Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/2540

12.12.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/2540

(2025. gada 9. decembris),

ar ko paredz noteikumus Eiropas Parlamenta un Padomes Regulas (ES) 2019/881 piemērošanai attiecībā uz salīdzinošās izvērtēšanas plāna izveidi

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) ([1]), un jo īpaši tās 59. panta 5. punktu,

tā kā:

(1) Saskaņā ar Regulas (ES) 2019/881 59. panta 4. punktu valstu kiberdrošības sertifikācijas iestāžu salīdzinošā izvērtēšana jeb profesionālizvērtēšana jāveic divu citu dalībvalstu valsts kiberdrošības sertifikācijas iestādēm un Komisijai. Lai panāktu līdzvērtīgus standartus attiecībā uz Eiropas kiberdrošības sertifikātiem un ES atbilstības apliecinājumiem, Komisijai būtu jāuzrauga aspekti, kas saistīti ar atbilstību šai regulai, un jānodrošina, ka salīdzinošā izvērtēšana visā Savienībā tiek veikta konsekventi. Lai palīdzētu apzināt labu praksi, problēmas un pieredzi, kas gūta, īstenojot Eiropas kiberdrošības sertifikācijas shēmas, Eiropas Savienības Kiberdrošības aģentūrai (*ENISA*) vajadzētu būt iespējai piedalīties salīdzinošajā izvērtēšanā novērotāja statusā. Lai atbalstītu šīs regulas noteikumu saskaņotu īstenošanu, Eiropas Savienības Kiberdrošības aģentūrai sadarbībā ar Komisiju un Eiropas Kiberdrošības sertifikācijas grupu (*ECCG*) arī būtu jāļauj izstrādāt veidnes.

(2) Lai nodrošinātu paredzamu plānošanu un resursu efektīvu piešķiršanu, katras valsts kiberdrošības sertifikācijas iestādes salīdzinošā izvērtēšana būtu jāveic saskaņā ar noteiktu grafiku. Valsts kiberdrošības sertifikācijas iestādei vajadzētu būt iespējai pieprasīt, lai tās salīdzinošā izvērtēšana tiek atlikta ārkārtas apstākļos, piemēram, neparedzēta personāla trūkuma vai nepārvaramas varas gadījumos. Šajā nolūkā ir jānosaka minētā pieprasījuma novērtēšanas kārtība, nodrošinot, ka tiek ievērots vispārējais grafiks un netiek apdraudēti salīdzinošās izvērtēšanas mehānisma mērķi.

(3) Lai nodrošinātu, ka visas dalībvalstis sniedz ieguldījumu salīdzinošās izvērtēšanas mehānisma īstenošanā, kā arī lai dotu tām iespēju gūt labumu no savstarpējas mācīšanās, katras dalībvalsts valsts kiberdrošības sertifikācijas iestādēm piecu gadu laikposmā būtu jāveic divas salīdzinošās izvērtēšanas. Tādēļ būtu jāizveido rotācijas sistēma, lai visu dalībvalstu valsts kiberdrošības sertifikācijas iestādes varētu organizēt savu līdzdalību. Ir arī jānosaka kritēriji, kas valstu kiberdrošības sertifikācijas iestādēm būtu jāņem vērā, izraugoties pārstāvjus salīdzinošās izvērtēšanas veikšanai, lai nodrošinātu atbilstošas speciālās zināšanas un kompetenci. Valstu kiberdrošības sertifikācijas iestādēm būtu arī jāļauj piedalīties salīdzinošajā izvērtēšanā kā novērotājām, lai uzraudzītu procesu un mācītos no tā. Šādos gadījumos nebūtu jāprasa, lai to pārstāvim būtu tādas pašas speciālās zināšanas un kompetence, kādas tiek gaidītas no tiem valstu kiberdrošības sertifikācijas iestāžu pārstāvjiem, kuri veic salīdzinošo izvērtēšanu.

(4) Lai nodrošinātu, ka valsts kiberdrošības sertifikācijas iestādi salīdzinoši izvērtē vismaz viena valsts kiberdrošības sertifikācijas iestāde, kas izmanto tādu pašu pieeju sertifikātu izdošanai ar līmeni "augsts", *ENISA*, aicinot valstu kiberdrošības sertifikācijas iestādes paust ieinteresētību veikt salīdzinošo izvērtēšanu, būtu jānorāda, vai salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde tieši izdod sertifikātus ar līmeni "augsts", izmanto Regulas (ES) 2019/881 56. panta 6. punkta a) apakšpunktā minēto iepriekš apstiprināto modeli, piešķir vispārēju deleģējumu saskaņā ar minētā punkta b) apakšpunktu vai kombinē minētos noteikumus.

([1]) OV L 151, 7.6.2019., 15. lpp., ELI: http://data.europa.eu/eli/reg/2019/881/oj.

(5) Lai nodrošinātu kopīgus izvērtēšanas kritērijus un procedūras salīdzinošās izvērtēšanas veikšanai visā Savienībā, katrā salīdzinošajā izvērtēšanā vienmēr būtu jāiekļauj pašnovērtējuma anketa, dokumentācijas izvērtēšana un apmeklējums uz vietas, ko papildina intervijas. Pēc apmeklējuma uz vietas salīdzinošās izvērtēšanas komandai būtu jāapspriež konstatējumi ar salīdzinoši izvērtējamo valsts kiberdrošības sertifikācijas iestādi, jāsagatavo ziņojuma projekts un jāiesniedz tas salīdzinoši izvērtējamajai valsts kiberdrošības sertifikācijas iestādei komentāru sniegšanai, lai pēc iespējas nodrošinātu vienprātību. Galīgais ziņojums, kurā drīkst ietvert pamatnostādnes vai ieteikumus, kas ļautu veikt uzlabojumus salīdzinoši izvērtētajā valsts kiberdrošības sertifikācijas iestādē, salīdzinošās izvērtēšanas komandai būtu jāiesniedz Eiropas Kiberdrošības sertifikācijas grupai. Eiropas Kiberdrošības sertifikācijas grupai pēc salīdzinošās izvērtēšanas komandas priekšlikuma būtu arī jāapstiprina kopsavilkuma ziņojums, kas jādara publiski pieejams.

(6) Lai nodrošinātu, ka salīdzinošās izvērtēšanas procesā iegūtā informācija tiek apstrādāta drošā veidā, salīdzinošās izvērtēšanas komandai būtu jānodrošina drošu saziņas kanālu, piemēram, drošas platformas dokumentu glabāšanai un kopīgošanai, izmantošana un atbilstošu aizsardzības pasākumu izmantošana attiecībā uz konfidenciāliem datiem, ar kuriem apmainās salīdzinošās izvērtēšanas komandas locekļi. *ENISA*, ņemot vērā valstu kiberdrošības sertifikācijas iestāžu paraugpraksi, būtu arī jāspēj izstrādāt pamatnostādnes par to, kā nodrošināt drošu saziņu, jo īpaši, lai nodrošinātu, ka drošības līmenis, ko salīdzinošās izvērtēšanas komanda piemēro, vācot, kopīgojot un apstrādājot informāciju, ir saskaņots ar salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes drošības vajadzībām.

(7) Lai veicinātu sadarbību un efektīvu informācijas apmaiņu starp valstu kiberdrošības sertifikācijas iestādēm, *ECCG* un jo īpaši tās salīdzinošās izvērtēšanas jautājumu apakšgrupai, būtu jāveicina veidņu izstrāde, kā arī jāpalīdz Komisijai īstenot šo regulu.

(8) Salīdzinošās izvērtēšanas mehānisms ir Eiropas digitālais sabiedriskais pakalpojums Eiropas Parlamenta un Padomes Regulas (ES) 2024/903 ([2]) nozīmē. Ar šo regulu ievieš jaunas saistošas prasības, kas ietekmē minēto pakalpojumu, un tādējādi uz to attiecas sadarbspējas novērtēšanas pienākums saskaņā ar Regulas (ES) 2024/903 3. pantu. Attiecīgi ir veikts sadarbspējas novērtējums, un no tā izrietošais ziņojums ir jāpublicē Sadarbspējīgas Eiropas portālā.

(9) Izstrādājot šo regulu, Komisija ir ņēmusi vērā *ECCG*, tai skaitā tās salīdzinošās izvērtēšanas jautājumu apakšgrupas, viedokļus.

(10) Šajā regulā noteiktie pasākumi ir saskaņā ar atzinumu, ko sniegusi ar Regulas (ES) 2019/881 66. pantu izveidotā komiteja,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Salīdzinošās izvērtēšanas grafiks, biežums un izmaksas

1. Valstu kiberdrošības sertifikācijas iestāžu salīdzinošo izvērtēšanu veic saskaņā ar grafiku, kas noteikts I pielikumā. Katru salīdzinošo izvērtēšanu pabeidz līdz grafikā norādītajam datumam, un pēc tam to veic reizi piecos gados.

2. Ārkārtas apstākļos salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde drīkst iesniegt Komisijai pienācīgi pamatotu pieprasījumu atlikt tās salīdzinošo izvērtēšanu uz vēlāku laiku pēc I pielikumā noteiktajā grafikā norādītā datuma. Komisija sadarbībā ar Eiropas Kiberdrošības sertifikācijas grupu (*ECCG*), kas izveidota ar Regulas (ES) 2019/881 62. pantu, bez kavēšanās novērtē pieprasījumu un informē visas attiecīgās puses par iznākumu.

([2]) Eiropas Parlamenta un Padomes Regula (ES) 2024/903 (2024. gada 13. marts), ar ko nosaka pasākumus augsta līmeņa publiskā sektora sadarbspējai visā Savienībā (Sadarbspējīgas Eiropas akts) (OV L, 2024/903, 22.3.2024., ELI: http://data.europa.eu/eli/reg/2024/903/oj).

3. Ja dalībvalsts saskaņā ar Regulas (ES) 2019/881 58. panta 1. punktu ir izraudzījusies:

a) vairāk nekā vienu valsts kiberdrošības sertifikācijas iestādi tās teritorijā, visām minētās dalībvalsts kiberdrošības sertifikācijas iestādēm salīdzinošo izvērtēšanu veic vienā laikā;

b) vienu vai vairākas valsts kiberdrošības sertifikācijas iestādes citā dalībvalstī, minētās valsts kiberdrošības sertifikācijas iestādes vai minēto valsts kiberdrošības sertifikācijas iestāžu salīdzinošo izvērtēšanu drīkst veikt pēc grafika, kas noteikts vai nu attiecībā uz dalībvalsti, kas veikusi izraudzīšanos, vai arī attiecībā uz dalībvalsti, kurā atrodas izraudzītā valsts kiberdrošības sertifikācijas iestāde vai izraudzītās valsts kiberdrošības sertifikācijas iestādes, attiecībā uz uzraudzības uzdevumiem, ko veic norīkotājā dalībvalstī.

4. Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) Eiropas kiberdrošības sertifikācijas shēmu tīmekļa vietnē, kas izveidota saskaņā ar Regulas (ES) 2019/881 50. pantu, dara publiski pieejamu šādu informāciju:

a) informācija par I pielikumā noteikto grafiku;

b) salīdzinošo izvērtēšanu veicošo valstu kiberdrošības sertifikācijas iestāžu sarakstu, ko uztur saskaņā ar 2. panta 5. punktu.

5. Katra valsts kiberdrošības sertifikācijas iestāde, kas iesaistīta salīdzinošās izvērtēšanas procesā, sedz savas dalības izmaksas.

2. pants

Salīdzinošo izvērtēšanu veicošo valsts kiberdrošības sertifikācijas iestāžu rotācijas sistēma

1. Saskaņā ar Regulas (ES) 2019/881 59. panta 4. punktu katru salīdzinošo izvērtēšanu veic divas citu dalībvalstu salīdzinošo izvērtēšanu veicošās valsts kiberdrošības sertifikācijas iestādes un Komisija. Katras dalībvalsts valsts kiberdrošības sertifikācijas iestādes katrā I pielikumā noteiktajā laikposmā piedalās vismaz divu valsts kiberdrošības sertifikācijas iestāžu salīdzinošajā izvērtēšanā.

2. Citu dalībvalstu valsts kiberdrošības sertifikācijas iestādes drīkst piedalīties salīdzinošajā izvērtēšanā kā novērotāji ar vienu vai vairākiem pārstāvjiem, vienojoties ar salīdzinoši izvērtējamo valsts kiberdrošības sertifikācijas iestādi, salīdzinošo izvērtēšanu veicošajām valsts kiberdrošības sertifikācijas iestādēm un Komisiju.

3. Viens *ENISA* pārstāvis drīkst piedalīties salīdzinošajā izvērtēšanā kā novērotājs. Ar salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes, salīdzinošo izvērtēšanu veicošo valsts kiberdrošības sertifikācijas iestāžu un Komisijas piekrišanu drīkst piedalīties arī papildu pārstāvji.

4. Novērotājiem ir piekļuve tādai pašai informācijai kā pārējiem salīdzinošās izvērtēšanas komandas dalībniekiem, bet viņi neveic uzdevumus, kas saistīti ar salīdzinošās izvērtēšanas veikšanu.

5. *ENISA* sadarbībā ar Komisiju un *ECCG* ierosina un uztur sarakstu ar valstu kiberdrošības sertifikācijas iestādēm, kuras veic salīdzinošo izvērtēšanu un kurām jāpilda uzdevumi I pielikumā noteiktajā grafikā. Konkrētā gadā *ENISA* sadarbībā ar Komisiju lūdz valstu kiberdrošības sertifikācijas iestādēm izteikt ieinteresētību veikt salīdzinošo izvērtēšanu attiecībā uz tām valstu kiberdrošības sertifikācijas iestādēm, kuru izvērtēšana saskaņā ar I pielikumu veicama nākamajā gadā, vai piedalīties tajā novērotāja statusā.

6. Ja interesi par vienas un tās pašas valsts kiberdrošības sertifikācijas iestādes salīdzinošās izvērtēšanas veikšanu pauž vairāk nekā divas valsts kiberdrošības sertifikācijas iestādes, Komisija un *ENISA* apspriežas ar ieinteresētajām valstu kiberdrošības sertifikācijas iestādēm un lemj par salīdzinošās izvērtēšanas dalībniekiem.

7. Ja konkrētā gadā nav pietiekami daudz salīdzinošo izvērtēšanu veicošo valstu kiberdrošības sertifikācijas iestāžu, kas pauž interesi veikt salīdzinošo izvērtēšanu, Komisija pēc apspriešanās ar *ECCG* izraugās valstu kiberdrošības sertifikācijas iestādes, kurām jāveic salīdzinošā izvērtēšana. Veicot atlasi, Komisija ņem vērā katras dalībvalsts valsts kiberdrošības sertifikācijas iestāžu pienākumu piedalīties vismaz divu valsts kiberdrošības sertifikācijas iestāžu salīdzinošajā izvērtēšanā, kā minēts 1. punktā.

3. pants

Salīdzinošās izvērtēšanas komandas sastāva kritēriji

1. Savlaicīgi pirms salīdzinošās izvērtēšanas sākuma katra salīdzinošo izvērtēšanu veicošā valsts kiberdrošības sertifikācijas iestāde ieceļ vienu pārstāvi salīdzinošās izvērtēšanas veikšanai. Salīdzinošo izvērtēšanu veicošās valsts kiberdrošības sertifikācijas iestādes drīkst iecelt vairāk nekā vienu pārstāvi, ja tas ir nepieciešams, lai nodrošinātu, ka salīdzinošās izvērtēšanas komandai ir nepieciešamās zināšanas, lai veiktu salīdzinošo izvērtēšanu.

2. Salīdzinošo izvērtēšanu veicošās valsts kiberdrošības sertifikācijas iestādes pārstāvis, izņemot tos valsts kiberdrošības sertifikācijas iestāžu pārstāvjus, kuri piedalās novērotāju statusā, atbilst šādiem kritērijiem:

a) vismaz divu gadu darba pieredze salīdzinošo izvērtēšanu veicošās valsts kiberdrošības sertifikācijas iestādē vai dalība vismaz divās salīdzinošajās izvērtēšanās novērotāja statusā;

b) pietiekamas zināšanas par Regulā (ES) 2019/881 noteikto kiberdrošības sertifikācijas satvaru;

c) labas angļu valodas zināšanas darbam nepieciešamajā līmenī un, ja iespējams, vienas vai vairāku tādu valodu zināšanas, kurās runā salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes dalībvalstī;

d) neatkarība no salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes.

3. Salīdzinošo izvērtēšanu veicošās valsts kiberdrošības sertifikācijas iestādes nodrošina, ka par jebkuru interešu konflikta risku attiecībā uz ieceltajiem pārstāvjiem pārējās valsts kiberdrošības sertifikācijas iestādes, Komisija un *ENISA* tiek informētas pirms salīdzinošās izvērtēšanas procesa sākuma. Salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde drīkst iebilst pret konkrētu pārstāvju iecelšanu saskaņā ar 5. punktu.

4. Lai koordinētu salīdzinošo izvērtēšanu, salīdzinošo izvērtēšanu veicošās valsts kiberdrošības sertifikācijas iestādes no sava vidus izvēlas vienu pārstāvi (“komandas vadītājs”).

5. Komisija pirms salīdzinošās izvērtēšanas procesa sākuma paziņo salīdzinoši izvērtējamajai valsts kiberdrošības sertifikācijas iestādei salīdzinošo izvērtēšanu veicošo valsts kiberdrošības sertifikācijas iestāžu pārstāvju vārdus un kontaktinformāciju. Ja salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde vēlas iebilst pret viena vai vairāku pārstāvju iecelšanu, tā divu nedēļu laikā sniedz Komisijai skaidru pamatojumu, informē *ENISA* un *ECCG* un pieprasa, lai salīdzinošo izvērtēšanu veicošā valsts kiberdrošības sertifikācijas iestāde ieceļ citu pārstāvi.

6. Ja 5. punktā izklāstītā procedūra ārkārtas apstākļu dēļ nepamatoti kavē salīdzinošās izvērtēšanas sākšanu, par salīdzinošās izvērtēšanas komandas sastāvu lemj Komisija, apspriežoties ar *ENISA* un *ECCG*.

4. pants

Salīdzinošās izvērtēšanas metodika

1. Salīdzinošajā izvērtēšanā novērtē II pielikumā uzskaitītos aspektus saskaņā ar Regulas (ES) 2019/881 59. panta 3. punktu.

2. *ENISA* sadarbībā ar *ECCG* un Komisiju drīkst izstrādāt veidnes, lai novērtētu procesus, ko izveidojusi salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde.

3. Salīdzinošā izvērtēšana ietver šādus elementus:

a) pašnovērtējuma anketa;

b) attiecīgo dokumentu novērtējums;

c) tiešsaistes vai klātienes intervijas, vai abas;

d) apmeklējums uz vietas.

4. Par salīdzinošās izvērtēšanas ilgumu drīkst iepriekš vienoties salīdzinošās izvērtēšanas komanda un salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde atkarībā no salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes darbības apjoma un sarežģītības. Apmeklējums uz vietas ilgst ne vairāk kā trīs darba dienas.

5. Ja vien salīdzinošās izvērtēšanas komanda, salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde un Komisija nevienojas citādi, sadarbības valoda ir angļu valoda. Salīdzinošās izvērtēšanas ziņojumu, kas minēts 5. pantā, sagatavo vismaz angļu valodā.

6. Salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde sadarbojas un nodrošina salīdzinošās izvērtēšanas komandai piekļuvi informācijai un dokumentiem, kas vajadzīgi salīdzinošās izvērtēšanas veikšanai. Salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde vismaz 21 dienu pirms apmeklējuma uz vietas iesniedz pašnovērtējuma anketu un jaunāko gada kopsavilkuma ziņojumu, kas pieņemts saskaņā ar Regulas (ES) 2019/881 58. panta 7. punkta g) apakšpunktu. Papildu dokumentus iesniedz pēc salīdzinošās izvērtēšanas komandas pieprasījuma septiņu dienu laikā pēc šādu pieprasījumu saņemšanas.

7. Dokumentus iesniedz angļu valodā, ja vien saskaņā ar 5. punktu nav panākta citāda vienošanās. Ja dokumenti nav iesniegti angļu valodā, salīdzinošās izvērtēšanas komanda drīkst pieprasīt, lai dokumenti, kas vajadzīgi salīdzinošās izvērtēšanas veikšanai, tiktu tulkoti angļu valodā.

8. Pirms salīdzinošās izvērtēšanas ziņojuma sagatavošanas saskaņā ar 5. pantu salīdzinošās izvērtēšanas komanda apspriež sākotnējos konstatējumus ar salīdzinoši izvērtējamo valsts kiberdrošības sertifikācijas iestādi.

5. pants

Salīdzinošās izvērtēšanas ziņojums

1. Divdesmit vienas dienas laikā pēc salīdzinošās izvērtēšanas veikšanas salīdzinošās izvērtēšanas komanda sagatavo salīdzinošās izvērtēšanas ziņojuma projektu, kurā iekļauj sīku informāciju par salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes dalībvalsti, salīdzinošo izvērtēšanu veicošo valsts kiberdrošības sertifikācijas iestādi, Komisiju un jebkuru novērotāju, kā arī salīdzinošās izvērtēšanas konstatējumus un secinājumus. Vajadzības gadījumā ziņojumā iekļauj ieteikumus, kā panākt uzlabojumus aspektos, uz kuriem attiecas salīdzinošā izvērtēšana.

2. *ENISA* sadarbībā ar Komisiju un *ECCG* drīkst izstrādāt salīdzinošās izvērtēšanas ziņojuma veidni.

3. Pēc salīdzinošās izvērtēšanas ziņojuma projekta sagatavošanas saskaņā ar 1. punktu salīdzinošās izvērtēšanas komanda to iesniedz salīdzinoši izvērtējamajai valsts kiberdrošības sertifikācijas iestādei, lai tā 14 dienu laikā varētu sniegt komentārus. Salīdzinošās izvērtēšanas komanda izvērtē komentārus un, ja iespējams, integrē tos galīgajā ziņojumā, lai nodrošinātu vienprātību. Domstarpību gadījumā salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes atbildi pievieno galīgajam ziņojumam.

4. Galīgo ziņojumu, tai skaitā kopsavilkumu publicēšanai, divu mēnešu laikā pēc salīdzinošās izvērtēšanas veikšanas nosūta *ECCG*. Saskaņā ar Regulas (ES) 2019/881 59. panta 6. punktu *ECCG* izskata ziņojumu un apstiprina tā kopsavilkumu, ko publicē Eiropas kiberdrošības sertifikācijas shēmu tīmekļa vietnē, kas izveidota saskaņā ar Regulas (ES) 2019/881 50. pantu. Kopsavilkumā iekļauj arī salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes atbildi vai tās daļas, vienojoties ar salīdzinoši izvērtējamo valsts kiberdrošības sertifikācijas iestādi.

5. Pirms salīdzinošās izvērtēšanas ziņojuma izplatīšanas ārpus salīdzinošās izvērtēšanas komandas ietvariem salīdzinošās izvērtēšanas komanda anonimizē personas datus, ko tā, iespējams, ir savākusi salīdzinošās izvērtēšanas laikā.

6. pants

Konfidencialitāte

1. Visas puses, kas ir iesaistītas salīdzinošajā izvērtēšanā, ievēro savu uzdevumu un darbību veikšanā iegūtās informāciju un datu konfidencialitāti tādā veidā, lai jo īpaši aizsargātu:

a) intelektuālā īpašuma tiesības un fiziskas vai juridiskas personas konfidenciālu uzņēmējdarbības informāciju vai komercnoslēpumus, ieskaitot pirmkodu, izņemot gadījumus, kas minēti Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/943 ([3]) 5. pantā;

b) šīs regulas efektīvu īstenošanu;

c) sabiedrības un valsts drošības intereses;

d) kriminālprocesu vai administratīvo procesu neaizskaramību.

2. Salīdzinošās izvērtēšanas komanda nodrošina, ka visa informācija, kas iegūta salīdzinošās izvērtēšanas procesā, tiek apstrādāta droši. Kad ir sagatavots galīgais ziņojums un 5. panta 4. punktā minētais kopsavilkums, salīdzinošās izvērtēšanas komanda, tai skaitā jebkurš novērotājs, dzēš vai iznīcina visus dokumentus, kas savākti vai ģenerēti salīdzinošās izvērtēšanas procesā, izņemot galīgo ziņojumu un kopsavilkumu.

3. *ENISA*, ņemot vērā valstu kiberdrošības sertifikācijas iestāžu pašreizējo paraugpraksi, sadarbībā ar *ECCG* var izstrādāt pamatnostādnes par drošu un konfidenciālu saziņu.

([3]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/943 (2016. gada 8. jūnijs) par zinātības un darījumdarbības neizpaužamas informācijas (komercnoslēpumu) aizsardzību pret nelikumīgu iegūšanu, izmantošanu un izpaušanu (OV L 157, 15.6.2016., 1. lpp., ELI: http://data.europa.eu/eli/dir/2016/943/oj).

7. pants

Spēju veidošana

ENISA analizē salīdzinošo izvērtēšanu apkopotos rezultātus un izceļ gūto pieredzi un paraugpraksi, lai veicinātu valstu kiberdrošības sertifikācijas iestāžu spēju veidošanu un Eiropas kiberdrošības sertifikācijas shēmu uzturēšanu. Minētā analīze attiecīgā gadījumā drīkst ietvert apmācību un papildu pamatnostādnes valstu kiberdrošības sertifikācijas iestādēm, kas izstrādātas sadarbībā ar *ECCG*.

8. pants

Stāšanās spēkā

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2025. gada 9. decembrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

I PIELIKUMS

Valstu kiberdrošības sertifikācijas iestāžu saraksts, uz kurām attiecas salīdzinošā izvērtēšana

Līdz 2026. gada 31. decembrim un pēc tam reizi piecos gados veic šādu dalībvalstu valsts kiberdrošības sertifikācijas iestāžu salīdzinošo izvērtēšanu:

Zviedrija, Beļģija, Slovākija, Vācija, Malta, Čehija.

Līdz 2027. gada 31. decembrim un pēc tam reizi piecos gados veic šādu dalībvalstu valsts kiberdrošības sertifikācijas iestāžu salīdzinošo izvērtēšanu:

Ungārija, Grieķija, Igaunija, Slovēnija, Nīderlande, Itālija.

Līdz 2028. gada 31. decembrim un pēc tam reizi piecos gados veic šādu dalībvalstu valsts kiberdrošības sertifikācijas iestāžu salīdzinošo izvērtēšanu:

Horvātija, Dānija, Lietuva, Spānija, Bulgārija, Īrija.

Līdz 2029. gada 31. decembrim un pēc tam reizi piecos gados veic šādu dalībvalstu valsts kiberdrošības sertifikācijas iestāžu salīdzinošo izvērtēšanu:

Somija, Austrija, Rumānija, Luksemburga, Latvija, Polija.

Līdz 2030. gada 31. decembrim un pēc tam reizi piecos gados veic šādu dalībvalstu valsts kiberdrošības sertifikācijas iestāžu salīdzinošo izvērtēšanu:

Kipra, Francija, Portugāle, Lihtenšteina, Norvēģija, Islande.

II PIELIKUMS

Salīdzinošās izvērtēšanas metodika

II.1. **Sertifikācijas un uzraudzības darbību nodalīšana**

Novērtējot Regulas (ES) 2019/881 59. panta 3. punkta a) apakšpunktā minēto salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes sertifikācijas darbību un uzraudzības darbību nodalīšanu, salīdzinošajā izvērtēšanā novērtē vismaz šādus aspektus:

a) detalizētu aprakstu par salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes darbību, skaidri norādot dažādās struktūras un/vai departamentus, kas iesaistīti Regulas (ES) 2019/881 īstenošanā;

b) salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes darbību kartēšana ar Regulas (ES) 2019/881 58. panta 7. punktā uzskaitītajām darbībām;

c) ja salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde izdod sertifikātus, paskaidrojums, kas pierāda, ka starp tās sertifikācijas darbībām un b) apakšpunktā minētajām uzraudzības darbībām nav nekādas iejaukšanās.

II.2. **Uzraudzība un noteikumu izpildes panākšana, ar ko pārrauga atbilstību sertifikātiem**

Atbilstīgi Regulas (ES) 2019/881 59. panta 3. punkta b) apakšpunktam novērtējot salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes uzraudzības un noteikumu izpildes panākšanas procedūras, ar ko pārrauga IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu atbilstību Eiropas kiberdrošības sertifikātiem, salīdzinošajā izvērtēšanā novērtē vismaz šādus aspektus:

a) šādu procesu un procedūru kvalitāti un detalizēta apraksta līmeni un to, cik lielā mērā tie ir dokumentēti;

b) vai un cik lielā mērā šādi procesi un procedūras aptver attiecīgās Eiropas kiberdrošības sertifikācijas shēmas;

c) vai salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde ir faktiski pilnvarota pārbaudīt atbilstības novērtēšanas struktūras, kas izdod sertifikātus, un vajadzības gadījumā panākt sertifikātu atsaukšanu;

d) cik lielā mērā salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde sadarbojas ar attiecīgajām tirgus uzraudzības iestādēm;

e) vai salīdzinoši izvērtējamajai valsts kiberdrošības sertifikācijas iestādei ir mehānisms fizisku vai juridisku personu sūdzību izskatīšanai, kas prasīts saskaņā ar Regulas (ES) 2019/881 58. panta 7. punkta f) apakšpunktu, tai skaitā pierādījumi par to, vai fiziskām un juridiskām personām ir tiesības iesniegt sūdzību un saņemt efektīvu tiesību aizsardzību tiesā saskaņā ar minētās regulas attiecīgi 63. un 64. pantu.

II.3. **Ražotāju vai pakalpojumu sniedzēju pienākumu pārraudzība un izpildes panākšana**

Atbilstīgi Regulas (ES) 2019/881 59. panta 3. punkta c) apakšpunktam novērtējot salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes procedūras, kas paredzētas ražotāju vai pakalpojumu sniedzēju pienākumu pārraudzībai un izpildes panākšanai, salīdzinošajā izvērtēšanā novērtē vismaz šādus aspektus:

a) vai salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde ir izveidojusi šādas procedūras un cik lielā mērā tās ir dokumentētas, jo īpaši, vai tā ir izveidojusi mehānismu informācijas saņemšanai no ārējiem avotiem un tās apstrādei;

b) vai un cik lielā mērā šādas procedūras aptver attiecīgās Eiropas kiberdrošības sertifikācijas shēmas;

c) vai un cik lielā mērā salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde veic pati savu izmeklēšanu un vai izmeklēšanas tvērums aptver ražotāju pienākumus, kas noteikti Regulas (ES) 2019/881 53. panta 2. un 3. punktā un attiecīgajās Eiropas kiberdrošības sertifikācijas shēmās;

d) vai pastāv procedūra informācijas apmaiņai starp salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes sertifikācijas darbībām un uzraudzības darbībām, kas attiecas uz ražotāju vai pakalpojumu sniedzēju pienākumu pārraudzību un izpildes panākšanu.

II.4. **Atbilstības novērtēšanas struktūru pārraudzība, pilnvarošana un uzraudzība**

Atbilstīgi Regulas (ES) 2019/881 59. panta 3. punkta d) apakšpunktam novērtējot salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes procedūras attiecībā uz atbilstības novērtēšanas struktūru darbību pārraudzību, pilnvarošanu un uzraudzību, salīdzinošajā izvērtēšanā novērtē vismaz šādus aspektus:

a) šādu procedūru kvalitāti un detalizēta apraksta līmeni un to, cik lielā mērā tās ir dokumentētas, tai skaitā attiecībā uz sadarbību ar valsts akreditācijas struktūru;

b) galvenos statistikas datus par piešķirto, apturēto vai atsaukto atļauju skaitu, aktīvo atbilstības novērtēšanas struktūru kopējo skaitu, izdoto sertifikātu skaitu un salīdzinoši izvērtējamās valsts kiberdrošības sertifikācijas iestādes veikto korektīvo pasākumu skaitu;

c) ja salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde ļauj izdot Eiropas kiberdrošības sertifikātus ar līmeni "augsts" pēc iepriekšēja apstiprinājuma vai pamatojoties uz vispārēju uzdevuma deleģējumu, kā noteikts Regulas (ES) 2019/881 56. panta 6. punktā, darbinieku lietpratību un procedūras, ar kuru palīdzību salīdzinoši izvērtējamā valsts kiberdrošības sertifikācijas iestāde pārrauga un uzrauga atbilstības novērtēšanas struktūru darbības.