EIROPAS
REVĪZIJAS
PALĀTA

Revīzijas palātas Lēmums Nr. 041–2021 par drošības noteikumiem ES klasificētas informācijas (ESKI) aizsardzībai

EIROPAS REVĪZIJAS PALĀTA,

ŅEMOT VĒRĀ Līguma par Eiropas Savienību 13. pantu,

ŅEMOT VĒRĀ Līguma par Eiropas Savienības darbību 287. pantu,

ŅEMOT VĒRĀ 257. pantu Eiropas Parlamenta un Padomes 2018. gada 18. jūlija Regulā (ES, Euratom) 2018/1046 par finanšu noteikumiem, ko piemēro Savienības vispārējam budžetam,

ŅEMOT VĒRĀ Revīzijas palātas reglamenta īstenošanas kārtības 1. panta 6. punktu (Revīzijas palātas Lēmums Nr. 21–2021),

ŅEMOT VĒRĀ citu Savienības iestāžu, aģentūru un struktūru drošības noteikumus Savienības klasificētas informācijas aizsardzībai,

ŅEMOT VĒRĀ Revīzijas palātas informācijas drošības politiku (DEC 127/15 FINAL) un informācijas klasifikācijas politiku (Paziņojums personālam 123/2020),

TĀ KĀ saskaņā ar LESD 287. panta 3. punktu Revīzijas palātai ir tiesības piekļūt visiem attiecīgajiem dokumentiem un informācijai, kas, pēc tās ieskatiem, ir nepieciešama, lai pildītu savas pilnvaras, tostarp Savienības klasificētajai informācijai (ESKI), un šīs tiesības ir jāīsteno, pilnībā ievērojot iestāžu lojālas sadarbības principu un kompetences piešķiršanas principu; ESKI autors nevar apšaubīt LESD garantētās tiesības piekļūt ESKI, savukārt Revīzijas palātai var lūgt ieviest un ievērot konkrētus drošības pasākumus, kā sīkāk izklāstīts šajā dokumentā;

TĀ KĀ Revīzijas palātas locekļiem, ierēdņiem un pārējiem darbiniekiem pat pēc aiziešanas no dienesta ir saistošs pienākums ievērot konfidencialitāti atbilstoši LESD 339. pantam un Civildienesta noteikumu 17. pantam, kā arī saskaņā ar tiem pieņemtiem aktiem;

TĀ KĀ ESKI sensitīvā būtība pieprasa, lai, rīkojoties ar šo informāciju, konfidencialitātes ievērošanas pienākums tiek nodrošināts ar atbilstošiem drošības pasākumiem, ar kuriem var garantēt augstu minētās informācijas aizsardzības līmeni un kuri ir līdzvērtīgi tiem, kas paredzēti citu Savienības iestāžu, aģentūru un struktūru pieņemtajos noteikumos par ESKI aizsardzību, ar to saprotot, ka gadījumā, ja Revīzijas palāta uzskata, ka, ņemot vērā ESKI būtību un veidu, jebkuri šādi drošības pasākumi nav pamatoti, tad Revīzijas palāta patur tiesības paust savus apsvērumus, vienlaikus ņemot vērā ESKI klasifikācijas līmeni;

TĀ KĀ drošības pasākumiem nolūkā aizsargāt Revīzijas palātai sniegtās informācijas konfidencialitāti, integritāti un pieejamību jāatbilst attiecīgās informācijas būtībai un veidam;

TĀ KĀ piekļuve klasificētai informācijai ir jānodrošina Revīzijas palātai saskaņā ar "vajadzību pēc informācijas", lai veiktu uzdevumus, kas uzticēti Līgumos un tiesību aktos, kuri pieņemti, pamatojoties uz Līgumiem;

TĀ KĀ ņemot vērā konkrētās informācijas būtību un sensitīvo saturu, ir lietderīgi izveidot īpašu procedūru tam, kā Revīzijas palāta rīkojas ar ESKI saturošiem dokumentiem;

TĀ KĀ iestādei jānodrošina šā lēmuma īstenošana saskaņā ar visiem piemērojamiem noteikumiem, jo īpaši noteikumiem par personas datu aizsardzību, personu, ēku un IT fizisko drošību un publisku piekļuvi dokumentiem;

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants. Priekšmets un piemērošanas joma

1) Ar šo lēmumu nosaka pamatprincipus un minimālos drošības standartus, lai aizsargātu klasificētu informāciju, ar kuru, īstenojot savas pilnvaras, rīkojas Revīzijas palāta.

2) Šajā lēmumā klasificēta informācija ir jebkura vai visa šāda veida informācija:

a) "ES klasificēta informācija" (ESKI), kura ir definēta citu Savienības iestāžu, aģentūru, struktūru vai biroju drošības noteikumos un kurai piemērots viens no šiem drošības klasifikācijas marķējumiem:

- TRÈS SECRET UE/EU TOP SECRET: informācija un materiāli, kuru neatļauta izpaušana var radīt ārkārtīgi smagu kaitējumu būtiskām Eiropas Savienības vai vienas vai vairāku dalībvalstu interesēm;
- SECRET UE/EU SECRET: informācija un materiāli, kuru neatļauta izpaušana var radīt nopietnu kaitējumu būtiskām Eiropas Savienības vai vienas vai vairāku dalībvalstu interesēm;
- CONFIDENTIEL UE/EU CONFIDENTIAL: informācija un materiāli, kuru neatļauta izpaušana var radīt kaitējumu būtiskām Eiropas Savienības vai vienas vai vairāku dalībvalstu interesēm;
- RESTREINT UE/EU RESTRICTED: informācija un materiāli, kuru neatļauta izpaušana var būt nevēlama Eiropas Savienības vai vienas vai vairāku dalībvalstu interesēm;

b) klasificēta informācija, ko sniegušas dalībvalstis un kam piemērots valsts drošības klasifikācijas marķējums, kas ir līdzvērtīgs vienam no a) punktā uzskaitītajiem ESKI drošības klasifikācijas marķējumiem[1];

c) klasificēta informācija, kuru Eiropas Revīzijas palātai sniegušas trešās valstis vai starptautiskas organizācijas un kurai piemērots drošības klasifikācijas marķējums, kas ir līdzvērtīgs vienam no a) punktā uzskaitītajiem ESKI drošības klasifikācijas marķējumiem, kā paredzēts attiecīgajos nolīgumos vai administratīvajos noteikumos par informācijas drošību.

[1] Sk. Padomē sanākušo Eiropas Savienības dalībvalstu Nolīgumu par tādas klasificētās informācijas aizsardzību, ar kuru apmainās Eiropas Savienības interesēs (2011. gada 4. maijs) un tā pielikumu (OV 2011/C 202/13).

3) Revīzijas palāta savās telpās rīkojas ar RESTREINT UE/EU RESTRICTED līmenī klasificētu informāciju un šim nolūkam īsteno visus nepieciešamos aizsardzības pasākumus. Tiek veikti pasākumi, lai Revīzijas palātas darbinieki, kuriem nepieciešama piekļuve augstāka līmeņa ESKI, piekļūtu tai piemērotās citu Savienības iestāžu, struktūru vai aģentūru telpās.

4) Šo lēmumu piemēro visām Revīzijas palātas struktūrvienībām un telpām.

5) Izņemot gadījumus, kad noteikums attiecas uz konkrētām personāla grupām, šo lēmumu piemēro Revīzijas palātas locekļiem, Revīzijas palātas darbiniekiem, kuriem ir piemērojami Civildienesta noteikumi un Eiropas Savienības Pārējo darbinieku nodarbināšanas kārtība[2], darbam Revīzijas palātā norīkotajiem valsts ekspertiem (NVE), pakalpojumu sniedzējiem un viņu darbiniekiem, stažieriem un ikvienai personai, kura var piekļūt Revīzijas palātas ēkām un citiem aktīviem, vai informācijai, kas ir Revīzijas palātas rīcībā.

6) Ja vien nav norādīts citādi, noteikumus par ESKI piemēro līdzvērtīgi šā panta 2. punkta b) un c) apakšpunktā minētajai klasificētajai informācijai.

2. pants. **Definīcijas**

Šajā lēmumā:

a) "atļauja piekļūt ESKI" ir Revīzijas palātas Cilvēkresursu, finanšu un vispārējo lietu direkcijas vadītāja lēmums, ko pieņem, pamatojoties uz dalībvalsts kompetentās iestādes apgalvojumu par to, ka Revīzijas palātas ierēdnim, citam darbiniekam vai NVE – ja ir konstatēts, ka viņiem ir vajadzība pēc informācijas, un viņi ir attiecīgi informēti par savu atbildību – līdz konkrētam datumam var piešķirt piekļuvi ESKI līdz konkrētam klasifikācijas līmenim (CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākam); var uzskatīt, ka tāda persona ir "saņēmusi drošības atļauju";

b) "klasifikācija" ir klasifikācijas līmeņa piešķiršana informācijai, pamatojoties uz kaitējuma pakāpi, ko varētu radīt neatļauta izpaušana;

c) "kriptogrāfijas materiāls" ir kriptogrāfijas algoritmi, kriptogrāfijas aparatūras un programmatūras moduļi un produkti, tostarp īstenošanas informācija un ar to saistītā dokumentācija, kā arī atslēgu materiāls;

d) "deklasifikācija" ir visas drošības klasifikācijas noņemšana;

e) "dokuments" ir jebkura fiksēta informācija neatkarīgi no tās veidola vai fiziskajām iezīmēm;

f) "klasifikācijas līmeņa pazemināšana" ir zemāka drošības klasifikācija līmeņa piešķiršana;

g) "iestādes drošības pielaide" (IDP) ir administratīvs atzinums, ko izsniedz kompetenta drošības iestāde par to, ka no drošības viedokļa iestāde var nodrošināt ESKI piešķirtajam drošības klasifikācijas līmenim atbilstošu aizsardzības līmeni;

h) "rīkošanās" ar ESKI ir visu veidu darbības, ko ar ESKI veic visā tās aprites cikla laikā: izveide, reģistrācija, apstrāde, pārvadāšana, klasifikācijas līmeņa pazemināšana, deklasifikācija un iznīcināšana. Saistībā ar komunikācijas un informācijas sistēmām (KIS) tajā ietilpst arī vākšana, uzrādīšana, pārsūtīšana un glabāšana;

i) "turētājs" ir pienācīgi pilnvarota persona, kurai ir pierādīta vajadzība pēc informācijas, kuras rīcībā ir klasificēta informācija un kura tādējādi ir atbildīga par tās aizsardzību;

[2] Grozītā Regula Nr. 31 (EEK), ar ko nosaka Civildienesta noteikumus un Pārējo darbinieku nodarbināšanas kārtību, OV 01 962R0031–1.1.2020–019.003–1 (https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:01 962R0031–20 200 101).

j) “informācijas drošības institūcija” ir Revīzijas palātas informācijas drošības speciālists, kas var pilnībā vai daļēji deleģēt šajā lēmumā paredzētos uzdevumus;

k) “informācija” ir jebkura rakstveida vai mutvārdu informācija neatkarīgi no tā, kādā nesējā tā ietverta vai kas to sagatavojis;

l) “materiāli” ir jebkurš medijs, datu nesējs vai iekārtas vai ierīces daļa;

m) “autors” ir Savienības iestāde, struktūra vai aģentūra, dalībvalsts, trešā valsts vai starptautiska organizācija, kuras pakļautībā klasificēta informācija bija sagatavota un/vai nodota Savienības struktūrām;

n) “personāla drošības pielaide” (PDP) ir dalībvalsts kompetentās iestādes deklarācija, kas pieņemta pēc tam, kad dalībvalsts kompetentās iestādes veikušas drošības izmeklēšanu, un ar ko apliecina, ka personai, ja ir konstatēts, ka tai ir vajadzība pēc informācijas un tā ir attiecīgi informēta par saviem pienākumiem un atbildību, līdz konkrētam datumam var piešķirt piekļuvi ESKI līdz konkrētam līmenim (CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākam);

o) “personāla drošības pielaides apliecība” (PDPA) ir Revīzijas palātas Cilvēkresursu, finanšu un vispārējo lietu direkcijas vadītāja izdota apliecība, kurā teikts, ka personai ir derīga drošības pielaide vai drošības atļauja, un kurā norādīts tas ESKI klasifikācijas līmenis, līdz kuram personai var piešķirt piekļuvi (CONFIDENTIEL UE/EU CONFIDENTIAL vai augstāks līmenis), attiecīgās drošības pielaides vai atļaujas derīguma termiņš un pašas apliecības derīguma termiņš;

p) “fiziskās drošības institūcija” ir Revīzijas palātas drošības dienesta vadītājs, kas ir atbildīgs par ESKI aizsardzībai nepieciešamo fiziskās drošības pasākumu un procedūru īstenošanu;

q) “Reģistra biroju” pārvalda Revīzijas palātas Sekretariāts. Šis birojs atrodas administratīvajā zonā, par kuru atbild Revīzijas palātas Cilvēkresursu, finanšu un vispārējo lietu direkcijas vadītājs. Birojs ir atbildīgs par RESTREINT UE/EU RESTRICTED līmenī klasificētas vai līdzvērtīgas informācijas, ar ko apmainās Revīzijas palāta, iekļūšanu un izkļūšanu;

r) “ESKI reģistrs” ir zona, kas izveidota drošības zonā. Minēto reģistru pārvalda Revīzijas palātas pilnvarots reģistra kontrolieris, kam ir piešķirta drošības pielaide. Reģistra kontrolieris ir atbildīgs par CONFIDENTIEL UE/EU CONFIDENTIAL līmenī klasificētas informācijas, augstāka līmeņa vai līdzvērtīgas informācijas, ar ko apmainās Revīzijas palāta, iekļūšanu un izkļūšanu;

s) “drošības akreditācijas institūcija (DAI)” ir Revīzijas palātas Cilvēkresursu, finanšu un vispārējo lietu direkcija.

3. pants. **ESKI aizsardzības pasākumi**

1) Revīzijas palāta nodrošina visas tai sniegtās klasificētās informācijas aizsardzību veidā, kas atbilst autora noteiktajam klasifikācijas līmenim, un saskaņā ar šo lēmumu.

2) Šim nolūkam Revīzijas palāta rīcībai ar ESKI piemēro fiziskus un, attiecīgā gadījumā, personāla drošības pasākumus, tostarp piekļuves atļauju izsniegšanu identificētajām personām un komunikācijas un informācijas sistēmu aizsardzības pasākumus. Šie pasākumi ir aprakstīti 4. līdz 6. pantā, un tos piemēro visā ESKI aprites ciklā. Tie ir samērīgi ar ESKI drošības klasifikācijas līmeni, informācijas vai materiāla veidu un apjomu, to ēku atrašanās vietu un uzbūvi, kurās ESKI atrodas, un vietēji izvērtētiem ļaunprātīgu un/vai noziedzīgu nodarījumu draudiem, tostarp spiegošanu, sabotāžu vai terorismu.

3) ESKI aizsargā ar fiziskās drošības pasākumiem, un informāciju, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī, papildus aizsargā ar personāla drošības pasākumiem.

4) ESKI var sniegt tikai tām personām, kurām ir vajadzība pēc informācijas iestādē. Jebkuras ESKI turētājam tā jāaizsargā, kā noteikts šajā lēmumā.

5) ESKI nedrīkst izpaust mutiski vai rakstiski. Revīzijas palātas sākotnējie apsvērumi, ziņojumi, atzinumi, preses relīzes un citi produkti, tās tīmekļa vietne un intranets, mutiskās uzstāšanās, atbildes uz lūgumiem piešķirt piekļuvi dokumentiem[3] un balss vai videoieraksti nedrīkst saturēt vai atsaukties uz ESKI vai tās izvilkumiem. Tomēr, ja autors ir publicējis dokumentus vai informāciju, kas satur atsauci uz ESKI, šo atsauci var minēt.

6) Neatkarīgi no 5. punkta Revīzijas palāta un autors var vienoties, ka īpašas revīzijas gadījumā Revīzijas palāta var dokumentā reproducēt vai izmantot daļu no ESKI. Šādā gadījumā minēto Revīzijas palātas dokumentu vispirms adresē attiecīgās ESKI autoram pirms pretrunu procedūras vai tās laikā. Šādā situācijā Revīzijas palāta un autors vienojas par to, vai Revīzijas palātas izdotais dokuments ir klasificējams. Ja Revīzijas palātas referējošais loceklis uzskata, ka — ņemot vērā visus ar šo Lēmumu saistītos drošības pasākumus —, revīzijas ziņojums, kas pilnībā vai daļēji klasificēts, ir jānosūta noteiktiem adresātiem Eiropas Parlamentā vai Padomē, ir nepieciešams saņemt klasificētās informācijas autora piekrišanu. Tiesiskais regulējums un procedūra šādu dokumentu apmaiņai ir izklāstīti 7. pantā.

7) Ja, īstenojot savas pilnvaras, ir nepieciešams plašāk izplatīt dažas klasificēta dokumenta vai informācijas daļas, Revīzijas palāta, pienācīgi ņemot vērā drošības klasifikācijas marķējumu, pirms lēmuma pieņemšanas par minēto daļu vai informācijas izmantošanu apspriežas ar autoru, ja tā uzskata, ka šādai rīcībai ir sevišķi svarīgas sabiedrības intereses. Ziņojumā informāciju izmanto tikai tā, lai nevarētu kaitēt autora interesēm. To varētu atbilstīgi aizsargāt, lūdzot autoram sniegt komentārus, lai vienotos par veidu, kā anonimizēt, saīsināt vai vispārināt informāciju utt., vienlaikus ievērojot to personu intereses, uz kurām galvenokārt attiecas publicētā informācija.

8) Revīzijas palāta nesniedz ESKI citai Savienības iestādei, aģentūrai, struktūrai vai birojam, dalībvalstij, trešai valstij vai starptautiskai organizācijai, iepriekš neapspriežoties ar autoru un bez tā skaidras un rakstiskas piekrišanas.

9) Ja vien dokumenta, kas klasificēts SECRET UE/EU SECRET vai zemākā līmenī, autors nav noteicis ierobežojumus tā pavairošanai vai tulkošanai, šādus dokumentus pēc turētāja pieprasījuma un saskaņā ar Revīzijas palātas informācijas drošības institūcijas praktiskajiem darba norādījumiem ļauts pavairot vai tulkot. Drošības pasākumi, kas piemērojami oriģināldokumentam, ir piemērojami arī tā kopijām un tulkojumiem.

10) Ja Revīzijas palātai ir vajadzīgs, lai klasificēts dokuments, kuru tā ir saņēmusi vai kuram tai ir atļauts piekļūt, tiktu klasificēts zemākā līmenī vai deklasificēts, Palāta apspriežas ar autoru, lai noskaidrotu, vai tas var iesniegt dokumenta zemākas klasifikācijas līmeņa vai deklasificētu versiju.

[3] Saskaņā ar Revīzijas palātas Lēmumu Nr. 12–2005 par publisku piekļuvi Palātas dokumentiem, kurā grozījumi izdarīti ar Lēmumu Nr. 14–2009 (OV 2009/C 67/1).

4. pants. **Personāla drošība**

1) Pamatojoties uz ieņemamo amatu, Revīzijas palātas locekļiem ir atļauts piekļūt visai ESKI un piedalīties sanāksmēs, kurās rīkojas ar ESKI. Locekļi tiek informēti par pienākumiem saistībā ar ESKI aizsardzību un rakstiski apliecina savu atbildību par šādas informācijas aizsardzību.

2) Revīzijas palātas darbiniekiem — ierēdņiem, personālam, uz kuru attiecas Pārējo darbinieku nodarbināšanas kārtība, un NVE — piešķir piekļuvi ESKI tikai pēc tam, kad:

   i. konstatēta personas vajadzība pēc informācijas;

   ii. persona ir iepazīstināta ar ESKI aizsardzībai paredzētajiem drošības noteikumiem un attiecīgajiem drošības standartiem un pamatnostādnēm, un tā ir rakstiski apliecinājusi savu atbildību saistībā ar šādas informācijas aizsargāšanu;

   iii. attiecībā uz informāciju, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī, personai ir piešķirta drošības pielaide un atļauja tai piekļūt.

3) Procedūru, lai noteiktu, vai ierēdnim vai citam Revīzijas palātas darbiniekam drīkst piešķirt piekļuvi informācijai, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī, ņemot vērā personas lojalitāti, integritāti un uzticamību, un pēc tam, kad ir saņemts 2. panta n) punktā minētais dalībvalsts kompetento iestāžu apgalvojums, nosaka deleģētajā lēmumā, ko pieņem saskaņā ar 10. panta 10. punktu. Lēmumus par piekļuves atļaujas piešķiršanu pieņem Revīzijas palātas Cilvēkresursu, finanšu un vispārējo lietu direkcijas vadītājs.

4) Revīzijas palātas Cilvēkresursu, finanšu un vispārējo lietu direkcijas vadītājs var izdot PDPA, norādot klasifikācijas līmeni, kādā personām var piešķirt piekļuvi ESKI (CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī), attiecīgās piekļuves atļaujas derīguma termiņu un PDPA derīguma termiņu.

5) Tikai personas ar 2. punkta iii) apakšpunktā minēto atļauju un Revīzijas palātas locekļi saskaņā ar 1. punktu drīkst piedalīties sanāksmēs, kurās rīkojas ar informāciju, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī. Revīzijas palāta un autors, izskatot katru gadījumu atsevišķi, veic praktiskus pasākumus šādām sanāksmēm.

6) Revīzijas palātas struktūrvienības, kas ir atbildīgas par tādu sanāksmju organizēšanu, kurās jārīkojas ar informāciju, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī, savlaicīgi informē informācijas drošības institūciju par sanāksmes datumu, laiku un vietu, norādot dalībnieku sarakstus.

7) Ikvienai personai, kuras rīcībā ir ESKI bez pienācīgas atļaujas un/vai kurai nav pierādītas vajadzības tādu zināt, pēc iespējas drīzāk jāziņo par situāciju informācijas drošības institūcijai un jānodrošina, ka ESKI tiek aizsargāta, kā prasīts šajā lēmumā.

5. pants. **Fiziskās drošības pasākumi klasificētas informācijas aizsardzībai**

1) "Fiziskā drošība" ir fizisku un tehnisku aizsardzības pasākumu pielietošana, lai novērstu neatļautu piekļuvi ESKI.

2) Fiziskās drošības pasākumu mērķis ir nepieļaut slepenu vai vardarbīgu ielaušanos, atturēt no neatļautām darbībām, kavēt un atklāt šādas neatļautas darbības un ļaut nošķirt darbiniekus attiecībā uz piekļuvi ESKI, pamatojoties uz to vajadzību pēc informācijas. Šos pasākumus nosaka, pamatojoties uz riska pārvaldības procedūru un saskaņā ar šo lēmumu.

3) Zonas, kur rīkojas ar ESKI vai to glabā, regulāri pārbauda kompetentā Revīzijas palātas drošības institūcija.

4) Rīkojoties ar ESKI un to glabājot, izmanto tikai iekārtas vai ierīces, kas atbilst noteikumiem, kurus piemēro Savienības iestādēs, aģentūrās vai struktūrās ESKI aizsardzībai.

5) Revīzijas palātas darbinieki var piekļūt ESKI, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī, vai līdzvērtīgai informācijai drošības zonās ārpus Revīzijas palātas telpām.

6) Revīzijas palāta var noslēgt pakalpojumu līmeņa vienošanos ar citu Savienības iestādi Luksemburgā, lai šīs iestādes drošības zonā varētu rīkoties ar informāciju, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī, un to glabāt. Ja vien autors nav sniedzis īpašu piekrišanu, ar šo ESKI nerīkojas un to neglabā Revīzijas palātas telpās, un Revīzijas palāta to nepavairo un nepārtulko.

7) Revīzijas palāta reģistrē saņemto RESTREINT UE/EU RESTRICTED līmenī klasificēto informāciju. Drošības nolūkos tiek reģistrēta CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī klasificētas informācijas aplūkošana ārpus Revīzijas palātas telpām.

8) ESKI, kas klasificēta RESTREINT UE/EU RESTRICTED līmenī, var tikt glabāta piemērotās aizslēdzamās biroja mēbelēs administratīvā zonā vai drošības zonā. ESKI, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai SECRET UE/EU SECRET līmenī, saskaņā ar pakalpojumu līmeņa nolīgumu glabā seifā citas Savienības iestādes drošības zonā Luksemburgā.

9) Ārpus reģistra ESKI pārvieto starp dienestiem un telpām šādā veidā:

   a) parasti ESKI pārsūta ar elektroniskiem līdzekļiem, kurus aizsargā ar kriptogrāfijas produktiem, kas apstiprināti atbilstīgi 6. panta 8. punktam;

   b) ja neizmanto a) punktā minētos līdzekļus, ESKI pārvieto, izmantojot datu nesēju (piemēram, zibatmiņas, kompaktdiskus, cietos diskus), kuru aizsargā ar kriptogrāfijas produktiem, kas apstiprināti atbilstīgi 6. panta 8. punktam, vai kā papīra kopiju necaurspīdīgā aizzīmogotā aploksnē.

10) Turētājs var iznīcināt RESTREINT UE/EU RESTRICED līmeņa informāciju, ievērojot Revīzijas palātas spēkā esošos arhivēšanas noteikumus. Informāciju, kas klasificēta CONFIDENTIEL UE/EUCONFIDENTIAL vai augstākā līmenī, iznīcina tikai reģistra kontrolieris pēc turētāja vai kompetentas iestādes rīkojuma saskaņā ar Revīzijas palātas spēkā esošajiem arhivēšanas noteikumiem. Dokumentus, kas klasificēti SECRET UE/EU SECRET līmenī, iznīcina tāda liecinieka klātbūtnē, kura drošības pielaide atbilst vismaz iznīcināmā dokumenta klasifikācijas līmenim. Reģistra kontrolieris un liecinieks, ja nepieciešama viņa klātbūtne, paraksta iznīcināšanas apliecinājumu, ko iekļauj reģistrā. Reģistra kontrolieris glabā CONFIDENTIEL UE/EU CONFIDENTIAL un SECRET UE/EU SECRET klasifikācijas līmeņa dokumentu iznīcināšanas apliecinājumus vismaz piecus gadus.

11) Pamatojoties uz vietējiem apstākļiem, fiziskās drošības institūcija un informācijas drošības institūcija izstrādā kopīgu plānu ESKI aizsardzībai krīzes gadījumos, tostarp, vajadzības gadījumā, iznīcināšanu ārkārtas gadījumos un evakuācijas plānus. Minētās institūcijas izdod norādījumus, ko tās uzskata par nepieciešamiem, lai nepieļautu ESKI nokļūšanu nesankcionētu personu rīcībā.

12) Ja ESKI ir jāpārvadā fiziski, Revīzijas palāta ievēro autora noteiktos pasākumus, lai aizsargātu ESKI pret neatļautu izpaušanu pārvadāšanas laikā.

13) Fiziskās drošības pasākumi, ko piemēro administratīvajās zonās, kur rīkojas ar RESTREINT UE/EU RESTRICTED līmenī klasificētu informāciju un to glabā, ir izklāstīti pielikumā.

6. pants. ESKI aizsardzība komunikācijas un informācijas sistēmās

1) Šajā pantā "komunikācijas un informācijas sistēma" ir jebkura sistēma, kas ļauj rīkoties ar ESKI elektroniskā formātā. Komunikācijas un informācijas sistēma ietver visus aktīvus, kas nepieciešami tās darbībai, tostarp infrastruktūru, organizāciju, personālu un informācijas resursus.

2) "Likumīgs lietotājs" ir Revīzijas palātas loceklis, ierēdnis, cits darbinieks vai NVE, kam ir konstatēta un atzīta vajadzība piekļūt konkrētai informācijas sistēmai.

3) Revīzijas palāta sniedz garantijas, ka tās sistēmas pienācīgi aizsargās informāciju, ar ko tās rīkojas, un darbosies, kā tas ir paredzēts, kad nepieciešams un likumīgu lietotāju kontrolē. Šajā nolūkā informācijas aizsardzība garantē atbilstīga līmeņa

- autentiskumu: garantiju, ka informācija ir īsta un saņemta no *bona fide* avotiem;
- pieejamību: tai var piekļūt un to var izmantot pēc pilnvarotas iestādes pieprasījuma;
- konfidencialitāti: informāciju neatklāj nesankcionētām personām, iestādēm vai procesiem;
- integritāti: spēju nosargāt informācijas un aktīvu precizitāti un pilnīgumu;
- neapstrīdamību: spēju pierādīt, ka darbība vai notikums ir noticis, lai vēlāk nevarētu noliegt, ka šāda darbība vai notikums ir noticis.

Pārliecības pamatā ir riska pārvaldības process. "Risks" ir iespēja, ka konkrēti draudi, izmantojot organizācijas vai kādas tās izmantotas sistēmas iekšēju vai ārēju vājo vietu, radīs kaitējumu organizācijai un tās materiālajiem un nemateriālajiem aktīviem. To izsaka kā draudu rašanās iespējamības un to ietekmes apvienojumu. Riska pārvaldības process ietver šādus posmus: draudu un vājo vietu apzināšana, riska novērtēšana, riska novēršana, riska uzņemšanās un informēšana par risku.

- "Riska izvērtējums" ir draudu un vājo vietu noteikšana un attiecīgas riska analīzes veikšana, t. i., varbūtības un ietekmes izvērtēšana;
- "riska novēršana" ir riska pavājināšana, likvidēšana, mazināšana (izmantojot atbilstīgu tehnisku, fizisku, organizatorisku vai procedūras pasākumu apvienojumu), nodošana vai uzraudzība;
- "riska uzņemšanās" ir lēmums, ar ko apzinās, ka pēc riska novēršanas pasākumu īstenošanas joprojām pastāv atlikušais risks;
- "atlikušais risks" ir risks, kas pastāv pēc drošības pasākumu īstenošanas, ņemot vērā to, ka ne pret visiem draudiem var cīnīties un ne visas vājās vietas var likvidēt;
- "informēšana par risku" ir komunikācijas un informācijas sistēmas lietotāju kopienas informētības par riskiem veicināšana, informējot apstiprināšanas iestādes par minētajiem riskiem un ziņojot par tiem rīcības iestādēm.

4) Visas elektroniskās ierīces un iekārtas, ko izmanto, lai rīkotos ar ESKI, atbilst noteikumiem, kas piemērojami ESKI aizsardzībai. Priekšroka dodama elektroniskām ierīcēm un iekārtām, kuras jau ir akreditējusi cita Savienības iestāde, aģentūra vai struktūra. Ierīču drošība jāgarantē visā to aprites ciklā.

5) Revīzijas palātas komunikācijas un informācijas sistēmu, kas rīkojas ar ESKI, akreditē atbilstīga iestāde. Lai saņemtu akreditācijas apstiprinājumu par RESTREINT UE/EU RESTRICTED līmenī klasificētu informāciju, kuru var apstrādāt Revīzijas palātas KIS, un attiecīgos darbības noteikumus un nosacījumus, Revīzijas palāta noslēdz pakalpojumu līmeņa nolīgumu (PLN) ar tādu Savienības iestādes drošības akreditācijas iestādi, kura spēj akreditēt komunikācijas un

informācijas sistēmu, kurās apstrādā ESKI. PLN attiecas arī uz standartiem, kas jāpiemēro akreditācijas procesā, un to noslēdz saskaņā ar 10. panta 3. punktā noteikto procedūru.

6) Ja Revīzijas palātai ir jāizveido savs KIS akreditācijas process, to izveido ar šā lēmuma 10. panta 10. punktā minēto deleģēto lēmumu saskaņā ar akreditācijas procesa standartiem, kas ir spēkā citās Savienības iestādēs, aģentūrās un struktūrās saistībā ar KIS, kurā rīkojas ar ESKI.

7) Par akreditācijas lietas un dokumentācijas sagatavošanu saskaņā ar pieņemtajiem standartiem ir atbildīgs vienīgi KIS īpašnieks.

8) Ja ESKI aizsargā ar kriptogrāfijas produktiem, Revīzijas palāta priekšroku dod produktiem, kurus ir apstiprinājusi Padome vai Padomes ģenerālsekretārs, kas darbojas kā Padomes kriptogrāfijas apstiprinātāja institūcija, vai citos gadījumos tiem produktiem, ko ESKI aizsardzības nolūkos apstiprinājušas citas Savienības iestādes, aģentūras un struktūras.

9) Ar RESTREINT UE/EU RESTRICTED līmenī klasificētu informāciju rīkojas tikai ar elektroniskām ierīcēm (piemēram, darbstacijām, printeriem, kopētājiem), kas atrodas administratīvā zonā vai drošības zonā. Elektroniskās ierīces, kas rīkojas ar RESTREINT UE/EU RESTRICTED līmenī klasificētu informāciju, nošķir no pārējiem datortīkliem un aizsargā ar attiecīgiem fiziskiem vai tehniskiem pasākumiem.

10) Visi Revīzijas palātas darbinieki, kas iesaistīti rīcībai ar ESKI paredzētu KIS plānošanā, izstrādē, testēšanā, darbībā, pārvaldībā vai izmantošanā, ziņo informācijas drošības speciālistam par visiem potenciāliem drošības trūkumiem, incidentiem, pārkāpumiem vai apdraudējumiem, kas var ietekmēt KIS un/vai tajā ietvertās ESKI aizsardzību.

7. pants. Procedūra klasificētas informācijas apmaiņai un piekļuves nodrošināšanai tai

1) Ja saskaņā ar Līgumiem vai tiesību aktiem, kas pieņemti, pamatojoties uz Līgumiem, tām ir juridisks pienākums to darīt, Savienības iestādes, aģentūras, struktūras un biroji un valstu iestādes pēc savas iniciatīvas vai pēc priekšsēdētāja, atbildīgā(-o) locekļa(-u) vai ģenerālsekretāra rakstiska pieprasījuma nodrošina Revīzijas palātai piekļuvi ESKI saskaņā ar turpmāk izklāstīto procedūru.

2) Piekļuves pieprasījumus attiecīgajām iestādēm nosūta ar Revīzijas palātas Reģistra biroja starpniecību.

3) Attiecīgā gadījumā Revīzijas palāta noslēdz administratīvu vienošanos par ESKI vai līdzvērtīgas informācijas apmaiņas praktiskajiem aspektiem.

4) Lai noslēgtu šādu administratīvu vienošanos, Revīzijas palāta sniedz autoram visu nepieciešamo informāciju par savu informācijas drošības sistēmu. Ja nepieciešams, var organizēt novērtējuma apmeklējumu.

5) Šādas administratīvās vienošanās noslēdz, pilnībā ievērojot kompetences piešķiršanas un lojālas sadarbības principus, kas izklāstīti Līguma par Eiropas Savienību 13. pantā. Tās noslēdz atbilstoši 10. panta 4. punktā paredzētajai procedūrai.

6) Ja nepastāv administratīva vienošanās ar konkrēto Savienības iestādi, struktūru vai aģentūru, trešo valsti vai starptautisku organizāciju par klasificētas informācijas sniegšanu Revīzijas palātai, Revīzijas palāta paraksta paziņojumu par apņemšanos aizsargāt saņemto klasificēto informāciju.

8. pants. **Klasificētas informācijas drošības prasību pārkāpumi, tās zudums vai apdraudēšana**

1) Drošības prasību pārkāpums ir personas tāda darbība vai bezdarbība, kas ir pretrunā šajā lēmumā un tā īstenošanas kārtībā paredzētajiem drošības noteikumiem.

2) Apdraudējums rodas gadījumos, kad drošības prasību pārkāpuma dēļ ESKI ir pilnībā vai daļēji izpausta nesankcionētām personām.

3) Par visiem drošības pārkāpumiem vai aizdomām par drošības pārkāpumiem nekavējoties ziņo Revīzijas palātas informācijas drošības institūcijai.

4) Ja ir zināms vai pastāv pamatotas aizdomas, ka ESKI ir apdraudēta vai zudusi, informācijas drošības iestāde informē Cilvēkresursu, finanšu un vispārējo lietu direkcijas vadītāju un Revīzijas palātas ģenerālsekretāru. Cilvēkresursu, finanšu un vispārējo lietu direkcijas vadītājs nekavējoties informē autora attiecīgo drošības iestādi. Minētais Revīzijas palātas direkcijas vadītājs veic izmeklēšanu, informējot Revīzijas palātas ģenerālsekretāru un autora drošības iestādi par rezultātiem un pasākumiem, kas veikti, lai novērstu situācijas atkārtošanos. Ja pārkāpumā iesaistīts Revīzijas palātas loceklis, pienākums rīkoties ir Revīzijas palātas priekšsēdētājam sadarbībā ar Revīzijas palātas ģenerālsekretāru.

5) Revīzijas palātas ierēdnim vai citam darbiniekam, kas ir atbildīgs par šajā lēmumā un tā īstenošanas kārtībā paredzēto drošības noteikumu pārkāpumu, piemēro sankcijas, kas paredzētas Eiropas Savienības Civildienesta noteikumos un Pārējo darbinieku nodarbināšanas kārtībā.

6) Ikvienam Revīzijas palātas loceklim, kas neievēro šā lēmuma noteikumus, piemēro Līguma 286. panta 6. punktā paredzētos pasākumus un sankcijas.

7) Personām, kuras ir atbildīgas par ESKI zudumu vai apdraudējumu, piemēro disciplināratbildību un/vai cita veida tiesvedību saskaņā ar spēkā esošajiem normatīvajiem aktiem.

9. pants. **Drošība ārējās iejaukšanās gadījumā**

1) Revīzijas palāta var uzticēt dalībvalstī reģistrētiem līgumslēdzējiem veikt uzdevumus, kas saistīti ar ESKI vai prasa piekļuvi tai, pamatojoties uz viņu noslēgto līgumu. Tas jo īpaši var notikt komunikācijas un informācijas sistēmu un datortīkla uzturēšanas jomā.

2) Ārējas iejaukšanās gadījumā Revīzijas palāta veic visus vajadzīgos drošības pasākumus, kas minēti šā panta 3. punktā, tostarp pieprasa objekta drošības pielaidi, lai nodrošinātu, ka kandidāti vai konkursa pretendenti visā konkursa un iepirkuma procedūras laikā, kā arī līgumslēdzēji un apakšuzņēmēji visā līguma darbības laikā aizsargā ESKI. Līgumslēdzēja iestāde nodrošina, ka šajā lēmumā paredzētie minimuma drošības standarti ir minēti līgumos, kas uzliek līgumslēdzējiem pienākumu tos ievērot.

3) Drošības noteikumi, iepirkuma procedūras, paraugi un modeļi līgumiem un apakšlīgumiem, kas saistīti ar piekļuvi ESKI, līgumu paziņojumi, norādes par apstākļiem, kad ir nepieciešama iestādes un personāla drošības pielaide, programmas vai projekta drošības instrukcijas, drošības aspektu vēstules, apmeklējumi un ESKI pārsūtīšana un pārvietošana saskaņā ar šādiem līgumiem un apakšlīgumiem atbilst noteikumiem, paraugiem un modeļiem, ko Eiropas Komisija izstrādājusi klasificētiem līgumiem Komisijas 2015. gada 13. marta Lēmumā (ES, Euratom) 2015/444 par drošības noteikumiem ES klasificētas informācijas aizsardzībai.

10. pants. **Lēmuma īstenošana un saistītie pienākumi**

1) Revīzijas palātas dienesti veic visus viņu kompetencē ietilpstošos nepieciešamos pasākumus, lai nodrošinātu, ka, rīkojoties ar ESKI vai jebkuru citu klasificētu informāciju vai glabājot to, piemēro šo lēmumu un attiecīgos īstenošanas noteikumus.

2) Ģenerālsekretārs ir iecēlējinstitūcija un institūcija, kas ir pilnvarota slēgt darba līgumus visiem ierēdņiem un pārējiem darbiniekiem. Ģenerālsekretārs var deleģēt Cilvēkresursu, finanšu un vispārējo lietu direkcijas vadībai pienākumu piešķirt ierēdņiem un citiem darbiniekiem atļauju piekļūt informācijai, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī, pildīt drošības akreditācijas institūcijas funkciju un pārraudzīt Revīzijas palātas sekretariātu attiecībā uz rīcību ar ESKI.

3) Ģenerālsekretārs ir pilnvarots noslēgt PLN par Revīzijas palātas komunikācijas un informācijas iekārtu un sistēmu akreditāciju, par drošības zonas izmantošanu citā Savienības iestādē un par procedūru attiecībā uz personīgās drošības pielaides pieprasījumiem piekļūt ESKI.

4) Cilvēkresursu, finanšu un vispārējo lietu direkcijas vadītājs ir pilnvarots slēgt administratīvās vienošanās ar Savienības iestādēm, aģentūrām un citām struktūrām par apmaiņu ar ESKI, kas Revīzijas palātai nepieciešama, lai īstenotu savas pilnvaras. Minētais direkcijas vadītājs var arī noslēgt administratīvās vienošanās ar trešām valstīm vai starptautiskām organizācijām par saņemtās klasificētās informācijas aizsardzību.

5) Cilvēkresursu, finanšu un vispārējo lietu direkcijas vadītājs ir pilnvarots parakstīt jebkuru paziņojumu par apņemšanos aizsargāt ESKI, kas jāsniedz saistībā ar ārkārtas un *ad hoc* nodošanu.

6) Revīzijas palātas informācijas drošības speciālists darbojas kā informācijas drošības institūcija. Informācijas drošības speciālistam un personām, kurām tā deleģē visus vai daļu savus uzdevumus, ir attiecīga drošības pielaide. Informācijas drošības institūcija pilda savus pienākumus ciešā sadarbībā ar Cilvēkresursu, finanšu un vispārējo lietu direkciju, Informācijas, darba vides un inovācijas direkciju un Revīzijas kvalitātes kontroles komitejas direkciju (sk. jo īpaši 4., 6. un 8. pantu). Informācijas drošības institūcija ir atbildīga arī par apmācību un izpratnes veidošanas sanāksmēm par informācijas drošību, kā arī par regulārām pārbaudēm, lai pārbaudītu atbilstību šim lēmumam, tostarp ārējās iejaukšanās gadījumā un saistībā ar visiem pasākumiem, kas veicami, lai nodrošinātu atbilstību.

7) Drošības dienesta vadītājs ir atbildīgs par fiziskās drošības pasākumiem (jo īpaši 5. panta izpratnē).

8) Reģistra birojs, kas izveidots Revīzijas palātas Sekretariātā, ir iekļūšanas un izkļūšanas punkts informācijai, kas klasificēta RESTREINT UE/EU RESTRICTED līmenī, ar kuru Revīzijas palāta var apmainīties ar citām Savienības iestādēm, aģentūrām, struktūrām, kā arī dalībvalstīm. Tas ir arī iekļūšanas un izkļūšanas punkts līdzvērtīgas informācijas apmaiņai ar trešām valstīm un starptautiskajām organizācijām. Reģistra biroju organizē, kā noteikts deleģētajā lēmumā. Reģistra kontrolieris uzņemas šādus galvenos pienākumus:

   a) reģistrē tādas informācijas iekļūšanu un izkļūšanu, kas klasificēta RESTREINT UE/EU RESTRICTED līmenī;

   b) pārvalda īpašās administratīvās zonas, kurās rīkojas ar RESTREINT UE/EU RESTRICTED līmenī klasificētu ESKI un kur to glabā un aplūko.

9) Saskaņā ar PLN par citas Savienības iestādes drošības zonas izmantošanu izveido reģistru. Šis reģistrs, kuru Revīzijas palātas Cilvēkresursu, finanšu un vispārējo lietu direkcijas vadītāja pārraudzībā organizē Revīzijas palātas sekretariāts, ir iekļūšanas un izkļūšanas punkts

informācijai, kas klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī, ar kuru Revīzijas palāta var apmainīties ar citām Savienības iestādēm, aģentūrām un struktūrām, kā arī dalībvalstīm. Tas ir arī iekļūšanas un izkļūšanas punkts līdzvērtīgas informācijas apmaiņai ar trešām valstīm un starptautiskajām organizācijām. Tas ir aprīkots ar atbilstīgiem seifiem un citām drošības iekārtām, kas piemērotas tādas informācijas aizsardzībai, kura klasificēta CONFIDENTIEL UE/EU CONFIDENTIAL vai augstākā līmenī. Reģistru organizē, kā noteikts deleģētajā lēmumā. Reģistra kontrolierim ir atbilstīga drošības pielaide, un viņš uzņemas šādus galvenos pienākumus:

a) pārvalda darbības, kas saistītas ar ESKI reģistrāciju, aplūkošanu, saglabāšanu, reproducēšanu, tulkošanu, pārraidi, nosūtīšanu un attiecīgā gadījumā arī iznīcināšanu,

b) uzņemas citus uzdevumus, kas saistīti ar ESKI aizsardzību un noteikti deleģētajā lēmumā.

10) Administratīvā komiteja pieņem deleģētu lēmumu, ar ko nosaka šā lēmuma īstenošanas kārtību. Informācijas drošības speciālists sagatavo informācijas drošības pamatnostādnes. Revīzijas kvalitātes kontroles komiteja izstrādā revīzijas pamatnostādnes.

<u>11. pants.</u> **Stāšanās spēkā**

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

Luksemburgā, 2021. gada 3. jūnijā

Revīzijas palātas vārdā —

Klaus-Heiner Lehne
priekšsēdētājs

Pielikums: FIZISKĀS DROŠĪBAS PASĀKUMI ATTIECĪBĀ UZ ESKI ADMINISTRATĪVAJĀM ZONĀM

PIELIKUMS

FIZISKĀS DROŠĪBAS PASĀKUMI ATTIECĪBĀ UZ ESKI ADMINISTRATĪVAJĀM ZONĀM

1) Šajā pielikumā ir izklāstīta lēmuma 5. panta īstenošanas kārtība. Šie ir minimālie noteikumi RESTREINT UE/EU RESTRICTED līmenī klasificētas informācijas administratīvo zonu fiziskai aizsardzībai Revīzijas palātā: zonas, kas paredzētas tādas informācijas reģistrēšanai, glabāšanai un aplūkošanai, kas klasificēta RESTREINT UE/EU RESTRICTED līmenī.

2) Administratīvās zonās ieviesto fiziskās drošības pasākumu mērķis ir novērst neatļautu piekļuvi šīm zonām, proti:

   a) izveido redzami nospraustu perimetru, kurā var pārbaudīt personas;

   b) piekļuvi bez eskorta piešķir tikai personām, kurām ir pienācīga Revīzijas palātas informācijas drošības institūcijas vai citas kompetentas iestādes atļauja; un

   c) visas pārējās personas vienmēr eskortē vai piemēro līdzvērtīgu kontroli.

3) Revīzijas palātas informācijas drošības institūcija izņēmuma kārtā var piešķirt piekļuvi nepiederošām personām, tostarp darbam administratīvā zonā, ar noteikumu, ka tas nav saistīts ar piekļuvi ESKI, kas paliek aiz slēgtām durvīm. Šādas personas drīkst ienākt tikai tad, ja tās pavada un pastāvīgi uzrauga informācijas drošības institūcija vai reģistra kontrolieris.

4) Informācijas drošības iestāde nosaka visu administratīvo zonu atslēgu un/vai kodu kombināciju un drošu mēbeļu pārvaldības procedūras. Šo procedūru mērķis ir aizsargāt pret neatļautu piekļuvi.

5) Kodu kombinācijas iegaumē pēc iespējas mazs to personu skaits, kam ir vajadzība tās zināt. Kodu kombinācijas drošajām mēbelēm, kurās glabā RESTREINT UE/EU RESTRICTED līmenī klasificētu informāciju, maina:

   - saņemot jaunu drošu mēbeli;
   - ja darbinieku lokā, kas zina šo kodu kombināciju, ir notikušas izmaiņas;
   - ja kombinācijai ir radies apdraudējums vai ir aizdomas, ka tas varētu būt radies;
   - veicot slēdzenes apkopi vai remontu;
   - vismaz reizi 12 mēnešos.

6) Informācijas drošības institūcija un Drošības dienesta vadītājs ir atbildīgi par šo noteikumu ievērošanu.