Eiropas Savienības
Padome

Briselē, 2022. gada 18. jūlijā
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2022. gada 14. jūlijs
Saņēmējs:	Padomes Ģenerālsekretariāts
K-jas dok. Nr.:	C(2022) 4882 final - ANNEX
Temats:	PIELIKUMS dokumentam - KOMISIJAS DELEĢĒTĀ REGULA, ar ko paredz noteikumus par Eiropas Parlamenta un Padomes Regulas (ES) 2018/1139 piemērošanu attiecībā uz prasībām par tādu informācijas drošības risku pārvaldību, kuri spēj ietekmēt aviācijas drošumu, kas noteiktas organizācijām, uz kurām attiecas Komisijas Regulas (ES) Nr. 748/2012 un Nr. 139/2014, un ar ko groza Komisijas Regulas (ES) Nr. 748/2012 un Nr. 139/2014

Pielikumā ir pievienots dokuments C(2022) 4882 *final - ANNEX*.

Pielikumā: C(2022) 4882 *final - ANNEX*

EIROPAS
KOMISIJA

Briselē, 14.7.2022.
C(2022) 4882 final

ANNEX

PIELIKUMS

dokumentam

KOMISIJAS DELEĢĒTĀ REGULA,

ar ko paredz noteikumus par Eiropas Parlamenta un Padomes Regulas (ES) 2018/1139 piemērošanu attiecībā uz prasībām par tādu informācijas drošības risku pārvaldību, kuri spēj ietekmēt aviācijas drošumu, kas noteiktas organizācijām, uz kurām attiecas Komisijas Regulas (ES) Nr. 748/2012 un Nr. 139/2014, un ar ko groza Komisijas Regulas (ES) Nr. 748/2012 un Nr. 139/2014

PIELIKUMS

INFORMĀCIJAS DROŠĪBA — PRASĪBAS ORGANIZĀCIJĀM

[*PART-IS.D.OR*]

IS.D.OR.100. Darbības joma

Šajā daļā paredzētas prasības, kas jāizpilda šīs regulas 2. pantā minētajām organizācijām.

IS.D.OR.200. Informācijas drošības pārvaldības sistēma (IDPS)

a) Lai sasniegtu 1. pantā noteiktos mērķus, organizācija izveido, īsteno un uztur informācijas drošības pārvaldības sistēmu (IDPS), kas nodrošina, ka organizācija:

   1) izveido informācijas drošības politiku, kurā izklāstīti organizācijas vispārējie principi, kas attiecas uz informācijas drošības risku iespējamo ietekmi uz aviācijas drošumu;

   2) identificē un pārskata informācijas drošības riskus saskaņā ar IS.D.OR.205. punktu;

   3) nosaka un īsteno informācijas drošības riska risināšanas pasākumus saskaņā ar

IS.D.OR.210. punktu;

4) īsteno sistēmu iekšējai ziņošanai par informācijas drošību saskaņā ar IS.D.OR.215. punktu;

5) saskaņā ar IS.D.OR.220. punktu nosaka un īsteno pasākumus, kas vajadzīgi, lai atklātu informācijas drošības notikumus, identificē tos notikumus, kuri uzskatāmi par incidentiem, kas spēj ietekmēt aviācijas drošumu, neskarot izņēmumus, kuri atļauti saskaņā ar IS.D.OR.205. punkta e) apakšpunktu, reaģē uz minētajiem informācijas drošības incidentiem un novērš to sekas;

6) īsteno kompetentās iestādes paziņotos pasākumus kā tūlītēju reakciju uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu;

7) lai reaģētu uz kompetentās iestādes paziņotajiem konstatējumiem, veic atbilstīgus pasākumus saskaņā ar IS.D.OR.225. punktu;

8) lai kompetentā iestāde varētu veikt atbilstīgus pasākumus, īsteno ārējās ziņošanas sistēmu saskaņā ar IS.D.OR.230. punktu;

9) ja tiek slēgts līgums ar citām organizācijām par jebkuru daļu no IS.D.OR.200. punktā minētajām darbībām, nodrošina atbilstību IS.D.OR.235. punktā ietvertajām prasībām;

10) nodrošina atbilstību prasībām, kas IS.D.OR.240. punktā noteiktas attiecībā uz personālu;

11) nodrošina atbilstību IS.D.OR.245. punktā noteiktajām reģistrācijas prasībām;

12) uzrauga organizācijas atbilstību šīs regulas prasībām un sniedz atbildīgajam vadītājam vai — projektēšanas organizāciju gadījumā — projektēšanas organizācijas vadītājam atsauksmes par konstatējumiem, lai nodrošinātu korektīvo pasākumu efektīvu īstenošanu;

13) neskarot ziņošanai par incidentiem piemērojamās prasības, aizsargā jebkuras tādas informācijas konfidencialitāti, ko organizācija, iespējams, ir saņēmusi no citām organizācijām, atkarībā no tās sensitivitātes līmeņa.

b) Lai nodrošinātu pastāvīgu atbilstību 1. pantā minētajām prasībām, organizācija īsteno pastāvīgu uzlabojumu procesu saskaņā ar IS.D.OR.260. punktu.

c) Organizācija saskaņā ar IS.D.OR.250. punktu dokumentē visus galvenos procesus, procedūras, funkcijas un pienākumus, kas vajadzīgi, lai izpildītu IS.D.OR.200. punkta a) apakšpunkta prasības, un izveido minētās dokumentācijas grozījumu veikšanas procesu. Šo procesu, procedūru, funkciju un pienākumu izmaiņas pārvalda saskaņā ar IS.D.OR.255. punktu.

d) Procesi, procedūras, funkcijas un pienākumi, ko organizācija noteikusi, lai izpildītu IS.D.OR.200. punkta a) apakšpunkta prasības, atbilst tās darbību veidam un sarežģītībai, pamatojoties uz šīm darbībām raksturīgo informācijas drošības risku novērtējumu, un

tos var integrēt citās esošās pārvaldības sistēmās, ko organizācija jau ir ieviesusi.

e) Neskarot pienākumu nodrošināt atbilstību Regulā (ES) Nr. 376/2014([1]) ietvertajām ziņošanas prasībām un IS.D.OR.200. punkta a) apakšpunkta 13. punkta prasībām, kompetentā iestāde var organizācijai dot atļauju neīstenot prasības, kas minētas a) līdz d) apakšpunktā, un saistītās prasības, kas ietvertas IS.D.OR.205. līdz IS.D.OR.260. punktā, ja organizācija minētajai iestādei pārliecinoši pierāda, ka tās darbības, objekti un resursi, kā arī tās sniegtie, nodrošinātie, saņemtie un uzturētie pakalpojumi ne attiecīgajai organizācijai, ne citām organizācijām nerada informācijas drošības riskus, kas spēj ietekmēt aviācijas drošumu. Atļauja pamatojas uz dokumentētu informācijas drošības riska novērtējumu, ko organizācija vai trešā persona veikusi saskaņā ar IS.D.OR.205. punktu un ko pārskatījusi un apstiprinājusi tās kompetentā iestāde.

Pēc piemērojamā pārraudzības revīzijas cikla un ikreiz, kad tiek ieviestas organizācijas darbības jomas izmaiņas, kompetentā iestāde pārskatīs minētās atļaujas turpmāko derīgumu.

IS.D.OR.205. Informācijas drošības riska novērtējums

a) Organizācija identificē visus tās elementus, kas varētu būt pakļauti informācijas drošības riskiem. Tas ietver:

1) organizācijas darbības, objektus un resursus, kā arī organizācijas sniegtos, nodrošinātos, saņemtos vai uzturētos pakalpojumus;

2) iekārtas, sistēmas, datus un informāciju, kas veicina 1. punktā uzskaitīto elementu darbību.

b) Organizācija identificē saskarnes, kas tai ir ar citām organizācijām un varētu radīt savstarpēju pakļautību informācijas drošības riskiem.

c) Attiecībā uz a) un b) apakšpunktā minētajiem elementiem un saskarnēm organizācija identificē informācijas drošības riskus, kas varētu spēt ietekmēt aviācijas drošumu. Attiecībā uz katru identificēto risku organizācija:

1) nosaka riska līmeni saskaņā ar organizācijas iepriekšnoteiktu klasifikāciju;

2) katru risku un tā līmeni sasaista ar attiecīgo elementu vai saskarni, ko identificē saskaņā ar a) un b) apakšpunktu.

Iepriekšnoteiktajā klasifikācijā, kas minēta 1. punktā, ņem vērā apdraudējuma scenārija īstenošanās iespējamību un to, cik smagi tā sekas ietekmētu drošumu. Pamatojoties uz minēto klasifikāciju un ņemot vērā to, vai organizācijā ir strukturēts un atkārtojams darbības riska pārvaldības process, organizācijai jāspēj noteikt, vai risks ir pieņemams,

([1]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 376/2014 (2014. gada 3. aprīlis) par ziņošanu, analīzi un turpmākajiem pasākumiem attiecībā uz atgadījumiem civilajā aviācijā un ar ko groza Eiropas Parlamenta un Padomes Regulu (ES) Nr. 996/2010 un atceļ Eiropas Parlamenta un Padomes Direktīvu 2003/42/EK, Komisijas Regulas (EK) Nr. 1321/2007 un (EK) Nr. 1330/2007 (OV L 122, 24.4.2014., 18. lpp.).

vai arī tas ir jārisina saskaņā ar IS.D.OR.210. punktu.

Lai veicinātu riska novērtējumu savstarpēju salīdzināmību, riska līmeņa noteikšanā saskaņā ar 1. punktu ņem vērā attiecīgo informāciju, kas iegūta koordinācijā ar b) apakšpunktā minētajām organizācijām.

d) Organizācija saskaņā ar a), b) un c) apakšpunktu veikto riska novērtējumu pārskata un atjaunina jebkurā no šādām situācijām:

1) mainās elementi, uz kuriem attiecas informācijas drošības riski;

2) mainās saskarnes starp attiecīgo organizāciju un citām organizācijām vai citu organizāciju paziņotie riski;

3) mainās informācija vai zināšanas, ko izmanto risku identificēšanai, analīzei un klasifikācijai;

4) ir gūta pieredze, kas izriet no informācijas drošības incidentu analīzes.

IS.D.OR.210. Informācijas drošības riska risināšana

a) Organizācija izstrādā pasākumus, ar kuriem novērst nepieņemamus riskus, kas identificēti saskaņā ar IS.D.OR.205. punktu, laikus īsteno tos un pārbauda to pastāvīgu rezultativitāti. Šie pasākumi organizācijai ļauj:

1) saglabāt kontroli pār apstākļiem, kas veicina apdraudējuma scenārija faktisku īstenošanos;

2) samazināt ietekmi uz aviācijas drošumu, kas saistīta ar apdraudējuma scenārija īstenošanos;

3) novērst riskus.

Šie pasākumi nerada jaunus iespējami nepieņemamus riskus, kas apdraud aviācijas drošumu.

b) Personu, kas minēta IS.D.OR.240. punkta a) un b) apakšpunktā, un citu ietekmēto organizācijas personālu informē par saskaņā ar IS.D.OR.205. punktu veiktā riska novērtējuma rezultātiem, attiecīgajiem apdraudējuma scenārijiem un īstenojamajiem pasākumiem.

Organizācija arī informē organizācijas, ar kurām tai ir saskarne saskaņā ar IS.D.OR.205. punkta b) apakšpunktu, par visiem abu organizāciju dalītajiem riskiem.

IS.D.OR.215. Sistēma iekšējai ziņošanai par informācijas drošību

a) Organizācija izveido iekšējās ziņošanas sistēmu, kas ļauj apkopot un izvērtēt informācijas drošības notikumus, tostarp notikumus, par kuriem jāziņo saskaņā ar

IS.D.OR.230. punktu.

b) Minētā sistēma un IS.D.OR.220. punktā minētais process organizācijai ļauj:

1) noteikt, kuri no notikumiem, par kuriem ziņots saskaņā ar a) apakšpunktu, ir uzskatāmi par informācijas drošības incidentiem vai ievainojamībām, kas spēj ietekmēt aviācijas drošumu;

2) noskaidrot saskaņā ar 1. punktu noteikto informācijas drošības incidentu un ievainojamību cēloņus un veicinošos faktorus un pievērsties tiem informācijas drošības riska pārvaldības procesā saskaņā ar IS.D.OR.205. un IS.D.OR.220. punktu;

3) nodrošināt, ka tiek izvērtēta visa zināmā un būtiskā informācija saistībā ar informācijas drošības incidentiem un ievainojamībām, kas noteikti saskaņā ar 1. punktu;

4) nodrošināt, ka tiek ieviesta metode informācijas iekšējai izplatīšanai pēc vajadzības.

c) Visām nolīgtām organizācijām, kuras var pakļaut attiecīgo organizāciju informācijas drošības riskiem, kas spēj ietekmēt aviācijas drošumu, ir pienākums ziņot organizācijai par informācijas drošības notikumiem. Minētos ziņojumus iesniedz, izmantojot procedūras, kas īpaši noteiktas līgumos, un tos izvērtē saskaņā ar b) apakšpunktu.

d) Organizācija izmeklēšanas jomā sadarbojas ar visām citām organizācijām, kas sniedz būtisku ieguldījumu organizācijas darbību informācijas drošībā.

e) Organizācija var minēto ziņošanas sistēmu integrēt ar citām ziņošanas sistēmām, ko tā jau ir ieviesusi.

IS.D.OR.220. Informācijas drošības incidenti — atklāšana, reaģēšana un seku novēršana

a) Pamatojoties uz saskaņā ar IS.D.OR.205. punktu veiktā riska novērtējuma rezultātiem, kā arī rezultātiem, kas gūti riska risināšanā saskaņā ar IS.D.OR.210. punktu, organizācija īsteno pasākumus, kuru mērķis ir atklāt incidentus un ievainojamības, kas norāda uz nepieņemamu risku iespējamo īstenošanos un spēj ietekmēt aviācijas drošumu. Šie incidentu atklāšanas pasākumi organizācijai ļauj:

1) konstatēt novirzes no iepriekšnoteiktām funkcionālās veiktspējas bāzlīnijām;

2) jebkādas novirzes gadījumā dot brīdinājumus, lai aktivizētu pienācīgus reaģēšanas pasākumus.

b) Organizācija īsteno pasākumus, kuru mērķis ir reaģēt uz visiem notikuma apstākļiem, kas konstatēti saskaņā ar a) apakšpunktu un var attīstīties vai ir attīstījušies par informācijas drošības incidentu. Šie reaģēšanas pasākumi organizācijai ļauj:

1) sākt reaģēšanu uz a) apakšpunkta 2. punktā minētajiem brīdinājumiem, aktivizējot iepriekšnoteiktus resursus un darbību gaitu;

2) ierobežot uzbrukuma izvēršanos un novērst apdraudējuma scenārija pilnīgu īstenošanos;

3) vadīt IS.D.OR.205. punkta a) apakšpunktā noteikto skarto elementu atteices režīmu.

c) Organizācija īsteno pasākumus, kuru mērķis ir novērst informācijas drošības incidentu sekas, tostarp ārkārtas pasākumus vajadzības gadījumā. Šie seku novēršanas pasākumi organizācijai ļauj:

1) novērst incidentu izraisījušo apstākli vai ierobežot to līdz pieļaujamam līmenim;

2) atjaunošanās laikā, ko iepriekš noteikusi organizācija, sasniegt IS.D.OR.205. punkta a) apakšpunktā noteikto skarto elementu drošu stāvokli.

IS.D.OR.225. Reaģēšana uz kompetentās iestādes paziņotajiem konstatējumiem

a) Saņēmusi kompetentās iestādes iesniegto paziņojumu par konstatējumiem, organizācija:

1) noskaidro neatbilstības pamatcēloni vai cēloņus un veicinošos faktorus;

2) nosaka korektīvo pasākumu plānu;

3) pierāda kompetentajai iestādei, ka neatbilstība ir novērsta.

b) Šā punkta a) apakšpunktā minētās darbības veic laikposmā, par kuru panākta vienošanās ar kompetento iestādi.

IS.D.OR.230. Sistēma ārējai ziņošanai par informācijas drošību

a) Organizācija ievieš informācijas drošības ziņošanas sistēmu, kas atbilst Regulā (ES) Nr. 376/2014 un tās deleģētajos un īstenošanas aktos noteiktajām prasībām, ja minētā regula ir piemērojama organizācijai.

b) Neskarot Regulā (ES) Nr. 376/2014 noteiktos pienākumus, organizācija nodrošina, ka par visiem informācijas drošības incidentiem un ievainojamībām, kas var radīt būtisku risku aviācijas drošumam, tiek ziņots tās kompetentajai iestādei. Turklāt:

1) ja šāds incidents vai ievainojamība ietekmē gaisa kuģi vai ar to saistītu sistēmu vai sastāvdaļu, organizācija par to ziņo arī projekta apstiprinājuma turētājam;

2) ja šāds incidents vai ievainojamība ietekmē organizācijas izmantotu sistēmu vai sastāvdaļu, organizācija par to ziņo organizācijai, kas atbild par sistēmas vai sastāvdaļas projektēšanu.

c) Organizācija par b) apakšpunktā minētajiem apstākļiem ziņo šādi:

1) tiklīdz organizācija ir uzzinājusi par apstākli, tā iesniedz paziņojumu kompetentajai iestādei un attiecīgā gadījumā projekta apstiprinājuma turētājam vai organizācijai, kas atbild par sistēmas vai sastāvdaļas projektēšanu;

2) ja vien ārkārtas apstākļi to neliedz, cik drīz vien iespējams, bet ne vēlāk kā 72 stundas pēc tam, kad organizācija ir uzzinājusi par apstākli, tā iesniedz ziņojumu kompetentajai iestādei un attiecīgā gadījumā projekta apstiprinājuma turētājam vai organizācijai, kas atbild par sistēmas vai sastāvdaļas projektēšanu.

Ziņojumu sagatavo kompetentās iestādes noteiktā formā, un tajā iekļauj visu attiecīgo informāciju par apstākli, kas zināma organizācijai;

3) iesniedz paveiktā darba pārbaudes ziņojumu kompetentajai iestādei un attiecīgā gadījumā projekta apstiprinājuma turētājam vai organizācijai, kas atbild par sistēmas vai sastāvdaļas projektēšanu, ziņojumā sīki izklāstot informāciju par darbībām, ko organizācija ir veikusi vai plāno veikt, lai novērstu incidenta sekas, un par darbībām, ko tā plāno veikt, lai nākotnē novērstu līdzīgus informācijas drošības incidentus.

Paveiktā darba pārbaudes ziņojumu iesniedz, tiklīdz minētās darbības ir noteiktas, un to sagatavo kompetentās iestādes noteiktā formā.

IS.D.OR.235. Informācijas drošības pārvaldības darbību līguma slēgšana

a) Ja organizācija noslēdz līgumu ar citām organizācijām par kādu daļu no IS.D.OR.200. punktā minētajām darbībām, organizācija nodrošina, ka darbības, par kurām noslēgts līgums, atbilst šīs regulas prasībām un ka nolīgtā organizācija darbojas tās pārraudzībā. Organizācija nodrošina, ka riski, kas saistīti ar darbībām, par kurām noslēgts līgums, tiek pienācīgi pārvaldīti.

b) Organizācija nodrošina, ka kompetentajai iestādei pēc pieprasījuma tiek dota piekļuve nolīgtajai organizācijai, lai kompetentā iestāde varētu pārliecināties par pastāvīgu atbilstību piemērojamajām prasībām, kas noteiktas šajā regulā.

IS.D.OR.240. Prasības personālam

a) Organizācijas atbildīgajam vadītājam vai — projektēšanas organizāciju gadījumā — projektēšanas organizācijas vadītājam, kas norīkots saskaņā ar Regulu (ES) Nr. 748/2012 un Regulu (ES) Nr. 139/2014, kā minēts šīs regulas 2. panta 1. punkta a) un b) apakšpunktā, ir organizācijas dotas pilnvaras nodrošināt, ka visas šajā regulā paredzētās darbības ir iespējams finansēt un veikt. Minētā persona:

1) nodrošina, ka ir pieejami visi šīs regulas prasību izpildei vajadzīgie resursi;

2) izveido informācijas drošības politiku, kas minēta IS.D.OR.200. punkta a) apakšpunkta 1. punktā, un veicina tās īstenošanu;

3) pierāda pamatizpratni par šo regulu.

b) Atbildīgais vadītājs vai — projektēšanas organizāciju gadījumā — projektēšanas organizācijas vadītājs ieceļ personu vai personu grupu, kas nodrošina, ka organizācija atbilst šīs regulas prasībām, un nosaka viņu pilnvaru apjomu. Minētā persona vai personu grupa ir tieši pakļauta atbildīgajam vadītājam vai — projektēšanas organizāciju gadījumā — projektēšanas organizācijas vadītājam, un tai ir pienākumu izpildei

atbilstošas zināšanas, agrāka darbība un pieredze. Procedūrās nosaka, kas aizvieto konkrētu personu tās ilgstošas prombūtnes laikā.

c) Atbildīgais vadītājs vai — projektēšanas organizāciju gadījumā — projektēšanas organizācijas vadītājs ieceļ personu vai personu grupu, kas atbild par IS.D.OR.200. punkta a) apakšpunkta 12. punktā minētās atbilstības uzraudzības funkcijas pārvaldību.

d) Ja organizācijas informācijas drošības organizatoriskās struktūras, politika, procesi un procedūras ir kopīgas ar citām organizācijām vai savas organizācijas jomām, kas nav apstiprinājuma vai deklarācijas daļa, atbildīgais vadītājs vai — projektēšanas organizāciju gadījumā — projektēšanas organizācijas vadītājs var deleģēt savas darbības kopīgai atbildīgajai personai.

Lai nodrošinātu informācijas drošības pārvaldības pienācīgu integrāciju organizācijā, šādā gadījumā nosaka pasākumus koordinācijai starp organizācijas atbildīgo vadītāju vai — projektēšanas organizāciju gadījumā — projektēšanas organizācijas vadītāju un kopīgo atbildīgo personu.

e) Atbildīgajam vadītājam vai projektēšanas organizācijas vadītājam, vai d) apakšpunktā minētajai kopīgajai atbildīgajai personai ir organizācijas dotas pilnvaras izveidot un uzturēt IS.D.OR.200. punkta īstenošanai vajadzīgās organizatoriskās struktūras, politiku, procesus un procedūras.

f) Organizācijā ir ieviests process, ar ko nodrošināt, ka tai pietiek dežurējošo darbinieku šajā pielikumā izklāstīto darbību veikšanai.

g) Organizācijā ir ieviests process, ar ko nodrošināt, ka f) apakšpunktā minētajiem darbiniekiem ir savu uzdevumu veikšanai vajadzīgā kompetence.

h) Organizācijā ir ieviests process, ar ko nodrošināt, ka darbinieki atzīst pienākumus, kas saistīti ar tiem uzticētajām funkcijām un uzdevumiem.

i) Organizācija nodrošina, ka tiek pienācīgi noteikta to darbinieku identitāte un uzticamība, kuriem ir piekļuve informācijas sistēmām un datiem, uz ko attiecas šīs regulas prasības.

IS.D.OR.245. Reģistrācija

a) Organizācija reģistrē savas informācijas drošības pārvaldības darbības.

1) Organizācija nodrošina, ka ir arhivēti un izsekojami šādi ieraksti:

i) visi saņemtie apstiprinājumi un visi saistītie informācijas drošības riska novērtējumi saskaņā ar IS.D.OR.200. punkta e) apakšpunktu;

ii) līgumi par darbībām, kas minēti IS.D.OR.200. punkta a) apakšpunkta 9. punktā;

iii) ieraksti par galvenajiem procesiem, kas minēti IS.D.OR.200. punkta d) apakšpunktā;

iv) ieraksti par IS.D.OR.205. punktā minētajā riska novērtējumā identificētajiem riskiem kopā ar saistītajiem IS.D.OR.210. punktā minētajiem riska risināšanas pasākumiem;

v) ieraksti par informācijas drošības incidentiem un ievainojamībām, par ko ziņots saskaņā ar IS.D.OR.215. un IS.D.OR.230. punktā minētajām ziņošanas sistēmām;

vi) ieraksti par informācijas drošības notikumiem, kuri varētu būt jāizvērtē atkārtoti, lai atklātu vēl neatklātus informācijas drošības incidentus vai ievainojamības.

2) Ierakstus, kas minēti 1. punkta i) apakšpunktā, glabā vismaz 5 gadus pēc tam, kad apstiprinājums ir zaudējis derīgumu.

3) Ierakstus, kas minēti 1. punkta ii) apakšpunktā, glabā vismaz 5 gadus pēc tam, kad līgums ir grozīts vai izbeigts.

4) Ierakstus, kas minēti 1. punkta iii), iv) un v) apakšpunktā, glabā vismaz 5 gadus.

5) Ierakstus, kas minēti 1. punkta vi) apakšpunktā, glabā tik ilgi, līdz šie informācijas drošības notikumi ir atkārtoti izvērtēti saskaņā ar organizācijas izveidotā procedūrā noteiktu periodiskumu.

b) Organizācija reģistrē savu informācijas drošības pārvaldības darbībās iesaistīto darbinieku kvalifikāciju un pieredzi.

1) Ierakstus par darbinieka kvalifikāciju un pieredzi glabā tik ilgi, kamēr persona strādā organizācijā, un vismaz 3 gadus pēc tam, kad persona ir aizgājusi no darba organizācijā.

2) Darbiniekiem pēc pieprasījuma dod piekļuvi viņu individuālajiem datiem. Turklāt pēc darbinieka pieprasījuma organizācija darbiniekam izsniedz viņa individuālo datu kopiju, kad darbinieks aiziet no darba organizācijā.

c) Ierakstu formāts ir noteikts organizācijas procedūrās.

d) Ierakstus information being identified, when required, according to its security classification level. glabā veidā, kas nodrošina aizsardzību pret bojājumiem, pārveidošanu un zādzību, vajadzības gadījumā informāciju identificējot atbilstīgi tās drošības klasifikācijas līmenim. Organizācija nodrošina, ka ierakstus glabā, izmantojot līdzekļus, kas nodrošina integritāti, autentiskumu un atļautu piekļuvi.

IS.D.OR.250. Informācijas drošības pārvaldības rokasgrāmata (IDPR)

a) Organizācija kompetentajai iestādei dara pieejamu informācijas drošības pārvaldības rokasgrāmatu (IDPR) un attiecīgā gadījumā visas saistītās rokasgrāmatas un procedūras, uz kurām ir sniegtas atsauces, un rokasgrāmatā ir:

1) paziņojums, ko parakstījis atbildīgais vadītājs vai — projektēšanas organizāciju gadījumā — projektēšanas organizācijas vadītājs, apstiprinot, ka organizācija vienmēr strādās saskaņā ar šo pielikumu un IDPR. Ja atbildīgais vadītājs vai —

projektēšanas organizāciju gadījumā — projektēšanas organizācijas vadītājs nav organizācijas izpilddirektors, tad paziņojumu paraksta izpilddirektors;

2) IS.D.OR.240. punkta b) un c) apakšpunktā minētās personas vai minēto personu amats, vārds un uzvārds, pienākumi, pakļautība, atbildība un pilnvaras;

3) vajadzības gadījumā IS.D.OR.240. punkta d) apakšpunktā minētās kopīgās atbildīgās personas amats, vārds un uzvārds, pienākumi, pakļautība, atbildība un pilnvaras;

4) organizācijas informācijas drošības politika, kas minēta IS.D.OR.200. punkta a) apakšpunkta 1. punktā;

5) vispārīgs apraksts par darbinieku skaitu un kategorijām un par sistēmu, kas ieviesta personāla pieejamības plānošanai, kā prasīts IS.D.OR.240. punktā;

6) galveno personu, kas atbild par IS.D.OR.200. punkta īstenošanu, tostarp personas vai personu, kas atbild par IS.D.OR.200. punkta a) apakšpunkta 12. punktā minēto atbilstības uzraudzības funkciju, amats, vārds un uzvārds, pienākumi, pakļautība, atbildība un pilnvaras;

7) struktūrshēma, kurā parādītas ar 2. un 6. punktā minētajām personām saistītās pakļautības un atbildības ķēdes;

8) IS.D.OR.215. punktā minētās iekšējās ziņošanas sistēmas apraksts;

9) procedūras, kas precizē, kā organizācija nodrošina atbilstību šai daļai, un jo īpaši:

i) IS.D.OR.200. punkta c) apakšpunktā minētā dokumentācija;

ii) procedūras, kas nosaka, kā organizācija kontrolē visas IS.D.OR.200. punkta a) apakšpunkta 9. punktā minētās darbības, par kurām noslēgts līgums;

iii) IDPR grozījumu procedūra, kas noteikta c) apakšpunktā;

10) sīka informācija par pašreizējiem apstiprinātajiem alternatīvajiem atbilstības nodrošināšanas līdzekļiem.

b) Kompetentā iestāde apstiprina IDPR sākotnējo izdevumu un saglabā tās eksemplāru. IDPR vajadzības gadījumā groza, lai organizācijas IDPS apraksts vienmēr būtu atjaunināts. Visu IDPR grozījumu eksemplāru iesniedz kompetentajai iestādei.

c) IDPR grozījumus pārvalda saskaņā ar organizācijas izveidotu procedūru. Visus grozījumus, kas nav iekļauti šīs procedūras darbības jomā, un visus grozījumus, kas saistīti ar IS.D.OR.255. punkta b) apakšpunktā minētajām izmaiņām, apstiprina kompetentā iestāde.

d) Organizācija IDPR var integrēt ar citiem tās rīcībā esošiem pārvaldības pašraksturojumiem vai rokasgrāmatām, ja ir dota skaidra savstarpēja atsauce, kas norāda, kuras pārvaldības pašraksturojuma vai rokasgrāmatas daļas atbilst dažādām šajā pielikumā ietvertajām prasībām.

IS.D.OR.255. Informācijas drošības pārvaldības sistēmas izmaiņas

a) IDPS izmaiņas var pārvaldīt un paziņot kompetentajai iestādei saskaņā ar organizācijas izstrādātu procedūru. Šo procedūru apstiprina kompetentā iestāde.

b) Attiecībā uz IDPS izmaiņām, uz kurām neattiecas a) apakšpunktā minētā procedūra, organizācija iesniedz pieteikumu un saņem kompetentās iestādes dotu apstiprinājumu.

Attiecībā uz šīm izmaiņām:

1) pirms šādu izmaiņu veikšanas iesniedz pieteikumu, lai kompetentajai iestādei dotu iespēju pārliecināties par pastāvīgu atbilstību šai regulai un vajadzības gadījumā grozīt organizācijas sertifikātu un tam pievienotos attiecīgos apstiprinājuma noteikumus;

2) organizācija kompetentajai iestādei dara pieejamu visu informāciju, ko tā pieprasa izmaiņu izvērtēšanai;

3) izmaiņas īsteno tikai pēc kompetentās iestādes oficiāla apstiprinājuma saņemšanas;

4) kamēr šādas izmaiņas tiek ieviestas, organizācija darbojas saskaņā ar nosacījumiem, ko noteikusi kompetentā iestāde.

IS.D.OR.260. Pastāvīgi uzlabojumi

a) Organizācija, izmantojot atbilstīgus darbības rādītājus, novērtē IDPS efektivitāti un gatavību. Minēto novērtēšanu veic, pamatojoties uz organizācijas iepriekšnoteiktu kalendāro grafiku vai pēc informācijas drošības incidenta.

b) Ja pēc novērtēšanas, kas veikta saskaņā ar a) apakšpunktu, tiek konstatēti trūkumi, organizācija īsteno uzlabošanas pasākumus, kuri vajadzīgi, lai nodrošinātu, ka IDPS joprojām atbilst piemērojamajām prasībām un uztur informācijas drošības riskus pieņemamā līmenī. Turklāt organizācija atkārtoti izvērtē tos IDPS elementus, kurus ietekmē pieņemtie pasākumi.