Euroopa Liidu
Teataja

ET
L-seeria

2025/2540

12.12.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/2540,

9. detsember 2025,

milles sätestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses vastastikuse hindamise kava koostamisega

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrust (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus), ([1]) eriti selle artikli 59 lõiget 5,

ning arvestades järgmist:

(1) Määruse (EL) 2019/881 artikli 59 lõike 4 kohaselt viivad vastastikuse hindamise läbi vähemalt kaks muu liikmesriigi riiklikku küberturvalisuse sertifitseerimise asutust ja komisjon. Et saavutada Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide puhul võrdväärsed standardid, peaks komisjon jälgima käesoleva määruse nõuetele vastavusega seotud aspekte ja tagama, et vastastikusi hindamisi tehakse järjepidevalt kogu liidus. Et aidata sõeluda välja Euroopa küberturvalisuse sertifitseerimise kavade rakendamise head tavad, teha kindlaks sellega seotud probleemid ja tuua esile õppetunnid, peaks Euroopa Liidu Küberturvalisuse Ametil (ENISA) olema võimalus osaleda vastastikustes hindamistes vaatlejana. Et toetada käesoleva määruse sätete ühtlustatud rakendamist, peaks ENISA-l olema lubatud töötada koostöös komisjoni ja Euroopa küberturvalisuse sertifitseerimise rühmaga välja näidisvorme.

(2) Planeerimise prognoositavuse ja vahendite tulemusliku jaotamise tagamiseks tuleks vastastikused hindamised teha vastavalt kehtestatud ajakavale. Riiklikul küberturvalisuse sertifitseerimise asutusel peaks olema võimalik taotleda erandlikel asjaoludel, nagu ootamatu personalipuudus või vääramatu jõud, vastastikuse hindamise edasilükkamist. Selleks on vaja kehtestada sellise taotluse hindamise kord, tagades sealjuures üldise ajakava ja vastastikuse hindamise mehhanismi eesmärkide järgimise.

(3) Et kõik liikmesriigid aitaksid vastastikuse hindamise mehhanismi rakendamisele kaasa ja saaksid üksteise kogemusest õppida, peaks iga liikmesriigi riiklikud küberturvalisuse sertifitseerimise asutused tegema viie aasta jooksul kaks vastastikust hindamist. Et võimaldada kõigi liikmesriikide riiklikel küberturvalisuse sertifitseerimise asutustel oma osalemist planeerida, tuleks luua asjakohane rotatsioonisüsteem. Samuti on vaja sätestada kriteeriumid, mida riiklikud küberturvalisuse sertifitseerimise asutused peaksid vastastikuse hindamise tegemiseks esindajate valimisel arvesse võtma, et tagada piisav oskusteave ja pädevus. Et jälgida protsessi ja õppida sellest, peaksid riiklikud küberturvalisuse sertifitseerimise asutused saama vastastikuses hindamises osaleda ka vaatlejana. Sellistel juhtudel ei tohiks nõuda, et nende esindajal oleksid samad teadmised ja pädevus, mida eeldatakse vastastikust hindamist tegeva riikliku küberturvalisuse sertifitseerimise asutuse esindajatelt.

(4) Tagamaks, et iga riiklikku küberturvalisuse sertifitseerimise asutust hindab vähemalt üks selline riiklik küberturvalisuse sertifitseerimise asutus, mis järgib kõrge usaldusväärsuse taseme sertifikaatide väljaandmisel sama lähenemisviisi, peaks ENISA, kui ta kutsub riiklikke küberturvalisuse sertifitseerimise asutusi avaldama huvi vastastikuse hindamise läbiviimise vastu, märkima, kas hinnatav küberturvalisuse sertifitseerimise asutus annab välja otse kõrge usaldusväärsuse taseme sertifikaate, lähtub määruse (EL) 2019/881 artikli 56 lõike 6 punktis a osutatud eelneva heakskiidu meetodist, delegeerib sertifikaadi väljaandmise kõnealuse lõike punkti b kohaselt või kombineerib neid meetodeid.

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

(5) Et tagada kogu liidus vastastikuse hindamise läbiviimiseks ühised hindamiskriteeriumid ja -menetlused, peaksid kõik vastastikused hindamised sisaldama enesehindamise küsimustiku täitmist, dokumentide hindamist ja kohapealset kontrollkäiku, millega kaasnevad intervjuud. Pärast kohapealset kontrollkäiku peaks vastastikuse hindamise rühm arutama tulemusi hinnatava küberturvalisuse sertifitseerimise asutusega, koostama aruande kavandi ja esitama selle hinnatavale küberturvalisuse sertifitseerimise asutusele märkuste tegemiseks, püüdes võimaluse korral jõuda temaga üksmeelele. Vastastikuse hindamise rühm peaks esitama Euroopa küberturvalisuse sertifitseerimise rühmale lõpparuande, mis võib sisaldada suuniseid või soovitusi, mille alusel saab hinnatav riiklik küberturvalisuse sertifitseerimise asutus oma tegevust täiustada. Euroopa küberturvalisuse sertifitseerimise rühm peaks vastastikuse hindamise rühma ettepanekul kinnitama ka kokkuvõtva aruande, mis tehakse üldsusele kättesaadavaks.

(6) Tagamaks, et vastastikuse hindamise käigus saadud teavet käideldakse turvaliselt, peaks vastastikuse hindamise rühm kasutama turvalisi sidekanaleid, nagu dokumentide salvestamise ja jagamise turvaline platvorm, ning vastastikuse hindamise rühma liikmete vahel konfidentsiaalsete andmete jagamise korral tuleks kasutada asjakohaseid kaitsemeetmeid. Võttes arvesse riiklike küberturvalisuse sertifitseerimise asutuste praegusi parimaid tavasid, peaks ENISA-l olema võimalik välja töötada suunised ka selle kohta, kuidas tagada turvaline side, pidades eelkõige silmas seda, et turvalisuse tase, mida vastastikuse hindamise rühm teabe kogumisel, jagamisel ja töötlemisel kohaldab, oleks kooskõlas hinnatava riikliku küberturvalisuse sertifitseerimise asutuse turbevajadustega.

(7) Et hõlbustada koostööd ja tõhusat teabevahetust riiklike küberturvalisuse sertifitseerimise asutuste vahel, peaksid Euroopa küberturvalisuse sertifitseerimise rühm ja selle vastastikuse hindamise alarühm aitama kaasa näidisvormide väljatöötamisele ning abistama komisjoni käesoleva määruse rakendamisel.

(8) Vastastikuse hindamise mehhanism kujutab endast üleeuroopalist digitaalset avalikku teenust Euroopa Parlamendi ja nõukogu määruse (EL) 2024/903 ([2]) tähenduses. Käesoleva määrusega kehtestatakse uued siduvad nõuded, mis mõjutavad nimetatud teenust, ning seetõttu kohaldatakse selle suhtes määruse (EL) 2024/903 artikli 3 kohast koostalitlusvõime hindamise kohustust. Sellest tulenevalt on tehtud koostalitlusvõime hindamine, mille põhjal koostatud aruanne avaldatakse Koostalitleva Euroopa portaalis.

(9) Käesoleva määruse väljatöötamisel on komisjon võtnud arvesse Euroopa küberturvalisuse sertifitseerimise rühma ja selle vastastikuse hindamise alarühma seisukohti.

(10) Käesoleva määrusega ette nähtud meetmed on kooskõlas määruse (EL) 2019/881 artikli 66 kohaselt asutatud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Vastastikuse hindamise ajakava, sagedus ja maksumus

1. Riiklike küberturvalisuse sertifitseerimise asutuste vastastikune hindamine toimub vastavalt I lisas esitatud ajakavale. Vastastikune hindamine viiakse lõpule ajakavas osutatud kuupäevaks ja seejärel tehakse hindamisi iga viie aasta tagant.

2. Erandlikel asjaoludel võib hinnatav riiklik küberturvalisuse sertifitseerimise asutus esitada komisjonile nõuetekohaselt põhjendatud taotluse lükata vastastikune hindamine edasi I lisas sätestatud ajakavas osutatust hilisemale kuupäevale. Komisjon hindab taotlust koostöös määruse (EL) 2019/881 artiklis 62 kehtestatud Euroopa küberturvalisuse sertifitseerimise rühmaga ja teavitab hindamise tulemusest õigeaegselt kõiki asjaomaseid osalisi.

([2]) Euroopa Parlamendi ja nõukogu 13. märtsi 2024. aasta määrus (EL) 2024/903, millega kehtestatakse meetmed avaliku sektori koostalitlusvõime kõrge taseme tagamiseks kogu liidus (Koostalitleva Euroopa määrus) (ELT L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

3. Kui liikmesriik on kooskõlas määruse (EL) 2019/881 artikli 58 lõikega 1:

a) määranud oma territooriumil rohkem kui ühe riikliku küberturvalisuse sertifitseerimise asutuse, toimub vastastikune hindamine kõigi selle liikmesriigi riiklike küberturvalisuse sertifitseerimise asutuste puhul paralleelselt;

b) määranud ühe või mitu teise liikmesriigi riikliku küberturvalisuse sertifitseerimise asutust, võib sellist riikliku küberturvalisuse sertifitseerimise asutust hinnata kas vastavalt ajakavale, mis on kehtestatud määrava liikmesriigi jaoks, või ajakavale, mis on kehtestatud liikmesriigi jaoks, kus asub see määratud riikliku küberturvalisuse sertifitseerimise asutus, mis määravas liikmesriigis järelevalveülesannete eest vastutab.

4. Euroopa Liidu Küberturvalisuse Amet (ENISA) teeb määruse (EL) 2019/881 artikli 50 kohaselt loodud Euroopa küberturvalisuse sertifitseerimise kavade veebisaidil üldsusele kättesaadavaks järgmise teabe:

a) teave I lisas sätestatud ajakava kohta;

b) artikli 2 lõike 5 kohaselt hallatav vastastikust hindamist tegevate riiklike küberturvalisuse sertifitseerimise asutuste loetelu.

5. Iga vastastikuses hindamises osalev riiklik küberturvalisuse sertifitseerimise asutus kannab ise oma osalemiskulud.

Artikkel 2

Vastastikust hindamist tegevate riiklike küberturvalisuse sertifitseerimise asutuste rotatsioonisüsteem

1. Määruse (EL) 2019/881 artikli 59 lõike 4 kohaselt viivad vastastikuse hindamise läbi vähemalt kaks vastastikust hindamist tegevat muu liikmesriigi riiklikku küberturvalisuse sertifitseerimise asutust ja komisjon. Iga liikmesriigi riiklikud küberturvalisuse sertifitseerimise asutused osalevad iga I lisas sätestatud ajavahemiku jooksul vähemalt kahe riikliku küberturvalisuse sertifitseerimise asutuse vastastikuses hindamises.

2. Kokkuleppel hinnatava riikliku küberturvalisuse sertifitseerimise asutuse, vastastikust hindamist tegevate riiklike küberturvalisuse sertifitseerimise asutuste ja komisjoniga võivad teiste liikmesriikide riiklikud küberturvalisuse sertifitseerimise asutused osaleda vastastikuses hindamises vaatlejana ühe või mitme esindajaga.

3. Vastastikuses hindamises võib osaleda vaatlejana üks ENISA esindaja. Hinnatava riikliku küberturvalisuse sertifitseerimise asutuse, vastastikust hindamist tegevate riiklike küberturvalisuse sertifitseerimise asutuste ja komisjoni nõusolekul võivad selles osaleda ka täiendavad esindajad.

4. Vaatlejatel on juurdepääs samale teabele nagu vastastikuse hindamise rühma teistel liikmetel, kuid nad ei täida vastastikuse hindamise tegemisega seotud ülesandeid.

5. Koostöös komisjoni ja Euroopa küberturvalisuse sertifitseerimise rühmaga koostab ENISA loetelu vastastikust hindamist tegevatest riiklikest küberturvalisuse sertifitseerimise asutustest, kes tegutsevad vastavalt I lisas sätestatud ajakavale, ja haldab seda. Igal aastal palub ENISA koostöös komisjoniga riiklikel küberturvalisuse sertifitseerimise asutustel avaldada soovi teha vastavalt I lisas eelseisva aasta jaoks ette nähtud ajakavale riiklike küberturvalisuse sertifitseerimise asutuste vastastikust hindamist või osaleda selles vaatlejana.

6. Kui ühe ja sama riikliku küberturvalisuse sertifitseerimise asutuse vastastikuse hindamise vastu tunneb huvi rohkem kui kaks riiklikku küberturvalisuse sertifitseerimise asutust, konsulteerivad komisjon ja ENISA asjaomaste riiklike küberturvalisuse sertifitseerimise asutustega ja otsustavad, kes vastastikuses hindamises osalevad.

7. Kui asjaomasel aastal ei ole piisaval hulgal riiklikke küberturvalisuse sertifitseerimise asutusi avaldanud soovi vastastikust hindamist teha, valib riiklikud küberturvalisuse sertifitseerimise asutused, kes hakkavad vastastikust hindamist tegema, komisjon, kes konsulteerib sealjuures Euroopa küberturvalisuse sertifitseerimise rühmaga. Valiku tegemisel võtab komisjon arvesse iga liikmesriigi riiklike küberturvalisuse sertifitseerimise asutuste lõike 1 kohast kohustust osaleda vähemalt kahe riikliku küberturvalisuse sertifitseerimise asutuse vastastikuses hindamises.

Artikkel 3

Vastastikuse hindamise rühma moodustamise kriteeriumid

1. Aegsasti enne vastastikuse hindamise algust määrab iga vastastikust hindamist tegev riiklik küberturvalisuse sertifitseerimise asutus ühe esindaja, kes vastastikuse hindamise teeb. Tagamaks, et vastastikuse hindamise rühmal on vastastikuse hindamise tegemiseks piisav pädevus, võib vastastikust hindamist tegev riiklik küberturvalisuse sertifitseerimise asutus määrata rohkem kui ühe esindaja.

2. Vastastikust hindamist tegeva riikliku küberturvalisuse sertifitseerimise asutuse esindaja, välja arvatud vaatlejana osaleva riikliku küberturvalisuse sertifitseerimise asutuse esindaja, peab vastama järgmistele kriteeriumitele:

a) esindaja on töötanud vastastikust hindamist tegevas riiklikus küberturvalisuse sertifitseerimise asutuses vähemalt kaks aastat või on osalenud vähemalt kahes vastastikuses hindamises vaatlejana;

b) esindajal on piisavad teadmised määruses (EL) 2019/881 sätestatud küberturvalisuse sertifitseerimise raamistiku kohta;

c) esindaja oskab praktilisel tasemel hästi inglise keelt ja võimaluse korral praktilisel tasemel hästi ühte või mitut hinnatava riikliku küberturvalisuse sertifitseerimise asutuse liikmesriigi keelt;

d) esindaja tegutseb hinnatavast riiklikust küberturvalisuse sertifitseerimise asutusest sõltumatult.

3. Vastastikust hindamist tegev riiklik küberturvalisuse sertifitseerimise asutus tagab, et mis tahes huvide konflikti oht seoses määratud esindajatega tehakse teistele riiklikele küberturvalisuse sertifitseerimise asutustele, komisjonile ja ENISA-le teatavaks enne vastastikuse hindamise protsessi algust. Hinnatav riiklik küberturvalisuse sertifitseerimise asutus võib esitada lõike 5 kohaselt teatavate esindajate määramise suhtes vastuväite.

4. Vastastikust hindamist tegevad riikliku küberturvalisuse sertifitseerimise asutused valivad endi hulgast ühe esindaja (edaspidi „rühmajuht“), kes vastastikuse hindamise tegemist koordineerib.

5. Komisjon edastab hinnatavale riiklikule küberturvalisuse sertifitseerimise asutusele vastastikust hindamist tegevate riikliku küberturvalisuse sertifitseerimise asutuste esindajate nimed ja kontaktandmed enne vastastikuse hindamise algust. Kui hinnatav riiklik küberturvalisuse sertifitseerimise asutus on ühe või mitme esindaja nimetamise vastu, esitab ta kahe nädala jooksul komisjonile selge põhjenduse, teavitab sellest ENISAt ja Euroopa küberturvalisuse sertifitseerimise rühma ning palub vastastikust hindamist tegeval riiklikul küberturvalisuse sertifitseerimise asutusel nimetada ametisse teise esindaja.

6. Kui lõikes 5 sätestatud menetlus põhjustab erandlike asjaolude tõttu vastastikuse hindamise alustamisel põhjendamatuid viivitusi, teeb otsuse vastastikuse hindamise rühma koosseisu kohta komisjon, kes konsulteerib sealjuures ENISA ja Euroopa küberturvalisuse sertifitseerimise rühmaga.

Artikkel 4

Vastastikuse hindamise metoodika

1. Vastastikuse hindamise käigus hinnatakse kooskõlas määruse (EL) 2019/881 artikli 59 lõikega 3 II lisas loetletud aspekte.

2. ENISA võib koostöös Euroopa küberturvalisuse sertifitseerimise rühma ja komisjoniga töötada hinnatava riikliku küberturvalisuse sertifitseerimise asutuse tööprotsesside hindamiseks välja näidisvormid.

3. Vastastikune hindamine hõlmab järgmist:

a) enesehindamise küsimustiku täitmine;

b) asjaomaste dokumentide hindamine;

c) veebipõhised või näost näkku intervjuud või mõlemad;

d) kohapealne kontrollkäik.

4. Johtuvalt hinnatava riikliku küberturvalisuse sertifitseerimise asutuse tegevuse mahust ja keerukusest võivad vastastikuse hindamise rühm ja hinnatav riiklik küberturvalisuse sertifitseerimise asutus vastastikuse hindamise kestuse eelnevalt kokku leppida. Kohapealne kontrollkäik ei kesta kauem kui kolm tööpäeva.

5. Kui vastastikuse hindamise rühm, hinnatav riiklik küberturvalisuse sertifitseerimise asutus ja komisjon ei ole kokku leppinud teisiti, on koostöökeeleks inglise keel. Artiklis 5 osutatud vastastikuse hindamise aruanne koostatakse vähemalt inglise keeles.

6. Hinnatav riiklik küberturvalisuse sertifitseerimise asutus teeb vastastikuse hindamise rühmaga koostööd ja annab sellele juurdepääsu teabele ja dokumentidele, mis on vastastikuse hindamise tegemiseks vajalikud. Hinnatav riiklik küberturvalisuse sertifitseerimise asutus esitab enesehindamise küsimustiku ja määruse (EL) 2019/881 artikli 58 lõike 7 punkti g kohaselt vastu võetud viimase iga-aastase kokkuvõtliku aruande vähemalt 21 päeva enne kohapealse kontrollkäigu kuupäeva. Täiendavad dokumendid esitatakse vastastikuse hindamise rühma taotlusel seitsme päeva jooksul alates sellise taotluse saamisest.

7. Dokumendid esitatakse inglise keeles, kui lõike 5 kohaselt ei ole kokku lepitud teisiti. Kui dokumente ei esitata inglise keeles, võib vastastikuse hindamise rühm nõuda vastastikuse hindamise tegemiseks vajalike dokumentide tõlkimist inglise keelde.

8. Enne artikli 5 kohase vastastikuse hindamise aruande koostamist arutab vastastikuse hindamise rühm esialgseid järeldusi hinnatava riikliku küberturvalisuse sertifitseerimise asutusega.

Artikkel 5

Vastastikuse hindamise aruanne

1. 21 päeva jooksul pärast vastastikuse hindamise lõpuleviimist koostab vastastikuse hindamise rühm vastastikuse hindamise aruande kavandi, mis sisaldab hinnatava riikliku küberturvalisuse sertifitseerimise asutuse liikmesriigi, vastastikust hindamist tegevate riiklike küberturvalisuse sertifitseerimise asutuste, komisjoni ja vaatlejate andmeid ning vastastikuse hindamise tulemusi ja järeldusi. Vajaduse korral sisaldab aruanne soovitusi vastastikuse hindamisega hõlmatud aspektide parandamiseks.

2. ENISA võib koostöös komisjoni ja Euroopa küberturvalisuse sertifitseerimise rühmaga töötada välja vastastikuse hindamise aruande näidisvormi.

3. Pärast lõike 1 kohase vastastikuse hindamise aruande kavandi koostamist esitab vastastikuse hindamise rühm selle hinnatavale riiklikule küberturvalisuse sertifitseerimise asutusele, kes saab esitada 14 päeva jooksul omapoolseid märkusi. Vastastikuse hindamise rühm hindab märkusi ja võtab neid lõpparuande koostamisel võimaluse korral arvesse, püüdes saavutada üksmeelt. Lahkarvamuse korral lisatakse lõpparuandele hinnatava riikliku küberturvalisuse sertifitseerimise asutuse vastus.

4. Lõpparuanne, sealhulgas avaldamiseks mõeldud kokkuvõte, saadetakse Euroopa küberturvalisuse sertifitseerimise rühmale kahe kuu jooksul pärast vastastikuse hindamise lõpuleviimist. Kooskõlas määruse (EL) 2019/881 artikli 59 lõikega 6 vaatab Euroopa küberturvalisuse sertifitseerimise rühm aruande läbi ja kinnitab selle kokkuvõtte, mis avaldatakse määruse (EL) 2019/881 artikli 50 kohaselt loodud Euroopa küberturvalisuse sertifitseerimise kavade veebisaidil. Kokkuleppel hinnatava riikliku küberturvalisuse sertifitseerimise asutusega sisaldab kokkuvõte ka hinnatava riikliku küberturvalisuse sertifitseerimise asutuse vastust või selle osi.

5. Enne vastastikuse hindamise aruande levitamist väljaspool vastastikuse hindamise rühma anonüümib vastastikuse hindamise rühm isikuandmed, mida ta on vastastikuse hindamise käigus kogunud.

Artikkel 6

Konfidentsiaalsus

1. Kõik vastastikuses hindamises osalejad austavad oma ülesannete täitmise ja tegevuse käigus saadud teabe ja andmete konfidentsiaalsust, kaitstes eeskätt järgmist:

a) intellektuaalomandiõigused ning füüsilise ja juriidilise isiku konfidentsiaalne äriteave ja ärisaladused, kaasa arvatud lähtekood, välja arvatud juhtudel, millele on viidatud Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/943 ([3]) artiklis 5;

b) käesoleva määruse tulemuslik rakendamine;

c) avaliku ja riigi julgeolekuga seotud huvid;

d) kriminaal- ja haldusmenetluste usaldusväärsus.

2. Vastastikuse hindamise rühm tagab, et vastastikuse hindamise käigus saadud teavet käideldakse turvaliselt. Kui lõpparuanne ja artikli 5 lõikes 4 osutatud kokkuvõte on koostatud, kustutab või hävitab vastastikuse hindamise rühm, sealhulgas teevad seda kõik vaatlejad, kõik dokumendid, mis on vastastikuse hindamise käigus kogutud või koostatud, välja arvatud lõpparuanne ja kokkuvõte.

3. Võttes arvesse riiklike küberturvalisuse sertifitseerimise asutuste praegusi parimaid tavasid, võib ENISA koostöös Euroopa küberturvalisuse sertifitseerimise rühmaga töötada välja suunised turvalise ja konfidentsiaalse teabevahetuse kohta.

([3]) Euroopa Parlamendi ja nõukogu 8. juuni 2016. aasta direktiiv (EL) 2016/943, milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset (ELT L 157, 15.6.2016, lk 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

Artikkel 7

Suutlikkuse suurendamine

ENISA analüüsib vastastikuste hindamiste koondtulemusi ning toob esile saadud kogemused ja parimad tavad, et aidata kaasa riiklike küberturvalisuse sertifitseerimise asutuste suutlikkuse suurendamisele ja Euroopa küberturvalisuse sertifitseerimise kavade haldamisele. See analüüs võib vajaduse korral hõlmata riiklike küberturvalisuse sertifitseerimise asutuste jaoks koostöös Euroopa küberturvalisuse sertifitseerimise rühmaga koolituste ja täiendavate suuniste väljatöötamist.

Artikkel 8

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 9. detsember 2025

Komisjoni nimel
president
Ursula VON DER LEYEN

I LISA

Riiklike küberturvalisuse sertifitseerimise asutuste vastastikuse hindamise ajakava

31. detsembriks 2026 ja seejärel iga viie aasta tagant hinnatakse järgmiste liikmesriikide riiklikke küberturvalisuse sertifitseerimise asutusi:

Rootsi, Belgia, Slovakkia, Saksamaa, Malta, Tšehhi.

31. detsembriks 2027 ja seejärel iga viie aasta tagant hinnatakse järgmiste liikmesriikide riiklikke küberturvalisuse sertifitseerimise asutusi:

Ungari, Kreeka, Eesti, Sloveenia, Madalmaad, Itaalia.

31. detsembriks 2028 ja seejärel iga viie aasta tagant hinnatakse järgmiste liikmesriikide riiklikke küberturvalisuse sertifitseerimise asutusi:

Horvaatia, Taani, Leedu, Hispaania, Bulgaaria, Iirimaa.

31. detsembriks 2029 ja seejärel iga viie aasta tagant hinnatakse järgmiste liikmesriikide riiklikke küberturvalisuse sertifitseerimise asutusi:

Soome, Austria, Rumeenia, Luksemburg, Läti, Poola.

31. detsembriks 2030 ja seejärel iga viie aasta tagant hinnatakse järgmiste liikmesriikide ja EMP/EFTA riikide riiklikke küberturvalisuse sertifitseerimise asutusi:

Küpros, Prantsusmaa, Portugal, Liechtenstein, Norra, Island.

II LISA

Vastastikuse hindamise metoodika

II.1. **Sertifitseerimise ja järelevalve lahusus**

Kui vastastikuse hindamise käigus on vaatluse all hinnatava riikliku küberturvalisuse sertifitseerimise asutuse määruse (EL) 2019/881 artikli 59 lõike 3 punkti a kohane sertifitseerimis- ja järelevalvetegevuse lahusus, hinnatakse vähemalt järgmisi detaile:

a) hinnatava riikliku küberturvalisuse sertifitseerimise asutuse toimimise üksikasjalik kirjeldus, milles on selgelt välja toodud määruse (EL) 2019/881 rakendamises osalevad üksused ja/või osakonnad;

b) hinnatava riikliku küberturvalisuse sertifitseerimise asutuse tegevuse kaardistus määruse (EL) 2019/881 artikli 58 lõikes 7 loetletud tegevuste põhjal;

c) kui hinnatav riiklik küberturvalisuse sertifitseerimise asutus annab välja sertifikaate, siis selgitus, millest nähtub, et tema sertifitseerimistegevus ja punkti b kohane järelevalvetegevus ei ole segunenud.

II.2. **Järelevalve sertifikaatide nõuetele vastavuse jälgimise reeglite üle ja selliste reeglite täitmise tagamine**

Kui vastastikuse hindamise käigus on vaatluse all hinnatava riikliku küberturvalisuse sertifitseerimise asutuse määruse (EL) 2019/881 artikli 59 lõike 3 punkti b kohased menetlused, mille alusel teeb asutus järelevalvet IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste Euroopa küberturvalisuse sertifikaatide nõuetele vastavuse jälgimise reeglite üle ning tagab selliste reeglite täitmise, hinnatakse vähemalt järgmisi aspekte:

a) selliste protsesside ja menetluste üksikasjaliku kirjelduse kvaliteet ja tase ning nende dokumenteerituse ulatus;

b) kas ja kui suures ulatuses hõlmavad sellised protsessid ja menetlused asjaomaseid Euroopa küberturvalisuse sertifitseerimise kavasid;

c) kas hinnataval riiklikul küberturvalisuse sertifitseerimise asutusel on toimiv volitus kontrollida sertifikaate väljastavaid vastavushindamisasutusi ja vajaduse korral sertifikaate tühistada;

d) hinnatava riikliku küberturvalisuse sertifitseerimise asutuse ja asjaomaste turujärelevalveasutuste koostöö ulatus;

e) kas hinnataval riiklikul küberturvalisuse sertifitseerimise asutusel on määruse (EL) 2019/881 artikli 58 lõike 7 punkti f kohaselt nõutav mehhanism füüsiliste ja juriidiliste isikute kaebuste käsitlemiseks, sealhulgas tõendid selle kohta, kas füüsilistel ja juriidilistel isikutel on kooskõlas kõnealuse määruse artiklitega 63 ja 64 õigus esitada kaebusi ja saada tõhusat kohtulikku õiguskaitset.

II.3. **Tootjate ja pakkujate kohustuste jälgimine ja täitmise tagamine**

Kui vastastikuse hindamise käigus on vaatluse all hinnatava riikliku küberturvalisuse sertifitseerimise asutuse määruse (EL) 2019/881 artikli 59 lõike 3 punkti c kohased menetlused, mille alusel jälgib asutus, kas vastavuse enesehindamist tegevad IKT-toodete, -teenuste ja -protsesside ja hallatud turbeteenuste tootjad ja pakkujad täidavad kohustusi, ja tagab selliste kohustuste täitmise, hinnatakse vähemalt järgmisi aspekte:

a) kas hinnatav riiklik küberturvalisuse sertifitseerimise asutus on need menetlused kehtestanud ja kui suures ulatuses on need dokumenteeritud ning kas ta on loonud mehhanismi välistest allikatest pärineva teabe vastuvõtmiseks ja töötlemiseks;

b) kas ja kui suures ulatuses hõlmavad sellised menetlused asjaomaseid Euroopa küberturvalisuse sertifitseerimise kavasid;

c) kas ja kui suures ulatuses viib hinnatav riiklik küberturvalisuse sertifitseerimise asutus läbi uurimisi ning kas uurimise alla kuuluvad ka tootjate kohustused, mis on sätestatud määruse (EL) 2019/881 artikli 53 lõigetes 2 ja 3 ning vastavates Euroopa küberturvalisuse sertifitseerimise kavades;

d) kas on olemas menetlus, millega reguleeritakse teabe vahetamist hinnatava riikliku küberturvalisuse sertifitseerimise asutuse sertifitseerimistegevuse ja järelevalvetegevuse vahel, kui selline sertifitseerimis- või järelevalvetegevus on tootjate ja pakkujate kohustuste jälgimise ja täitmise tagamise seisukohast oluline.

II.4. **Vastavushindamisasutuste jälgimine, neile lubade andmine ja järelevalve nende üle**

Kui vastastikuse hindamise käigus on vaatluse all hinnatava riikliku küberturvalisuse sertifitseerimise asutuse määruse (EL) 2019/881 artikli 59 lõike 3 punkti d kohased menetlused, mille alusel jälgib asutus vastavushindamisasutusi, annab neile lubasid ja teeb nende üle järelevalvet, hinnatakse vähemalt järgmisi aspekte:

a) selliste menetluste üksikasjaliku kirjelduse kvaliteet ja tase ning see, kui suures ulatuses on need dokumenteeritud, sealhulgas koostöö tegemiseks riikliku akrediteerimisasutusega;

b) peamised statistilised andmed hinnatava riikliku küberturvalisuse sertifitseerimise asutuse antud, peatatud ja tühistatud lubade arvu, tegutsevate vastavushindamisasutuste koguarvu, väljastatud sertifikaatide arvu ja võetud parandusmeetmete arvu kohta;

c) kui hinnatav riiklik küberturvalisuse sertifitseerimise asutus lubab Euroopa küberturvalisuse kõrge usaldusväärsuse taseme sertifikaate välja anda määruse (EL) 2019/881 artikli 56 lõike 6 kohase eelneva heakskiidu või delegeerimise alusel, siis töötajate eksperditeadmised ja menetlused, mille abil hinnatav riiklik küberturvalisuse sertifitseerimise asutus jälgib vastavushindamisasutuste tegevust ja teeb selle üle järelevalvet.