ДЕЛЕГИРАНА РЕГУЛАТИВА (ЕУ) 2022/1645 НА КОМИСИЈАТА

од 14 јули 2022 година

за воспоставување на правила за примена на Регулативата (ЕУ) 2018/1139 на Европскиот парламент и на Советот во однос на барањата за управување со ризиците врз обезбедувањето на информациите што можат да влијаат на воздухопловната безбедност кај организациите што се опфатени со регулативите (ЕУ) бр. 748/2012 и (ЕУ) бр. 139/2014 на Комисијата и за изменување на регулативите (ЕУ) бр. 748/2012 и (ЕУ) бр. 139/2014 на Комисијата

ЕВРОПСКАТА КОМИСИЈА,

имајќи го предвид Договорот за функционирањето на Европската Унија,

имајќи ја предвид Регулативата (ЕУ) бр. 2018/1139 на Европскиот парламент и на Советот, од 4 јули 2018 година, за заеднички правила во областа на цивилното воздухопловство и за основање на Агенција на Европската Унија за безбедност во воздухопловството, и за изменување и дополнување на регулативите (ЕЗ) бр. 2111/2005, (ЕЗ) бр. 1008/2008, (ЕУ) бр. 996/2010, (ЕУ) бр. 376/2014 и директивите 2014/30/ЕУ и 2014/53/ЕУ на Европскиот парламент и на Советот, и за укинување на регулативите (ЕЗ) бр. 552/2004 и (ЕЗ) бр. 216/2008 на Европскиот парламент и на Советот и Регулатива (ЕЕЗ) бр. 3922/91([1]) на Советот, и особено член 19(1), точка (е) и 39(1) точка (б) од истата,

со оглед на тоа што:

(1) Во согласност со битните барања дадени во Анекс II, точка 3.1(б), кон Регулативата (ЕУ) бр. 2018/1139, проектантските и производствените организации спроведуваат и одржуваат систем за управување за потребите на управување со ризиците по безбедноста.

(2) Дополнително, во согласност со битните барања дадени во точките 2.2.1 и 5.2 од Анекс VII, кон Регулативата (ЕУ) 2018/1139, операторите на аеродром и организациите одговорни за обезбедување на услуги за управување со платформа, мора да применуваат и одржуваат систем за управување со ризиците по безбедноста.

(3) Ризиците по безбедноста наведени во рециталите (1) и (2) може да произлезат од различни извори, вклучувајќи ги недостатоците во проектот и одржувањето, аспектите на човечките перформанси, заканите по животната средина и заканите врз обезбедувањето на информациите. Затоа, системите за управување што ги применуваат организациите споменати во рециталите (1) и (2) треба да ги земат предвид не само ризиците по безбедноста што произлегуваат од случајни настани, туку и ризици по безбедноста што произлегуваат од заканите врз обезбедувањето на информациите кога постоечките недостатоци може да се искористат од поединци во злонамерни цели. Тие ризици врз обезбедувањето на информациите постојано се зголемуваат во опкружувањето на цивилното воздухопловство, поради тоа што постоечките информациски системи стануваат сè по поврзани и почеста мета на злонамерни актери.

([1]) Сл. весник. L 212, 22.8.2018 год., стр. 1.

(4) Ризиците поврзани со тие информациски системи не се ограничени на можните напади на сајбер просторот, туку ги вклучуваат и заканите што можат да влијаат врз процесите и процедурите и врз човековата ефикасност.

(5) Голем број на организации веќе користат меѓународни стандарди, како што е ISO 27001, за решавање на проблемот со обезбедувањето на дигиталните информации и податоците. Овие стандарди можеби нема да можат целосно да ги покријат сите особености на цивилното воздухопловство.

(6) Затоа, соодветно е да се воспостават барања за управување со ризиците врз обезбедувањето на информациите што би можеле да влијаат врз воздухопловната безбедност.

(7) Од клучно значење е тие барања да ги покриваат различните воздухопловни области и нивното поврзување, бидејќи воздухопловството е систем на меѓусебно високо поврзани системи. Затоа, тие треба да се применуваат на сите организации од кои веќе се бара да имаат воспоставен систем за управување во согласност со постојното законодавство на Унијата за воздухопловна безбедност.

(8) Барањата утврдени во оваа регулатива треба да се применуваат доследно во сите области од воздухопловството, притоа создавајќи минимално влијание врз законодавството на Унијата за безбедност во воздухопловството кое веќе се применува во тие области.

(9) Барањата утврдени во оваа регулатива не треба да ги доведат во прашање барањата поврзани со обезбедувањето на информациите и сајбер обезбедувањето утврдени во точка 1.7 од Анексот кон Регулативата за спроведување (ЕУ) 2015/1998([2]) на Комисијата и член 14 од Директивата (ЕУ) 2016/1148 на Европскиот парламент и Советот([3]).

(10) Дефиницијата за обезбедувањето на информациите што се користи за целите на овој правен акт не треба да се толкува како различна од дефиницијата за обезбедување на мрежните и информациски системи утврдена во Директивата (ЕУ) 2016/1148.

(11) Со цел да се избегне дуплирање на законските барања, доколку организациите опфатени со оваа регулатива веќе подлежат на барањата за обезбедување што произлегуваат од други акти на Унијата наведени во рециталот (9) и што се еквивалентни во силата на одредбите утврдени во оваа регулатива, усогласеноста со тие барања за обезбедување треба да се смета дека претставува усогласеност со барањата наведени во оваа регулатива.

(12) Организациите опфатени со оваа регулатива што веќе подлежат на барањата за обезбедување кои произлегуваат од Регулативата за спроведување (ЕУ) 2015/1998, исто така, треба да ги исполнуваат барањата од Анекс I (Дел IS.D.OR.230 „План за надворешно известување за обезбедување на информациите“) кон оваа Регулатива бидејќи Регулативата за спроведување (ЕУ) 2015/1998 не содржи одредби поврзани со надворешно известување за инциденти поврзани со обезбедувањето на информациите.

([2]) Регулатива за спроведување (ЕУ) 2015/1998 на Комисијата од 5 ноември 2015 година, за утврдување на деталните мерки за спроведување на заедничките основни стандарди за обезбедувањето во цивилното воздухопловството (Сл. весник бр. L 299, 14.11.2015 год., стр 1).

([3]) Директива (ЕУ) 2016/1148 на Европскиот парламент и на Советот од 6 јули 2016 година за мерки за високо заедничко ниво на обезбедување на мрежните и информациските системи низ Унијата (Сл. весник бр. L 97, 19.7.2016 год., стр. 1).

(13) Регулативите (ЕУ) бр. 748/2012 ([4]) и (ЕУ) бр. 139/2014 ([5]) на Комисијата треба да се изменат и дополнат со цел да се воспостави врска помеѓу системите за управување пропишани во горенаведените регулативи и барањата за управување со обезбедувањето на информациите пропишани со оваа регулатива.

(14) За да им се даде на организациите доволно време да гарантираат усогласеност со новите правила и процедури воведени со оваа регулатива, оваа регулатива треба да отпочне да се применува три години по датумот на влегување во сила.

(15) Барањата утврдени со оваа регулатива се засноваат на Мислење бр. 03/2021([6]), издадено од Агенцијата во согласност со член 75(2) точки (б) и (в) и член 76(1) од Регулативата (ЕУ) 2018/1139.

(16) Во согласност со член 128(4) од Регулативата (ЕУ) 2018/1139, Комисијата консултираше експерти назначени од секоја земја членка во согласност со принципите утврдени во Меѓу-институционалниот договор за подобро креирање закони од 13 април 2016 година ([7]),

ЈА ДОНЕСЕ СЛЕДНАТА РЕГУЛАТИВА:

Член 1

Предмет

Оваа регулатива ги утврдува барањата што треба да ги исполнат организациите наведени во член 2 со цел да се идентификуваат и управуваат ризиците врз обезбедување на информациите што можат да влијаат врз воздухопловната безбедност, а кои би можеле да влијаат врз системите и податоците за информатичка и комуникациска технологија што се користат во цивилното воздухопловство, за да се откријат настани поврзани со обезбедување на информациите и да се идентификуваат инциденти што се сметаат за поврзани со обезбедувањето на информациите, а што би можеле да влијаат врз воздухопловната безбедност и да реагираат и да закрепнат од тие инциденти поврзани со обезбедувањето на информациите.

Член 2

Опсег

1. Оваа регулатива се применува на следниве организации:

(а) на производствените и проектантските организации што се предмет на подделите E и S од Одделот А од Анекс I (Дел 21) кон Регулативата (ЕУ) бр. 748/2012, освен за

([4]) Регулатива (ЕЗ) бр. 748/2009 на Комисијата од 3 август 2012 година, за утврдување на правила за спроведување за сертификација на пловидбеноста и заштитата на животната средина и за воздухоплови и сродни производи, делови и уреди, како и за сертификација на проектантски и производствени организации (Сл. весник бр. L 224, 21.8.2012 год., стр. 1).

([5]) Регулатива (ЕУ) бр. 139/2014 на Комисијата од 12 февруари 2014 година, за утврдување на услови и управните постапки во врска со аеродромите во согласност со Регулатива (ЕЗ) бр. 216/2008 на Европскиот парламент и на Советот (Сл. весник бр. L 44, 14.2.2014 год., стр. 1).

([6]) https://www.easa.europa.eu/document-library/opinions

([7]) Сл. весник L 123, 12.5.2016 год., стр. 1.

проектантските и производствени организации што се вклучени само во проектот и/или производството на воздухопловите ELA2 како што е дефинирано во член 1(2), точка (s) од Регулативата (ЕУ) бр. 748/2012;

(б) на операторите на аеродром и давателите на услуги за управување со платформа што се предмет во Анекс III „Барања за организациите (Дел-ADR.OR)“ кон Регулативата (ЕУ) бр. 139/2014.

2. Оваа регулатива не ги доведува во прашање барањата во врска со обезбедувањето на информациите и сајбер обезбедувањето утврдени во точка 1.7 од Анексот кон Регулативата за спроведување (ЕУ) 2015/1998 и член 14 од Директивата (ЕУ) 2016/1148.

Член 3

Дефиниции

За целите на оваа регулатива, се применуваат следните дефиниции:

(1) „обезбедување на информации (*information security)*“ е заштита на доверливоста, интегритетот, автентичноста и достапноста на мрежните и информациските системи;

(2) „настан поврзан со обезбедување на информации (*information security event)*“ е идентификуван настан кај систем, услуга или мрежа што укажува на можно прекршување на политиката за обезбедување на информации или отказ на контролите за обезбедување на информациите, или од претходно непозната ситуација што може да биде релевантна за обезбедувањето на информациите;

(3) „инцидент (*incident*) е секој настан кој има негативен ефект врз обезбедувањето на мрежните и информациските системи како што е дефинирано во член 4(7) од Директивата (ЕУ) 2016/1148;

(4) „ризик врз обезбедувањето на информациите (*information security risk)*“ е ризикот по операциите во цивилното воздухопловство, имотот, поединците и другите организации поради можен настан поврзан со обезбедувањето на информациите. Ризиците врз обезбедувањето на информациите се поврзани со можноста дека заканите ќе ја искористат ранливоста на информациско средство или на група информациски средства;

(5) „закана (*threat*)“ е можност за нарушување на обезбедувањето на информациите што постои кога има субјект, околност, акција или настан што може да предизвика штета;

(6) „ранливост (*vulnerability*)“ е недостаток или слаба точка кај средство или систем, процедура, проект, имплементација, или кај мерките за обезбедување на информациите што можат да се искористат и да доведат до прекршување на политиката за обезбедување на информациите.

Член 4

Барања кои произлегуваат од други акти на Унијата

1. Доколку организацијата наведена во член 2 ги исполнува барањата за обезбедување утврдени во член 14 од Директивата (ЕУ) 2016/1148 кои се еквивалентни на барањата утврдени во оваа регулатива, усогласеноста со тие барања за обезбедување се смета за усогласеност со барањата утврдени во оваа регулатива.

2. Доколку организацијата наведена во член 2 е оператор или субјект од националните програми за обезбедување во цивилното воздухопловство на земјите членки утврдени во согласност со член 10 од Регулативата (ЕЗ) бр. 300/2008 на Европскиот парламент и Советот ([8]), барањата за сајбер обезбедување од точка 1.7. од Анексот кон Регулативата за спроведување (ЕУ) 2015/1998 се сметаат за еквивалентни на барањата утврдени во оваа регулатива, освен во однос на точката IS.D.OR.230 од Анексот кон оваа регулатива, со која што мора да постои усогласеност.

3. По консултација со EASA и групата за соработка наведена во член 11 од Директивата (ЕУ) 2016/1148, Комисијата може да издаде упатства за проценка на еквивалентноста на барањата утврдени во оваа регулатива и во Директивата (ЕУ) 2016/1148.

Член 5

Надлежен орган

1. Органот што е одговорен за издавање на уверенија за работа и следење на усогласеноста со оваа регулатива е:

(а) во однос на организациите наведени во член 2 точката (а), надлежниот орган назначен во согласност со Анекс I (Дел 21) кон Регулативата (ЕУ) бр. 748/2012;

(б) во однос на организациите наведени во член 2 точка (б), надлежниот орган назначен во согласност со Анекс III (Дел ADR.OR) кон Регулативата (ЕУ) бр. 139/2014.

2. За целите на оваа регулатива, земјите членки можат да назначат независен и самостоен субјект за извршување на доделената улога и одговорностите на надлежните органи наведени во став 1. Во тој случај, мерките за координација се воспоставуваат помеѓу тој субјект и надлежните органи, како што е наведено во став 1, со цел да се обезбеди ефективен надзор над сите барања што организацијата мора да ги исполни.

Член 6

Измена и дополнување на Регулативата (ЕУ) бр. 748/2012

Анекс I (Дел 21) кон Регулативата (ЕУ) бр. 748/2012 се изменува и дополнува како што следува:

(1) Содржината се изменува и дополнува на следниов начин:

(а) по насловот 21.А.139 се вметнува следниот наслов:

„**21.A.139A Систем за управување со обезбедувањето на информациите**“;

(б) по насловот 21.А.239 се вметнува следниот наслов:

„**21.A.239A Систем за управување со обезбедувањето на информациите**“;

(2) по точката 21.А.139 се вметнува следнава точка 21.А.139А:

„**21.A.139A Систем за управување со обезбедувањето на информациите**

([8]) Регулатива (ЕЗ) бр. 300/2008 на Европскиот Парламент и на Советот од 11 март 2008 година за заеднички правила во областа на обезбедувањето на цивилното воздухопловство и за укинување на Регулатива (ЕЗ) бр. 2320/2002 (Сл. весник L 97, 9.4.2008 год., стр. 72.)

Покрај системот за управување со производството што се бара според точката 21.А.139, производствена организација мора да воспостави, спроведува и одржува систем за управување со обезбедувањето на информациите во согласност со Делегираната регулатива (ЕУ) 2022/1645 на Комисијата (*) за да се обезбеди правилно управување со ризиците врз обезбедувањето на информациите што можат да влијаат врз воздухопловната безбедност.

(*) Делегирана регулатива (ЕУ) 2022/1645 на Комисијата од 14 јули 2022 година за утврдување на правилата за примена на Регулативата (ЕУ) 2018/1139 на Европскиот парламент и на Советот во однос на барањата за управување со ризиците врз обезбедувањето на информациите што можат да влијаат на воздухопловната безбедност кај организациите што се опфатени со регулативите (ЕУ) бр. 748/2012 и (ЕУ) бр. 139/2014 на Комисијата и за измена на регулативите (ЕУ) бр. 748/2012 и (ЕУ) бр. 139/2014 на Комисијата (Службен весник 248, 26.9.2022, стр. 18). “ ;

(3) по точката 21.А.239 се вметнува следнава точка 21.А.239А:

„**21.А.239А Систем за управување со обезбедувањето на информациите**

Покрај системот за управување со проекти што се бара според точката 21.А.239, проектантската организација воспоставува, спроведува и одржува систем за управување со обезбедувањето на информациите во согласност со Делегираната регулатива (ЕУ) 2022/1645 за да се обезбеди правилно управување со ризиците врз обезбедувањето на информациите што можат да влијаат врз воздухопловната безбедност.“.

Член 7

Измена и дополнување на Регулативата (ЕУ) бр. 139/2014

Анекс III (Дел-ADR.OR) кон Регулативата (ЕУ) бр. 139/2014 се изменува и дополнува како што следува:

(1) по точката ADR.OR.D.005 се вметнува следнава точката ADR.OR.D.005A:

„ **ADR.OR.D.005A Систем за управување со обезбедувањето на информациите**

Операторот на аеродромот мора да воспостави, спроведува и одржува систем за управување со обезбедувањето на информациите во согласност со Делегираната регулатива (ЕУ) 2022/1645 на Комисијата(*) за да се обезбеди правилно управување со ризиците врз обезбедувањето на информациите што можат да влијаат врз воздухопловната безбедност.

(*) Делегирана регулатива (ЕУ) 2022/1645 на Комисијата од 14 јули 2022 година за утврдување на правилата за примена на Регулативата (ЕУ) 2018/1139 на Европскиот парламент и на Советот во однос на барањата за управување со ризиците врз обезбедувањето на информациите што можат да влијаат на воздухопловната безбедност кај организациите што се опфатени со регулативите (ЕУ) бр. 748/2012 и (ЕУ) бр. 139/2014 на Комисијата и за измена на регулативите

(ЕУ) бр. 748/2012 и (ЕУ) бр. 139/2014 на Комисијата (Службен весник 248, 26.9.2022, стр. 18). “ ;

(2) точката ADR.OR.D.007 се заменува со следново:

„**ADR.OR.D.007 Управување со воздухопловни податоци и воздухопловни информации**

(а) Како дел од својот систем за управување, операторот на аеродром воведува и одржува систем за управување со квалитет, кој ги опфаќа следните активности:

(1) неговите активности за воздухопловни податоци;

(2) неговите активности за давање воздухопловни информации.

(б) Како дел од својот систем за управување, операторот на аеродром мора да воспостави систем за управување со обезбедувањето, а сè со цел да го гарантира обезбедувањето над оперативните податоци што ги прима, произведува или на друг начин ги користи, така што само овластени лица да имаат пристап до овие оперативни податоци.

(в) Системот за управување со обезбедувањето ги дефинира следниве елементи:

(1) процедурите поврзани со проценка и ублажување на ризици поврзани со обезбедувањето на податоците, следење и подобрување на обезбедувањето, ревизија на состојбата поврзана со обезбедувањето и ширење на ново знаење;

(2) средствата наменети за откривање на нарушувања на обезбедувањето и за предупредување на персоналот со соодветни сигнали за предупредување;

(3) средствата за контролирање на последиците од нарушување на обезбедувањето и идентификување на активности за враќање во првобитната состојба и процедури за ублажување на последиците за да се спречи повторување на настаните.

(г) Операторот на аеродромот е должен да гарантира безбедносна проверка на својот персонал во однос на обезбедувањето на воздухопловните податоци.

(д) Аспектите поврзани со обезбедувањето на информациите се управуваат во согласност со точката ADR.OR.D.005.A.“;

(3) по точката ADR.OR.F.045 се вметнува точката ADR.OR.F.045A:

„**ADR.OR.F.045A Систем за управување со обезбедувањето на информациите**

Организацијата што е одговорна за давање на AMS услуги воспоставува, спроведува и одржува систем за управување со обезбедувањето на информациите во согласност со Делегираната регулатива (ЕУ) 2022/1645 за да се обезбеди правилно управување со ризиците врз обезбедувањето на информациите што можат да влијаат врз воздухопловната безбедност.“.

Член 8

Оваа регулатива влегува во сила на дваесеттиот ден по денот на нејзиното објавување во *Службениот весник на Европската Унија*.

Се применува од 16 октомври 2025 година.

Оваа регулатива е целосно обврзувачка и директно применлива во сите земји членки.

Брисел, 14 јули 2022 година.

За Комисијата

Претседател

Урсула ВОН ДЕР ЛЕЈЕН

АНЕКС

ОБЕЗБЕДУВАЊЕ НА ИНФОРМАЦИИТЕ – БАРАЊА ЗА ОРГАНИЗАЦИЈАТА

IS.D.OR.100 Опсег

Во овој дел се утврдуваат барањата што мора да ги исполнуваат организациите од член 2 на оваа регулатива.

IS.D.OR.200 Систем за управување со обезбедувањето на информациите (ISMS)

(a) Со цел да се постигнат целите дадени во член 1, организацијата поставува, спроведуваи одржува систем за управување со обезбедувањето на информациите (ISMS) што гарантира дека организацијата:

(1) воспоставува политика за обезбедувањето на информациите со што ги утврдува општите принципи на организацијата во однос на можното влијание на ризиците врз обезбедувањето на информациите во воздухопловната безбедност;

(2) идентификува и разгледува ризици врз обезбедувањето на информациите во согласност со точката IS.D.OR.205;

(3) дефинира и спроведува мерки за справување со ризикот врз обезбедувањето на информациите во согласност со точка IS.D.OR.210;

(4) применува внатрешниот план за внатрешно известување за обезбедувањето на информациите во согласност со точка IS.D.OR.215;

(5) во согласност со точката IS.D.OR.220 дефинира и спроведува мерки неопходни за откривање на настани поврзани со обезбедувањето на информациите, идентификување на настани кои се сметаат за инциденти што можат да влијаат на воздухопловната безбедност освен за оние што се дозволени според точката

IS.D.OR.205 (д), и одговора и закрепнува од тие инциденти поврзани со обезбедувањето на информациите;

(6) спроведува мерки пријавени од надлежниот орган како непосредна реакција на инцидент или ранливост поврзани со обезбедувањето на информациите што влијаат врз воздухопловната безбедност;

(7) презема соодветни мерки, во согласност со точката IS.D.OR.225, со цел да постапи во согласност со наодите пријавени од надлежниот орган;

(8) спроведува план за надворешно известување во согласност со точката IS.D.OR.230 со цел да им овозможи на надлежните власти да преземат соодветни мерки;

(9) ги исполнува барањата од точката IS.D.OR.235 при доделување договори за било кој дел од активностите наведени во точката IS.D.OR.200 кон други организации;

(10) ги исполнува условите за персоналот наведени во точка IS.D.OR.240;

(11) ги исполнува барања поврзани со водење на евиденција наведени во точка IS.D.OR.245;

(12) ја следи усогласеноста на организацијата со барањата од оваа регулатива и дава повратни информации за наодите до одговорниот менаџер или, во случај на проектантски организации, до раководителот на проектантската организација, со цел обезбедување на ефикасно спроведување на корективните мерки;

(13) без да е во спротивност со применливите барања за известување за инциденти, да ја заштити доверливоста на сите информации што ги добива организацијата од други организации, во согласност со нивното ниво на чувствителност.

(б) Со цел континуирано исполнување на барањата од член 1, организацијата спроведува процес на континуирано подобрување согласно точката IS.D.OR.260.

(в) Организацијата, во согласност со точката IS.D.OR.250, ги документира сите клучни процеси, процедури, улоги и одговорности неопходни за усогласување со точката IS.D.OR.200(а) и воспоставува постапка за изменување и дополнување на таа документација. Промените на овие процеси, процедури, улоги и одговорности се управуваат во согласност со точката IS.D.OR.255.

(г) Процесите, процедурите, улогите и одговорностите воспоставени од страна на организацијата со цел усогласување со точката IS.D.OR.200(а), се соодветни на природата и сложеноста на нејзините активности, засновани на проценка на ризиците врз обезбедувањето на информациите својствени за тие активности, и може да се интегрираат во други постоечки системи за управување кои организацијата веќе ги спроведува.

(д) Без да во спротивност со обврската за усогласеност со барањата за известување кои се содржани во Регулативата (ЕУ) бр. 376/2014 на Европскиот парламент и на Советот ([1]) и барањата од точка IS.D.OR.205(а)13, надлежниот орган може да ѝ издаде овластување на организацијата да не ги спроведува барањата од точките од (а) до (г) и сродните барања од точките од IS.D.OR.205 до IS.D.OR.260, доколку позитивно му докаже на тоа тело дека нејзините активности, капацитети и ресурси, како и услугите што ги обезбедува, дава, прима и одржува, не претставуваат никакви ризици врз обезбедувањето на информациите со можно влијание врз воздухопловната безбедност, ниту врз себе или пак ниту врз други организации. Одобрувањето се заснова на документирана проценка на ризикот врз

обезбедувањето на информациите спроведена од страна на организацијата или трето лице во согласност со точката IS.D.OR.205 и прегледана и одобрена од надлежниот орган.

---

[8] Регулатива (ЕУ) бр. 376/2014 на Европскиот парламент и на Советот од 3 април 2014 година за пријавување, анализа и последователно постапување во врска со настани во цивилното воздухопловство, со која се изменува Регулатива (ЕУ) бр. 996/2010 на Европскиот парламент и на Советот и се укинува Директива 2003/42/ЕЗ на Европскиот парламент и на Советот и Регулативи (ЕЗ) бр. 1321/2007 и (ЕЗ) бр. 1330/2007 на Комисијата (Сл. весник L 122, 24.4.2014, стр.18).

Надлежниот орган ја разгледува континуираната важност на тоа одобрение по применливиот циклус на безбедносен надзор и секогаш кога се спроведуваат промени во опсегот на работата на организацијата.

IS.D.OR.205 Проценка на ризик врз обезбедувањето на информациите

(а) Организацијата е должна да ги идентификува сите нејзини елементи што би можеле да бидат изложени на ризици врз обезбедување на информациите. Тоа вклучува:

(1) активности, капацитети и ресурси на организацијата, како и услуги кои организацијата ги обезбедува, дава, прима или одржува;

(2) опрема, системи, податоци и информации што придонесуваат за функционирање на елементите наведени во точката (1).

(б) Организацијата ги идентификува поврзувањата што ги има со други организации кои би можеле да доведат до взаемна изложеност на ризиците врз обезбедување на информациите.

(в) Во однос на елементите и поврзувањата наведени во точките (а) и (б), организацијата ги идентификува ризиците врз обезбедувањето на информациите што би можеле да влијаат врз воздухопловната безбедност. За секој идентификуван ризик, организацијата е должна да:

(1) го одреди нивото на ризик во согласност со однапред дефинираната класификација утврдена од организацијата;

(2) го поврзе секој ризик и неговото ниво со соодветниот елемент или поврзаност идентификуван во согласност со точките (а) и (б).

Во однапред дефинираната класификација од точката (1) се зема предвид можноста за појава на сценарио за закана и сериозноста на нејзините последици по безбедноста. Врз основа на оваа класификација и земајќи предвид дали организацијата има структурирана и повторлива процедура за управување со ризик за операции, организацијата може да утврди дали ризикот е прифатлив или треба да се постапува со него во согласност со точката IS.D.OR.210.

Со цел да се олесни меѓусебната споредливост на проценките на ризикот, при определувањето на нивото на ризик во согласност со точката (1), се земаат предвид релевантните информации собрани во координација со организациите наведени во точката (б).

(г) Организацијата ја прегледува и ажурира проценката од ризикот спроведена во согласност со точките (а), (б) и (в) во која било од следниве ситуации:

(1) постои промена во елементите што се изложени на ризици врз обезбедувањето на информациите;

(2) постои промена во поврзувањата помеѓу организацијата и другите организации или во ризиците соопштени од други организации;

(3) постои промена во информациите или знаењата што се користат за идентификација, анализа и класификација на ризицоте;

(4) постојат извлечени поуки врз основа на анализа на инцидентите поврзани со обезбедувањето на информациите.

IS.D.OR.210 Справување со ризиците врз обезбедувањето на информациите

(а) Организацијата подготвува мерки за елиминирање на неприфатливите ризици идентификувани во согласност со точката IS.D.OR.205, ги спроведува навремено и ја потврдува нивната континуирана ефективност. Овие мерки ѝ овозможуваат на организацијата да ги:

(1) контролира околностите што придонесуваат за вистинското појавување на сценариото за закана;

(2) ублажува последиците за воздухопловната безбедност поврзани со појавата на сценарио за закана;

(3) избегнува ризиците.

Овие мерки не смеат да внесат нови неприфатливи ризици по воздухопловната безбедност.

(б) Лицето наведено во точка IS.D.OR.240(а) и (б) и друг вклучен персонал од организацијата се информираат за исходот од проценката на ризикот спроведена во согласност со точка IS.D.OR.205, за соодветните сценарија за закана и за мерките што треба да се спроведат.

Организацијата ги информира и организациите со кои има соработка во согласност со точката IS.D.OR.205(б) за сите ризици што се заеднички и за двете организации.

IS.D.OR.215 План за внатрешно известување за обезбедувањето на информациите

(а) Организацијата воспоставува План за внатрешно известување за да овозможи собирање и проценка на настани поврзани со обезбедувањето на информациите, вклучувајќи ги и оние што треба да се пријават во согласност со точката IS.D.OR.230.

(б) Тој план и процесот наведен во точката IS.D.OR.220 ѝ овозможуваат на организацијата да:

(1) идентификува кои од настаните пријавени во согласност со точката (а) се сметаат за инциденти или ранливости поврзани со обезбедувањето на информациите што можат да влијаат на воздухопловната безбедност;

(2) ги идентификува причините за инцидентите и ранливостите поврзани со обезбедувањето на информациите идентификувани во согласност со точка (1), како и факторите што доведуваат до нивното настанување, и справување со нив во рамките на процесот на управување со ризик врз обезбедувањето на информациите во согласност со точките IS.D.OR.205 и IS.D.OR.220;

(3) гарантира проценка на сите познати и релевантни информации поврзани со инцидентите и ранливостите поврзани со обезбедувањето на информациите идентификувани во согласност со точка (1);

(4) гарантира спроведување на методот за внатрешна дистрибуција на информации по потреба.

(в) Секоја договорна организација која може да ја изложи организацијата на ризици врз обезбедувањето на информациите што би можеле да влијаат врз воздухопловната безбедност мора да пријави настаните поврзани со обезбедувањето на информациите до организацијата. Тие извештаи се поднесуваат користејќи ги процедурите утврдени во посебните договорни аранжмани и се оценуваат во согласност со точката (б).

(г) Организацијата соработува во истрагите со која било друга организација која значително придонесува за обезбедувањето на информациите од нејзините сопствени активности.

(д) Организацијата може да го интегрира овој план за известување со другите планови за известување што веќе ги има спроведено.

IS.D.OR.220 Инциденти поврзани со обезбедувањето на информациите - откривање, одговор и обновување

(а) Врз основа на резултатите од проценката на ризикот спроведена во согласност со точката IS.D.OR.205 и резултатите од справувањето со ризикот спроведено во согласност со точката IS.D.OR.210, организацијата спроведува мерки за откривање на инциденти и ранливости што укажуваат на можната појава на неприфатливи ризици и што би можеле да влијаат врз воздухопловната безбедност. Овие мерки за откривање ѝ овозможуваат на организацијата да ги:

(1) идентификува отстапувањата од претходно утврдените основни вредности на перформансите;

(2) активира предупредувањата за примена на соодветни мерки за одговор, во случај на какво било отстапување.

(б) Организацијата спроведува мерки за одговор на сите состојби на настанот идентификувани во точката (а) што можат да придонесат или да придонеле да се појави инцидент поврзан со обезбедувањето на информациите. Овие мерки за одговор ѝ овозможуваат на организацијата да:

(1) иницира реакција на предупредувањата од точката (а)2 со активирање на однапред дефинирани ресурси и процедури;

(2) го ограничи ширењето на нападот и избегнување на целосна реализација на сценариото за закана;

(3) го контролира режимот на неисправност на засегнатите елементи дефинирани во точката IS.D.OR.205(а).

(в) Организацијата спроведува мерки насочени кон закрепнување од инцидентите поврзани со обезбедувањето на информациите, вклучително и итни мерки, доколку е потребно. Тие мерки за закрепнување ѝ овозможуваат на организацијата да:

(1) ги отстрани или ограничи на прифатливо ниво условите што го предизвикале инцидентот;

(2) постигне безбедна состојба на засегнатите елементи дефинирани во точката IS.D.OR.205(а) во рамките на времето за закрепнување што претходно го определила организацијата.

IS.D.OR.225 Одговор на наодите пријавени од надлежниот орган

(а) По добивањето на известувањето за наодите доставено од надлежниот орган, организацијата:

(1) утврдува основна причина или основни причини за неусогласеноста и факторите што придонесуваат за тоа;

(2) утврдува план на корективни мерки;

(3) ја докажува исправката на неусогласеноста на начин прифатлив за надлежниот орган.

(б) Мерките наведени во точката (а) се спроведуваат во периодот договорен со надлежниот орган.

IS.D.OR.230 План за надворешно известување за обезбедувањето на информациите

(а) Организацијата спроведува систем за известување за обезбедување на информациите што е во согласност со барањата утврдени во Регулативата (ЕУ) бр. 376/2014 и нејзините делегирани акти и акти за спроведување, доколку таа регулатива е применлива за организацијата.

(б) Без да е во спротивност со обврските од Регулативата (ЕУ) бр. 376/2014, организацијата гарантира дека секој инцидент или ранливост поврзан со обезбедувањето на информациите што може да претставува значителен ризик врз воздухопловната безбедност, е пријавен до надлежниот орган. Исто така:

(1) доколку таков инцидент или ранливост влијае врз воздухоплов или поврзан систем или составен дел, организацијата, исто така, ова го пријавува и до имателот на одобрението на проектот;

(2) доколку таков инцидент или ранливост влијае врз систем или составен дел што го користи организацијата, таа исто така ова го пријавува и до организацијата одговорна за проектирање на системот или составниот дел.

(в) Организацијата ја пријавува состојбата наведена во точката (б) на следниов начин:

(1) се доставува известување до надлежниот орган и, доколку е применливо, до имателот на одобрението за проектот или до организацијата одговорна за проектирање на системот или составниот дел, веднаш штом организацијата ќе дознае за ситуацијата;

(2) се доставува извештај до надлежниот орган и, доколку е применливо, до имателот на одобрението за проектот или до организацијата одговорна за проектирање на системот или составниот дел што е можно поскоро, но најдоцна во рок од 72 часа од моментот кога организацијата ќе дознае за ситуацијата, освен ако за тоа не ја спречат вонредни околности.

Извештајот се составува во форма утврдена од надлежниот орган и ги содржи сите релевантни информации за ситуацијата познати на организацијата;

(3) се доставува извештај за понатамошните мерки до надлежниот орган и, доколку е применливо, до имателот на одобрението за проект или до организација одговорна за проектирање на системот или составниот дел, и содржи детали за мерките преземени

или планирани да бидат преземени од страна организацијата за да закрепне од инцидентот и мерките што има намера да ги преземе за да спречи слични инциденти за обезбедувањето на информациите во иднина.

Извештајот за понатамошните мерки се поднесува веднаш штом ќе се утврдат овие мерки и се составува во форма што ја утврдува надлежниот орган.

IS.D.OR.235 Договорни активности за управување со обезбедувањето на информациите

(а) Организацијата гарантира дека при склучување договор за кој било дел од активностите од точката IS.D.OR.200 со други организации, договорените активности се во согласност со барањата на оваа регулатива и дека организацијата со која е склучен договорот работи под нејзин надзор. Организацијата гарантира соодветно управување со ризиците поврзани со договорените активности.

(б) Организацијата обезбедува дека надлежниот орган може, на барање, да има пристап до договорната организација со цел да се утврди континуираната усогласеност со применливите барања наведени во оваа регулатива.

IS.D.OR.240 Услови за персоналот

(а) Одговорниот менаџер на организацијата или, во случај на проектантска организација, раководителот на проектантската организација, назначен во согласност со Регулативата (ЕУ) бр. 748/2012 и Регулативата (ЕУ) бр. 139/2014, како што е наведено во член 2, точка 1(а) и (б) од оваа регулатива, има корпоративно овластување да гарантира финансирање и спроведување на сите активности што се бараат со оваа регулатива. Таа личност мора да:

(1) гарантира достапност на сите потребни средства за исполнување на барањата од оваа регулатива;

(2) воспостави и да ја промовира политиката за обезбедувањето на информациите наведени во точка IS.D.OR.200(а)(1);

(3) покаже основно разбирање за оваа регулатива.

(б) Одговорниот менаџер или, во случај на проектантски организации, раководителот на проектантската организација назначува лице или група на лица за да гарантира дека организацијата ги исполнува барањата од оваа регулатива и го одредува опсегот на нивните овластувања. Тоа лице или група на лица директно одговараат пред одговорниот менаџер или, во случај на проектантска организација, пред раководителот на проектантска организација и мора да имаат соодветно знаење, образование и искуство за извршување на своите одговорности. Процедурите одредуваат кој заменува одредено лице во случај на негово подолго отсуство.

(в) Одговорниот менаџер или, во случај на проектантски организации, раководителот на проектантската организација назначува лице или група на лица за управување со функцијата за следење на усогласеноста наведена во точка IS.D.OR.200(а)(12).

(г) Доколку организацијата споделува организациски структури, политики, процеси и процедури поврзани со обезбедувањето на информациите со други организации или области на активност од нејзината организација што не се дел од одобрението или декларацијата, одговорниот менаџер или, во случај на проектантски организации, раководителот на проектантската организација може да ги довери овие активности на заедничко одговорно лице.

Во таков случај, мерки за координација се воспоставуваат помеѓу одговорниот менаџер на организацијата или, во случај на проектантска организација, раководителот на проектантската организација и заедничкото одговорно лице со цел да се обезбеди соодветна интеграција на управувањето со обезбедувањето на информациите во рамките на организацијата.

(д) Одговорниот менаџер или раководителот на проектантската организација или заедничкото одговорно лице од точката (г), имаат законско овластување да ги воспостават и одржуваат организационите структури, политики, процеси и процедури неопходни за примена на точката IS.D.OR.200.

(ѓ) Организацијата мора да има воспоставена процедура за да гарантира дека има доволно персонал за извршување на активностите опфатени со овој анекс.

(е) Организацијата мора да има воспоставено процедура за да гарантира дека персоналот наведен во точката (ѓ) ја има потребната експертиза за извршување на своите задачи.

(ж) Организацијата мора да има воспоставена процедура за да гарантира дека персоналот е свесен за одговорностите поврзани со нивните доделени улоги и задачи.

(з) Организацијата гарантира дека идентитетот и доверливоста на персоналот кој има пристап до информатичките системи и податоците кои се предмет на барањата на оваа регулатива се соодветно утврдени.

IS.D.OR.245 Водење евиденција

(а) Организацијата води евиденција за своите активности поврзани со управувањето со обезбедувањето на информациите.

(1) Организацијата гарантира архивирање и следливост на следнава евиденција:

(i) сите добиени одобренија и сите поврзани проценки на ризикот врз обезбедувањето на информациите во согласност со точката IS.D.OR.200(д);

(ii) договори за активности од точката IS.D.OR.200(а)(9);

(iii) евиденција на клучните постапки од точката IS.D.OR.200(г);

(iv) евиденција за ризиците утврдени во проценката на ризикот од точка IS.D.OR.205 и соодветните мерки за справување со ризиците од точка IS.D.OR.210;

(v) евиденција за инциденти и ранливости поврзани со обезбедувањето на информациите пријавени во согласност со плановите за известување од точките IS.D.OR.215 и IS.D.OR.230;

(vi) евиденција за настаните поврзани со обезбедувањето на информациите што можеби ќе треба да се преиспитаат за да се откријат неоткриени инциденти или ранливости поврзани со обезбедувањето на информациите.

(2) Евиденцијата наведена во точката (1)(i) се чува најмалку пет години откако одобрението ќе престане да важи.

(3) Евиденцијата од точката (1)(ii) се чува најмалку пет години по измената или раскинувањето на договорот.

(4) Евиденцијата од точката (1)(iii), (iv) и (v) се чува најмалку пет години.

(5) Евиденцијата од точка (1)(vi) се чува се додека овие настани поврзани со обезбедување на информациите не се повторно проценети во согласност со фреквенцијата дефинирана во постапката што е утврдена од страна на организацијата.

(б) Организацијата води евиденција за квалификациите и искуството на сопствениот персонал вклучен во активностите за управување со обезбедувањето на информациите.

(1) Евиденцијата за квалификациите и искуството на персоналот се чува се додека лицето работи во организацијата и најмалку три години откако лицето ќе ја напушти организацијата.

(2) На членовите на персоналот, на нивно барање, им се дава пристап до нивните индивидуални досиеја. Дополнително, на нивно барање, организацијата им дава копија од нивната лична евиденција при напуштање на организацијата.

(в) Форматот на евиденцијата мора да се утврди во процедурите на организацијата.

(г) Евиденцијата се чува на начин што гарантира заштита од оштетување, промена или кражба, а информациите се идентификуваат, доколку е потребно, во согласност со нивниот степен на тајност. Организацијата гарантира дека записите се чуваат на начин кој обезбедува интегритет, автентичност и овластен пристап.

IS.D.OR.250 Прирачник за управување со обезбедувањето на информациите (ISSM)

(а) Организацијата му става на располагање на надлежниот орган прирачник за управување со обезбедувањето на информациите (ISMM) и, доколку е применливо, сите поврзани прирачници и референтни процедури, кои содржат:

(1) изјава потпишана од одговорниот менаџер или, во случај на проектантски организации, од раководителот на проектантската организација, со која се потврдува дека организацијата во секое време ќе постапува во согласност со овој анекс и ISMM. Доколку одговорниот менаџер или, во случај на проектантски организации, раководителот на проектантската организација не е главен извршен директор (CEO) на организацијата, тогаш главниот извршен директор (CEO) ја потпишува изјавата;

(2) титула(-и), име(-ња), должност(-и), одговорност(-и) и овластување(-а) на лицето или лицата наведени во точката IS.D.OR.240(б) и (в);

(3) титулата, името, должностите, одговорностите и овластувањата на заеднички одговорното лице од точка IS.D.OR.240(г), доколку е применливо;

(4) политиката за обезбедувањето на информациите на организацијата од точка IS.D.OR.200(a)(1);

(5) општ опис на бројот и категориите на персонал и воспоставениот систем за планирање на достапноста на персоналот како што е пропишано во точка IS.D.OR.240;

(6) титула(-и), име(-ња), должности, одговорности и овластувања на клучните лица одговорни за спроведувањето на точката IS.D.OR.200, вклучувајќи го и лицето или лицата одговорни за функцијата за следење на усогласеноста наведена во точка IS.D.OR.200(a)(12);

(7) организациона шема што ги прикажува поврзаните синџири на одговорност за лицата од точките (2) и (6);

(8) опис на планот за внатрешно известување од точка IS.D.OR.215;

(9) процедури за да се утврди како организацијата обезбедува усогласеност со овој дел, а особено:

(i) документацијата од точка IS.D.OR.200(в);

(ii) процедурите со кои се дефинира како организацијата ги контролира сите договорени активности од точката IS.D.OR.200(а)(9);

(iii) процедура за измена на ISMM дефинирана во точката (в);

(10) листа на тековно одобрени алтернативни начини на усогласување.

(б) Првото издание на ISMM се одобрува, а еден примерок го задржува надлежниот орган. ISMM се изменува и дополнува зависно од потребата за да остане ажуриран опис на ISMS на организацијата. Примерок од сите измени и дополнувања на ISMM се доставува до надлежниот орган.

(в) Измените и дополнувањата на ISMM се управуваат во согласност со процедура утврдена од организацијата. Сите измени и дополнувања што не се опфатени со оваа процедура и измените и дополнувањата поврзани со промените наведени во точката IS.D.OR.255(б) се одобруваат од страна на надлежниот орган.

(г) Организацијата може да го интегрира ISMM со другите прирачници за управување или прирачници што ги складира, под услов да има јасна вкрстена референца која покажува кои делови од прирачникот за управување одговараат на различните барања содржани во овој анекс.

IS.D.OR.255 Промени во системот за управување со обезбедувањето на информациите

(а) Промените на ISMS може да се управуваат и да се известат до надлежниот орган со спроведување на процедура развиена од организацијата. Оваа процедура ја одобрува надлежниот орган.

(б) Во однос на промените на ISMS кои не се опфатени со процедурата наведена во точка (а), организацијата поднесува барање и добива одобрение издадено од надлежниот орган.

Во врска со овие промени:

(1) барањето се поднесува пред да се воведе каква било таква промена, така што надлежниот орган да може да утврди континуирана усогласеност со оваа регулатива и, доколку е потребно, да го измени сертификатот на организацијата и придружните барања за одобрување приложени кон него;
(2) организацијата му ги става на располагање на надлежниот орган сите информации што ги бара за да ја оцени промената;
(3) промената се спроведува само по добивањето официјално одобрение од надлежниот орган;
(4) организацијата мора да постапува во согласност со условите пропишани од надлежниот орган при спроведувањето на таквите измени.

IS.D.OR.260 Континуирано подобрување

(а) Организацијата ја проценува, користејќи соодветни индикатори за успешност, ефективноста и зрелоста на ISMS. Оваа проценка се спроведува врз основа на календарот што е однапред утврден од организацијата или по инцидент поврзан со обезбедувањето на информациите.

(б) Доколку се утврдат недостатоци по извршената проценка во согласност со точката (а), организацијата ги презема неопходните мерки за подобрување за да гарантира дека ISMS

продолжува да ги исполнува применливите барања и ги одржува ризиците врз обезбедувањето на информациите на прифатливо ниво. Дополнително, организацијата повторно ги проценува оние елементи на ISMS кои се засегнати од усвоените мерки.

_____