeiten.

Artikel 7

Übermittlung relevanter Informationen an die zuständigen NIS-Behörden

Die gemäß dieser Verordnung zuständigen Behörden unterrichten die nach Artikel 8 der Richtlinie (EU) 2016/1148 benannte zentrale Anlaufstelle unverzüglich über alle relevanten Informationen, die in Meldungen enthalten sind, die nach Anhang II Punkt IS.I.OR.230 dieser Verordnung und nach Anhang I Punkt IS.D.OR.230 Delegierten Verordnung (EU) 2022/1645 von nach Artikel 5 der Richtlinie (EU) 2016/1148 ermittelten Betreibern wesentlicher Dienste übermittelt wurden.

Artikel 8

Änderung der Verordnung (EU) Nr. 1178/2011

Anhang VI (Teil-ARA) und Anhang VII (Teil-ORA) der Verordnung (EU) Nr. 1178/2011 werden gemäß Anhang III dieser Verordnung geändert.

Artikel 9

Änderung der Verordnung (EU) Nr. 748/2012

Anhang I (Teil 21) der Verordnung (EU) Nr. 748/2012 wird gemäß Anhang IV dieser Verordnung geändert.

Artikel 10

Änderung der Verordnung (EU) Nr. 965/2012

Anhang II (Teil-ARO) und Anhang III (Teil-ORO) der Verordnung (EU) Nr. 965/2012 werden gemäß Anhang V dieser Verordnung geändert.

Artikel 11

Änderung der Verordnung (EU) Nr. 139/2014

Anhang II (Teil-ADR.AR) der Verordnung (EU) Nr. 139/2014 wird gemäß Anhang VI dieser Verordnung geändert.

Artikel 12

Änderung der Verordnung (EU) Nr. 1321/2014

Anhang II (Teil-145), Anhang III (Teil-66) und Anhang Vc (Teil-CAMO) der Verordnung (EU) Nr. 1321/2014 werden gemäß Anhang VII dieser Verordnung geändert.

Artikel 13

Änderung der Verordnung (EU) 2015/340

Anhang II (Teil ATCO.AR) und Anhang III (Teil ATCO.OR) der Verordnung (EU) 2015/340 werden gemäß Anhang VIII dieser Verordnung geändert.

Artikel 14

Änderung der Durchführungsverordnung (EU) 2017/373

Anhang II (Teil-ATM/ANS.AR) und Anhang III (Teil-ATM/ANS.OR) der Durchführungsverordnung (EU) 2017/373 werden gemäß Anhang IX dieser Verordnung geändert.

Artikel 15

Änderung der Durchführungsverordnung (EU) 2021/664

Die Durchführungsverordnung (EU) 2021/664 wird wie folgt geändert:

1. Artikel 15 Absatz 1 Buchstabe f erhält folgende Fassung:

„f) ein Sicherheitsmanagementsystem nach Anhang III Teilabschnitt D Punkt ATM/ANS.OR.D.010 der Durchführungsverordnung (EU) 2017/373 und ein Informationssicherheitsmanagementsystem nach Anhang II (Teil-IS.I.OR) der Durchführungsverordnung (EU) 2023/203 implementieren und pflegen."

2. In Artikel 18 wird folgender Buchstabe l angefügt:

„l) ein Informationssicherheitsmanagementsystem nach Anhang I (Teil-IS.AR) der Durchführungsverordnung (EU) 2023/203 festlegen, implementieren und pflegen."

Artikel 16

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem 22. Februar 2026.

Für die Anbieter von EGNOS-Flugsicherungsdiensten nach der Durchführungsverordnung (EU) 2017/373, gilt sie jedoch ab dem 1. Januar 2026.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 27. Oktober 2022

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG I

INFORMATIONSSICHERHEIT — ANFORDERUNGEN AN DIE BEHÖRDE

[TEIL-IS.AR]

IS.AR.100 Umfang

IS.AR.200 Informationssicherheitsmanagementsystem (ISMS)

IS.AR.205 Bewertung des Informationssicherheitsrisikos

IS.AR.210 Umgang mit dem Informationssicherheitsrisiko

IS.AR.215 Störungen der Informationssicherheit — Erkennung, Reaktion und Wiederherstellung

IS.AR.220 Auftragsvergabe für Tätigkeiten des Informationssicherheitsmanagements

IS.AR.225 Anforderungen an das Personal

IS.AR.230 Führen von Aufzeichnungen

IS.AR.235 Kontinuierliche Verbesserung

IS.AR.100 Umfang

In diesem Teil werden die Anforderungen festgelegt, die die in Artikel 2 Absatz 2 dieser Verordnung genannten zuständigen Behörden erfüllen müssen.

Die Anforderungen, die diese zuständigen Behörden bei der Durchführung ihrer Zertifizierungs-, Aufsichts- und Durchsetzungstätigkeiten erfüllen müssen, sind in den Verordnungen enthalten, die in Artikel 2 Absatz 1 dieser Verordnung und in Artikel 2 der Delegierten Verordnung (EU) 2022/1645 aufgeführt sind.

IS.AR.200 Informationssicherheitsmanagementsystem (ISMS)

a) Damit die in Artikel 1 genannten Ziele erreicht werden, muss die zuständige Behörde ein Informationssicherheitsmanagementsystem (ISMS) einrichten, umsetzen und pflegen, mit dem sie Folgendes sicherstellt:

1. Festlegung eines Konzepts für die Informationssicherheit, in dem die allgemeinen Grundsätze der zuständigen Behörde im Hinblick auf die potenziellen Auswirkungen von Informationssicherheitsrisiken auf die Flugsicherheit dargelegt werden;

2. Identifizierung und Überprüfung von Informationssicherheitsrisiken nach Punkt IS.AR.205;

3. Festlegung und Umsetzung der Maßnahmen für den Umgang mit Informationssicherheitsrisiken nach Punkt IS.AR.210;

4. Festlegung und Umsetzung nach Punkt IS.AR.215 der zur Erkennung von Informationssicherheitsereignissen notwendigen Maßnahmen, Identifizierung solcher Ereignisse, die als Störungen mit potenziellen Auswirkungen auf die Flugsicherheit gelten, sowie Reaktion auf diese Störungen der Informationssicherheit und Wiederherstellung;

5. Erfüllung der Anforderungen von Punkt IS.AR.220 für den Fall, dass ein Teil der unter Punkt IS.AR.200 genannten Tätigkeiten an andere Organisationen vergeben wird;

6. Erfüllung der Anforderungen an das Personal nach Punkt IS.AR.225;

7. Erfüllung der Anforderung an das Führen von Aufzeichnungen nach Punkt IS.AR.230;

8. Überwachung der Einhaltung der Anforderungen dieser Verordnung durch die eigene Organisation und Unterrichtung der unter Punkt IS.AR.225 Buchstabe a genannten Person über Beanstandungen, damit Abhilfemaßnahmen wirksam umgesetzt werden;

9. Schutz der Vertraulichkeit aller Informationen, die der zuständigen Behörde möglicherweise im Zusammenhang mit ihrer Aufsicht unterliegenden Organisationen vorliegen, und der Informationen, die sie über Systeme der Organisation für externe Meldungen erhalten hat, die nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.230 dieser Verordnung und nach dem Anhang (Teil-IS.D.OR) Punkt IS.D.OR.230 der Delegierten Verordnung (EU) 2022/1645 eingerichtet wurden;

10. Mitteilung von Änderungen an die Agentur, die sich auf die Fähigkeit der zuständigen Behörde auswirken, ihre Aufgaben und Zuständigkeiten im Sinne dieser Verordnung wahrzunehmen;

11. Festlegung und Umsetzung von Verfahren für die praktische und zeitnahe Weitergabe relevanter Informationen an andere zuständige Behörden und Agenturen sowie Organisationen, die dieser Verordnung unterliegen, damit diese wirksame Sicherheitsrisikobewertungen in Bezug auf ihre Tätigkeiten vornehmen können.

b) Zur kontinuierlichen Einhaltung der in Artikel 1 genannten Anforderungen muss die zuständige Behörde nach Punkt IS.AR.235 einen Prozess für kontinuierliche Verbesserungen implementieren.

c) Die zuständige Behörde muss alle wesentlichen Prozesse, Verfahren, Aufgaben und Verantwortlichkeiten dokumentieren, die zur Einhaltung von Punkt IS.AR.200(a) erforderlich sind, und ein Verfahren zur Änderung dieser Dokumentation festlegen.

d) Die Prozesse, Verfahren, Funktionen und Zuständigkeiten, die von der zuständigen Behörde festgelegt wurden, um Punkt IS.AR.200(a) zu erfüllen, müssen — beruhend auf einer Bewertung der mit diesen Tätigkeiten verbundenen Informationssicherheitsrisiken — der Art und Komplexität ihrer Tätigkeiten entsprechen und können in andere bestehende Managementsysteme integriert werden, die die zuständige Behörde bereits eingeführt hat.

IS.AR.205 Bewertung des Informationssicherheitsrisikos

a) Die zuständige Behörde muss alle Elemente ihrer eigenen Organisation ermitteln, die Informationssicherheitsrisiken ausgesetzt sein könnten. Dies schließt Folgendes ein:

1. Die Tätigkeiten, Einrichtungen und Ressourcen der zuständigen Behörde sowie die Dienste, die die zuständige Behörde betreibt, erbringt, erhält oder aufrechterhält;

2. die Ausrüstung, Systeme, Daten und Informationen, die zur Funktionsfähigkeit der unter Nummer 1 aufgeführten Elemente beitragen.

b) Die zuständige Behörde identifiziert die Schnittstellen zwischen ihrer eigenen Organisation und anderen Organisationen, die dazu führen könnten, dass sie gegenseitig Informationssicherheitsrisiken ausgesetzt sind.

c) In Bezug auf die unter den Buchstaben a und b genannten Elemente und Schnittstellen identifiziert die zuständige Behörde die Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können.

Für jedes identifizierte Risiko muss die zuständige Behörde

1. eine Eistufung des Risikoniveaus gemäß einer vorab von der zuständigen Behörde definierten Klassifizierung vornehmen;

2. jedes Risiko und dessen Niveau mit den entsprechenden gemäß den Buchstaben a und b identifizierten Elementen oder Schnittstellen verknüpfen.

Bei der in Nummer 1 genannten vordefinierten Klassifizierung müssen das Potenzial des Auftretens des Bedrohungsszenarios sowie die Schwere seiner Folgen für die Sicherheit berücksichtigt werden. Auf der Grundlage dieser Klassifizierung und unter Berücksichtigung der Frage, ob die zuständige Behörde über einen strukturierten und wiederholbaren Risikomanagementprozess für den Betrieb verfügt, muss die zuständige Behörde feststellen können, ob das Risiko hinnehmbar ist oder ein Tätigwerden nach Punkt IS.AR.210 erfordert.

Im Sinne einer leichteren gegenseitigen Vergleichbarkeit der Risikobewertungen müssen bei der Zuweisung des Risikoniveaus nach Nummer 1 einschlägige Informationen berücksichtigt werden, die in Abstimmung mit den unter Buchstabe b genannten Organisationen gewonnen wurden.

d) Die zuständige Behörde muss die nach den Buchstaben a, b und c durchgeführte Risikobewertung immer dann überprüfen und aktualisieren, wenn einer der folgenden Fälle eintritt:

1. Bei den Elementen, die Risiken für die Informationssicherheit ausgesetzt sind, ist eine Änderung eingetreten.

2. Bei den Schnittstellen zwischen der Organisation der zuständigen Behörde und anderen Organisationen oder bei den von den anderen Organisationen mitgeteilten Risiken ist eine Änderung eingetreten.

3. Bei den für die Identifizierung, Analyse und Klassifizierung von Risiken verwendeten Informationen und Kenntnissen ist eine Änderung eingetreten.

4. Aus der Analyse der Störungen der Informationssicherheit haben sich neue Erkenntnisse ergeben.

IS.AR.210 Umgang mit dem Informationssicherheitsrisiko

a) Die zuständige Behörde muss Maßnahmen für nach Punkt IS.AR.205 identifizierte und nicht hinnehmbare Risiken entwickeln, zeitnah umsetzen und kontinuierlich auf deren Wirksamkeit prüfen. Diese Maßnahmen müssen die zuständige Behörde in die Lage versetzen,

1. die Umstände zu kontrollieren, die zum tatsächlichen Auftreten des Bedrohungsszenarios beitragen;

2. die Folgen des tatsächlichen Eintretens des Bedrohungsszenarios für die Flugsicherheit zu verringern;

3. die Risiken zu vermeiden.

Diese Maßnahmen dürfen nicht dazu führen, dass neue potenzielle und nicht hinnehmbare Risiken für die Flugsicherheit entstehen.

b) Die in Punkt IS.AR.225(a) genannte Person und sonstiges betroffenes Personal der zuständigen Behörde müssen über das Ergebnis der nach Punkt IS.AR.205 durchgeführten Risikobewertung, die entsprechenden Bedrohungsszenarien und die durchzuführenden Maßnahmen unterrichtet werden.

Die zuständige Behörde muss auch Organisationen, zu denen sie eine Schnittstelle nach Punkt IS.AR.205(b) aufweist, über alle zwischen der zuständigen Behörde und der Organisation geteilten Risiken informieren.

IS.AR.215 Störungen der Informationssicherheit — Erkennung, Reaktion und Wiederherstellung

a) Auf der Grundlage des Ergebnisses der nach Punkt IS.AR.205 durchgeführten Risikobewertung und des Ergebnisses nach Punkt IS.AR.210 aus dem Umgang mit dem Risiko muss die zuständige Behörde Maßnahmen ergreifen, um Ereignisse zu erkennen, die auf das potenzielle Eintreten nicht hinnehmbarer Risiken, die sich auf die Flugsicherheit auswirken können, schließen lassen. Diese Detektionsmaßnahmen müssen die Organisation in die Lage versetzen,

1. Abweichungen von vorab festgelegten funktionalen Leistungsgrundwerten zu identifizieren,

2. Warnungen auszulösen, mit denen bei Abweichungen geeignete Gegenmaßnahmen aktiviert werden.

b) Die zuständige Behörde muss Maßnahmen ergreifen, mit denen sie auf alle nach Buchstabe a identifizierten Ereigniszustände reagiert, die sich zu einer Störung der Informationssicherheit entwickeln können oder sich zu einer solchen entwickelt haben. Diese Reaktionsmaßnahmen müssen die zuständige Behörde in die Lage versetzen,

1. die Reaktion auf die Warnhinweise ihrer eigenen Organisation nach Buchstabe a Nummer 2 einzuleiten, indem vordefinierte Ressourcen und Handlungsabläufe aktiviert werden;

2. die Ausbreitung eines Angriffs einzudämmen und die vollständige Entfaltung eines Bedrohungsszenarios zu verhindern;

3. den Ausfallmodus der betroffenen Elemente nach Punkt IS.AR.205(a) zu steuern.

c) Die zuständige Behörde muss Maßnahmen ergreifen, die der Wiederherstellung nach Störungen der Informationssicherheit dienen, auch gegebenenfalls durch Notfallmaßnahmen. Diese Wiederherstellungsmaßnahmen müssen die zuständige Behörde in die Lage versetzen,

1. den Zustand, der die Störung verursacht hat, zu beseitigen oder ihn auf ein tolerierbares Maß zu beschränken;

2. innerhalb einer zuvor von ihrer eigenen Organisation festgelegten Wiederherstellungszeit einen sicheren Zustand der in Punkt IS.AR.205(a) bereits definierten betroffenen Elemente wiederherzustellen.

IS.AR.220 Auftragsvergabe für Tätigkeiten des Informationssicherheitsmanagements

Die zuständige Behörde muss sicherstellen, dass bei der Vergabe eines Teils der unter Punkt IS.AR.200 genannten Tätigkeiten an andere Organisationen die in Auftrag gegebenen Tätigkeiten den Anforderungen dieser Verordnung genügen und dass die beauftragte Organisation unter ihrer Aufsicht arbeitet. Die zuständige Behörde muss sicherstellen, dass die mit den vertraglich vereinbarten Tätigkeiten verbundenen Risiken angemessen gemanagt werden.

IS.AR.225 Anforderungen an das Personal

Die zuständige Behörde muss

a) über eine Person verfügen, die befugt ist, die zur Durchführung dieser Verordnung erforderlichen organisatorischen Strukturen, Strategien, Prozesse und Verfahren festzulegen und aufrechtzuerhalten.

   Diese Person muss

   1. über die Befugnis verfügen, uneingeschränkt auf die Ressourcen zuzugreifen, die die zuständige Behörde zur Erfüllung aller in dieser Verordnung vorgeschriebenen Aufgaben benötigt;

   2. die Befugnisse übertragen bekommen, die sie zur Wahrnehmung der ihr übertragenen Aufgaben benötigt;

b) über ein Verfahren verfügen, mit dem sichergestellt wird, dass sie über genügend Personal verfügt, das die Durchführung der unter diesen Anhang fallenden Tätigkeiten wahrnehmen kann;

c) über ein Verfahren verfügen, mit dem sichergestellt wird, dass das unter Buchstabe b genannte Personal über die für die Wahrnehmung seiner Aufgaben erforderliche Kompetenz verfügt;

d) über ein Verfahren verfügen, mit dem sichergestellt wird, dass das Personal die mit den zugewiesenen Funktionen und Aufgaben verbundene Verantwortung anerkennt;

e) sicherstellen, dass die Identität und Vertrauenswürdigkeit des Personals, das Zugang zu Informationssystemen und Daten hat, die den Anforderungen dieser Verordnung unterliegen, angemessen festgestellt wird.

IS.AR.230 Führen von Aufzeichnungen

a) Die zuständige Behörde muss Aufzeichnungen über ihre Tätigkeiten im Bereich des Informationssicherheitsmanagements führen.

   1. Die zuständige Behörde muss sicherstellen, dass die folgenden Aufzeichnungen archiviert werden und zurückverfolgt werden können:

      i) Auftragsvergaben für Tätigkeiten nach Punkt IS.AR.200(a)(5);

      ii) Aufzeichnungen der wichtigsten in Punkt IS.AR.200(d) genannten Prozesse;

      iii) Aufzeichnungen über die bei der Risikobewertung nach Punkt IS.AR.205 ermittelten Risiken zusammen mit den damit verbundenen Maßnahmen zum Umgang mit den Risiken nach Punkt IS.AR.210;

      iv) Aufzeichnungen über Informationssicherheitsereignisse, die möglicherweise neu bewertet werden müssen, um unentdeckte Störungen und Schwachstellen der Informationssicherheit aufzudecken.

   2. Die Aufzeichnungen nach Nummer 1 Ziffer i müssen mindestens fünf Jahre nach Änderung oder Beendigung des Auftrags aufbewahrt werden.

   3. Die Aufzeichnungen nach Nummer 1 Ziffern ii und iii müssen mindestens fünf Jahre lang aufbewahrt werden.

   4. Die Aufzeichnungen nach Nummer 1 Ziffer iv müssen so lange aufbewahrt werden, bis diese Informationssicherheitsereignisse gemäß der Periodizität neu bewertet worden sind, die in einem von der zuständigen Behörde festgelegten Verfahren definiert wurde.

b) Die zuständige Behörde muss Aufzeichnungen über die Qualifikation und Erfahrung ihres eigenen Personals führen, das an Tätigkeiten des Informationssicherheitsmanagements beteiligt ist.

1. Die Aufzeichnungen über Qualifikation und Erfahrung des Personals müssen so lange aufbewahrt werden, wie die Person für die zuständige Behörde tätig ist, und für einen Zeitraum von mindestens drei Jahren, nachdem die Person die zuständige Behörde verlassen hat.

2. Mitglieder des Personals erhalten auf Antrag Zugang zu ihren Personalakten. Darüber hinaus muss die zuständige Behörde ihnen zum Zeitpunkt des Verlassens der zuständigen Behörde auf Anfrage eine Kopie ihrer Personalakte aushändigen.

c) Das Format der Aufzeichnungen muss in den Verfahren der zuständigen Behörde festgelegt werden.

d) Die Aufzeichnungen müssen so aufbewahrt werden, dass sie vor Beschädigung, Änderung und Diebstahl geschützt sind, wobei die Informationen bei Bedarf entsprechend dem Niveau der Sicherheitsklassifizierung zu kennzeichnen sind. Die zuständige Behörde muss sicherstellen, dass die Aufzeichnungen so aufbewahrt werden, dass Integrität, Authentizität und autorisierter Zugang gewährleistet werden.

IS.AR.235 Kontinuierliche Verbesserung

a) Die zuständige Behörde muss anhand geeigneter Leistungsindikatoren die Wirksamkeit und Ausgereiftheit ihres eigenen ISMS bewerten. Diese Bewertung muss nach einem von der zuständigen Behörde vorab festgelegten Zeitplan oder nach einer Störung der Informationssicherheit durchgeführt werden.

b) Werden bei der Bewertung nach Buchstabe a Mängel festgestellt, muss die zuständige Behörde die erforderlichen Verbesserungsmaßnahmen ergreifen, damit das ISMS weiterhin den geltenden Anforderungen entspricht und die Informationssicherheitsrisiken auf einem annehmbaren Niveau hält. Darüber hinaus muss die zuständige Behörde die Elemente des ISMS, die von den angenommenen Maßnahmen betroffen sind, neu bewerten.

ANHANG II

INFORMATIONSSICHERHEIT — ANFORDERUNGEN AN ORGANISATIONEN

[TEIL-IS.I.OR]

IS.I.OR.100 Umfang

IS.I.OR.200 Informationssicherheitsmanagementsystem (ISMS)

IS.I.OR.205 Bewertung des Informationssicherheitsrisikos

IS.I.OR.210 Umgang mit dem Informationssicherheitsrisiko

IS.I.OR.215 Informationssicherheitssystem für interne Meldungen

IS.I.OR.220 Störungen der Informationssicherheit — Erkennung, Reaktion und Wiederherstellung

IS.I.OR.225 Reaktion auf von der zuständigen Behörde gemeldete Beanstandungen

IS.I.OR.230 Informationssicherheitssystem für externe Meldungen

IS.I.OR.235 Auftragsvergabe für Tätigkeiten des Informationssicherheitsmanagements

IS.I.OR.240 Anforderungen an das Personal

IS.I.OR.245 Führen von Aufzeichnungen

IS.I.OR.250 Handbuch zum Informationssicherheitsmanagement (ISMM)

IS.I.OR.255 Änderungen des Informationssicherheitsmanagementsystems

IS.I.OR.260 Kontinuierliche Verbesserung

IS.I.OR.100 Umfang

In diesem Teil werden die Anforderungen festgelegt, die die in Artikel 2 Absatz 1 dieser Verordnung genannten Organisationen erfüllen müssen.

IS.I.OR.200 Informationssicherheitsmanagementsystem (ISMS)

a) Damit die in Artikel 1 genannten Ziele erreicht werden, muss die Organisation ein Informationssicherheitsmanagementsystem (ISMS) einrichten, umsetzen und pflegen, mit dem sie Folgendes sicherstellt:

   1. Festlegung eines Konzepts für die Informationssicherheit, in dem die allgemeinen Grundsätze der Organisation im Hinblick auf die potenziellen Auswirkungen von Informationssicherheitsrisiken auf die Flugsicherheit dargelegt werden;

   2. Identifizierung und Überprüfung von Informationssicherheitsrisiken nach Punkt IS.I.OR.205;

   3. Festlegung und Umsetzung der Maßnahmen für den Umgang mit Informationssicherheitsrisiken nach Punkt IS.I.OR.210;

   4. Umsetzung eines Informationssicherheitssystems für interne Meldungen nach Punkt IS.I.OR.215;

   5. Festlegung und Umsetzung nach Punkt IS.I.OR.220 der zur Erkennung von Informationssicherheitsereignissen notwendigen Maßnahmen, Identifizierung solcher Ereignisse, die als Störungen mit potenziellen Auswirkungen auf die Flugsicherheit gelten, es sei denn, dies ist nach Punkt IS.I.OR.205(e) zulässig, sowie Reaktion auf diese Störungen der Informationssicherheit und Wiederherstellung;

6. Umsetzung der Maßnahmen, die von der zuständigen Behörde als unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit gemeldet wurden;

7. Ergreifung geeigneter Maßnahmen nach Punkt IS.I.OR.225, um den von der zuständigen Behörde mitgeteilten Beanstandungen Rechnung zu tragen;

8. Umsetzung eines Systems für externe Meldungen nach Punkt IS.I.OR.230, damit die zuständige Behörde geeignete Maßnahmen ergreifen kann;

9. Erfüllung der Anforderungen von Punkt IS.I.OR.235 für den Fall, dass ein Teil der unter Punkt IS.I.OR.200 genannten Tätigkeiten an andere Organisationen vergeben wird;

10. Erfüllung der Anforderungen an das Personal nach Punkt IS.I.OR.240;

11. Erfüllung der Anforderung an das Führen von Aufzeichnungen nach Punkt IS.I.OR.245;

12. Überwachung der Einhaltung der Anforderungen dieser Verordnung durch die Organisation und Unterrichtung des leitenden Managers über Beanstandungen, damit Abhilfemaßnahmen wirksam umgesetzt werden;

13. Schutz der Vertraulichkeit aller Informationen, die die Organisation möglicherweise von anderen Organisationen erhalten hat, unbeschadet geltender Vorschriften über die Meldung von Störungen und abhängig von deren Sensibilitätsgrad.

b) Zur kontinuierlichen Einhaltung der in Artikel 1 genannten Anforderungen muss die Organisation nach Punkt IS.I.OR.260 einen Prozess für kontinuierliche Verbesserungen implementieren.

c) Die Organisation muss nach Punkt IS.I.OR.250 alle wesentlichen Prozesse, Verfahren, Aufgaben und Verantwortlichkeiten dokumentieren, die zur Einhaltung von Punkt IS.I.OR.200(a) erforderlich sind, und ein Verfahren zur Änderung dieser Dokumentation festlegen. Änderungen dieser Prozesse, Verfahren, Funktionen und Zuständigkeiten müssen nach Punkt IS.I.OR.255 verwaltet werden.

d) Die Prozesse, Verfahren, Funktionen und Zuständigkeiten, die von der Organisation festgelegt wurden, um Punkt IS.I.OR.200(a) zu erfüllen, müssen — beruhend auf einer Bewertung der mit diesen Tätigkeiten verbundenen Informationssicherheitsrisiken — der Art und Komplexität ihrer Tätigkeiten entsprechen und können in andere bestehende Managementsysteme integriert werden, die die Organisation bereits eingeführt hat.

e) Unbeschadet der Meldepflichten gemäß der Verordnung (EU) Nr. 376/2014 und der Anforderungen von Punkt IS.I.OR.200(a)(13) kann die zuständige Behörde der Organisation die Genehmigung erteilen, die unter den Buchstaben a bis d genannten und die diesbezüglich in den Punkten IS.I.OR.205 bis IS.I.OR.260 enthaltenen Anforderungen nicht umzusetzen, wenn diese zur Zufriedenheit der Behörde nachweist, dass ihre Tätigkeiten, Einrichtungen und Ressourcen sowie die von ihr betriebenen, angebotenen, erhaltenen und aufrechterhaltenen Dienste keine Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit weder für ihre eigene noch für andere Organisationen darstellen. Voraussetzung für die Genehmigung ist eine dokumentierte Bewertung des Informationssicherheitsrisikos, die von der Organisation oder einem Dritten nach Punkt IS.I.OR.205 durchgeführt und von ihrer zuständigen Behörde überprüft und genehmigt wurde.

Die Aufrechterhaltung der Gültigkeit dieser Genehmigung wird von der zuständigen Behörde nach dem geltenden Auditzyklus für die Aufsicht und immer dann überprüft, wenn Änderungen im Tätigkeitsumfang der Organisation vorgenommen werden.

IS.I.OR.205 Bewertung des Informationssicherheitsrisikos

a) Die Organisation muss alle Elemente ermitteln, die bei ihr vorliegen und die Informationssicherheitsrisiken ausgesetzt sein könnten. Dies schließt Folgendes ein:

1. die Tätigkeiten, Einrichtungen und Ressourcen der Organisation sowie die Dienste, die die Organisation betreibt, erbringt, erhält oder aufrechterhält;

2. die Ausrüstung, Systeme, Daten und Informationen, die zur Funktionsfähigkeit der unter Nummer 1 aufgeführten Elemente beitragen.

b) Die Organisation identifiziert die Schnittstellen zu anderen Organisationen, die dazu führen könnten, dass sie gegenseitig Informationssicherheitsrisiken ausgesetzt sind.

c) In Bezug auf die unter den Buchstaben a und b genannten Elemente und Schnittstellen identifiziert die Organisation die Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können. Für jedes identifizierte Risiko muss die Organisation

1. eine Eistufung des Risikoniveaus gemäß einer vorab von der Organisation definierten Klassifizierung vornehmen;

2. jedes Risiko und dessen Niveau mit den entsprechenden gemäß den Buchstaben a und b identifizierten Elementen oder Schnittstellen verknüpfen.

Bei der in Nummer 1 genannten vordefinierten Klassifizierung müssen das Potenzial des Auftretens des Bedrohungsszenarios sowie die Schwere seiner Folgen für die Sicherheit berücksichtigt werden. Auf der Grundlage dieser Klassifizierung und unter Berücksichtigung der Frage, ob die Organisation über einen strukturierten und wiederholbaren Risikomanagementprozess für den Betrieb verfügt, muss die Organisation feststellen können, ob das Risiko hinnehmbar ist oder ein Tätigwerden nach Punkt IS.I.OR.210 erfordert.

Im Sinne einer leichteren gegenseitigen Vergleichbarkeit der Risikobewertungen müssen bei der Zuweisung des Risikoniveaus nach Nummer 1 einschlägige Informationen berücksichtigt werden, die in Abstimmung mit den unter Buchstabe b genannten Organisationen gewonnen wurden.

d) Die Organisation muss die nach den Buchstaben a und b sowie gegebenenfalls c oder e durchgeführte Risikobewertung immer dann überprüfen und aktualisieren, wenn eine der folgenden Situationen eintritt:

1. Bei den Elementen, die Risiken für die Informationssicherheit ausgesetzt sind, ist eine Änderung eingetreten.

2. Bei den Schnittstellen zwischen der Organisation und anderen Organisationen oder bei den von den anderen Organisationen mitgeteilten Risiken ist eine Änderung eingetreten.

3. Bei den für die Identifizierung, Analyse und Klassifizierung von Risiken verwendeten Informationen und Kenntnissen ist eine Änderung eingetreten.

4. Aus der Analyse der Störungen der Informationssicherheit haben sich neue Erkenntnisse ergeben.

e) Abweichend von Buchstabe c müssen Organisationen, die die Anforderungen von Anhang III (Teil-ATM/ANS.OR) Unterabschnitt C der Durchführungsverordnung (EU) 2017/373 erfüllen müssen, die Analyse der Auswirkungen auf die Flugsicherheit durch eine Analyse der Auswirkungen auf ihre Dienste im Rahmen der nach Punkt ATM/ANS.OR.C.005 geforderten unterstützenden Sicherheitsbeurteilung ersetzen. Diese unterstützende Sicherheitsbeurteilung muss den Anbietern von Flugverkehrsdiensten, für die sie Dienste erbringen und die auch für die Bewertung der Auswirkungen auf die Flugsicherheit verantwortlich sind, zur Verfügung gestellt werden.

IS.I.OR.210 Umgang mit dem Informationssicherheitsrisiko

a) Die Organisation muss Maßnahmen für nach Punkt IS.I.OR.205 identifizierte und nicht hinnehmbare Risiken entwickeln, zeitnah umsetzen und kontinuierlich auf deren Wirksamkeit prüfen. Diese Maßnahmen müssen die Organisation in die Lage versetzen,

1. die Umstände zu kontrollieren, die zum tatsächlichen Auftreten des Bedrohungsszenarios beitragen;

2. die Folgen des tatsächlichen Eintretens des Bedrohungsszenarios für die Flugsicherheit zu verringern;

3. die Risiken zu vermeiden.

Diese Maßnahmen dürfen nicht dazu führen, dass neue potenzielle und nicht hinnehmbare Risiken für die Flugsicherheit entstehen.

b) Die in Punkt IS.I.OR.240(a) und (b) genannte Person und sonstiges betroffenes Personal der Organisation müssen über das Ergebnis der nach Punkt IS.I.OR.205 durchgeführten Risikobewertung, die entsprechenden Bedrohungsszenarien und die durchzuführenden Maßnahmen unterrichtet werden.

Die Organisation muss auch Organisationen, zu denen sie eine Schnittstelle nach Punkt IS.I.OR.205(b) aufweist, über alle zwischen beiden Organisationen geteilten Risiken informieren.

IS.I.OR.215 Informationssicherheitssystem für interne Meldungen

a) Die Organisation muss ein System für interne Meldungen einrichten, das die Erfassung und Bewertung von Informationssicherheitsereignissen, einschließlich solcher, die nach Punkt IS.I.OR.230 zu melden sind, ermöglicht.

b) Dieses System und das Verfahren nach Punkt IS.I.OR.220 müssen der Organisation Folgendes ermöglichen:

1. Identifizierung, welche der nach Buchstabe a gemeldeten Ereignisse als Störungen oder Schwachstellen der Informationssicherheit mit potenziellen Auswirkungen auf die Flugsicherheit gelten;

2. Identifizierung der Ursachen der nach Nummer 1 identifizierten Störungen und Schwachstellen der Informationssicherheit und der dazu beitragenden Faktoren sowie deren Bewältigung im Rahmen des Prozesses für das Sicherheitsrisikomanagement nach den Punkten IS.I.OR.205 und IS.I.OR.220;

3. Gewährleistung einer Bewertung aller bekannten und relevanten Informationen im Zusammenhang mit den nach Nummer 1 identifizierten Störungen und Schwachstellen der Informationssicherheit;

4. Gewährleistung, dass eine Methode eingeführt wird, nach der die Informationen je nach Bedarf intern verbreitet werden.

c) Jeder Auftragnehmer, der die Organisation möglicherweise Informationssicherheitsrisiken aussetzt, die sich auf die Flugsicherheit auswirken können, ist verpflichtet, der Organisation Informationssicherheitsereignisse zu melden. Diese Meldungen müssen nach den in den jeweiligen vertraglichen Vereinbarungen festgelegten Verfahren vorgelegt und nach Buchstabe b bewertet werden.

d) Bei Untersuchungen muss die Organisation mit jeder anderen Organisation, die einen wesentlichen Beitrag zur Informationssicherheit ihrer eigenen Tätigkeiten leistet, zusammenarbeiten.

e) Die Organisation kann dieses Meldesystem in andere von ihr bereits umgesetzte Meldesysteme integrieren.

IS.I.OR.220 Störungen der Informationssicherheit — Erkennung, Reaktion und Wiederherstellung

a) Auf der Grundlage des Ergebnisses der nach Punkt IS.I.OR.205 durchgeführten Risikobewertung und des Ergebnisses nach Punkt IS.I.OR.210 aus dem Umgang mit dem Risiko muss die Organisation Maßnahmen ergreifen, um Störungen und Schwachstellen zu erkennen, die auf das potenzielle Eintreten nicht hinnehmbarer Risiken, die sich auf die Flugsicherheit auswirken können, schließen lassen. Diese Detektionsmaßnahmen müssen die Organisation in die Lage versetzen,

1. Abweichungen von vorab festgelegten funktionalen Leistungsgrundwerten zu identifizieren;

2. Warnungen auszulösen, mit denen bei Abweichungen geeignete Gegenmaßnahmen aktiviert werden.

b) Die Organisation muss Maßnahmen ergreifen, mit denen sie auf alle nach Buchstabe a identifizierten Ereigniszustände reagiert, die sich zu einer Störung der Informationssicherheit entwickeln können oder sich zu einer solchen entwickelt haben. Diese Reaktionsmaßnahmen müssen die Organisation in die Lage versetzen,

1. die Reaktion auf die Warnhinweise nach Buchstabe a Nummer 2 einzuleiten, indem vordefinierte Ressourcen und Handlungsabläufe aktiviert werden;

2. die Ausbreitung eines Angriffs einzudämmen und die vollständige Entfaltung eines Bedrohungsszenarios zu verhindern;

3. den Ausfallmodus der betroffenen Elemente nach Punkt IS.I.OR.205(a) zu steuern.

c) Die Organisation muss Maßnahmen ergreifen, die der Wiederherstellung nach Störungen der Informationssicherheit dienen, auch gegebenenfalls durch Notfallmaßnahmen. Diese Wiederherstellungsmaßnahmen müssen die Organisation in die Lage versetzen,

1. den Zustand, der die Störung verursacht hat, zu beseitigen oder ihn auf ein tolerierbares Maß zu beschränken;

2. innerhalb einer zuvor von der Organisation festgelegten Wiederherstellungszeit einen sicheren Zustand der in Punkt IS.I.OR.205(a) bereits definierten betroffenen Elemente zu erreichen.

IS.I.OR.225 Reaktion auf von der zuständigen Behörde gemeldete Beanstandungen

a) Nach Erhalt einer Mitteilung über Beanstandungen durch die zuständige Behörde muss die Organisation

1. die Ursache(n) für die Nichteinhaltung und die dazu beitragenden Faktoren ermitteln,

2. einen Abhilfeplan erstellen;

3. die Behebung der Beanstandung zur Zufriedenheit der zuständigen Behörde nachweisen.

b) Die unter Buchstabe a genannten Maßnahmen müssen innerhalb der mit der zuständigen Behörde vereinbarten Frist durchgeführt werden.

IS.I.OR.230 Informationssicherheitssystem für externe Meldungen

a) Die Organisation muss ein Meldesystem für die Informationssicherheit einrichten, das den Anforderungen der Verordnung (EU) Nr. 376/2014 und deren delegierten Rechtsakten und Durchführungsrechtsakten genügt, sofern jene Verordnung auf die Organisation anwendbar ist.

b) Unbeschadet ihrer Verpflichtungen aus der Verordnung (EU) Nr. 376/2014 muss die Organisation sicherstellen, dass alle Störungen oder Schwachstellen der Informationssicherheit, die ein erhebliches Risiko für die Flugsicherheit darstellen können, ihrer zuständigen Behörde gemeldet werden. Darüber hinaus gilt Folgendes:

1. Beeinträchtigt eine solche Störung oder Schwachstelle ein Luftfahrzeug oder zugehörige Systeme oder Komponenten, muss die Organisation dies auch dem Inhaber der Konstruktionsgenehmigung melden.

2. Beeinträchtigt eine solche Störung oder Schwachstelle von der Organisation verwendete Systeme oder Komponenten, muss die Organisation dies der für die Konstruktion des Systems oder der Komponente verantwortlichen Organisation melden.

c) Die Organisation muss die unter Buchstabe b genannten Zustände wie folgt melden:

1. Sie übermittelt der zuständigen Behörde und gegebenenfalls dem Inhaber der Konstruktionsgenehmigung oder der für die Konstruktion des Systems oder der Komponente verantwortlichen Organisation eine Mitteilung, sobald die Organisation von dem Zustand Kenntnis erlangt hat.

2. Sie übermittelt — sofern dem nicht außergewöhnliche Umstände entgegenstehen — der zuständigen Behörde und gegebenenfalls dem Inhaber der Konstruktionsgenehmigung oder der für die Konstruktion des Systems oder der Komponente verantwortlichen Organisation so bald wie möglich, höchstens jedoch 72 Stunden nachdem sie von dem Zustand Kenntnis erlangt hat, eine Meldung.

   Die Meldung muss in der von der zuständigen Behörde festgelegten Form erstellt werden und alle relevanten Informationen über den der Organisation bekannten Zustand enthalten.

3. Sie übermittelt der zuständigen Behörde und gegebenenfalls dem Inhaber der Konstruktionsgenehmigung oder der für die Konstruktion des Systems oder der Komponente verantwortlichen Organisation eine Folgemeldung, in der sie im Einzelnen darlegt, welche Maßnahmen sie für die Wiederherstellung nach der Störung ergriffen hat oder zu ergreifen beabsichtigt und welche Maßnahmen sie zu ergreifen gedenkt, um ähnliche Störungen der Informationssicherheit in Zukunft zu verhindern.

   Die Folgemeldung muss in der von der zuständigen Behörde festgelegten Form vorgelegt werden, sobald diese Maßnahmen festgelegt wurden.

IS.I.OR.235 Auftragsvergabe für Tätigkeiten des Informationssicherheitsmanagements

a) Die Organisation muss sicherstellen, dass bei der Vergabe eines Teils der unter Punkt IS.I.OR.200 genannten Tätigkeiten an andere Organisationen die in Auftrag gegebenen Tätigkeiten den Anforderungen dieser Verordnung genügen und dass die beauftragte Organisation unter ihrer Aufsicht arbeitet. Die Organisation muss sicherstellen, dass die mit den vertraglich vereinbarten Tätigkeiten verbundenen Risiken angemessen gemanagt werden.

b) Die Organisation muss sicherstellen, dass die zuständige Behörde auf Anfrage Zugang zu der unter Vertrag genommenen Organisation hat, um festzustellen, ob die geltenden Anforderungen dieser Verordnung weiterhin eingehalten werden.

IS.I.OR.240 Anforderungen an das Personal

a) Der in Artikel 2 Absatz 1 der vorliegenden Verordnung genannte verantwortliche Manager der Organisation, der auf der Grundlage der Verordnungen (EU) Nr. 1321/2014, (EU) Nr. 965/2012, (EU) Nr. 1178/2011 und (EU) 2015/340 sowie der Durchführungsverordnung (EU) 2017/373 bzw. der Durchführungsverordnung (EU) 2021/664 benannt wurde, muss über die Befugnis verfügen, sicherzustellen, dass alle nach dieser Verordnung erforderlichen Tätigkeiten finanziert und durchgeführt werden können. Diese Person muss

1. sicherstellen, dass alle zur Erfüllung der Anforderungen dieser Verordnung erforderlichen Ressourcen zur Verfügung stehen;

2. das in Punkt IS.I.OR.200(a)(1) genannte Konzept für die Informationssicherheit festlegen und fördern;

3. nachweisen, dass sie grundlegende Kenntnisse über diese Verordnung besitzt.

b) Der verantwortliche Manager muss zur Gewährleistung der Einhaltung der Anforderungen dieser Verordnung eine Person oder eine Gruppe von Personen benennen und den Umfang ihrer Befugnisse festlegen. Diese Person oder Gruppe von Personen ist gegenüber dem verantwortlichen Manager unmittelbar rechenschaftspflichtig und muss über die erforderlichen Kenntnisse, Ausbildungen und Erfahrungen verfügen, um ihren Aufgaben gerecht werden zu können. Die Verfahren müssen Festlegungen dazu enthalten, wer eine bestimmte Person im Fall einer längeren Abwesenheit jener Person vertritt.

c) Der verantwortliche Manager muss eine Person oder eine Gruppe von Personen benennen, die dafür zuständig ist, die in Punkt IS.I.OR.200(a)(12) genannte Funktion zur Überwachung der Compliance zu verwalten.

d) Nutzt die Organisation Organisationsstrukturen, Konzepte, Prozesse und Verfahren der Informationssicherheit gemeinsam mit anderen Organisationen oder mit Bereichen ihrer eigenen Organisation, die nicht Teil der Genehmigung oder Erklärung sind, kann der verantwortliche Manager seine Tätigkeiten an eine gemeinsam verantwortliche Person übertragen.

In diesem Fall müssen zwischen dem verantwortlichen Manager der Organisation und der gemeinsam verantwortlichen Person Koordinierungsmaßnahmen festgelegt werden, damit eine angemessene Integration des Informationssicherheitsmanagements innerhalb der Organisation gewährleistet ist.

e) Der verantwortliche Manager oder die in Buchstabe d genannte gemeinsam verantwortliche Person ist befugt, die zur Umsetzung von Punkt IS.I.OR.200 erforderlichen Organisationsstrukturen, Konzepte, Prozesse und Verfahren festzulegen und aufrechtzuerhalten.

f) Die Organisation muss über ein Verfahren verfügen, mit dem sichergestellt wird, dass sie über genügend Personal verfügt, das die Durchführung der unter diesen Anhang fallenden Tätigkeiten wahrnehmen kann.

g) Die Organisation muss über ein Verfahren verfügen, mit dem sichergestellt wird, dass das unter Buchstabe f genannte Personal über die für die Wahrnehmung seiner Aufgaben erforderliche Kompetenz verfügt.

h) Die Organisation muss über ein Verfahren verfügen, mit dem sichergestellt wird, dass das Personal die mit den zugewiesenen Funktionen und Aufgaben verbundene Verantwortung anerkennt.

i) Die Organisation muss sicherstellen, dass die Identität und Vertrauenswürdigkeit des Personals, das Zugang zu Informationssystemen und Daten hat, die den Anforderungen dieser Verordnung unterliegen, angemessen festgestellt wird.

IS.I.OR.245 Führen von Aufzeichnungen

a) *Die Organisation muss Aufzeichnungen über ihre Tätigkeiten im Bereich des Informationssicherheitsmanagements führen.*

1. Die Organisation muss sicherstellen, dass die folgenden Aufzeichnungen archiviert werden und zurückverfolgt werden können:

   i) jede eingegangene Genehmigung und jede damit verbundene Bewertung des Informationssicherheitsrisikos nach Punkt IS.I.OR.200(e);

   ii) Auftragsvergaben für Tätigkeiten nach Punkt IS.I.OR.200(a)(9);

   iii) Aufzeichnungen der wichtigsten in Punkt IS.I.OR.200(d) genannten Prozesse;

   iv) Aufzeichnungen über die bei der Risikobewertung nach Punkt IS.I.OR.205 ermittelten Risiken zusammen mit den damit verbundenen Maßnahmen zum Umgang mit den Risiken nach Punkt IS.I.OR.210;

   v) Aufzeichnungen von Störungen und Schwachstellen der Informationssicherheit, die gemäß den Meldesystemen nach Punkt IS.I.OR.215 und Punkt IS.I.OR.230 gemeldet wurden;

   vi) Aufzeichnungen über Informationssicherheitsereignisse, die möglicherweise neu bewertet werden müssen, um unentdeckte Störungen und Schwachstellen der Informationssicherheit aufzudecken.

2. Die Aufzeichnungen nach Nummer 1 Ziffer i müssen mindestens fünf Jahre nach Ablauf der Gültigkeit der Genehmigung aufbewahrt werden.

3. Die Aufzeichnungen nach Nummer 1 Ziffer ii müssen mindestens fünf Jahre nach Änderung oder Beendigung des Auftrags aufbewahrt werden.

4. Die Aufzeichnungen nach Nummer 1 Ziffern iii, iv und v müssen mindestens fünf Jahre lang aufbewahrt werden.

5. Die Aufzeichnungen nach Nummer 1 Ziffer vi müssen so lange aufbewahrt werden, bis diese Informationssicherheitsereignisse gemäß der Periodizität neu bewertet worden sind, die in einem von der Organisation festgelegten Verfahren definiert wurde.

b) *Die Organisation muss Aufzeichnungen über die Qualifikation und Erfahrung ihres eigenen Personals führen, das an Tätigkeiten des Informationssicherheitsmanagements beteiligt ist.*

1. Die Aufzeichnungen über Qualifikation und Erfahrung des Personals müssen so lange aufbewahrt werden, wie die Person für die Organisation tätig ist, und für einen Zeitraum von mindestens drei Jahren, nachdem die Person die Organisation verlassen hat.

2. Mitglieder des Personals erhalten auf Antrag Zugang zu ihren Personalakten. Darüber hinaus muss die Organisation ihnen zum Zeitpunkt des Verlassens der Organisation auf Anfrage eine Kopie ihrer Personalakte aushändigen.

c) Das Format der Aufzeichnungen muss in den Verfahren der Organisation festgelegt werden.

d) Die Aufzeichnungen müssen so aufbewahrt werden, dass sie vor Beschädigung, Änderung und Diebstahl geschützt sind, wobei die Informationen bei Bedarf entsprechend dem Niveau der Sicherheitsklassifizierung zu kennzeichnen sind. Die Organisation muss sicherstellen, dass die Aufzeichnungen so aufbewahrt werden, dass Integrität, Authentizität und autorisierter Zugang gewährleistet werden.

IS.I.OR.250 Handbuch zum Informationssicherheitsmanagement (ISMM)

a) Die Organisation muss der zuständigen Behörde ein Handbuch zum Informationssicherheitsmanagement (*Information Security Management Manual*, ISMM) und gegebenenfalls zugehörige Handbücher und Verfahren zur Verfügung stellen, die Folgendes enthalten:

1. Eine vom verantwortlichen Manager unterzeichnete Erklärung zur Bestätigung, dass die Organisation ihre Tätigkeiten zu jedem Zeitpunkt in Übereinstimmung mit diesem Anhang und mit dem ISMM ausführt. Ist der verantwortliche Manager nicht gleichzeitig der Hauptgeschäftsführer (CEO) der Organisation, muss dieser Letztere die Erklärung gegenzeichnen;

2. Titel, Name(n), Pflichten, Rechenschaftspflichten, Zuständigkeiten und Befugnisse der in Punkt IS.I.OR.240(b) und (c) genannten Person(en);

3. gegebenenfalls Titel, Name(n), Pflichten, Rechenschaftspflichten, Zuständigkeiten und Befugnisse der in Punkt IS.I.OR.240(d) genannten gemeinsamen verantwortlichen Person(en);

4. das Informationssicherheitskonzept der Organisation nach Punkt IS.I.OR.200(a)(1);

5. allgemeine Angaben zu Personalstärke und Personalkategorien sowie zum bestehenden System für die Planung der Verfügbarkeit von Personal nach Punkt IS.I.OR.240,

6. Titel, Name(n), Pflichten, Rechenschaftspflichten, Zuständigkeiten und Befugnisse der wichtigsten Personen, die für die Umsetzung von Punkt IS.I.OR.200 verantwortlich sind, einschließlich der Person(en), die für die Überwachung der Compliance nach Punkt IS.I.OR.200(a)(12) verantwortlich ist/sind;

7. ein Organigramm, aus dem die entsprechende Hierarchie der Rechenschaftspflichten und Zuständigkeiten der in den Nummern 2 und 6 genannten Personen hervorgeht;

8. Angaben zu dem in Punkt IS.I.OR.215 genannten System für interne Meldungen;

9. die Verfahren, mit denen festgelegt wird, wie die Organisation die Einhaltung dieses Teils gewährleistet, insbesondere:

i) die Dokumentation nach Punkt IS.I.OR.200(c);

ii) die Verfahren, mit denen festgelegt wird, wie die Organisation die im Zuge einer Auftragsvergabe nach Punkt IS.I.OR.200(a)(9) vergebenen Tätigkeiten kontrolliert;

iii) das ISMM-Änderungsverfahren nach Buchstabe c;

10. die Einzelheiten der derzeit zugelassenen alternativen Nachweisverfahren.

b) Die Erstausgabe des ISMM muss von der zuständigen Behörde genehmigt werden, die auch ein Exemplar dieses Handbuchs aufbewahrt. Das ISMM muss erforderlichenfalls geändert werden, damit die Beschreibung des ISMS der Organisation aktuell bleibt. Der zuständigen Behörde muss ein Exemplar aller Änderungen des ISMM vorgelegt werden.

c) Änderungen des ISMM müssen nach einem von der Organisation festgelegten Verfahren verwaltet werden. Änderungen, die nicht in den Anwendungsbereich dieses Verfahrens fallen, sowie Änderungen im Zusammenhang mit den Änderungen nach Punkt IS.I.OR.255(b) müssen von der zuständigen Behörde genehmigt werden.

d) Die Organisation kann das ISMM mit anderen von ihr verwalteten Managementhandbüchern zusammenführen, sofern durch eindeutige Bezugnahme klar erkennbar ist, welche Teile der Managementhandbücher den verschiedenen Anforderungen dieses Anhangs entsprechen.

IS.I.OR.255 Änderungen des Informationssicherheitsmanagementsystems

a) Änderungen des ISMS können nach einem von der Organisation entwickelten Verfahren verwaltet und der zuständigen Behörde mitgeteilt werden. Dieses Verfahren muss von der zuständigen Behörde genehmigt werden.

b) Für Änderungen des ISMS, die nicht unter das unter Buchstabe a genannte Verfahren fallen, muss die Organisation eine von der zuständigen Behörde zu erteilende Genehmigung beantragen und erhalten.

In Bezug auf diese Änderungen gilt Folgendes:

1. Der Antrag muss vor solchen Änderungen gestellt werden, damit die zuständige Behörde die fortgesetzte Einhaltung dieser Verordnung überprüfen und erforderlichenfalls die Organisationszulassung und den damit zusammenhängenden Genehmigungsumfang ändern kann.

2. Die Organisation muss der zuständigen Behörde alle Informationen zur Verfügung stellen, die diese zur Bewertung der Änderung anfordert.

3. Die Änderung darf erst nach Eingang der förmlichen Genehmigung durch die zuständige Behörde umgesetzt werden.

4. Während der Umsetzung solcher Änderungen unterliegt die Weiterführung des Betriebs der Organisation den von der zuständigen Behörde vorgegebenen Bedingungen.

IS.I.OR.260 Kontinuierliche Verbesserung

a) Die Organisation muss anhand geeigneter Leistungsindikatoren die Wirksamkeit und Ausgereiftheit des ISMS bewerten. Diese Bewertung muss nach einem von der Organisation vorab festgelegten Zeitplan oder nach einer Störung der Informationssicherheit durchgeführt werden.

b) Werden bei der Bewertung nach Buchstabe a Mängel festgestellt, muss die Organisation die erforderlichen Verbesserungsmaßnahmen ergreifen, damit das ISMS weiterhin den geltenden Anforderungen entspricht und die Informationssicherheitsrisiken auf einem annehmbaren Niveau hält. Darüber hinaus muss die Organisation die Elemente des ISMS, die von den angenommenen Maßnahmen betroffen sind, neu bewerten.

ANHANG III

Anhang VI (Teil-ARA) und Anhang VII (Teil-ORA) der Verordnung (EU) Nr. 1178/2011 werden wie folgt geändert:

1. Anhang VI (Teil-ARA) wird wie folgt geändert:

a) In Punkt ARA.GEN.125 wird folgender Buchstabe c angefügt:

„c) Die zuständige Behörde des betreffenden Mitgliedstaats übermittelt der Agentur so bald wie möglich sicherheitsrelevante Informationen, die sie im Rahmen der Meldungen zur Informationssicherheit nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.230 der Durchführungsverordnung (EU) 2023/203 erhalten hat."

b) Nach Punkt ARA.GEN.135 wird folgender Punkt ARA.GEN.135A eingefügt:

„**ARA.GEN.135A Unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit**

a) Die zuständige Behörde richtet ein System zur angemessenen Erfassung, Analyse und Verbreitung von Informationen im Zusammenhang mit von Organisationen gemeldeten Störungen und Schwachstellen der Informationssicherheit ein, die sich auf die Flugsicherheit auswirken können. Zur Verbesserung der Koordinierung und Kompatibilität der Meldesysteme erfolgt dies in Abstimmung mit allen anderen einschlägigen Behörden, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig sind.

b) Die Agentur richtet ein System zur angemessenen Analyse aller sicherheitsrelevanten Informationen ein, die sie nach Punkt ARA.GEN.125(c) erhalten hat, und übermittelt den Mitgliedstaaten und der Kommission unverzüglich alle Informationen, auch Empfehlungen oder zu ergreifende Abhilfemaßnahmen, die diese benötigen, um zeitnah auf Störungen oder Schwachstellen der Informationssicherheit zu reagieren, die sich auf die Flugsicherheit auswirken können und von denen auch Erzeugnisse, Teile, nicht eingebaute Ausrüstung, Personen oder Organisationen betroffen sein können, die der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten unterliegen.

c) Nach Eingang der unter den Buchstaben a und b genannten Informationen ergreift die zuständige Behörde geeignete Maßnahmen, um den potenziellen Auswirkungen der Störung oder Schwachstelle der Informationssicherheit auf die Flugsicherheit zu begegnen.

d) Nach Buchstabe c ergriffene Maßnahmen müssen unverzüglich allen Personen bzw. Organisationen mitgeteilt werden, die diese nach Maßgabe der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten befolgen müssen. Die zuständige Behörde des betreffenden Mitgliedstaats muss diese Maßnahmen auch der Agentur und, falls ein gemeinsames Handeln erforderlich ist, den übrigen betroffenen Mitgliedstaaten mitteilen."

c) In Punkt ARA.GEN.200 wird folgender Buchstabe e angefügt:

„e) Zusätzlich zu den Anforderungen nach Buchstabe a muss das von der zuständigen Behörde eingerichtete und gepflegte Managementsystem Anhang I (Teil-IS.AR) der Durchführungsverordnung (EU) 2023/203 genügen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

d) Punkt ARA.GEN.205 wird wie folgt geändert:

i) Die Überschrift erhält folgende Fassung:

„**ARA.GEN.205 Zuweisung von Aufgaben**".

ii) Folgender Buchstabe c wird angefügt:

„c) In Bezug auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt ORA.GEN.200A durch die Organisation kann die zuständige Behörde nach Buchstabe a qualifizierten Stellen oder jeder einschlägigen Behörde, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig ist, Aufgaben zuweisen. Bei der Zuweisung von Aufgaben stellt die zuständige Behörde sicher, dass

1. die qualifizierte Stelle oder die einschlägige Behörde alle Aspekte im Zusammenhang mit der Flugsicherheit koordiniert und berücksichtigt;

2. die Ergebnisse der von der qualifizierten Stelle oder der einschlägigen Behörde durchgeführten Zertifizierungs- und Aufsichtstätigkeiten in die gesamten Zertifizierungs- und Aufsichtsunterlagen der Organisation integriert werden;

3. ihr eigenes nach Punkt ARA.GEN.200(e) eingerichtetes Informationssicherheitsmanagementsystem alle in ihrem Namen wahrgenommenen Aufgaben der Zertifizierung und fortlaufenden Aufsicht erfasst."

e) In Punkt ARA.GEN.300 wird folgender Buchstabe g angefügt:

„g) Im Hinblick auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt ORA.GEN.200A durch die Organisation überprüft die zuständige Behörde im Anschluss an den anwendbaren Aufsichts-Auditzyklus und bei jeder Änderung des Arbeitsumfangs der Organisation zusätzlich zur Einhaltung der Buchstaben a bis f jede nach Punkt IS.I.OR.200(e) dieser Verordnung oder Punkt IS.D.OR.200(e) der Delegierten Verordnung (EU) 2022/1645 erteilte Genehmigung."

f) Nach Punkt ARA.GEN.330 wird folgender Punkt ARA.GEN.330A eingefügt:

„ARA.GEN.330A Änderungen des Informationssicherheitsmanagementsystems

a) Änderungen, die gemäß dem Verfahren nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(a) der Durchführungsverordnung (EU) 2023/203 verwaltet und der zuständigen Behörde gemeldet werden, muss die zuständige Behörde nach den in Punkt ARA.GEN.300 festgelegten Grundsätzen in ihre fortlaufende Aufsicht zur Überprüfung aufnehmen. Wird eine Nichteinhaltung festgestellt, teilt die zuständige Behörde dies der Organisation mit, verlangt weitere Änderungen und verfährt nach Punkt ARA.GEN.350.

b) Für sonstige Änderungen, deren Genehmigung nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(b) der Durchführungsverordnung (EU) 2023/203 beantragt werden muss, gilt Folgendes:

1. Bei Eingang eines Änderungsantrags prüft die zuständige Behörde, ob die Organisation die geltenden Anforderungen erfüllt, bevor sie die Genehmigung erteilt.

2. Die zuständige Behörde legt die Bedingungen fest, unter denen die Organisation während der Umsetzung der Änderung tätig sein darf.

3. Hat sich die zuständige Behörde vergewissert, dass die Organisation die geltenden Anforderungen erfüllt, genehmigt sie die Änderung."

2. Anhang VII (Teil-ORA) wird wie folgt geändert:

Nach Punkt ORA.GEN.200 wird folgender Punkt ORA.GEN.200A eingefügt:

„ORA.GEN.200A Informationssicherheitsmanagementsystem

Zusätzlich zu dem nach Punkt ORA.GEN.200 vorgeschriebenen Managementsystem muss die Organisation ein Informationssicherheitsmanagementsystem gemäß der Durchführungsverordnung (EU) 2023/203 einrichten, umsetzen und pflegen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

ANHANG IV

Anhang I (Teil 21) der Verordnung (EU) Nr. 748/2012 wird wie folgt geändert:

1. Das Inhaltsverzeichnis wird wie folgt geändert:

   a) Nach der Überschrift von Punkt 21.B.20 wird die folgende Überschrift eingefügt:

   „21.B.20A Unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit".

   b) Die Überschrift von Punkt 21.B.30 erhält folgende Fassung:

   „21.B.30 Zuweisung von Aufgaben".

   c) Nach der Überschrift von Punkt 21.B.240 wird die folgende Überschrift eingefügt:

   „21.B.240A Änderungen des Informationssicherheitsmanagementsystems ".

   d) Nach der Überschrift von Punkt 21.B.435 wird die folgende Überschrift eingefügt:

   „21.B.435A Änderungen des Informationssicherheitsmanagementsystems ".

2. In Punkt 21.B.15 wird der folgende Buchstabe c angefügt:

   „c) Die zuständige Behörde des betreffenden Mitgliedstaats übermittelt der Agentur so bald wie möglich sicherheitsrelevante Informationen, die sie im Rahmen der Meldungen zur Informationssicherheit nach dem Anhang Punkt IS.D.OR.230 (Teil-IS.D.OR) der Delegierten Verordnung (EU) 2022/1645 erhalten hat."

3. Nach Punkt 21.B.20 wird folgender Punkt 21.B.20A eingefügt:

„21.B.20A Unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit

   a) Die zuständige Behörde richtet ein System zur angemessenen Erfassung, Analyse und Verbreitung von Informationen im Zusammenhang mit von Organisationen gemeldeten Störungen und Schwachstellen der Informationssicherheit ein, die sich auf die Flugsicherheit auswirken können. Zur Verbesserung der Koordinierung und Kompatibilität der Meldesysteme erfolgt dies in Abstimmung mit allen anderen einschlägigen Behörden, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig sind.

   b) Die Agentur richtet ein System zur angemessenen Analyse aller sicherheitsrelevanten Informationen ein, die sie nach Punkt 21.B.15(c) erhalten hat, und übermittelt den Mitgliedstaaten und der Kommission unverzüglich alle Informationen, auch Empfehlungen oder zu ergreifende Abhilfemaßnahmen, die diese benötigen, um zeitnah auf Störungen oder Schwachstellen der Informationssicherheit zu reagieren, die sich auf die Flugsicherheit auswirken können und von denen auch Erzeugnisse, Teile, nicht eingebaute Ausrüstung, Personen oder Organisationen betroffen sein können, die der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten unterliegen.

   c) Nach Eingang der unter den Buchstaben a und b genannten Informationen ergreift die zuständige Behörde geeignete Maßnahmen, um den potenziellen Auswirkungen der Störung oder Schwachstelle der Informationssicherheit auf die Flugsicherheit zu begegnen.

   d) Nach Buchstabe c ergriffene Maßnahmen müssen unverzüglich allen Personen bzw. Organisationen mitgeteilt werden, die diese nach Maßgabe der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten befolgen müssen. Die zuständige Behörde des betreffenden Mitgliedstaats muss diese Maßnahmen auch der Agentur und, falls ein gemeinsames Handeln erforderlich ist, den übrigen betroffenen Mitgliedstaaten mitteilen."

4. In Punkt 21.B.25 wird folgender Buchstabe e angefügt:

   „e) Zusätzlich zu den Anforderungen nach Buchstabe a muss das von der zuständigen Behörde eingerichtete und gepflegte Managementsystem Anhang I (Teil-IS.AR) der Durchführungsverordnung (EU) 2023/203 genügen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

5. Punkt 21.B.30 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„21.B.30 Zuweisung von Aufgaben“.

b) Folgender Buchstabe c wird angefügt:

„c) In Bezug auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt 21.A.139A und Punkt 21.A.239A durch die Organisation kann die zuständige Behörde nach Buchstabe a qualifizierten Stellen oder jeder einschlägigen Behörde, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig ist, Aufgaben zuweisen. Bei der Zuweisung von Aufgaben stellt die zuständige Behörde sicher, dass

1. die qualifizierte Stelle oder die einschlägige Behörde alle Aspekte im Zusammenhang mit der Flugsicherheit koordiniert und berücksichtigt;

2. die Ergebnisse der von der qualifizierten Stelle oder der einschlägigen Behörde durchgeführten Zertifizierungs- und Aufsichtstätigkeiten in die gesamten Zertifizierungs- und Aufsichtsunterlagen der Organisation integriert werden;

3. ihr eigenes nach Punkt 21.B.25(e) eingerichtetes Informationssicherheitsmanagementsystem alle in ihrem Namen wahrgenommenen Aufgaben der Zertifizierung und fortlaufenden Aufsicht erfasst.“

6. In Punkt 21.B.221 wird folgender Buchstabe g angefügt:

„g) Im Hinblick auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt 21.A.139A durch die Organisation überprüft die zuständige Behörde im Anschluss an den anwendbaren Aufsichts-Auditzyklus und bei jeder Änderung des Arbeitsumfangs der Organisation zusätzlich zur Einhaltung der Buchstaben a bis f jede nach Punkt IS.I.OR.200(e) dieser Verordnung oder Punkt IS.D.OR.200(e) der Delegierten Verordnung (EU) 2022/1645 erteilte Genehmigung.“

7. Nach Punkt 21.B.240 wird folgender Punkt 21.B.240A eingefügt:

„**21.B.240A Änderungen des Informationssicherheitsmanagementsystems**

a) Änderungen, die gemäß dem Verfahren nach dem Anhang (Teil IS.D.OR) Punkt IS.D.OR.255(a) der Delegierten Verordnung (EU) 2022/1645 verwaltet und der zuständigen Behörde gemeldet werden, muss die zuständige Behörde nach den in Punkt 21.B.221 festgelegten Grundsätzen in ihre fortlaufende Aufsicht zur Überprüfung aufnehmen. Wird eine Nichteinhaltung festgestellt, teilt die zuständige Behörde dies der Organisation mit, verlangt weitere Änderungen und verfährt nach Punkt 21.B.225.

b) Für sonstige Änderungen, deren Genehmigung nach dem Anhang (Teil-IS.D.OR) Punkt IS.D.OR.255(b) der Delegierten Verordnung (EU) 2022/1645 beantragt werden muss, gilt Folgendes:

1. Bei Eingang eines Änderungsantrags prüft die zuständige Behörde, ob die Organisation die geltenden Anforderungen erfüllt, bevor sie die Genehmigung erteilt.

2. Die zuständige Behörde legt die Bedingungen fest, unter denen die Organisation während der Umsetzung der Änderung tätig sein darf.

3. Hat sich die zuständige Behörde vergewissert, dass die Organisation die geltenden Anforderungen erfüllt, genehmigt sie die Änderung.“

8. In Punkt 21.B.431 wird der folgende Buchstabe d angefügt:

„d) In Bezug auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt 21.A.239A durch die Organisation muss die zuständige Behörde zusätzlich zu den Buchstaben a bis c den folgenden Grundsätzen genügen:

1. Die zuständige Behörde überprüft die Schnittstellen und damit verbundenen Risiken, die von jeder ihrer Aufsicht unterliegenden Organisation nach dem Anhang (Teil-IS.D.OR) Punkt IS.D.OR.205(b) der Delegierten Verordnung (EU) 2022/1645 identifiziert wurden.

2. Werden bei den gemeinsamen Schnittstellen und damit verbundenen Risiken von unterschiedlichen Organisationen Abweichungen festgestellt, muss die zuständige Behörde diese mit den betroffenen Organisationen überprüfen und erforderlichenfalls entsprechende Beanstandungen feststellen, damit die Durchführung von Abhilfemaßnahmen gewährleistet ist.

3. Geht aus den nach Nummer 2 geprüften Unterlagen hervor, dass im Zusammenhang mit Schnittstellen zu Organisationen, die der Aufsicht einer anderen zuständigen Behörde in demselben Mitgliedstaat unterliegen, signifikante Risiken bestehen, müssen diese Informationen der entsprechenden zuständigen Behörde mitgeteilt werden."

9. Nach Punkt 21.B.435 wird folgender Punkt 21.B.435A eingefügt:

„**21.B.435A Änderungen des Informationssicherheitsmanagementsystems**

a) Änderungen, die gemäß dem Verfahren nach dem Anhang (Teil-IS.D.OR) Punkt IS.D.OR.255(a) der Delegierten Verordnung (EU) 2022/1645 verwaltet und der zuständigen Behörde gemeldet werden, muss die zuständige Behörde nach den in Punkt 21.B.431 festgelegten Grundsätzen in ihre fortlaufende Aufsicht zur Überprüfung aufnehmen. Wird eine Nichteinhaltung festgestellt, teilt die zuständige Behörde dies der Organisation mit, verlangt weitere Änderungen und verfährt nach Punkt 21.B.433.

b) Für sonstige Änderungen, deren Genehmigung nach dem Anhang (Teil-IS.D.OR) Punkt IS.D.OR.255(b) der Delegierten Verordnung (EU) 2022/1645 beantragt werden muss, gilt Folgendes:

1. Bei Eingang eines Änderungsantrags prüft die zuständige Behörde, ob die Organisation die geltenden Anforderungen erfüllt, bevor sie die Genehmigung erteilt.

2. Die zuständige Behörde legt die Bedingungen fest, unter denen die Organisation während der Umsetzung der Änderung tätig sein darf.

3. Hat sich die zuständige Behörde vergewissert, dass die Organisation die geltenden Anforderungen erfüllt, genehmigt sie die Änderung."

ANHANG V

Anhang II (Teil-ARO) und Anhang III (Teil-ORO) der Verordnung (EU) Nr. 965/2012 werden wie folgt geändert:

1. Anhang II (Teil-ARO) wird wie folgt geändert:

a) In Punkt ARO.GEN.125 wird der folgenden Buchstabe c angefügt:

„c) Die zuständige Behörde des betreffenden Mitgliedstaats übermittelt der Agentur so bald wie möglich sicherheitsrelevante Informationen, die sie im Rahmen der Meldungen zur Informationssicherheit nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.230 der Durchführungsverordnung (EU) 2023/203 erhalten hat."

b) Nach Punkt ARO.GEN.135 wird folgender Punkt ARO.GEN.135A eingefügt:

„**ARO.GEN.135A Unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit**

a) Die zuständige Behörde richtet ein System zur angemessenen Erfassung, Analyse und Verbreitung von Informationen im Zusammenhang mit von Organisationen gemeldeten Störungen und Schwachstellen der Informationssicherheit ein, die sich auf die Flugsicherheit auswirken können. Zur Verbesserung der Koordinierung und Kompatibilität der Meldesysteme erfolgt dies in Abstimmung mit allen anderen einschlägigen Behörden, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig sind.

b) Die Agentur richtet ein System zur angemessenen Analyse aller sicherheitsrelevanten Informationen ein, die sie nach Punkt ARO.GEN.125(c) erhalten hat, und übermittelt den Mitgliedstaaten und der Kommission unverzüglich alle Informationen, auch Empfehlungen oder zu ergreifende Abhilfemaßnahmen, die diese benötigen, um zeitnah auf Störungen oder Schwachstellen der Informationssicherheit zu reagieren, die sich auf die Flugsicherheit auswirken können und von denen auch Erzeugnisse, Teile, nicht eingebaute Ausrüstung, Personen oder Organisationen betroffen sein können, die der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten unterliegen.

c) Nach Eingang der unter den Buchstaben a und b genannten Informationen ergreift die zuständige Behörde geeignete Maßnahmen, um den potenziellen Auswirkungen der Störung oder Schwachstelle der Informationssicherheit auf die Flugsicherheit zu begegnen.

d) Nach Buchstabe c ergriffene Maßnahmen müssen unverzüglich allen Personen bzw. Organisationen mitgeteilt werden, die diese nach Maßgabe der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten befolgen müssen. Die zuständige Behörde des betreffenden Mitgliedstaats muss diese Maßnahmen auch der Agentur und, falls ein gemeinsames Handeln erforderlich ist, den übrigen betroffenen Mitgliedstaaten mitteilen."

c) In Punkt ARO.GEN.200 wird folgender Buchstabe e angefügt:

„e) Zusätzlich zu den Anforderungen nach Buchstabe a muss das von der zuständigen Behörde eingerichtete und gepflegte Managementsystem Anhang I (Teil-IS.AR) der Durchführungsverordnung (EU) 2023/203 genügen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

d) Punkt ARO.GEN.205 wird wie folgt geändert:

i) Die Überschrift erhält folgende Fassung:

„**ARO.GEN.205 Zuweisung von Aufgaben**".

ii) Folgender Buchstabe c wird angefügt:

„c) In Bezug auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt ORO.GEN.200A durch die Organisation kann die zuständige Behörde nach Buchstabe a qualifizierten Stellen oder jeder einschlägigen Behörde, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig ist, Aufgaben zuweisen. Bei der Zuweisung von Aufgaben stellt die zuständige Behörde sicher, dass

1. die qualifizierte Stelle oder die einschlägige Behörde alle Aspekte im Zusammenhang mit der Flugsicherheit koordiniert und berücksichtigt;

2. die Ergebnisse der von der qualifizierten Stelle oder der einschlägigen Behörde durchgeführten Zertifizierungs- und Aufsichtstätigkeiten in die gesamten Zertifizierungs- und Aufsichtsunterlagen der Organisation integriert werden;

3. ihr eigenes nach Punkt ARO.GEN.200(e) eingerichtetes Informationssicherheitsmanagementsystem alle in ihrem Namen wahrgenommenen Aufgaben der Zertifizierung und fortlaufenden Aufsicht erfasst."

e) In Punkt ARO.GEN.300 wird folgender Buchstabe g angefügt:

„g) Im Hinblick auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt ORO.GEN.200A durch die Organisation überprüft die zuständige Behörde im Anschluss an den anwendbaren Aufsichts-Auditzyklus und bei jeder Änderung des Arbeitsumfangs der Organisation zusätzlich zur Einhaltung der Buchstaben a bis f jede nach Punkt IS.I.OR.200(e) dieser Verordnung oder Punkt IS.D.OR.200(e) der Delegierten Verordnung (EU) 2022/1645 erteilte Genehmigung."

f) Nach Punkt ARO.GEN.330 wird folgender Punkt ARO.GEN.330A eingefügt:

„**ARO.GEN.330A Änderungen des Informationssicherheitsmanagementsystems**

a) Änderungen, die gemäß dem Verfahren nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(a) der Durchführungsverordnung (EU) 2023/203 verwaltet und der zuständigen Behörde gemeldet werden, muss die zuständige Behörde nach den in Punkt ARO.GEN.300 festgelegten Grundsätzen in ihre fortlaufende Aufsicht zur Überprüfung aufnehmen. Wird eine Nichteinhaltung festgestellt, teilt die zuständige Behörde dies der Organisation mit, verlangt weitere Änderungen und verfährt nach Punkt ARO.GEN.350.

b) Für sonstige Änderungen, deren Genehmigung nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(b) der Durchführungsverordnung (EU) 2023/203 beantragt werden muss, gilt Folgendes:

1. Bei Eingang eines Änderungsantrags prüft die zuständige Behörde, ob die Organisation die geltenden Anforderungen erfüllt, bevor sie die Genehmigung erteilt.

2. Die zuständige Behörde legt die Bedingungen fest, unter denen die Organisation während der Umsetzung der Änderung tätig sein darf.

3. Hat sich die zuständige Behörde vergewissert, dass die Organisation die geltenden Anforderungen erfüllt, genehmigt sie die Änderung."

2. Anhang III (Teil-ORO) wird wie folgt geändert:

Nach Punkt ORO.GEN.200 wird folgender Punkt ORO.GEN.200A eingefügt:

„**ORO.GEN.200A Informationssicherheitsmanagementsystem**

Zusätzlich zu dem nach Punkt ORO.GEN.200 vorgeschriebenen Managementsystem muss der Betreiber ein Informationssicherheitsmanagementsystem gemäß der Durchführungsverordnung (EU) 2023/203 einrichten, umsetzen und pflegen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

ANHANG VI

Anhang II (Teil-ADR.AR) der Verordnung (EU) Nr. 139/2014 wird wie folgt geändert:

1. In Punkt ADR.AR.A.025 wird der folgenden Buchstabe c angefügt:

„c) Die zuständige Behörde des betreffenden Mitgliedstaats übermittelt der Agentur so bald wie möglich sicherheitsrelevante Informationen, die sie im Rahmen der Meldungen zur Informationssicherheit nach Punkt IS.D.OR.230 des Anhangs (Teil-IS.D.OR) der Delegierten Verordnung (EU) 2022/1645 erhalten hat."

2. Nach Punkt ADR.AR.A.030 wird folgender Punkt ADR.AR.A.030A eingefügt:

„**ADR.AR.A.030A Unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit**

a) Die zuständige Behörde richtet ein System zur angemessenen Erfassung, Analyse und Verbreitung von Informationen im Zusammenhang mit von Organisationen gemeldeten Störungen und Schwachstellen der Informationssicherheit ein, die sich auf die Flugsicherheit auswirken können. Zur Verbesserung der Koordinierung und Kompatibilität der Meldesysteme erfolgt dies in Abstimmung mit allen anderen einschlägigen Behörden, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig sind.

b) Die Agentur richtet ein System zur angemessenen Analyse aller sicherheitsrelevanten Informationen ein, die sie nach Punkt ADR.AR.A.025(c) erhalten hat, und übermittelt den Mitgliedstaaten und der Kommission unverzüglich alle Informationen, auch Empfehlungen oder zu ergreifende Abhilfemaßnahmen, die diese benötigen, um zeitnah auf Störungen oder Schwachstellen der Informationssicherheit zu reagieren, die sich auf die Flugsicherheit auswirken können und von denen auch Erzeugnisse, Teile, nicht eingebaute Ausrüstung, Personen oder Organisationen betroffen sein können, die der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten unterliegen.

c) Nach Eingang der unter den Buchstaben a und b genannten Informationen ergreift die zuständige Behörde geeignete Maßnahmen, um den potenziellen Auswirkungen der Störung oder Schwachstelle der Informationssicherheit auf die Flugsicherheit zu begegnen.

d) Nach Buchstabe c ergriffene Maßnahmen müssen unverzüglich allen Personen bzw. Organisationen mitgeteilt werden, die diese nach Maßgabe der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten befolgen müssen. Die zuständige Behörde des betreffenden Mitgliedstaats muss diese Maßnahmen auch der Agentur und, falls ein gemeinsames Handeln erforderlich ist, den übrigen betroffenen Mitgliedstaaten mitteilen."

3. In Punkt ADR.AR.B.005 wird der folgende Buchstabe d angefügt:

„d) Zusätzlich zu den Anforderungen nach Buchstabe a muss das von der zuständigen Behörde eingerichtete und gepflegte Managementsystem Anhang I (Teil-IS.AR) der Durchführungsverordnung (EU) 2023/203 genügen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

4. Punkt ADR.AR.B.010 wird wie folgt geändert:

i) Die Überschrift erhält folgende Fassung:

„**ADR.AR.B.010 Zuweisung von Aufgaben**".

ii) Folgender Buchstabe c wird angefügt:

„c) In Bezug auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt ADR.OR.D.005A durch die Organisation kann die zuständige Behörde nach Buchstabe a qualifizierten Stellen oder jeder einschlägigen Behörde, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig ist, Aufgaben zuweisen. Bei der Zuweisung von Aufgaben stellt die zuständige Behörde sicher, dass

1. die qualifizierte Stelle oder die einschlägige Behörde alle Aspekte im Zusammenhang mit der Flugsicherheit koordiniert und berücksichtigt;

2. die Ergebnisse der von der qualifizierten Stelle oder der einschlägigen Behörde durchgeführten Zertifizierungs- und Aufsichtstätigkeiten in die gesamten Zertifizierungs- und Aufsichtsunterlagen der Organisation integriert werden;

3. ihr eigenes nach Punkt ADR.AR.B.005(e) eingerichtetes Informationssicherheitsmanagementsystem alle in ihrem Namen wahrgenommenen Aufgaben der Zertifizierung und fortlaufenden Aufsicht erfasst."

5. In Punkt ADR.AR.C.005 wird folgender Buchstabe f angefügt:

„f) Im Hinblick auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt ADR.OR.D.005A durch die Organisation überprüft die zuständige Behörde im Anschluss an den anwendbaren Aufsichts-Auditzyklus und bei jeder Änderung des Arbeitsumfangs der Organisation zusätzlich zur Einhaltung der Buchstaben a bis e jede nach Punkt IS.I.OR.200(e) dieser Verordnung oder Punkt IS.D.OR.200(e) der Delegierten Verordnung (EU) 2022/1645 erteilte Genehmigung."

6. Nach Punkt ADR.AR.C.040 wird folgender Punkt ADR.AR.C.040A eingefügt:

„**ADR.AR.C.040A Änderungen des Informationssicherheitsmanagementsystems**

a) Änderungen, die gemäß dem Verfahren nach Punkt IS.D.OR.255(a) des Anhangs (Teil-IS.D.OR) der Delegierten Verordnung (EU) 2022/1645 verwaltet und der zuständigen Behörde gemeldet werden, muss die zuständige Behörde nach den in Punkt ADR.AR.C.005 festgelegten Grundsätzen in ihre fortlaufende Aufsicht zur Überprüfung aufnehmen. Wird eine Nichteinhaltung festgestellt, teilt die zuständige Behörde dies der Organisation mit, verlangt weitere Änderungen und verfährt nach Punkt ADR.AR.C.055.

b) Für sonstige Änderungen, deren Genehmigung nach Punkt IS.D.OR.255(b) des Anhangs (Teil-IS.D.OR) der Delegierten Verordnung (EU) 2022/1645 beantragt werden muss, gilt Folgendes:

1. Bei Eingang eines Änderungsantrags prüft die zuständige Behörde, ob die Organisation die geltenden Anforderungen erfüllt, bevor sie die Genehmigung erteilt.

2. Die zuständige Behörde legt die Bedingungen fest, unter denen die Organisation während der Umsetzung der Änderung tätig sein darf.

3. Hat sich die zuständige Behörde vergewissert, dass die Organisation die geltenden Anforderungen erfüllt, genehmigt sie die Änderung."

ANHANG VII

Anhang II (Teil-145), Anhang III (Teil-66) und Anhang Vc (Teil-CAMO) der Verordnung (EU) Nr. 1321/2014 werden wie folgt geändert:

1. Anhang II (Teil-145) wird wie folgt geändert:

a) Das Inhaltsverzeichnis wird wie folgt geändert:

i) Nach der Überschrift von Punkt 145.A.200 wird die folgende Überschrift eingefügt:

„145.A.200A Informationssicherheitsmanagementsystem ".

ii) Nach der Überschrift von Punkt 145.B.135 wird die folgende Überschrift eingefügt:

„145.B.135A Unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit".

iii) Die Überschrift von Punkt 145.B.205 erhält folgende Fassung:

„145.B.205 Zuweisung von Aufgaben".

iv) Nach der Überschrift von Punkt 145.B.330 wird die folgende Überschrift eingefügt:

„145.B.330A Änderungen des Informationssicherheitsmanagementsystems ".

b) Nach Punkt 145.A.200 wird folgender Punkt 145.A.200A eingefügt:

„145.A.200A **Informationssicherheitsmanagementsystem**

Zusätzlich zu dem nach Punkt 145.A.200 vorgeschriebenen Managementsystem muss die Instandhaltungsorganisation ein Informationssicherheitsmanagementsystem gemäß der Durchführungsverordnung (EU) 2023/203 einrichten, umsetzen und pflegen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

c) In Punkt 145.B.125 wird der folgende Buchstabe c angefügt:

„c) Die zuständige Behörde des betreffenden Mitgliedstaats übermittelt der Agentur so bald wie möglich sicherheitsrelevante Informationen, die sie im Rahmen der Meldungen zur Informationssicherheit nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.230 der Durchführungsverordnung (EU) 2023/203 erhalten hat."

d) Nach Punkt 145.B.135 wird folgender Punkt 145.B.135A eingefügt:

„145.B.135A **Unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit**

a) Die zuständige Behörde richtet ein System zur angemessenen Erfassung, Analyse und Verbreitung von Informationen im Zusammenhang mit von Organisationen gemeldeten Störungen und Schwachstellen der Informationssicherheit ein, die sich auf die Flugsicherheit auswirken können. Zur Verbesserung der Koordinierung und Kompatibilität der Meldesysteme erfolgt dies in Abstimmung mit allen anderen einschlägigen Behörden, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig sind.

b) Die Agentur richtet ein System zur angemessenen Analyse aller sicherheitsrelevanten Informationen ein, die sie nach Punkt 145.B.125(c) erhalten hat, und übermittelt den Mitgliedstaaten und der Kommission unverzüglich alle Informationen, auch Empfehlungen oder zu ergreifende Abhilfemaßnahmen, die diese benötigen, um zeitnah auf Störungen oder Schwachstellen der Informationssicherheit zu reagieren, die sich auf die Flugsicherheit auswirken können und von denen auch Erzeugnisse, Teile, nicht eingebaute Ausrüstung, Personen oder Organisationen betroffen sein können, die der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten unterliegen.

c) Nach Eingang der unter den Buchstaben a und b genannten Informationen ergreift die zuständige Behörde geeignete Maßnahmen, um den potenziellen Auswirkungen der Störung oder Schwachstelle der Informationssicherheit auf die Flugsicherheit zu begegnen.

d) Nach Buchstabe c ergriffene Maßnahmen müssen unverzüglich allen Personen bzw. Organisationen mitgeteilt werden, die diese nach Maßgabe der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten befolgen müssen. Die zuständige Behörde des betreffenden Mitgliedstaats muss diese Maßnahmen auch der Agentur und, falls ein gemeinsames Handeln erforderlich ist, den übrigen betroffenen Mitgliedstaaten mitteilen."

e) In Punkt 145.B.200 wird folgender Buchstabe e angefügt:

„e) Zusätzlich zu den Anforderungen nach Buchstabe a muss das von der zuständigen Behörde eingerichtete und gepflegte Managementsystem Anhang I (Teil-IS.AR) der Durchführungsverordnung (EU) 2023/203 genügen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

f) Punkt 145.B.205 wird wie folgt geändert:

i) Die Überschrift erhält folgende Fassung:

„145.B.205 **Zuweisung von Aufgaben**".

ii) Folgender Buchstabe c wird angefügt:

„c) In Bezug auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt 145.A.200A durch die Organisation kann die zuständige Behörde nach Buchstabe a qualifizierten Stellen oder jeder einschlägigen Behörde, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig ist, Aufgaben zuweisen. Bei der Zuweisung von Aufgaben stellt die zuständige Behörde sicher, dass

1. die qualifizierte Stelle oder die einschlägige Behörde alle Aspekte im Zusammenhang mit der Flugsicherheit koordiniert und berücksichtigt;

2. die Ergebnisse der von der qualifizierten Stelle oder der einschlägigen Behörde durchgeführten Zertifizierungs- und Aufsichtstätigkeiten in die gesamten Zertifizierungs- und Aufsichtsunterlagen der Organisation integriert werden;

3. ihr eigenes nach Punkt 145.B.200(e) eingerichtetes Informationssicherheitsmanagementsystem alle in ihrem Namen wahrgenommenen Aufgaben der Zertifizierung und fortlaufenden Aufsicht erfasst."

g) In Punkt 145.B.300 wird folgender Buchstabe g angefügt:

„g) Im Hinblick auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt 145.A.200A durch die Organisation überprüft die zuständige Behörde im Anschluss an den anwendbaren Aufsichts-Auditzyklus und bei jeder Änderung des Arbeitsumfangs der Organisation zusätzlich zur Einhaltung der Buchstaben a bis f jede nach Punkt IS.I.OR.200(e) dieser Verordnung oder Punkt IS.D.OR.200(e) der Delegierten Verordnung (EU) 2022/1645 erteilte Genehmigung."

h) Nach Punkt 145.B.330 wird folgender Punkt 145.B.330A eingefügt:

„145.B.330A **Änderungen des Informationssicherheitsmanagementsystems**

a) Änderungen, die gemäß dem Verfahren nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(a) der Durchführungsverordnung (EU) 2023/203 verwaltet und der zuständigen Behörde gemeldet werden, muss die zuständige Behörde nach den in Punkt 145.B.300 festgelegten Grundsätzen in ihre fortlaufende Aufsicht zur Überprüfung aufnehmen. Wird eine Nichteinhaltung festgestellt, teilt die zuständige Behörde dies der Organisation mit, verlangt weitere Änderungen und verfährt nach Punkt 145.B.350.

b) Für sonstige Änderungen, deren Genehmigung nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(b) der Durchführungsverordnung (EU) 2023/203 beantragt werden muss, gilt Folgendes:

1. Bei Eingang eines Änderungsantrags prüft die zuständige Behörde, ob die Organisation die geltenden Anforderungen erfüllt, bevor sie die Genehmigung erteilt.

2. Die zuständige Behörde legt die Bedingungen fest, unter denen die Organisation während der Umsetzung der Änderung tätig sein darf.

3. Hat sich die zuständige Behörde vergewissert, dass die Organisation die geltenden Anforderungen erfüllt, genehmigt sie die Änderung."

2. Anhang III (Teil-66) wird wie folgt geändert:

a) Nach der Überschrift von Punkt 66.B.10 wird die folgende Überschrift eingefügt:

„66.B.15 Informationssicherheitsmanagementsystem ".

b) Nach Punkt 66.B.10 wird folgender Punkt 66.B.15 eingefügt:

„66.B.15 **Informationssicherheitsmanagementsystem**

Die zuständige Behörde muss ein Informationssicherheitsmanagementsystem nach Anhang I (Teil-IS.AR) der Durchführungsverordnung (EU) 2023/203 einrichten, umsetzen und pflegen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

3. Anhang Vc (Teil-CAMO) wird wie folgt geändert:

a) Das Inhaltsverzeichnis wird wie folgt geändert:

i) Nach der Überschrift von Punkt CAMO.A.200 wird die folgende Überschrift eingefügt:

„CAMO.A.200A Informationssicherheitsmanagementsystem ".

ii) Nach der Überschrift von Punkt CAMO.B.135 wird die folgende Überschrift eingefügt:

„CAMO.B.135A Unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit".

iii) Die Überschrift von Punkt CAMO.B.205 erhält folgende Fassung:

„CAMO.B.205 Zuweisung von Aufgaben".

iv) Nach der Überschrift von Punkt CAMO.B.330 wird die folgende Überschrift eingefügt:

„CAMO.B.330A Änderungen des Informationssicherheitsmanagementsystems ".

b) Nach Punkt CAMO.A.200 wird folgender Punkt CAMO.A.200A eingefügt:

„CAMO.A.200A **Informationssicherheitsmanagementsystem**

Zusätzlich zu dem nach Punkt CAMO.A.200 vorgeschriebenen Managementsystem muss die Organisation ein Informationssicherheitsmanagementsystem gemäß der Durchführungsverordnung (EU) 2023/203 einrichten, umsetzen und pflegen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

c) In Punkt CAMO.B.125 wird der folgenden Buchstabe c angefügt:

„c) Die zuständige Behörde des betreffenden Mitgliedstaats übermittelt der Agentur so bald wie möglich sicherheitsrelevante Informationen, die sie im Rahmen der Meldungen zur Informationssicherheit nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.230 der Durchführungsverordnung (EU) 2023/203 erhalten hat."

d) Nach Punkt CAMO.B.135 wird folgender Punkt CAMO.B.135A eingefügt:

„CAMO.B.135A **Unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit**

a) Die zuständige Behörde richtet ein System zur angemessenen Erfassung, Analyse und Verbreitung von Informationen im Zusammenhang mit von Organisationen gemeldeten Störungen und Schwachstellen der Informationssicherheit ein, die sich auf die Flugsicherheit auswirken können. Zur Verbesserung der Koordinierung und Kompatibilität der Meldesysteme erfolgt dies in Abstimmung mit allen anderen einschlägigen Behörden, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig sind.

b) Die Agentur richtet ein System zur angemessenen Analyse aller sicherheitsrelevanten Informationen ein, die sie nach Punkt CAMO.B.125(c) erhalten hat, und übermittelt den Mitgliedstaaten und der Kommission unverzüglich alle Informationen, auch Empfehlungen oder zu ergreifende Abhilfemaßnahmen, die diese benötigen, um zeitnah auf Störungen oder Schwachstellen der Informationssicherheit zu reagieren, die sich auf die Flugsicherheit auswirken können und von denen auch Erzeugnisse, Teile, nicht eingebaute Ausrüstung, Personen oder Organisationen betroffen sein können, die der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten unterliegen.

c) Nach Eingang der unter den Buchstaben a und b genannten Informationen ergreift die zuständige Behörde geeignete Maßnahmen, um den potenziellen Auswirkungen der Störung oder Schwachstelle der Informationssicherheit auf die Flugsicherheit zu begegnen.

d) Nach Buchstabe c ergriffene Maßnahmen müssen unverzüglich allen Personen bzw. Organisationen mitgeteilt werden, die diese nach Maßgabe der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten befolgen müssen. Die zuständige Behörde des betreffenden Mitgliedstaats muss diese Maßnahmen auch der Agentur und, falls ein gemeinsames Handeln erforderlich ist, den übrigen betroffenen Mitgliedstaaten mitteilen."

e) In Punkt CAMO.B.200 wird folgender Buchstabe e angefügt:

„e) Zusätzlich zu den Anforderungen nach Buchstabe a muss das von der zuständigen Behörde eingerichtete und gepflegte Managementsystem Anhang I (Teil-IS.AR) der Durchführungsverordnung (EU) 2023/203 genügen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

f) Punkt CAMO.B.205 wird wie folgt geändert:

i) Die Überschrift erhält folgende Fassung:

„CAMO.B.205 **Zuweisung von Aufgaben**".

ii) Folgender Buchstabe c wird angefügt:

„c) In Bezug auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt CAMO.A.200A durch die Organisation kann die zuständige Behörde nach Buchstabe a qualifizierten Stellen oder jeder einschlägigen Behörde, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig ist, Aufgaben zuweisen. Bei der Zuweisung von Aufgaben stellt die zuständige Behörde sicher, dass

1. die qualifizierte Stelle oder die einschlägige Behörde alle Aspekte im Zusammenhang mit der Flugsicherheit koordiniert und berücksichtigt;

2. die Ergebnisse der von der qualifizierten Stelle oder der einschlägigen Behörde durchgeführten Zertifizierungs- und Aufsichtstätigkeiten in die gesamten Zertifizierungs- und Aufsichtsunterlagen der Organisation integriert werden;

3. ihr eigenes nach Punkt CAMO.B.200(e) eingerichtetes Informationssicherheitsmanagementsystem alle in ihrem Namen wahrgenommenen Aufgaben der Zertifizierung und fortlaufenden Aufsicht erfasst."

g) In Punkt CAMO.B.300 wird folgender Buchstabe g angefügt:

„g) Im Hinblick auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt CAMO.A.200A durch die Organisation überprüft die zuständige Behörde im Anschluss an den anwendbaren Aufsichts-Auditzyklus und bei jeder Änderung des Arbeitsumfangs der Organisation zusätzlich zur Einhaltung der Buchstaben a bis f jede nach Punkt IS.I.OR.200(e) dieser Verordnung oder Punkt IS.D.OR.200(e) der Delegierten Verordnung (EU) 2022/1645 erteilte Genehmigung."

h) Nach Punkt CAMO.B.330 wird folgender Punkt CAMO.B.330A eingefügt:

„CAMO.B.330A **Änderungen des Informationssicherheitsmanagementsystems**

a) Änderungen, die gemäß dem Verfahren nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(a) der Durchführungsverordnung (EU) 2023/203 verwaltet und der zuständigen Behörde gemeldet werden, muss die zuständige Behörde nach den in Punkt CAMO.B.300 festgelegten Grundsätzen in ihre fortlaufende Aufsicht zur Überprüfung aufnehmen. Wird eine Nichteinhaltung festgestellt, teilt die zuständige Behörde dies der Organisation mit, verlangt weitere Änderungen und verfährt nach Punkt CAMO.B.350.

b) Für sonstige Änderungen, deren Genehmigung nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(b) der Durchführungsverordnung (EU) 2023/203 beantragt werden muss, gilt Folgendes:

1. Bei Eingang eines Änderungsantrags prüft die zuständige Behörde, ob die Organisation die geltenden Anforderungen erfüllt, bevor sie die Genehmigung erteilt.

2. Die zuständige Behörde legt die Bedingungen fest, unter denen die Organisation während der Umsetzung der Änderung tätig sein darf.

3. Hat sich die zuständige Behörde vergewissert, dass die Organisation die geltenden Anforderungen erfüllt, genehmigt sie die Änderung."

ANHANG VIII

Anhang II (Teil-ATCO.AR) und Anhang III (Teil-ATCO.OR) der Verordnung (EU) 2015/340 werden wie folgt geändert:

1. Anhang II (Teil-ATCO.AR) wird wie folgt geändert:

a) In Punkt ATCO.AR.A.020 wird der folgenden Buchstabe c angefügt:

„c) Die zuständige Behörde des betreffenden Mitgliedstaats übermittelt der Agentur so bald wie möglich sicherheitsrelevante Informationen, die sie im Rahmen der Meldungen zur Informationssicherheit nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.230 der Durchführungsverordnung (EU) 2023/203 erhalten hat."

b) Nach Punkt ATCO.AR.A.025 wird folgender Punkt ATCO.AR.A.025A eingefügt:

„**ATCO.AR.A.025A Unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit**

a) Die zuständige Behörde richtet ein System zur angemessenen Erfassung, Analyse und Verbreitung von Informationen im Zusammenhang mit von Organisationen gemeldeten Störungen und Schwachstellen der Informationssicherheit ein, die sich auf die Flugsicherheit auswirken können. Zur Verbesserung der Koordinierung und Kompatibilität der Meldesysteme erfolgt dies in Abstimmung mit allen anderen einschlägigen Behörden, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig sind.

b) Die Agentur richtet ein System zur angemessenen Analyse aller sicherheitsrelevanten Informationen ein, die sie nach Punkt ATCO.AR.A.020 erhalten hat, und übermittelt den Mitgliedstaaten und der Kommission unverzüglich alle Informationen, auch Empfehlungen oder zu ergreifende Abhilfemaßnahmen, die diese benötigen, um zeitnah auf Störungen oder Schwachstellen der Informationssicherheit zu reagieren, die sich auf die Flugsicherheit auswirken können und von denen auch Erzeugnisse, Teile, nicht eingebaute Ausrüstung, Personen oder Organisationen betroffen sein können, die der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten unterliegen.

c) Nach Eingang der unter den Buchstaben a und b genannten Informationen ergreift die zuständige Behörde geeignete Maßnahmen, um den potenziellen Auswirkungen der Störung oder Schwachstelle der Informationssicherheit auf die Flugsicherheit zu begegnen.

d) Nach Buchstabe c ergriffene Maßnahmen müssen unverzüglich allen Personen bzw. Organisationen mitgeteilt werden, die diese nach Maßgabe der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten befolgen müssen. Die zuständige Behörde des betreffenden Mitgliedstaats muss diese Maßnahmen auch der Agentur und, falls ein gemeinsames Handeln erforderlich ist, den übrigen betroffenen Mitgliedstaaten mitteilen."

c) In Punkt ATCO.AR.B.001 wird folgender Buchstabe e angefügt:

„e) Zusätzlich zu den Anforderungen nach Buchstabe a muss das von der zuständigen Behörde eingerichtete und gepflegte Managementsystem Anhang I (Teil-IS.AR) der Durchführungsverordnung (EU) 2023/203 genügen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

d) Punkt ATCO.AR.B.005 wird wie folgt geändert:

i) Die Überschrift erhält folgende Fassung:

„**ATCO.AR.B.005 Zuweisung von Aufgaben**".

ii) Folgender Buchstabe c wird angefügt:

„c) In Bezug auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt ATCO.OR.C.001A durch die Organisation kann die zuständige Behörde nach Buchstabe a qualifizierten Stellen oder jeder einschlägigen Behörde, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig ist, Aufgaben zuweisen. Bei der Zuweisung von Aufgaben stellt die zuständige Behörde sicher, dass

1. die qualifizierte Stelle oder die einschlägige Behörde alle Aspekte im Zusammenhang mit der Flugsicherheit koordiniert und berücksichtigt;

2. die Ergebnisse der von der qualifizierten Stelle oder der einschlägigen Behörde durchgeführten Zertifizierungs- und Aufsichtstätigkeiten in die gesamten Zertifizierungs- und Aufsichtsunterlagen der Organisation integriert werden;

3. ihr eigenes nach Punkt ATCO.AR.B.001(e) eingerichtetes Informationssicherheitsmanagementsystem alle in ihrem Namen wahrgenommenen Aufgaben der Zertifizierung und fortlaufenden Aufsicht erfasst."

e) In Punkt ATCO.AR.C.001 wird folgender Buchstabe f angefügt:

„f) Im Hinblick auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt ATCO.OR.C.001A durch die Organisation überprüft die zuständige Behörde im Anschluss an den anwendbaren Aufsichts-Auditzyklus und bei jeder Änderung des Arbeitsumfangs der Organisation zusätzlich zur Einhaltung der Buchstaben a bis e jede nach Punkt IS.I.OR.200(e) dieser Verordnung oder Punkt IS.D.OR.200(e) der Delegierten Verordnung (EU) 2022/1645 erteilte Genehmigung."

f) Nach Punkt ATCO.AR.E.010 wird folgender Punkt ATCO.AR.E.010A eingefügt:

„**ATCO.AR.E.010A Änderungen des Informationssicherheitsmanagementsystems**

a) Änderungen, die gemäß dem Verfahren nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(a) der Durchführungsverordnung (EU) 2023/203 verwaltet und der zuständigen Behörde gemeldet werden, muss die zuständige Behörde nach den in Punkt ATCO.AR.C.001 festgelegten Grundsätzen in ihre fortlaufende Aufsicht zur Überprüfung aufnehmen. Wird eine Nichteinhaltung festgestellt, teilt die zuständige Behörde dies der Organisation mit, verlangt weitere Änderungen und verfährt nach Punkt ATCO.AR.C.010.

b) Für sonstige Änderungen, deren Genehmigung nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(b) der Durchführungsverordnung (EU) 2023/203 beantragt werden muss, gilt Folgendes:

1. Bei Eingang eines Änderungsantrags prüft die zuständige Behörde, ob die Organisation die geltenden Anforderungen erfüllt, bevor sie die Genehmigung erteilt.

2. Die zuständige Behörde legt die Bedingungen fest, unter denen die Organisation während der Umsetzung der Änderung tätig sein darf.

3. Hat sich die zuständige Behörde vergewissert, dass die Organisation die geltenden Anforderungen erfüllt, genehmigt sie die Änderung."

2. Anhang III (Teil-ATCO.OR) wird wie folgt geändert:

Nach Punkt ATCO.OR.C.001 wird folgender Punkt ATCO.OR.C.001A eingefügt:

„**ATCO.OR.C.001A Informationssicherheitsmanagementsystem**

Zusätzlich zu dem nach Punkt ATCO.OR.C.001 vorgeschriebenen Managementsystem muss die Ausbildungsorganisation ein Informationssicherheitsmanagementsystem gemäß der Durchführungsverordnung (EU) 2023/203 einrichten, umsetzen und pflegen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

ANHANG IX

Anhang II (Teil-ATM/ANS.AR) und Anhang III (Teil-ATM/ANS.OR) der Durchführungsverordnung (EU) 2017/373 werden wie folgt geändert:

1. Anhang II (Teil-ATM/ANS.AR) wird wie folgt geändert:

a) In Punkt ATM/ANS.AR.A.020 wird der folgenden Buchstabe c angefügt:

„c) Die zuständige Behörde des betreffenden Mitgliedstaats übermittelt der Agentur so bald wie möglich sicherheitsrelevante Informationen, die sie im Rahmen der Meldungen zur Informationssicherheit nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.230 der Durchführungsverordnung (EU) 2023/203 erhalten hat."

b) Nach Punkt ATM/ANS.AR.A.025 wird folgender Punkt ATM/ANS.AR.A.025A eingefügt:

„**ATM/ANS.AR.A.025A Unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit**

a) Die zuständige Behörde richtet ein System zur angemessenen Erfassung, Analyse und Verbreitung von Informationen im Zusammenhang mit von Organisationen gemeldeten Störungen und Schwachstellen der Informationssicherheit ein, die sich auf die Flugsicherheit auswirken können. Zur Verbesserung der Koordinierung und Kompatibilität der Meldesysteme erfolgt dies in Abstimmung mit allen anderen einschlägigen Behörden, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig sind.

b) Die Agentur richtet ein System zur angemessenen Analyse aller sicherheitsrelevanten Informationen ein, die sie nach Punkt ATM/ANS.AR.A.020(c) erhalten hat, und übermittelt den Mitgliedstaaten und der Kommission unverzüglich alle Informationen, auch Empfehlungen oder zu ergreifende Abhilfemaßnahmen, die diese benötigen, um zeitnah auf Störungen oder Schwachstellen der Informationssicherheit zu reagieren, die sich auf die Flugsicherheit auswirken können und von denen auch Erzeugnisse, Teile, nicht eingebaute Ausrüstung, Personen oder Organisationen betroffen sein können, die der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten unterliegen.

c) Nach Eingang der unter den Buchstaben a und b genannten Informationen ergreift die zuständige Behörde geeignete Maßnahmen, um den potenziellen Auswirkungen der Störung oder Schwachstelle der Informationssicherheit auf die Flugsicherheit zu begegnen.

d) Nach Buchstabe c ergriffene Maßnahmen müssen unverzüglich allen Personen bzw. Organisationen mitgeteilt werden, die diese nach Maßgabe der Verordnung (EU) 2018/1139 und deren delegierten Rechtsakten und Durchführungsrechtsakten befolgen müssen. Die zuständige Behörde des betreffenden Mitgliedstaats muss diese Maßnahmen auch der Agentur und, falls ein gemeinsames Handeln erforderlich ist, den übrigen betroffenen Mitgliedstaaten mitteilen."

c) In Punkt ATM/ANS.AR.B.001 wird der folgenden Buchstabe e angefügt:

„e) Zusätzlich zu den Anforderungen nach Buchstabe a muss das von der zuständigen Behörde eingerichtete und gepflegte Managementsystem Anhang I (Teil-IS.AR) der Durchführungsverordnung (EU) 2023/203 genügen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

d) Punkt ATM/ANS.AR.B.005 wird wie folgt geändert:

i) Die Überschrift erhält folgende Fassung:

„**ATM/ANS.AR.B.005 Zuweisung von Aufgaben**".

ii) Folgender Buchstabe c wird angefügt:

„c) In Bezug auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt ATM/ANS.OR.B.005A durch die Organisation kann die zuständige Behörde nach Buchstabe a qualifizierten Stellen oder jeder einschlägigen Behörde, die in dem betreffenden Mitgliedstaat für Informationssicherheit oder Cybersicherheit zuständig ist, Aufgaben zuweisen. Bei der Zuweisung von Aufgaben stellt die zuständige Behörde sicher, dass

1. die qualifizierte Stelle oder die einschlägige Behörde alle Aspekte im Zusammenhang mit der Flugsicherheit koordiniert und berücksichtigt;

2. die Ergebnisse der von der qualifizierten Stelle oder der einschlägigen Behörde durchgeführten Zertifizierungs- und Aufsichtstätigkeiten in die gesamten Zertifizierungs- und Aufsichtsunterlagen der Organisation integriert werden;

3. ihr eigenes nach Punkt ATM/ANS.AR.B.001(e) eingerichtetes Informationssicherheitsmanagementsystem alle in ihrem Namen wahrgenommenen Aufgaben der Zertifizierung und fortlaufenden Aufsicht erfasst."

e) In Punkt ATM/ANS.AR.C.010 wird der folgenden Buchstabe d angefügt:

„d) Im Hinblick auf die Zertifizierung und Beaufsichtigung der Einhaltung von Punkt ANS.OR.B.005A durch die Organisation überprüft die zuständige Behörde im Anschluss an den anwendbaren Aufsichts-Auditzyklus und bei jeder Änderung des Arbeitsumfangs der Organisation zusätzlich zur Einhaltung der Buchstaben a bis c jede nach Punkt IS.I.OR.200(e) dieser Verordnung oder Punkt IS.D.OR.200(e) der Delegierten Verordnung (EU) 2022/1645 erteilte Genehmigung."

f) Nach Punkt ATM/ANS.AR.C.025 wird folgender Punkt ATM/ANS.AR.C.025A eingefügt:

„**ATM/ANS.AR.C.025A Änderungen des Informationssicherheitsmanagementsystems**

a) Änderungen, die gemäß dem Verfahren nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(a) der Durchführungsverordnung (EU) 2023/203 verwaltet und der zuständigen Behörde gemeldet werden, muss die zuständige Behörde nach den in Punkt ATM/ANS.AR.C.010 festgelegten Grundsätzen in ihre fortlaufende Aufsicht zur Überprüfung aufnehmen. Wird eine Nichteinhaltung festgestellt, teilt die zuständige Behörde dies der Organisation mit, verlangt weitere Änderungen und verfährt nach Punkt ATM/ANS.AR.C.050.

b) Für sonstige Änderungen, deren Genehmigung nach Anhang II (Teil-IS.I.OR) Punkt IS.I.OR.255(b) der Durchführungsverordnung (EU) 2023/203 beantragt werden muss, gilt Folgendes:

1. Bei Eingang eines Änderungsantrags prüft die zuständige Behörde, ob die Organisation die geltenden Anforderungen erfüllt, bevor sie die Genehmigung erteilt.

2. Die zuständige Behörde legt die Bedingungen fest, unter denen die Organisation während der Umsetzung der Änderung tätig sein darf.

3. Hat sich die zuständige Behörde vergewissert, dass die Organisation die geltenden Anforderungen erfüllt, genehmigt sie die Änderung."

2. Anhang III (Teil-ATM/ANS.OR) wird wie folgt geändert:

a) Nach Punkt ATM/ANS.OR.B.005 wird folgender Punkt ATM/ANS.OR.B.005A eingefügt:

„**ATM/ANS.OR.B.005A Informationssicherheitsmanagementsystem**

Zusätzlich zu dem nach Punkt ATM/ANS.OR.B.005 vorgeschriebenen Managementsystem muss der Diensteanbieter ein Informationssicherheitsmanagementsystem gemäß der Durchführungsverordnung (EU) 2023/203 einrichten, umsetzen und pflegen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist."

b) Punkt ATM/ANS.OR.D.010 erhält folgende Fassung:

„**ATM/ANS.OR.D.010 Sicherheitsmanagement**

a) Die Anbieter von Flugsicherungsdiensten und Verkehrsflussregelungsanbieter sowie die Netzmanager müssen im Rahmen ihres Managementsystems nach Punkt ATM/ANS.OR.B.005 ein Sicherheitsmanagementsystem einrichten, mit dem Folgendes gewährleistet wird:

1. die Sicherheit ihrer Einrichtungen und ihres Personals, so dass unrechtmäßige Eingriffe in die Erbringung ihrer Dienste verhindert werden;

2. die Sicherheit der Betriebsdaten, die sie erhalten oder erzeugen oder auf sonstige Weise nutzen, so dass der Zugang zu diesen Daten auf Befugte beschränkt ist.

b) Für das Sicherheitsmanagementsystem sind folgende Festlegungen zu treffen:

1. Prozesse und Verfahren zur Bewertung des Sicherheitsrisikos und dessen Minderung, Überwachung und Verbesserung der Sicherheit, Überprüfungen der Sicherheit und Verbreitung der daraus gezogenen Lehren;

2. die zur Identifizierung, Überwachung und Erkennung von Sicherheitsverletzungen sowie zur Alarmierung des Personals durch geeignete Sicherheitswarnungen vorgesehenen Mittel;

3. die Mittel zur Beherrschung der Auswirkungen von Sicherheitsverletzungen sowie zur Identifizierung von Maßnahmen zur Wiederherstellung und von Abhilfeverfahren mit dem Ziel, eine Wiederholung zu verhindern.

c) Die Anbieter von Flugsicherungsdiensten, Verkehrsflussregelungsanbieter und der Netzmanager müssen gewährleisten, dass ihr Personal gegebenenfalls sicherheitsüberprüft ist, und stimmen sich mit den zuständigen zivilen und militärischen Behörden ab, um den Schutz ihrer Einrichtungen, ihres Personals und ihrer Daten zu gewährleisten.

d) Die mit der Informationssicherheit zusammenhängenden Aspekte müssen nach Punkt ATM/ANS.OR.B.005A geregelt werden.“