

RÈGLEMENT D'EXÉCUTION (UE) 2019/1583 DE LA COMMISSION**du 25 septembre 2019****modifiant le règlement d'exécution (UE) 2015/1998 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, en ce qui concerne les mesures de cybersécurité****(Texte présentant de l'intérêt pour l'EEE)**

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002 ⁽¹⁾, et notamment son article 1^{er} et son article 4, paragraphe 3,

considérant ce qui suit:

- (1) L'un des principaux objectifs du règlement (CE) n° 300/2008 est d'établir la base d'une interprétation commune de l'annexe 17 («Sûreté») de la convention relative à l'aviation civile internationale ⁽²⁾ du 7 décembre 1944, 10^e édition, 2017, dont tous les États membres de l'Union européenne sont signataires.
- (2) Les moyens d'atteindre les objectifs sont les suivants: a) établissement de règles communes et de normes de base communes en matière de sûreté de l'aviation civile et b) mécanismes de contrôle de la conformité.
- (3) La modification de la législation d'exécution vise à aider les États membres à garantir le respect intégral de l'amendement le plus récent (amendement 16) de l'annexe 17 de la convention relative à l'aviation civile internationale, qui a introduit de nouvelles normes au point 3.1.4 concernant l'organisation nationale et l'autorité compétente, et au point 4.9.1 concernant les mesures de prévention en matière de cybersécurité.
- (4) En transposant ces normes dans la législation d'exécution de l'Union européenne relative à la sûreté de l'aviation, il sera fait en sorte que les autorités compétentes établissent et mettent en œuvre des procédures pour partager des informations de manière pratique et opportune, selon qu'il convient, avec les autres autorités et agences nationales, les exploitants d'aéroport, les transporteurs aériens et les autres entités concernées, afin de les aider à effectuer des évaluations des risques efficaces concernant leurs opérations et, ce faisant, à mener des évaluations efficaces des risques en matière de sûreté concernant, entre autres, la cybersécurité et à mettre en œuvre des mesures visant à lutter contre les cybermenaces.
- (5) La directive (UE) 2016/1148 du Parlement européen et du Conseil ⁽³⁾ concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (ci-après la «directive SRI») établit des mesures visant à atteindre un niveau élevé commun de sécurité des réseaux et des systèmes d'information au sein de l'Union afin d'améliorer le fonctionnement du marché intérieur. Les mesures découlant de la directive SRI et du présent règlement devraient être coordonnées au niveau national afin d'éviter les lacunes et les obligations redondantes.
- (6) Il convient dès lors de modifier le règlement d'exécution (UE) 2015/1998 de la Commission ⁽⁴⁾ en conséquence.
- (7) Les mesures prévues par le présent règlement sont conformes à l'avis du comité pour la sûreté de l'aviation civile, institué en vertu de l'article 19, paragraphe 1, du règlement (CE) n° 300/2008,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

L'annexe du règlement d'exécution (UE) 2015/1998 est modifiée conformément à l'annexe du présent règlement.

⁽¹⁾ JO L 97 du 9.4.2008, p. 72.⁽²⁾ <https://icao.int/publications/pages/doc7300.aspx>⁽³⁾ Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).⁽⁴⁾ Règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile (JO L 299 du 14.11.2015, p. 1).

Article 2

Le présent règlement entre en vigueur le 31 décembre 2020.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 25 septembre 2019.

Par la Commission
Le président
Jean-Claude JUNCKER

ANNEXE

L'annexe du règlement d'exécution (UE) 2015/1998 est modifiée comme suit:

1) le point 1.0.6 suivant est ajouté:

«1.0.6. L'autorité compétente établit et met en œuvre des procédures pour partager des informations de manière pratique et opportune, selon qu'il convient, avec les autres autorités et agences nationales, les exploitants d'aéroport, les transporteurs aériens et les autres entités concernées, afin de les aider à effectuer des évaluations des risques efficaces concernant leurs opérations.»

2) le point 1.7 suivant est ajouté:

«1.7. IDENTIFICATION DES DONNÉES ET SYSTÈMES DE TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION CRITIQUES POUR L'AVIATION CIVILE ET PROTECTION DE CES DONNÉES ET SYSTÈMES CONTRE LES CYBERMENACES

1.7.1. L'autorité compétente veille à ce que les exploitants d'aéroport, les transporteurs aériens et les entités tels que définis dans le programme national de sûreté de l'aviation civile identifient et protègent leurs données et systèmes de technologies de l'information et de la communication critiques contre les cyberattaques pouvant affecter la sûreté de l'aviation civile.

1.7.2. Les exploitants d'aéroport, les transporteurs aériens et les entités déterminent dans leur programme de sûreté, ou tout document pertinent référencé dans le programme de sûreté, les données et systèmes de technologies de l'information et de la communication critiques décrits au point 1.7.1.

Le programme de sûreté, ou tout document pertinent référencé dans le programme de sûreté, détaille les mesures de protection contre les cyberattaques décrites au point 1.7.1, de détection de ces attaques, de réaction à celles-ci et de rétablissement après celles-ci.

1.7.3. Les mesures détaillées visant à protéger ces systèmes et données contre toute intervention illicite sont définies, mises au point et appliquées conformément à une évaluation des risques effectuée par l'exploitant de l'aéroport, le transporteur aérien ou l'entité, selon le cas.

1.7.4. Lorsqu'une autorité ou une agence spécifique est compétente pour les mesures liées aux cybermenaces à l'intérieur d'un même État membre, cette autorité ou agence peut être désignée comme compétente pour la coordination et/ou le suivi des dispositions du présent règlement relatives à la cybersécurité.

1.7.5. Lorsque les exploitants d'aéroport, les transporteurs aériens et les entités tels que définis dans le programme national de sûreté de l'aviation civile sont soumis à des exigences distinctes en matière de cybersécurité découlant d'autres législations de l'Union européenne ou nationales, l'autorité compétente peut remplacer la conformité aux exigences du présent règlement par le respect des éléments figurant dans les autres législations de l'Union européenne ou nationales. L'autorité compétente se consulte avec les autres autorités compétentes pour garantir la coordination ou la compatibilité des régimes de surveillance.»

3) le point 11.1.2 est remplacé par le texte suivant:

«11.1.2. Le personnel suivant devra avoir subi avec succès une vérification ordinaire ou renforcée des antécédents:

- a) les personnes recrutées pour mettre en œuvre ou être responsables de la mise en œuvre de l'inspection/filtrage, du contrôle d'accès ou d'autres contrôles de sûreté ailleurs que dans une zone de sûreté à accès réglementé;
- b) les personnes disposant d'un accès non accompagné au fret aérien et au courrier aérien, au courrier des transporteurs aériens et au matériel des transporteurs aériens, aux approvisionnements de bord et aux fournitures destinées aux aéroports qui ont fait l'objet des contrôles de sûreté requis;
- c) les personnes ayant des droits d'administrateur ou un accès non surveillé et illimité aux données et systèmes de technologies de l'information et de la communication critiques utilisés aux fins de la sûreté de l'aviation civile comme décrit au point 1.7.1 conformément au programme national de sûreté de l'aviation, ou qui ont été identifiées d'une autre manière dans l'évaluation des risques conformément au point 1.7.3.

Sauf indication contraire dans le présent règlement, la nécessité de procéder à une vérification ordinaire ou renforcée des antécédents doit être déterminée par l'autorité compétente conformément aux dispositions nationales applicables.»

4) le point 11.2.8 suivant est ajouté:

«11.2.8. Formation des personnes ayant un rôle ou une responsabilité en lien avec les cybermenaces

11.2.8.1. Les personnes mettant en œuvre les mesures visées au point 1.7.2 doivent avoir les compétences et aptitudes requises pour mener à bien de manière efficace les tâches qui leur sont assignées. Elles sont informées des cyber-risques pertinents selon le principe du “besoin d’en connaître”.

11.2.8.2. Les personnes ayant accès aux données ou aux systèmes reçoivent une formation appropriée et spécifique en rapport avec leur fonction, à la hauteur de leur rôle et de leurs responsabilités, comprenant une information sur les risques pertinents lorsque leur fonction l'exige. L'autorité compétente, ou l'autorité ou l'agence visée au point 1.7.4, détermine ou approuve le contenu du cours.»
