KOMISIJAS LĒMUMS (ES) 2022/640

(2022. gada 7. aprīlis)

par īstenošanas noteikumiem attiecībā uz galveno drošības jomas dalībnieku uzdevumiem un pienākumiem

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 249. pantu,

ņemot vērā Komisijas Lēmumu (ES, Euratom) 2015/443 (2015. gada 13. marts) par drošību Komisijā, ([1])

ņemot vērā Komisijas Lēmumu (ES, Euratom) 2015/444 (2015. gada 13. marts) par drošības noteikumiem ES klasificētas informācijas aizsardzībai ([2]),

tā kā:

(1) Lēmumus (ES, Euratom) 2015/443 un (ES, Euratom) 2015/444 piemēro visiem Komisijas dienestiem un visās Komisijas telpās.

(2) Vajadzības gadījumā saskaņā ar Lēmuma (ES, Euratom) 2015/444 60. pantu jāpieņem īstenošanas noteikumi, lai papildinātu vai atbalstītu šo lēmumu.

(3) Drošības pasākumiem, kuru mērķis ir aizsargāt ES klasificētu informāciju visā tās aprites laikā, jo īpaši vajadzētu atbilst tās drošības klasifikācijas līmenim.

(4) Drošības pasākumi komunikācijas un informācijas sistēmu aizsardzībai Komisijā ir noteikti Komisijas Lēmumā (ES, Euratom) 2017/46 ([3]), jo īpaši 3. pantā par IT drošības principiem Komisijā un 9. pantā par sistēmas īpašniekiem.

(5) Īstenošanas noteikumu par galveno drošības jomas dalībnieku uzdevumiem un pienākumiem mērķis ir sniegt norādījumus par priekšnoteikumiem un pienākumiem, kas attiecībā uz minētajiem uzdevumiem ir noteikti Lēmumos (ES, Euratom) 2015/443 un (ES, Euratom) 2015/444.

(6) Lēmuma (ES, Euratom) 2015/444 36. panta 7. punktā ir noteiktas vairākas ar drošību saistītas papildu funkcijas, ko pilda Komisijas Drošības iestāde. Ar šīm funkcijām saistītie uzdevumi ir noteikti šajā lēmumā.

(7) Vietējiem drošības speciālistiem un reģistra kontrolieriem ir īpaši pienākumi attiecībā uz ES klasificētās informācijas aizsardzību savos dienestos saskaņā ar Lēmumu (ES, Euratom) 2015/444.

(8) Komisija 2016. gada 4. maijā pieņēma lēmumu ([4]), ar ko pilnvaroja par drošības jautājumiem atbildīgo Komisijas locekli pieņemt Komisijas vārdā un tās atbildībā īstenošanas noteikumus, kuri paredzēti Lēmuma (ES, Euratom) 2015/444 60. pantā; pēc tam 2021. gada 13. aprīlī par drošības jautājumiem atbildīgais Komisijas loceklis Komisijas vārdā un tās atbildībā pieņēma lēmumu ([5]), ar kuru šos īstenošanas noteikumus pastarpināti deleģē Cilvēkresursu un drošības ģenerāldirektorāta ģenerāldirektoram,

([1]) OV L 72, 17.3.2015., 41. lpp.
([2]) OV L 72, 17.3.2015., 53. lpp.
([3]) Komisijas Lēmums (ES, Euratom) 2017/46 (2017. gada 10. janvāris) par komunikācijas un informācijas sistēmu drošību Eiropas Komisijā (OV L 6, 11.1.2017., 40. lpp.).
([4]) Komisijas Lēmums C(2016) 2797 final (2016. gada 4. maijs) par pilnvarojumu drošības jomā.
([5]) Komisijas Lēmums C(2021) 2684 final (2021. gada 13. aprīlis), ar ko pastarpināti deleģē pilnvaras, kuras piešķirtas ar Komisijas Lēmumu C(2016) 2797 par pilnvarojumu drošības jomā.

IR PIEŅĒMUSI ŠO LĒMUMU.

1. NODAĻA

Vispārīgi noteikumi

1. pants

Priekšmets un piemērošanas joma

1. Šajā lēmumā ir izklāstīti to galveno drošības dalībnieku uzdevumi un pienākumi, kuri ir atbildīgi par ES klasificētas informācijas (ESKI) aizsardzību Komisijā saskaņā ar Lēmumiem (ES, Euratom) 2015/443 un (ES, Euratom) 2015/444.

2. Šo lēmumu piemēro visiem Komisijas dienestiem un visās Komisijas telpās.

2. NODAĻA

Cilvēkresursu un drošības ģenerāldirektorāts

2. pants

Komisijas drošības iestāde

1. Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorāta direktors ir Komisijas drošības iestāde (KDI), kas minēta Lēmuma (ES, Euratom) 2015/444 7. pantā.

2. KDI veic savas funkcijas šādās Lēmumā (ES, Euratom) 2015/444 noteiktajās jomās saskaņā ar šā lēmuma 3.–7. pantu:

a) personāla drošība;

b) fiziskā drošība;

c) ESKI pārvaldība;

d) jebkuras komunikācijas un informācijas sistēmas (KIS), kas rīkojas ar ESKI, akreditācija;

e) industriālā drošība, kā arī

f) klasificētas informācijas apmaiņa.

3. KDI nodrošina obligātu apmācību vietējiem drošības speciālistiem (*LSO*), *LSO* vietniekiem, reģistra kontrolieriem (RK) un RK vietniekiem par viņu pienākumiem.

3. pants

Informācijas aizsardzības iestāde

Informācijas aizsardzības iestāde ir atbildīga par šādām darbībām saistībā ar ESKI aizsardzību:

a) izstrādāt informācijas nodrošinājuma drošības politiku un drošības pamatnostādnes un uzraudzīt to efektivitāti un piemērotību;

b) nodrošināt un administrēt tehnisko informāciju, kas attiecas uz kriptogrāfijas produktiem;

c) nodrošināt, ka informācijas nodrošināšanas pasākumi attiecīgā gadījumā atbilst Komisijas drošības un iepirkuma politikai;

d) nodrošināt, ka kriptogrāfijas produktus izraugās saskaņā ar politiku, kas nosaka to atbilstību un atlasi;

e) apspriesties ar sistēmas īpašniekiem, sistēmas nodrošinātājiem, drošības dalībniekiem un lietotāju pārstāvjiem par informācijas nodrošināšanas drošības politiku un drošības pamatnostādnēm.

4. pants

Drošības akreditācijas iestāde

1. KDI ir atbildīga par to drošības zonu akreditāciju, kas atbilst Lēmuma 2015/444 18. panta prasībām, un par KIS akreditēšanu attiecībā uz rīcību ar ESKI.

2. Komisijas dienesti apspriežas ar Drošības akreditācijas iestādi, vajadzības gadījumā saskaņojot ar tās *LSO* un vietējo IT drošības speciālistu (*LISO*), ja dienests plāno:

a) ierīkot drošības zonu;

b) ieviest KIS rīcībai ar ESKI;

c) uzstādīt jebkādu citu aprīkojumu rīcībai ar klasificētu informāciju, tostarp savienojumus ar trešo personu KIS.

DAI sniedz konsultācijas par šīm darbībām gan plānošanas, gan ierīkošanas un izstrādes procesu laikā.

3. Ar ESKI nerīkojas drošības zonā vai KIS, pirms drošības akreditācijas iestāde nav izsniegusi attiecīgā līmeņa ESKI akreditāciju.

4. Drošības zonas akreditācijas prasības ietver:

a) drošības zonas plānu apstiprināšanu;

b) jebkādu līgumu apstiprināšanu par darbiem, ko veic ārēji līgumslēdzēji, ņemot vērā noteikumus par industriālo drošību, piemēram, prasības līgumslēdzēju un to darbinieku drošības pielaidei;

c) visu vajadzīgo deklarāciju un atbilstības sertifikātu pieejamību;

d) drošības zonas fizisku pārbaudi, lai pārliecinātos, ka celtniecības materiāli un metodes, piekļuves kontrole, drošības aprīkojums un citi priekšmeti atbilst KDI noteiktajām prasībām;

e) pret elektromagnētisko starojumu vērstu pretpasākumu validāciju jebkurā tehniskā drošības zonā;

f) drošības zonai paredzētu drošības darba procedūru (*SecOPs*) apstiprināšanu.

5. Prasības tādu KIS, kurās rīkojas ar ESKI, akreditēšanai ietver:

a) sistēmas akreditācijas stratēģijas izveidi;

b) KIS drošības plāna apstiprināšanu, pamatojoties uz riska pārvaldības pieeju;

c) KIS *SecuOPs* validēšanu;

d) visu pārējo vajadzīgo drošības dokumentu validēšanu, kā noteikusi Drošības akreditācijas iestāde;

e) šifrēšanas tehnoloģiju izmantošanas apstiprināšanu;

f) pret elektromagnētisko starojumu vērsto pretpasākumu validāciju tādai KIS, kurā rīkojas ar informāciju, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī;

g) KIS pārbaudi, lai pārliecinātos, ka dokumentētie drošības pasākumi ir pareizi īstenoti.

6. Pēc akreditācijas prasību sekmīgas izpildes drošības akreditācijas iestāde izsniedz oficiālu atļauju rīkoties ar ESKI drošības zonā vai KIS noteiktā maksimālā ESKI līmenī un uz laiku līdz pieciem gadiem atkarībā no apstrādātās ESKI līmeņa un saistītajiem riskiem.

7. Pēc paziņojuma par drošības pārkāpumu vai būtiskām izmaiņām drošības pasākumu izstrādē vai drošības pasākumos drošības zonā vai KIS drošības akreditācijas iestāde pārskata un vajadzības gadījumā var atsaukt atļauju rīkoties ar ESKI, līdz tiek atrisinātas visas konstatētās problēmas.

5. pants

TEMPEST iestāde

1. *TEMPEST* drošības pasākumus īsteno, lai aizsargātu KIS, kurās rīkojas ar informāciju, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, un tos var īstenot attiecībā uz informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī.

2. *TEMPEST* iestāde ir atbildīga par to pasākumu apstiprināšanu, kas veikti, lai aizsargātu pret ESKI apdraudējumu, ko rada netīšas elektroniskas emisijas.

3. Pēc KIS, kas rīkojas ar ESKI, sistēmas īpašnieka pieprasījuma *TEMPEST* iestāde izdod *TEMPEST* drošības pasākumu specifikācijas atbilstoši informācijas klasifikācijas līmenim.

4. *TEMPEST* iestāde veic tehnisko testēšanu drošības zonu un tādu KIS akreditācijas laikā, kuras paredzētas rīcībai ar ESKI, kas klasificēta *CONFIDENTIAL UE/EU CONFIDENTIAL* vai augstākā līmenī, un pēc sekmīgas testēšanas izdod *TEMPEST* sertifikātu.

5. *TEMPEST* sertifikātā norāda vismaz:

a) testa datumu;

b) *TEMPEST* drošības pasākumu aprakstu un telpu plānus;

c) sertifikāta derīguma termiņu;

d) jebkādas izmaiņas, kuru rezultātā sertifikāts kļūst nederīgs;

e) *TEMPEST* iestādes parakstu.

6. *LSO* vai sanāksmes organizētājs, kas atbild par klasificētas sanāksmes organizēšanu, sadarbībā ar *LSO* var pieprasīt *TEMPEST* iestādei pārbaudīt sanāksmju telpas, lai nodrošinātu, ka tās ir tehniski drošas.

6. pants

Kriptogrāfijas apstiprinātāja iestāde

1. Kriptogrāfijas apstiprinātāja iestāde ir atbildīga par šifrēšanas tehnoloģiju izmantošanas apstiprināšanu.

2. Kriptogrāfijas apstiprinātāja iestāde izdod norādījumus par šifrēšanas tehnoloģiju izmantošanas un apstiprināšanas prasībām.

3. Kriptogrāfijas apstiprinātāja iestāde apstiprina šifrēšanas risinājumu izmantošanu, pamatojoties uz sistēmas īpašnieka pieprasījumu. Apstiprinājuma pamatā ir apmierinošs novērtējums vismaz par:

a) aizsargājamās informācijas drošības vajadzībām;

b) pārskatu par KIS, kas iesaistīta risinājumā;

c) raksturīgo un atlikušo risku novērtējumu;

d) paredzētā risinājuma aprakstu;

e) šifrēšanas risinājumu *SecOPs*.

4. Kriptogrāfijas apstiprinātāja iestāde uztur apstiprināto šifrēšanas risinājumu reģistru.

7. pants

Kriptogrāfijas izplatīšanas iestāde

1. Kriptogrāfijas izplatīšanas iestāde ir atbildīga par ESKI aizsardzībai izmantoto kriptogrāfisko materiālu (galvenokārt šifrēšanas iekārtu, kriptogrāfisko atslēgu, sertifikātu un saistītu autentificētāju) izplatīšanu:

a) lietotājiem vai dienestiem Komisijā attiecībā uz KIS, ko pārvalda ārējas personas;

b) lietotājiem vai organizācijām ārpus Komisijas attiecībā uz KIS, ko pārvalda Komisija.

2. Kriptogrāfijas izplatīšanas iestāde var uzticēt trešām personām paredzētu kriptogrāfijas materiālu izplatīšanu citiem dienestiem saskaņā ar Lēmuma 2015/443 17. panta 3. punktu.

3. Kriptogrāfijas izplatīšanas iestāde nodrošina, ka visi kriptogrāfijas materiāli tiek nosūtīti, izmantojot drošus kanālus, lai aizsargātu pret manipulācijām un uzrādītu pierādījumus par tām, saskaņā ar drošības noteikumiem, ko piemēro ESKI klasifikācijas līmenim, ar kuru aizsargās minētos materiālus.

4. Kriptogrāfijas izplatīšanas iestāde sniedz norādījumus *LSO* un attiecīgā gadījumā vietējam informātikas drošības speciālistam katrā Komisijas dienestā, kas ir iesaistīts kriptogrāfisko materiālu ražošanā, izplatīšanā vai izmantošanā.

5. Kriptogrāfijas izplatīšanas iestāde nodrošina, ka izplatīšanas procesam tiek izveidotas piemērotas *SecOPs*.

3. NODAĻA

Komisijas dienesti

8. pants

Dienestu vadītāji

1. Katrs dienesta vadītājs ieceļ:

a) *LSO* un vienu vai attiecīgā gadījumā vairākus vietniekus dienesta vai kabineta ietvaros;

b) RK un attiecīgā gadījumā vienu vai vairākus vietniekus katrā dienestā, kas pārvalda ESKI reģistru;

c) sistēmas īpašnieku katrai KIS, kurā rīkojas ar ESKI.

2. Pirms *LSO*, *LSO* vietnieku, RK un RK vietnieku iecelšanas dienesta vadītājs lūdz Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorāta direktora apstiprinājumu.

3. Dienesta vadītājs, apspriežoties ar *LSO*, identificē visus amatus, kam vajadzīga pielaide piekļūt ESKI. Darbā pieņemšanas procesā kandidātus uz šādiem amatiem informē par prasību pēc pielaides.

4. Jebkura tāda dienesta vadītājs, kura rīcībā ir ESKI, vajadzības gadījumā ir atbildīgs par ārkārtas iznīcināšanas un evakuācijas plānu aktivizēšanu. Plānos iekļauj alternatīvu risinājumu situācijām, kad nav iespējams sazināties ar dienesta vadītāju.

9. pants

KIS, kurā rīkojas ar ESKI, sistēmas īpašnieki

1. Strādājot pie projekta, sistēmas īpašnieks pēc iespējas ātrāk sazinās ar drošības akreditācijas iestādi, lai ieviestu KIS, kurā rīkojas ar ESKI, lai noteiktu attiecīgos drošības standartus un prasības un sāktu drošības akreditācijas procesu.

2. Sistēmas īpašnieks nodrošina, ka drošības pasākumi atbilst drošības akreditācijas iestādes prasībām un ka KIS nerīkojas ar ESKI, pirms tā ir akreditēta.

3. Sistēmas īpašnieks sazinās ar kriptogrāfijas apstiprinātāju iestādi, lai saņemtu apstiprinājumu jebkādu šifrēšanas tehnoloģiju izmantošanai. Sistēmas īpašnieki neizmanto šifrēšanas tehnoloģijas ražošanas sistēmās bez iepriekšēja apstiprinājuma.

4. Sistēmas īpašnieks par jautājumiem, kas saistīti ar KIS drošību, apspriežas ar dienesta *LISO*.

5. Sistēmas īpašnieks vismaz reizi gadā pārskata sistēmai piemērotos drošības pasākumus, tostarp tās drošības plānu.

6. Ja KIS notiek drošības incidents un ir norādīts, ka KIS vairs nespēj pienācīgi aizsargāt ESKI, sistēmas īpašnieks informē *LSO* un nekavējoties sazinās ar Drošības akreditācijas iestādi, lai saņemtu ieteikumus par turpmāko rīcību. Šādā gadījumā akreditāciju var apturēt un sistēmas darbību var pārtraukt, līdz tiek veikti piemēroti koriģējoši pasākumi.

7. Sistēmas īpašnieks vienmēr sniedz Drošības akreditācijas iestādei pilnīgu atbalstu tās pienākumu veikšanā saistībā ar KIS akreditāciju.

10. pants

Informācijas aizsardzības operatīvā iestāde

Informācijas aizsardzības operatīvā iestāde katrai KIS:

a) izveido drošības dokumentāciju saskaņā ar drošības politiku un pamatnostādnēm, jo īpaši drošības plānu, ar sistēmu saistītās *SecOPs* un KIS akreditācijas procesā esošo kriptogrāfisko dokumentāciju;

b) piedalās katrai sistēmai īpašu tehnisku drošības pasākumu, iekārtu un programmatūras izvēlē un pārbaudē, uzrauga to īstenošanu un nodrošina, ka tās tiek droši instalētas, konfigurētas un uzturētas atbilstīgi attiecīgajiem drošības dokumentiem;

c) piedalās *TEMPEST* drošības pasākumu un ierīču atlasē, ja tas prasīts drošības plānā, un sadarbībā ar *TEMPEST* iestādi nodrošina to drošu uzstādīšanu un uzturēšanu;

d) uzrauga ar sistēmas darbību saistīto *SecOPs* īstenošanu un piemērošanu;

e) sadarbībā ar kriptogrāfijas produktu izplatīšanas iestādi pārvalda kriptogrāfijas produktus un rīkojas ar tiem, lai nodrošinātu kriptogrāfijas materiālu un kontrolēto preču pienācīgu glabāšanu un vajadzības gadījumā nodrošinātu kriptogrāfisku mainīgo ģenerēšanu;

f) veic drošības analīzes, pārskatus un testus, jo īpaši, lai sagatavotu attiecīgos riska ziņojumus, kā to pieprasa Drošības akreditācijas iestāde;

g) nodrošina ar KIS saistītas mācības informācijas aizsardzības jomā;

h) īsteno un izpilda drošības pasākumus attiecībā uz katru KIS.

4. NODAĻA

Vietējais drošības speciālists (*LSO*)

11. pants

***LSO* iecelšana amatā**

1. *LSO* un *LSO* vietnieki ir ierēdņi vai pagaidu darbinieki.

2. Visiem *LSO* un *LSO* vietniekiem ir derīga drošības atļauja piekļūt ESKI līdz *SECRET UE/EU SECRET* līmenim un vajadzības gadījumā līdz *TRES SECRET UE/EU TOP SECRET* līmenim. *LSO* vai *LSO* vietnieks pirms iecelšanas saņem drošības atļauju.

3. Komisijas pārstāvniecības var pieprasīt, lai KDI piešķir izņēmumu no 1. un 2. punktā noteiktajām prasībām.

12. pants

Drošības darba procedūras (*SecOPs*) drošības zonās

1. Attiecīgā Komisijas dienesta *LSO* sagatavo *SecOPs* katrai drošības zonai, par kuru tas ir atbildīgs.

2. *LSO* nodrošina, ka *SecOPs* ietver šādas prasības:

a) darba laikā bez pavadības piekļuve drošības zonai ir atļauta tikai tiem darbiniekiem, kuriem ir derīga drošības atļauja un noteikta vajadzība piekļūt dokumentiem, kas klasificēti *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī;

b) piekļuvi drošības zonai bez pavadības ārpus darba laika piešķir tikai dienesta *LSO*, drošības zonas RK, to vietniekiem un Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorāta pilnvarotajam personālam;

c) ierakstīšanas un sakaru ierīces, piemēram, mobilie tālruņi, datori, kameras vai citas viedierīces nav atļautas drošības zonās bez iepriekšējas KDI atļaujas; jebkuru atkāpi iepriekš pieprasa no KDI; *LSO* darbojas kā kontaktpunkts;

d) visus štata vai ārštata darbiniekus, kuriem vajadzīga piekļuve drošības zonai, bet kuri neatbilst a) apakšpunktā noteiktajiem kritērijiem, vienmēr pavada un uzrauga pienācīgi pilnvarots darbinieks; visu šādu piekļuvi drošības zonai reģistrē reģistrācijas žurnālā, ko glabā pie ieejas drošības zonā;

e) *LSO* nodrošina, ka ielaušanās atklāšanas sistēmas, kas uzrauga drošības zonu, vienmēr ir aktīvas un pienācīgi darbojas, un pārvalda visas saistītās paroles, atslēgas, *PIN* vai citus piekļuves un autentifikācijas mehānismus;

f) par trauksmes signāliem drošības zonā ziņo Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorātam, kas par to nekavējoties informē *LSO*;

g) tā dienesta *LSO*, kurā atrodas drošības zona, reģistrē katru iejaukšanos pēc trauksmes signāla vai drošības incidenta;

h) ir ieviestas procedūras, kas attiecas uz trauksmes vai citu ārkārtas situāciju drošības zonā, tostarp personāla evakuāciju un vajadzības gadījumā KDI pakļautībā esošas avārijas vienības un ārējo neatliekamās palīdzības dienestu ātras reaģēšanas nodrošināšanu;

i) lai noteiktu piemērotu reakciju, *LSO* nekavējoties ziņo KDI par visiem drošības pārkāpumiem, kas notiek drošības zonā vai saistībā ar drošības zonu;

j) ja drošības zonā esošus atsevišķus birojus, telpas un seifus atstāj bez uzraudzības, tos tur aizslēgtus;

k) darbinieki izvairās no klasificētas informācijas apspriešanas gaiteņos vai citās kopējās drošības zonas telpās, ja tuvumā atrodas personas, kurām nav atļaujas.

13. pants

Drošības atslēgas un kombinācijas

1. *LSO* uzņemas vispārēju atbildību par to, lai nodrošinātu, ka tiek pareizi apstrādātas un glabātas atslēgas un kombinācijas, ko izmanto drošības zonās vai piekļūšanai tām. Atslēgas un kombinācijas glabā seifā, un tās aizsargā vismaz tādā pašā līmenī kā materiālu, kuram tās nodrošina piekļuvi.

2. *LSO* uztur seifu un glabātavu reģistru, kā arī atjauninātu sarakstu ar visiem darbiniekiem, kuriem tās ir pieejamas bez pavadības.

3. *LSO* uztur seifu un glabātavu atslēgu reģistru, tostarp to darbinieku sarakstu, kuriem tās ir piešķirtas. Par katru izsniegto atslēgu saglabā kvīti, kurā norādīta atslēgas identifikācija, saņēmējs, datums un laiks.

4. Atslēgas un kombinācijas izsniedz tikai tiem darbiniekiem, kuriem ir vajadzība pēc informācijas un kuriem ir piešķirta atbilstoša atļauja piekļūt ESKI. *LSO* savāc atpakaļ visas atslēgas, kad šie nosacījumi vairs netiek izpildīti.

5. *LSO* glabā rezerves atslēgas un rakstisku ierakstu par katru kombinācijas iestatījumu atsevišķā aizzīmogotā, necaurredzamā, parakstītā un datētā aploksnē, ko nodrošina par atslēgām atbildīgais darbinieks. Šīs aploksnes glabā seifā, kas atbilst visaugstākajam attiecīgajā seifā vai glabātavā uzglabātā materiāla klasifikācijas līmenim.

6. Ja, mainot kombināciju vai nododot atslēgu rotācijā, izskatās, ka aploksne ir tikusi atvērta vai bojāta, *LSO* to uzskata par drošības incidentu un nekavējoties informē KDI.

7. Seifu kombināciju iestatījumu izmaiņas drošības zonās veic *LSO* uzraudzībā. Kombinācijas atiestata vismaz reizi 12 mēnešos un ikreiz, kad:

a) tiek saņemts jauns seifs vai uzstādīta jauna slēdzene (nekavējoties jāmaina it īpaši noklusējuma kombinācijas);

b) ir radies apdraudējums vai ir aizdomas, ka tas varētu būt radies;

c) personai, kura zina attiecīgo kombināciju, piekļuve vairs nav nepieciešama.

8. *LSO* reģistrē 7. punktā minēto kombināciju izmaiņu datumus.

14. pants

ESKI ārkārtas evakuācijas un iznīcināšanas plāni

1. *LSO* palīdz dienesta vadītājam izstrādāt ārkārtas evakuācijas un ESKI iznīcināšanas plānus, pamatojoties uz HR.DS sniegtajiem norādījumiem.

2. *LSO* nodrošina, ka visas iekārtas, kas vajadzīgas 1. punktā minēto plānu darbībai, ir viegli pieejamas un tiek uzturētas labā darba kārtībā.

3. *LSO* kopā ar 1. punktā minētajos plānos noteiktajām amatpersonām vismaz reizi 12 mēnešos pārskata plānu sagatavotību un veic visus vajadzīgos pasākumus, lai tos atjauninātu.

15. pants

Drošības atļaujas

1. *LSO* uztur reģistru par visiem dienesta amatiem, kuros nepieciešama Komisijas drošības atļauja, un par darbiniekiem, kas ieņem šos amatus. Prasība saņemt drošības atļauju ir jānorāda paziņojumā par vakanci darbā pieņemšanas procesa laikā un jāpaziņo kandidātam intervijas laikā.

2. *LSO* pārrauga visus drošības atļauju pieprasījumus piekļuvei ESKI. *LSO* ir dienesta kontaktpunkts un sadarbojas ar KDI, lai saņemtu drošības atļaujas.

3. *LSO* iesniedz pieprasījumu sākt drošības atļaujas procedūru attiecībā uz attiecīgo personāla locekli un nodrošina, ka personāla loceklis nekavējoties nosūta KDI valsts drošības pielaides anketu.

4. *LSO* nodrošina, ka dienesta darbinieki, kam piešķirta drošības pielaide, apmeklē ESKI instruktāžu, kas ir obligāta drošības atļaujas saņemšanai.

5. *LSO* regulāri sazinās ar dienesta cilvēkresursu daļu, lai iegūtu informāciju par visām izmaiņām amatos, kam vajadzīga drošības atļauja, un nekavējoties informē KDI par visām šādām izmaiņām.

6. *LSO* informē KDI par tāda jauna personāla locekļa ierašanos, kuram ir spēkā esoša drošības pielaide un kurš ieņems amatu, kam vajadzīga drošības atļauja.

7. *LSO* nodrošina, ka dienesta darbinieki pabeidz drošības pielaides atjaunošanas procedūru noteiktajā termiņā. Ikvienam darbiniekam, kas atsakās pabeigt procedūru, ir pienākums pāriet amatā, kurā nav vajadzīga drošības atļauja.

16. pants

ESKI reģistrs

1. Ja dienests uztur ESKI reģistru, *LSO* uzrauga RK darbības attiecībā uz rīcību ar ESKI un atbilstību drošības noteikumiem par ESKI aizsardzību.

2. Vismaz reizi 12 mēnešos un pēc RK vai RK vietnieka maiņas *LSO* veic šādas pārbaudes:

a) ESKI reģistrā iekļauto dokumentu paraugu pārbaudi, lai apstiprinātu to statusu un klasificēto dokumentu reģistra pareizību;

b) ESKI izplatīšanai uz ESKI reģistru un no tā nosūtīto kvīšu un nosūtīšanas kvīšu paraugu pārbaudi;

c) iznīcināšanas sertifikātu parauga pārbaudi.

3. Vismaz reizi mēnesī *LSO* uz vietas pārbauda klasificēto dokumentu reģistru un nesen saņemtos klasificētos dokumentus, lai pārliecinātos, ka dokumenti tiek pareizi reģistrēti.

4. Visas pārbaudes reģistrē klasificēto dokumentu reģistrā.

17. pants

Citi pienākumi drošības jomā

Pārējos *LSO* pienākumus drošības jomā izklāsta drošības paziņojumā, kas jo īpaši attiecas uz personu, telpu un citu aktīvu, kā arī informācijas fizisko drošību.

5. NODAĻA

Reģistra kontrolieris (RK)

18. pants

RK iecelšana

1. RK un RK vietnieki ir ierēdņi vai pagaidu darbinieki.

2. Visiem RK un RK vietniekiem ir derīga drošības atļauja piekļūt ESKI līdz *SECRET UE/EU SECRET* līmenim un vajadzības gadījumā līdz *TRES SECRET UE/EU TOP SECRET* līmenim. RK vai RK vietnieks pirms iecelšanas saņem drošības atļauju.

3. Komisijas pārstāvniecības var pieprasīt, lai KDI piešķir izņēmumu no 1. un 2. punktā noteiktajām prasībām.

19. pants

Pienākumi

1. RK reģistrē informāciju, kas drošības nolūkos klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, ja:

a) tā nonāk Komisijas dienestā vai tiek izsūtīta no tā; vai

b) tā tiek saņemta KIS vai izsūtīta no tās.

2. RK reģistrē visus notikumus visas tās informācijas aprites ciklā, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī. RK arī nodrošina, ka tiek reģistrēta visa informācija, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, vai tai līdzvērtīga informācija, ar kuru apmainās ar trešām valstīm un starptautiskām organizācijām. To dara sadarbībā ar ESKI reģistru, ko pārvalda Ģenerālsekretariāts.

3. RK klasificēto dokumentu reģistrā reģistrē dokumentus, kas klasificēti *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, un nodrošina, ka tie tiek droši glabāti ESKI reģistrā.

4. RK palīdz Komisijas darbiniekiem izveidot un nosūtīt informāciju, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī.

5. Ja dokumentus, kas klasificēti *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, saņem no citiem dienestiem vai ārējām personām, RK nodrošina, ka piegādes kvīts tiek pienācīgi nogādāta dokumenta autoram.

6. Pirms ļaut darbiniekam piekļūt klasificētam dokumentam, kas atrodas ESKI reģistrā, RK pie *LSO* pārliecinās, ka personāla loceklim ir drošības atļauja, ko piešķīrusi KDI.

7. RK reģistrē visus darbiniekus, kuri ierodas ESKI reģistrā un dodas prom no tā un kuriem nav atļauta piekļuve bez pavadības, un pavada tos visā apmeklējuma laikā.

8. Ja darbinieks saņem dokumentu darbam ārpus ESKI reģistra, RK nodrošina, ka darbinieks ir informēts par attiecīgajiem kompensējošajiem drošības pasākumiem un atdod dokumentu, tiklīdz tas vairs nav vajadzīgs. RK atgādina darbiniekiem, ka šādi dokumenti ir jāatdod pēc iespējas drīz.

9. ESKI reģistrs izsniedz kurjera apliecību, ja klasificētus dokumentus pārnēsā rokās ārpus valsts, kurā atrodas reģistrs.

10. Drošības paziņojumā izklāsta sīki izstrādātus norādījumus RK par klasificētu dokumentu reģistrēšanu.

20. pants

Klasifikācijas līmeņa pazemināšana un deklasifikācija

RK palīdz dienestiem, kas sagatavojuši reģistrēto ESKI, to pārskatīt, lai pārliecinātos, vai sākotnējais klasifikācijas līmenis joprojām ir atbilstīgs, vai arī dokumentu var pazemināt vai deklasificēt.

21. pants

Iznīcināšana

1. RK ir atbildīgi par tādas informācijas iznīcināšanu, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* un augstākā līmenī, izmantojot apstiprinātus paņēmienus, vajadzības gadījumā klātesot lieciniekiem, kuriem ir drošības pielaide.

2. RK reģistrē jebkādu tādas informācijas iznīcināšanu, kas klasificēto dokumentu reģistrā klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* un augstākā līmenī, un glabā attiecīgos iznīcināšanas sertifikātus ESKI reģistrā.

22. pants

Papildu uzdevumi

1. RK sniedz *LSO* visu nepieciešamo palīdzību, kad *LSO* veic uzraudzības darbības ESKI reģistrā.

2. RK ziņo *LSO* par visiem iespējamiem vai faktiskiem starpgadījumiem drošības jomā, kas savukārt par tiem ziņo KDI.

3. Tāda Komisijas dienesta ESKI reģistra RK, kas organizē klasificētu sanāksmi *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, sagatavo ESKI, ar ko notiks rīcība sanāksmes laikā, un koordinē darbības ar sanāksmes organizētāju, lai nodrošinātu, ka visi dokumenti un kvītis tiek apstrādāti saskaņā ar attiecīgajiem noteikumiem.

6. NODAĻA

Nobeiguma noteikumi

23. pants

Pārredzamība

Šo lēmumu dara zināmu Komisijas darbiniekiem un visām personām, uz ko tas attiecas, un publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

24. pants

Šis lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē, 2022. gada 7. aprīlī

Komisijas
un tās priekšsēdētājas vārdā –
Cilvēkresursu un drošības ģenerāldirektorāta
ģenerāldirektore
Gertrud INGESTAD