EUROOPA
KOMISJON

Strasbourg, 20.1.2026
COM(2026) 11 final

2026/0011 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

mis käsitleb Euroopa Liidu Küberturvalisuse Ametit (ENISA), Euroopa küberturvalisuse sertifitseerimise raamistikku ja IKT tarneahela turvalisust ning millega tunnistatakse kehtetuks määrus (EL) 2019/881 (küberturvalisuse 2. määrus)

{SEC(2026) 11 final} - {SWD(2026) 11 final} - {SWD(2026) 12 final}

(EMPs kohaldatav tekst)

SELETUSKIRI

1. ETTEPANEKU TAUST

• Ettepaneku põhjused ja eesmärgid

Alates küberturvalisuse määruse vastuvõtmisest 2019. aastal on küberohtude pilt üha keerukamas geopoliitilises olukorras märkimisväärselt muutunud[1]. Elutähtsa taristu, ettevõtjate ja üldsuse vastu suunatud küberründed, eelkõige lunavararünded, on järsult sagenenud ja muutunud keerukamaks[2]. Kujunemisjärgus tehnoloogiad, nagu tehisintellekt ja kvantarvutus, kujundavad ümber kaitsevahendeid ja vastaste taktikat. Mario Draghi rõhutas oma 2024. aasta **aruandes „Euroopa konkurentsivõime tulevik“**, et vajadus suurendada turvalisust ja vähendada sõltuvust on üks peamine valdkond, millega tuleb Euroopa Liidus tegeleda[3]. Nii ELi kriisivalmiduse strateegias[4] kui ka Euroopa sisejulgeoleku strateegias (ProtectEU)[5] on küberturvalisus seatud liidu vastupanuvõime suurendamise tegevuskava keskmesse. Neis strateegiates tunnistatakse, et püsivad küberohud ei ole pelgalt tehnilised probleemid, vaid ka strateegilised riskid meie demokraatiale, majandusele ja eluviisile. Samamoodi peetakse teatises ELi majandusjulgeoleku tugevdamise kohta[6] esmatähtsateks eesmärkideks juurdepääsu takistamist tundlikule teabele ja andmetele, mis võib kahjustada ELi majandusjulgeolekut, ning ELi majandust mõjutavate elutähtsa taristu häirete ennetamist ja leevendamist, milles on oluline koht tulemuslikel küberturvalisuse meetmetel.

Seda arvesse võttes püütakse küberturvalisuse määruse kavandatud läbivaatamisega lahendada **neli peamist probleemi**: i) ebakõla liidu küberturvalisuse poliitikaraamistiku ja sidusrühmade vajaduste vahel üha vaenulikumal ohumaastikul; ii) Euroopa küberturvalisuse sertifitseerimise raamistiku rakendamise takerdumine; iii) liidu turvaolekut mõjutavate küberturvalisusega seotud poliitikameetmete keerukus ja mitmekesisus ning iv) suurenevad turvariskid IKT tarneahelates.

Kindlakstehtud peamisi probleeme arvesse võttes on sekkumise **kaks üldeesmärki** suurendada küberturvalisuse alast suutlikkust ja kerksust ning vältida killustumist kogu ühtsel turul,

- aidates tugevdada küberturvalisuse juhtimist liidus ning aidates tagada, et asjaomased institutsioonid, asutused ja muud sidusrühmad on paremini ette valmistatud, et koordineeritud viisil ja tõhusalt ennetada ja avastada küberohte ja neile reageerida, ning
- toetades liidu ühiste küberturvalisuse vahendite, näiteks sertifitseerimiskavade väljatöötamist, rakendamist ja kasutuselevõttu ning luues ühtlustatud raamistikud, mis suurendavad usaldust ja koostalitlusvõimet kõigis liikmesriikides.

---

1 ENISA, ENISA ohtude kaardistamise aruanne 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

2 ENISA, ENISA ohtude kaardistamise aruanne 2025.

3 Euroopa Komisjon, „The future of European Competitiveness“ (Euroopa konkurentsivõime tulevik), https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.

4 JOIN(2025) 130 final.

5 COM(2025) 148 final.

6 JOIN(2025) 977 final.

Need üldeesmärgid on vastus probleemi püstituses nimetatud peamistele probleemidele. Need kajastavad üldist poliitilist eesmärki tugevdada liidus küberturvalisuse juhtimist ning toetada turvalise, vastupidava ja konkurentsivõimelise digitaalse ühtse turu arengut.

Selleks et aidata saavutada eespool nimetatud üldeesmärgid, taotletakse sekkumisega järgmisi **erieesmärke**:

- et kaotada ebakõla liidu küberturvalisuse poliitikaraamistiku ja sidusrühmade vajaduste vahel:
    - 1. erieesmärk: luua suutlikkus küberturvalisuse alaste liidu poliitikameetmete tulemuslikuks rakendamiseks ja pidevaks operatiivkoostööks, mis võimaldab struktureeritumat koostööd liikmesriikide vahel;
    - 2. erieesmärk: töötada välja ja võtta kasutusele vahendid ja mehhanismid, et liikmesriike, tööstust ja muid sidusrühmi tulemuslikult toetada ning rahuldada nende vajadusi;
- et lahendada Euroopa küberturvalisuse sertifitseerimise raamistiku piiratud kasutamise ja tulemuslikkuse probleem:
    - 3. erieesmärk: luua eeltingimused turuvajadustest lähtuvate küberturvalisuse sertifitseerimise kavade kiiremaks elluviimiseks, laiendades Euroopa küberturvalisuse sertifitseerimise raamistiku kohaldamisala, tagades tõhusa haldamise ja paindlikud menetlused ning suurendades läbipaistvust;
- et vähendada killustatust nõuete täitmisel ning horisontaalsete ja valdkondlike raamistike keerukust:
    - 4. erieesmärk: luua mehhanismid ja tingimused, et hõlbustada küberturvalisuse nõuete täitmist, muutes seeläbi nende rakendamise sidusamaks ja tulemuslikumaks;
- et vähendada küberriske tarneahelas:
    - 5. erieesmärk: vähendada riske kriitilise tähtsusega IKT tarneahelates, mis saavad alguse küberturvalisuse seisukohast muret tekitavates kolmandates riikides asutatud või sealt pärit üksuste kontrolli all olevatest üksustest (suure riskiga tarnijad), ning vähendada kriitilist sõltuvust, töötades ELi tasandil välja sidusa ja tulemusliku raamistiku IKT tarneahelates esinevate turvariskidega käsitlemiseks.

Küberturvalisuse määruse läbivaatamine on osa **õigusloome kvaliteedi ja tulemuslikkuse programmist**. See aitab olulisel määral suurendada selgust, kaotada ebatõhusust ja ühtlustada menetlusi eri õigusraamistikes. Küberturvalisuse määruse läbivaatamine aitab kaasa siseturu nõuetekohasele toimimisele, tagades samal ajal liidu julgeoleku ja strateegilise autonoomia.

Konkreetsemalt hõlmab see ettepanekut täielikult reformida Euroopa Liidu Küberturvalisuse Ameti (ENISA) volitused, et pakkuda tõhusat tuge poliitika rakendamisel ja lisaväärtust, mis seisneb liikmesriikidevahelise operatiivkoostöö toetamises.

Arvestades liidu ees seisvate küberriskide ja probleemide kasvu, on ettepaneku eesmärk suurendada ENISA finants- ja inimressursse, et need vastaksid ENISA ulatuslikumale rollile,

ülesannetele ja kriitilise tähtsusega positsioonile liidu digitaalse ökosüsteemi kaitsmisel ja võimaldaksid ENISA-l tulemuslikult täita talle käesoleva ettepanekuga pandud ülesandeid.

Läbivaatamine aitab ka vähendada tavade killustatust ja parandada koordineerimist, vähendades samal ajal pikas perspektiivis nõuete täitmise ja tegevuskulusid. Kehtiva küberturvalisuse määruse kehtetuks tunnistamisega ja reformitud Euroopa küberturvalisuse sertifitseerimise raamistiku kehtestamisega luuakse tulemuslikum ja tõhusam vahend, mis nii kasvatab usaldust ettevõtjate, üldsuse ja avaliku sektori asutuste seas kui ka lihtsustab asjakohaste liidu õigusaktide järgimist. Ettepanekuga suurendatakse tõhusust, vaadates läbi juhtimismudeli ning toetades prognoositavamaid, sidusamaid ja kiiremaid sertifitseerimismenetlusi, et kavu saaks kiiremini välja töötada ja rakendada .

Suurem koostoime asjakohaste kehtivate liidu õigusraamistikega edendab sertifitseerimist kui nõuetelevastavuse kinnitamise vahendit ettevõtjate jaoks ja vähendab mitme küberturvalisust käsitleva õigusakti alusel tegutsevate vastavushindamisasutuste halduskoormust. Euroopa küberturvalisuse sertifitseerimise raamistiku kohaldamisala laiendamise ja üksuste turvaoleku kava koostamise võimaldamise kaudu vähendatakse ettepanekuga nõuete täitmisega seotud kulusid üksuste jaoks, kelle suhtes kohaldatakse asjakohaseid küberturvalisust käsitlevaid liidu õigusakte, alustades küberturvalisuse 2. direktiivi kohaldamisalasse kuuluvatest üksustest. See lähenemisviis lihtsustab märkimisväärselt nende üksuste seadusest tulenevaid kohustusi, kelle suhtes kohaldatakse mitmeid vastavusnõudeid, ja tagab vahendite tõhusama kasutamise riiklikes asutustes. Lisaks käesolevale läbivaatamisele püütakse küberturvalisuse 2. direktiivi sihipäraste muudatuste tegemise direktiivi ettepanekuga, lihtsustada küberturvalisuse sertifitseerimise raamistiku konkreetsete aspektide järgimist ning tagada nende ühtlustatud ja sidus rakendamine, muuhulgas seoses kohaldamisala, määratluste, lunavarast teatamise ja piiriüleseid teenuseid osutavate üksuste järelevalvega.

Uue määrusega luuakse ka ühtlustatud raamistik IKT tarneahelaid mõjutavate mittetehniliste riskidega tegelemiseks, et vähendada liikmesriikide lähenemisviiside praegust killustatust. See kõik kokku tähendab liidu küberturvalisuse õigusraamistiku märkimisväärset lihtsustamist ja ajakohastamist, mis on täielikult kooskõlas õigusloome kvaliteedi ja tulemuslikkuse programmis sätestatud selguse, tõhususe ja digivalmiduse põhimõttega.

- **Kooskõla poliitikavaldkonnas praegu kehtivate õigusnormidega**

Liit on laiendanud oma õiguslikke ja poliitilisi vahendeid, võttes vastu mitu õigusakti ja poliitikameedet: i) küberturvalisuse 2. direktiivi eesmärk on tugevdada elutähtsa taristu küberturvalisust; ii) selle nn sõsardirektiivis, elutähtsa teenuse osutajate toimepidevuse direktiivis, on määratletud füüsilise turvalisuse meetmed; iii) küberkerksuse määrusega suurendatakse toodete küberturvalisust; iv) kübersolidaarsuse määrusega parandatakse kogu ELis reageerimissuutlikkust; v) ELi kübervaldkonna tegevuskavaga[7] toetatakse ELi tasandi koostööd kriisiohje valdkonnas, kus komisjonil ja kõrgel esindajal on oluline roll ulatuslikeks küberintsidentideks valmistumisel ja neile reageerimisel; vi) 5G küberturvalisuse meetmepaketiga toetatakse 5G-võrkude küberturvalisust; vii) Euroopa haiglate ja tervishoiuteenuste osutajate küberturvalisuse tegevuskava[8] aitab parandada haiglate ja

[7] COM(2025) 66 final.
[8] COM(2025) 10 final.

teenuseosutajate küberturvalisust ning viii) küberturbeoskuste akadeemia[9] kaudu lahendatakse üha suuremat küberturvalisuse valdkonna talendinappuse probleemi.

Eespool kirjeldatud küberturvalisuse õigusraamistikku on täiendatud valdkondlike õigusaktidega, nagu digitaalse tegevuskerksuse määrus (DORA määrus) finantssektori jaoks, võrgueeskiri piiriüleste elektrivoogude küberturvalisust käsitlevate sektoripõhiste normide kohta elektri allsektori jaoks ning infoturbe eeskirjad[10] lennutranspordi allsektori jaoks.

Küberturvalisuse määruse läbivaatamine on kooskõlas küberturvalisuse 2. direktiiviga ja tugevdab selle sätteid selles osas, mis puudutab ENISA toetavat rolli direktiivi rakendamisel, sh operatiivkoostöö toetamisel. Läbivaatamine on kooskõlas ka küberkerksuse määrusega, muu hulgas selles osas, mis puudutab ülevaadet siseturu nõrkustest ja nende nõrkuste haldamist, ning suurendab ühise olukorrateadlikkuse lisaväärtust. Euroopa küberturvalisuse sertifitseerimise raamistiku osas on küberkerksuse määruse läbivaatamine kooskõlas küberkerksuse määrusega, mis puudutab toodete turvalisuse eesmärke ja nõrkuste käsitlemist, ning akrediteerimist käsitleva uue õigusraamistikuga. Peale selle on olemas tugev koostoime, mis tuleneb turvaoleku sertifitseerimise väljatöötamisest küberturvalisuse 2. direktiivi jaoks ning võimalik et ka selle jaoks, et hõlbustada muude asjakohaste liidu õigusaktide, näiteks isikuandmete kaitse üldmääruse järgimist, ilma et see piiraks neis õigusaktides sätestatud sertifitseerimisnõuete kohaldamist. Samuti toetab horisontaalne raamistik, mis käsitleb IKT tarneahelates esinevaid küberriske, küberturvalisuse 2. direktiivi üldeesmärki saavutada küberturvalisuse ühtlaselt kõrge tase kogu liidus ning tugineb selle direktiivi riskipõhisele lähenemisviisile.

Lisaks tagab küberturvalisuse määruse läbivaatamine koos küberturvalisuse 2. direktiivi sihipäraste muudatuste tegemise direktiivi ettepanekuga vajalikud vahendid, et suurendada selle tervikliku raamistiku tulemuslikkust ja tõhusust oodatavate tulemuste saavutamisel, tagada tugevam Euroopa mõõde ja täita allesjäänud regulatiivsed lüngad.

- **Kooskõla muude liidu tegevuspõhimõtetega**

Küberturvalisuse määruse läbivaatamine täiendaks elutähtsa teenuse osutajate toimepidevuse direktiivi, mis hõlmab tarneahelaga seotud kaalutlusi kui osa elutähtsa teenuse osutajate toimepidevusmeetmetest. Peale selle täiendaks läbivaatamine tulevasi algatusi, nagu i) ELi pilvandmetöötluse ja tehisintellekti arendamise õigusakt, mille üks eesmärke on tegeleda probleemiga, et liidus ei pakuta piisavas ulatuses konkurentsivõimelisi pilvandmetöötlusteenuseid, et rahuldada eriti kriitilise tähtsusega kasutusjuhtude või sektorite vajadusi; ii) digivõrkude õigusakti ettepanek; iii) määruse (EL) 2023/1781[11] eelseisev läbivaatamine; iv) riigihangete raamistik,[12] mida praegu hinnatakse,[13] ning ettepanek võtta vastu määrus digivaldkonna õigusaktide lihtsustamise kohta (digivaldkonna koondpakett),[14]

---

9 COM(2023) 207 final.

10 Komisjoni rakendusmäärus (EL) 2023/203 ja komisjoni delegeeritud määrus (EL) 2022/1645.

11 Euroopa Parlamendi ja nõukogu 13. septembri 2023. aasta määrus (EL) 2023/1781, millega kehtestatakse meetmete raamistik Euroopa pooljuhiökosüsteemi tugevdamiseks ja muudetakse määrust (EL) 2021/694 (kiibimäärus) (ELT L 229, 18.9.2023, lk 1–53).

12 Eelkõige direktiivid 2014/23/EL, 2014/24/EL ja 2014/25/EL.

13 Euroopa Komisjon, „Commission launches call for evidence and public consultation on the evaluation of the Public Procurement Directives“ (Komisjon kuulutab välja tagasisidekorje ja avaliku konsultatsiooni seoses riigihankedirektiivide hindamisega), https://single-market-economy.ec.europa.eu/news/commission-launches-call-evidence-and-public-consultation-evaluation-public-procurement-directives-2024-12-13_en.

14 COM(2025) 837 final.

milles on sätestatud ENISA kohustus luua intsidentidest teatamiseks ühtne kontaktpunkt, mis võimaldab üksustel samaaegselt täita mitme õigusakti kohaseid intsidentidest teatamise kohustusi. Lisaks tugevdaks läbivaatamine liidu ametiasutuste ja ettevõtjate positsiooni suhtlemisel Vahemere lõunapiirkonna partneritega, eelkõige parandades kogu Vahemere piirkonnas ühendatust turvaliste ja usaldusväärsete digitaristute kaudu, mis on üks Vahemere pakti põhieesmärke.

Küberturvalisuse määruse läbivaatamine on kooskõlas ka liidu strateegiliste dokumentidega, eelkõige mis puudutab IKT tarneahela turvalisuse raamistikku. Komisjon on strateegias ProtectEU märkinud, et ühtlustatud lähenemisviis IKT tarneahela turvalisusele võib vähendada siseturu praegust killustatust, mille on põhjustanud erinevad lähenemisviisid riikide tasandil, aidata vältida kriitilist sõltuvust ja muuta IKT tarneahelad suure riskiga tarnijate osas riskikindlamaks, kindlustades seeläbi elutähtsat taristut. Majandusjulgeoleku strateegias on samuti rõhutatud vajadust suurendada ELi majanduse ja tarneahelate vastupanuvõimet, et edendada ELi konkurentsivõimet[15]. Vajadust käsitleda häireid tarneahelates ja küberründe on rõhutatud ka ELi kriisivalmiduse strateegias ja valges raamatus Euroopa kaitse tuleviku kohta[16]. Küberturvalisuse määruse läbivaatamine on kooskõlas ka Mario Draghi aruandega Euroopa konkurentsivõime tuleviku kohta, nagu on märgitud eespool. Ja veel, küberturvalisuse määruse läbivaatamine IKT tarneahela turvalisuse osas on kooskõlas hiljuti vastu võetud ühisteatisega Euroopa Parlamendile ja nõukogule ELi majandusjulgeoleku tugevdamise kohta[17].

2. ÕIGUSLIK ALUS, SUBSIDIAARSUS JA PROPORTSIONAALSUS

• Õiguslik alus

Käesoleva ettepaneku õiguslik alus on Euroopa Liidu toimimise lepingu (edaspidi „ELi toimimise leping“) artikkel 114. ELi toimimise lepingu artikliga 114 on ette nähtud meetmete võtmine, et tagada siseturu loomine ja toimimine. Selle sätte alusel on vastu võetud ka määrus (EL) 2019/881, mis käsitleb ENISAt ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist,[18] tuntud kui küberturvalisuse määrus.

IKT tarneahela küberturvalisuse valdkonnas avaldab siseturu toimimisele kahjulikku mõju mittetehnilisi riskitegureid käsitlevate riiklike raamistike killustatus, kuna erinevused riiklikes lähenemisviisides võivad lõppkokkuvõttes suurendada mõne liikmesriigi haavatavust, millel võib olla üldist vastupanuvõimet ja ka usaldusväärsust kahjustav ülekanduv mõju kogu liidus.

Võttes arvesse küberohtude muutuvat olemust ja liikmesriikide digisüsteemide üha suuremat vastastikust sõltuvust, on ELi toimimise lepingu artikkel 114 jätkuvalt põhjendatud õiguslik alus küberturvalisuse määruse läbivaatamiseks. Kavandatud määrus kajastab viimaseid arengusuundumusi küberturvalisuse õigusmaastikul, eriti pidades silmas ENISA suurenevaid kohustusi ning sertifitseerimise ja riskijuhtimise ulatuse laienemist.

---

15 JOIN(2023) 20 final.
16 JOIN(2025) 120 final.
17 JOIN(2025) 977 final.
18 Määrus – 2019/881 – ET – EUR-Lex.

- **Subsidiaarsus (ainupädevusse mittekuuluva valdkonna puhul)**

Subsidiaarsuse põhimõtte kohaselt tuleb hinnata liidu meetme vajalikkust ja lisaväärtust. Subsidiaarsuse põhimõtte järgimist selles valdkonnas tunnistati juba kehtiva küberturvalisuse määruse vastuvõtmisel.

Nagu leiti küberturvalisuse määruse puhul, on liidu sekkumine väga oluline, kuna küberohud ja nendega seotud probleemid ulatuvad üksikutest liikmesriikidest kaugemale. Killustatud riiklikud lahendused on osutunud ebapiisavaks, et saavutada usaldus ja koordineerimine kogu turul. Selleks et kõrvaldada tõkked, tagada järjekindel rakendamine ja toetada liikmesriike üha keerukamas regulatiivses ja ohukeskkonnas on vaja läbivaadatud liidu õigusraamistikku. Küberturvalisus on liidule ühist huvi pakkuv küsimus.

Kavandatud määrusega hõlmatud meetmed pakuvad selget lisaväärtust, toetades ühtlustamist, õigusselgust ja koordineeritud reageerimist küberturvalisusega seotud probleemidele.

ENISA ülesandeid on hiljem vastu võetud õigusaktidega laiendatud, ilma et oleks põhjalikult läbi vaadatud ameti põhikohustusi ja vahendeid. See on tekitanud ebatõhusust ja toonud kaasa selle, et liikmesriikide toetamisega seotud põhiülesandeid pole peetud piisavalt prioriteetseks. Seepärast püütakse sekkumisettepanekuga ENISA praeguseid ülesandeid täpsustada ja prioriseerida, et tugevdada ENISA volitusi, võimaldades tal tegutseda liidu tasandi ühtse küberturvalisuse eksperdikeskusena. Selles küsimuses ei ole subsidiaarsuse vaatenurgast märkimisväärseid erinevusi võrreldes küberturvalisuse määrusega. Lisaks põhjustavad liikmesriikide erinevad sertifitseerimiskavad ja regulatiivsed lähenemisviisid turu killustatust ja täiendavat nõuete täitmisega seotud koormust, mis kahjustab konkurentsivõimet.

Ettepanekuga nähakse ette ka uued meetmed seoses tarneahela poliitika ja lihtsustamispüüdlustega liidu tasandil. Sellega tugevdatakse veelgi tarneahela turvalisust ja küberturvalisuse sektorit liidus ning suurendatakse liikmesriikide ja tööstusharu valmisolekut ja vastupanuvõimet.

Sõltuvus üksustest, mis on asutatud küberturvalisuse seisukohast muret tekitavates kolmandates riikides või mida sellised kolmandad riigid, neis asutatud üksused või nende kodanikud kontrollivad (suure riskiga tarnijad), mõjutab üksusi kogu liidus, kuna tarneahelas aset leidvad olulised küberintsidendid levivad sageli üle riigipiiride. Lisaks, võttes arvesse IKT tarneahelate piiriülest olemust, kahjustab vastavusnõuete killustatus siseturul üksuste õiguskindlust. Peale selle on mitmeaastast finantsraamistikku käsitlevate ettepanekutega ette nähtud suure riskiga tarnijate väljajätmine, et kaitsta ELi eelarve terviklikkust ja julgeolekuhuve. Kavandatud määruses sisalduv tarneahela raamistik hõlmab mehhanismi, et selgitada välja küberturvalisuse seisukohast muret tekitavad riigid, mida saab tulemuslikult teha vaid ELi tasandil. Mis puudutab IKT tarneahela turvalisust, siis ühesuguse minimaalse turvalisuse taseme kogu liidus ja lähenemisviiside vajaliku ühtlustamise tagab vaid ELi tasandi sekkumine.

Läbivaatamisel säilitatakse kehtiva küberturvalisuse määruse eesmärk ja seda tugevdatakse veelgi. Liikmesriigid ei suuda seda eesmärki piisavalt saavutada, küll aga saab seda saavutada liidu tasandil kooskõlas Euroopa Liidu lepingu artikliga 5.

- **Proportsionaalsus**

Kavandatud meetmed ei lähe ettepaneku poliitikaeesmärkide saavutamiseks vajalikust kaugemale. Liidu sekkumise ulatus ei takista täiendavate riiklike meetmete võtmist riikliku

julgeoleku valdkonnas. Seega on liidu meede subsidiaarsuse ja proportsionaalsuse seisukohast põhjendatud.

Ettepaneku eesmärk on kajastada õiguslikult paremini ENISA volitusi ning Euroopa küberturvalisuse sertifikaatide väljatöötamise, vastuvõtmise ja haldamise protsessi. Kuigi ettepanek sisaldab ENISA jaoks teatavaid uusi ülesandeid, on nende eesmärk toetada liikmesriike valdkondades, kus on kindlaks tehtud märkimisväärsed lüngad. ENISA ei asenda liikmesriikide küberintsidentidele reageerimise üksuseid (CSIRT). Mis puudutab Euroopa küberturvalisuse sertifitseerimise raamistikku, siis sertifitseerimine jääb vabatahtlikuks ja see võib aidata üksustel tõendada vastavust liidu küberturvalisuse nõuetele. Selline lähenemisviis tagab proportsionaalsuse põhimõtte järgimise.

Mis puudutab lahendusi, mis on kavandatud seoses IKT tarneahela turvalisusega, siis raamistikus nähakse ette tõendite kogumine selle kohta, mis on olulised varad ning millised meetmed oleksid proportsionaalsed ja vajalikud, et vähendada riske kriitilise tähtsusega tarneahelates. Enne nende meetmete kindlaksmääramist tehakse majandusliku mõju hindamine, mille raames vaadeldakse muu hulgas majanduslikku teostatavust, turul kättesaadavaid alternatiive ja konkreetsete toodete elutsüklit. See hindamine võimaldab saada teavet selle kohta, millised riskipõhised meetmed on vajalikud ja kõige asjakohasemad.

- **Vahendi valik**

Käesoleva ettepanekuga vaadatakse läbi määrus (EL) 2019/881, milles on sätestatud ENISA praegused volitused ja ülesanded ning Euroopa küberturvalisuse sertifitseerimise raamistik. Seetõttu on kõige parem kehtestada ENISA läbivaadatud volitused ja Euroopa küberturvalisuse sertifitseerimise raamistiku muudatused, kasutades sama õiguslikku vahendit, st määrust. Kavandatud õigusakt hõlmab ka tõhusat ELi tasandi raamistikku IKT tarneahela turvariskide käsitlemiseks, mille puhul kindlakstehtud probleemide lahendamise ja sõnastatud eesmärkide saavutamise jaoks oles määrus tulemuslikum, kuna vaid ELi tasandi sekkumine tagab ühesuguse turvalisuse taseme kogu liidus ja lähenemisviiside vajaliku ühtlustamise. Sellise sekkumise jaoks direktiivi kasutamise korral võib ülevõtmisprotsessis olla riigi tasandil liiga palju kaalutlusruumi, mis võib põhjustada teatavate oluliste küberturvalisuse nõuete ebaühtlust, õiguskindlusetust, täiendavat killustumist või isegi diskrimineerivaid piiriüleseid olukordi.

3. JÄRELHINDAMISE, SIDUSRÜHMADEGA KONSULTEERIMISE JA MÕJU HINDAMISE TULEMUSED

- **Praegu kehtivate õigusaktide järelhindamine või toimivuse kontroll**

Euroopa Komisjon hindas kooskõlas määruse (EL) 2019/881 artikliga 67 ENISA ja Euroopa küberturvalisuse sertifitseerimise raamistiku asjakohasust, mõju, tulemuslikkust, tõhusust, sidusust ja lisaväärtust, võttes arvesse muutuvat tehnoloogiamaastikku ja regulatiivset keskkonda. Hindamine, mis viidi lõpule 2024. aasta detsembris, hõlmas ajavahemikku 2017–2023 ning selle eesmärk oli vaadata läbi ENISA volitused ja tegevus ning hinnata Euroopa küberturvalisuse sertifitseerimise raamistiku rolli turvalise küberkeskkonna edendamisel kogu ELis. Peamised tähelepanekud saab kokku võtta järgmiselt.

- **Asjakohasus.** ENISA asjakohasust küberturvalisuse valdkonnas kinnitab tema võime reageerida sidusrühmade muutuvatele vajadustele ja kohaneda muutuva olukorraga. Kuigi sidusrühmade rahulolu on üldiselt hea, on ENISA mõju võimalik suurendada. Seda saab teha, parandades pakutavat tuge ja nähtavust eri sektorite

jaoks, eelkõige pidades silmas väikeseid ja keskmise suurusega ettevõtjaid (VKEd), kellel on sageli raskusi küberturvalisuse nõuete täitmisel. Oluline on vahendite parem korraldus ja selgem koordineerimine riiklike asutustega. Prioriteetide muutmine ja olemasolevate vahendite optimeerimine viib ENISA tegevuse paremini kooskõlla dünaamiliste vajadustega Euroopa küberturvalisuse maastikul.

Euroopa küberturvalisuse sertifitseerimise raamistiku puhul leitakse, et ehkki raamistik on paljutõotav, on sel endiselt rohkem potentsiaali kui praktilist mõju, kuna viimasel ajal on kasutusele võetud ainult üks sertifitseerimiskava. Raamistik on kavandatud integreeruma sujuvalt muude liidu õigusaktidega, et ühtlustada menetlusi ja hõlbustada piiriülest kaubandust. Raamistiku olulisust rõhutatakse sellistes suurt kindlust nõudvates valdkondades nagu pilvteenused ja 5G-taristud.

- **Tulemuslikkus.** ENISA on täitnud edukalt oma volitusi ja saavutanud peaaegu kõik kavandatud väljundid, näidates üles paindlikkust ja vastupanuvõimet selliste kriiside ajal nagu COVID-19 pandeemia ja Venemaa Ukraina-vastane agressioonisõda. Tulemuslikkuse suurendamiseks on siiski vaja paremat prioriteetide seadmist, selget fookust ja vahendite strateegilist jaotamist. Selleks et kohaneda muutuvate vajadustega küberturvalisuse valdkonnas ja minimeerida viivitusi, on oluline paindlikum lähenemisviis sisejuhtimisele.

  Euroopa küberturvalisuse sertifitseerimise raamistikuga on püütud ühtlustada küberturvalisuse sertifitseerimist kogu liidus, kuid selle rakendamisel on seistud silmitsi märkimisväärsete probleemide, sh menetluslike piirangute ja killustatusega, mis on põhjustanud viivitusi ja ebatõhusust, näiteks lükanud edasi Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava vastuvõtmise. Euroopa küberturvalisuse sertifitseerimise raamistiku eesmärkide saavutamist on veelgi raskendanud välised tegurid, nagu geopoliitilised pinged ja COVID-19 pandeemia, mis osutab sellele, et vaja on kohandatavaid meetmeid ja vahendite järjekindlat jaotamist sidusrühmade vahel, et saavutada ühetaoline ja tulemuslik küberturvalisuse sertifitseerimine. Neist takistustest hoolimata on saavutatud rõõmustavaid tulemusi, eelkõige on suurendatud liikmesriikide teadlikkust küberturvalisuse sertifitseerimise tähtsusest ja üksikasjadest.

- **Tõhusus.** ENISA on tegutsenud oma maatriksipõhises organisatsioonilises raamistikus tõhusalt, edendades koostööd ja ülesannete prioriseerimist. Samas on ENISA seisnud kasvavate vajaduste rahuldamisel ja spetsiifilisemate ametikohtade täitmisel silmitsi raskustega (mida on süvendanud IT-spetsialistide ülemaailmne nappus), mis on põhjustanud viivitusi ja suurt töökoormust. Nende probleemide lahendamiseks saaks ENISA optimeerida oma asutusesisest tööjõudu ja jaotada vahendid tulemuslikult ümber, mida näitavad tehtud strateegilised kohandused, nagu vahendite ümberpaigutamine küberturvalisuse toetusmeetmesse 2022. aastal. Lisaks saaks muuta ENISA tegevuse veelgi tõhusamaks, kui parandada eelarve haldamist ja vähendada halduskulusid.

  Euroopa küberturvalisuse sertifitseerimise raamistiku tõhusust on kritiseeritud küberturvalisuse sertifitseerimise kavade vastuvõtmise pikale venitatud ajakava ja seonduva keerukuse tõttu – esimene kava võeti vastu alles 2024. aasta alguses, st peaaegu viis aastat pärast küberturvalisuse määruse vastuvõtmist. Muu hulgas on viivitusi põhjustanud poliitilised ja tehnilised probleemid, nagu arutelud andmesuveräänsuse üle ja raskused eelnõude õigusaktideks muutmisel. Poliitilised probleemid ja tehnilised nõudmised on takistanud edasiminekut, nagu on näha ELi pilvandmetöötluse sertifitseerimise kava ja kava EU5G puhul. Sellest ebatõhususest

hoolimata võib raamistikuga seoses täheldada mitut positiivset aspekti. Sidusrühmade kaasamist ja sisejuhtimist on siiski vaja parandada, et tagada optimaalne toimimine ja strateegiline panus.

- **Sidusus.** ENISA sidusust toetab sidusrühmade märkimisväärne kaasamine ja vastavusseviimine hiljutiste õigusraamistikega. Sidususe ja vahendite eraldamise edendamiseks on siiski oluline parandada koostoimet teiste liidu organitega, nagu küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus, ja riiklike asutustega. Peale selle tuleb täiustada ENISA-sisest suhtlust ja vahendite haldamist ning läbipaistvat suhtlust erasektori sidusrühmadega. ENISA ülesannete selge piiritlemine kooskõlas küberkerksuse määruse ja küberturvalisuse 2. direktiiviga parandab nii tõhusust kui ka regulatiivset järjepidevust.

  Euroopa küberturvalisuse sertifitseerimise raamistiku puhul on küberturvalisuse vallas ühtse lähenemisviisi tagamiseks väga oluline täielik kooskõla muude liidu õigusaktidega, sh küberturvalisuse 2. direktiivi ja küberkerksuse määrusega. Kuigi raamistik on nende seadusandlike meetmetega teoreetiliselt kooskõlas, on tegelik integratsioon endiselt keeruline ja nõuab hoolikat järelevalvet. Oluliseks proovikiviks saab olema vastu võetud Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava rakendamine küberkerksuse määruse raamistikus.

- **ELi lisaväärtus.** ENISA on andnud märkimisväärse panuse liidu küberturvalisuse ökosüsteemi, edendades koostööd ja kooskõlastades tavasid. Ametil on olnud väga oluline roll riikide jõupingutuste hõlbustamisel ja esilekerkivate ohtude kohta teabe andmisel. Erasektori sidusrühmade kriitika, milles osutatakse vajadusele paremini kohandatud toetuse järele, näitab siiski, et vaja on sidusrühmade paremat kaasamist ja tööstusharu koostööd. Vahendite haldamise strateegiline ümberhindamine võimaldaks ENISA-l paremini kohaneda muutuvate küberturvalisuse alaste probleemidega ja teenida tulemuslikumalt eri sidusrühmade huve. Euroopa küberturvalisuse sertifitseerimise raamistiku eesmärk oli kehtestada ühtlustatud sertifitseerimisprotsessid, kuid selle rakendamisel on esinenud pikale venitatud ajakavast ja killustatusest tingitud probleeme. Seoses vajakajäämistega eesmärkide saavutamisel ja vähese tõhususega on raamistiku lisaväärtus olnud piiratud. Neist probleemidest hoolimata on raamistik parandanud liikmesriikidevahelist ühtlustamist ja toonud kaasa paremad koostöövõimalused, eelkõige tänu loodud sidusrühmade koostööfoorumitele, nagu Euroopa küberturvalisuse sertifitseerimise rühm.

- **Konsulteerimine sidusrühmadega**

Aastatel 2023–2025 peeti küberturvalisuse määruse hindamise ja läbivaatamise raames sidusrühmadega mitmeid konsultatsioone, nagu on näha allpool.

– **2023. aastal** korraldati 65 intervjuud (52 neist keskendusid rohkem ENISA-le ja 13 peamiselt Euroopa küberturvalisuse sertifitseerimise raamistikule), viidi läbi uuring, mille raames saadi 209 vastust (neist 70 Euroopa küberturvalisuse sertifitseerimise raamistiku kohta), viidi lõpule avalik konsultatsioon ning korraldati kaks seminari, kus käsitleti tugevuste, nõrkuste, võimaluste ja ohtude analüüsi (SWOT-analüüs) ning soovitusi (vastavalt 26 ja 70 osalejat). Nende ettevõtmiste konkreetne eesmärk oli koguda sidusrühmade seisukohti, et hinnata ENISA mõju, tulemuslikkust ja tõhusust. PwC, Intellera Consulting ja PPMI tegid komisjoni jaoks ENISA ja Euroopa küberturvalisuse sertifitseerimise raamistiku hindamist toetava uuringu, mille lõpparuanne valmis 2024. aasta detsembris.

– **2025. aastal** kuulutas komisjon välja tagasisidekorje. Sidusrühmadel paluti esitada kirjalik tagasiside, sh seisukohavõtud, tehnilised aruanded ja märkused konkreetsete reformiettepanekute kohta. Mitmesugustelt sidusrühmadelt, sh tööstusliitudelt, küberturvalisuse ettevõtetelt, VKEdelt, akadeemilistelt asutustelt ja avaliku huvi organisatsioonidelt, saadi kokku 184 vastust.

– **2025. aasta aprillist juunini** korraldas komisjon küberturvalisuse määruse läbivaatamise raames avaliku konsultatsiooni ja sai 193 vastust. Konsultatsioon hõlmas 38 suletud ja avatud küsimust ENISA volituste, Euroopa küberturvalisuse sertifitseerimise raamistiku, IKT tarneahela turvalisuse ja lihtsustamise kohta.

– **Sihtkonsultatsioon (intervjuud).** Viidi läbi mitu poolstruktureeritud intervjuud valitud sidusrühmadega. Nende hulka kuulusid ENISA esindajad ja riikliku teatamisplatvormi välja töötanud või seda haldavad riikide ametiasutused. Intervjuudes keskenduti ENISA rollile ja suutlikkusele, Euroopa küberturvalisuse sertifitseerimise raamistiku toimimisele, praktilistele probleemidele riiklike ja liidu tasandi sertifitseerimisprotsesside ühtlustamisel, aruandluskoormusele ja rakendamistakistustele. Vestluste käigus saadi kvalitatiivset teavet, mis võimaldas paremini tõlgendada avaliku konsultatsiooni tulemusi ja täpsustada poliitikavariante.

– **Konsultatsioonid liikmesriikide esindajatega nõukogu töörühma[19] raames ja kahepoolsetel aruteludel** võimaldasid liikmesriikidel väljendada oma seisukohti küberturvalisuse määruse läbivaatamise kohta.

– **Sihtkonsultatsioon Euroopa küberturvalisuse sertifitseerimise rühmaga ja sidusrühmade küberturvalisuse sertifitseerimise rühmaga.** Komisjon kui mõlema rühma eesistuja tutvustas Euroopa küberturvalisuse sertifitseerimise rühma koosolekutel 12. märtsil ja 3. juulil 2025 ning sidusrühmade küberturvalisuse sertifitseerimise rühma koosolekul 17. märtsil 2025 küberturvalisuse määruse läbivaatamise seisu. Lisaks koguti Euroopa küberturvalisuse sertifitseerimise rühma liikmetelt täiendavaid eksperdiarvamusi, kasutades küsimustikke.

Konsulteerimisel keskenduti viiele liidu küberturvalisuse raamistiku tulevase toimimise ja sidususe seisukohast kesksele põhivaldkonnale:

- **ENISA volitused ja operatiivroll**, sh liikmesriikide toetamine ja eksperditeadmised kujunemisjärgus tehnoloogiate valdkonnas;
- **Euroopa küberturvalisuse sertifitseerimise raamistiku**, sh juhtimis- ja arendusprotsesside **tulemuslikkus**;
- **küberturvalisusega seotud kohustuste keerukus ja killustatus**, pöörates tähelepanu aruandluskoormusele ja lihtsustamisvõimalustele;
- **nõuete proportsionaalsus VKEde jaoks** ja nõuete täitmise eri viiside võimalus ning
- küberturvalisust käsitlevate ühtlustatud normide **sotsiaalne ja majanduslik mõju**, sh mõju tarbijatele, õigustele, innovatsioonile ja konkurentsivõimele.
- **Mõjuhinnang**

Küberturvalisuse määruse läbivaatamist ning küberturvalisuse 2. direktiivi sihipäraste muudatuste tegemise direktiivi ettepanekut toetab mõjuhinnang (vt kokkuvõte allpool).

[19] Horisontaalne küberküsimuste töörühm.

Õiguskontrollikomitee esitas küberturvalisuse määruse[20] läbivaatamisega seotud esialgse mõjuhinnangu uuesti esitatud aruande kohta reservatsioonidega positiivse arvamuse. Õiguskontrollikomitee soovituste ja märkuste arvesse võtmiseks mõjuhinnangut kohandati.

Lõplik poliitikaettepanek ei kaldu kõrvale mõjuhinnangus hinnatud poliitikavariantidest.

Komisjon uuris saavutatavaid konkreetseid eesmärke silmas pidades poliitikavariante neljas sekkumisvaldkonnas: 1) ENISA volitused (mis on ka kehtiva küberturvalisuse määruse osa); 2) Euroopa küberturvalisuse sertifitseerimise raamistik (mis on samuti kehtiva küberturvalisuse määruse osa); 3) küberturvalisuse 2. direktiivi sihipärased muudatused, et direktiivi lihtsustada, mis on seotud ka ENISA volituste ja Euroopa küberturvalisuse sertifitseerimise raamistikuga, ning 4) IKT tarneahela turvalisus, mis on oluline nii küberturvalisuse 2. direktiivi ökosüsteemi kui ka Euroopa küberturvalisuse sertifitseerimise raamistiku jaoks. Kõik kindlaksmääratud poliitikavariandid on eraldiseisvad sekkumisvaldkonnad, mis on samal ajal omavahel seotud ja vastastikku olulised.

Poliitikavariandid ELi küberturvalisuse poliitikaraamistiku ja sidusrühmade vajaduste kooskõlastamiseks üha vaenulikumas keskkonnas

Variant A.1: *ENISA volituste täpsustamine ja prioriteetide seadmine* – see variant tagaks selge ja stabiilse raamistiku ENISA ülesannete täitmiseks, sest hõlmaks ka muudes õigusaktides sätestatud ülesandeid.

Variant A.2: *ENISA volituste reform* – selle variandiga tunnistataks küberturvalisuse määrus kehtetuks ja asendataks see, korraldades ameti volitused põhjalikult ümber.

Variant A.3: *ENISA volituste reform, milles pööratakse suurt tähelepanu operatiivtoetusele* – see variant oleks variandi A.2 edasiarendus. Täiendavalt arendataks ENISA suutlikkust, et pakkuda küberturvalisuse 2. direktiivi kohaldamisalasse kuuluvatele üksustele liikmesriigi taotlusel otsest tuge küberintsidentidele reageerimisel ja neist taastumisel.

Euroopa küberturvalisuse sertifitseerimise raamistikuga seotud poliitikavariandid

Variant B.1: *Euroopa küberturvalisuse sertifitseerimise raamistiku kohaldamisala, elementide ja eesmärkide täpsustamine ning haldusmehhanismi kasutuselevõtt* – selle variandiga nähakse ette uus kavade haldamise mehhanism, mida ENISA hakkaks rakendmaa pärast kavade vastuvõtmist.

Variant B.2: *Euroopa küberturvalisuse sertifitseerimise raamistiku reform, mille käigus vaadatakse läbi raamistiku menetlused ja laiendatakse selle kohaldamisala, et aidata lihtsustada õigusnormide järgimist* – selle variandi puhul tunnistataks küberturvalisuse määrus kehtetuks ja asendataks uue määrusega. Lisaks variandis B.1 kavandatule vaadataks läbi kavade taotlemise, väljatöötamise ja vastuvõtmisega seotud menetlused, et suurendada vastutust ja tõhusust.

Variant B.3: *Euroopa küberturvalisuse sertifitseerimise raamistiku reform, nagu on ette nähtud variandi B.2 korral, ja turvaoleku sertifitseerimise kohustuse kehtestamine* – see variant põhineks variandil B.2, kuid selle eesmärk on raamistiku mõju veelgi tugevdada, kehtestades elutähtsate üksuste sertifitseerimise kohustuse, võttes arvesse konkreetseid riskistsenaariume, selle asemel, et tugineda ainult üksuste vabatahtlikule sertifitseerimisele.

Lihtsustamisega seotud poliitikavariandid

[20] Määrus (EL) 2019/881 (http://data.europa.eu/eli/reg/2019/881/oj).

Variant C.1: *pehmel õigusel ja muudel kui seadusandlikel vahenditel põhineva lähenemisviisi, sh olemasolevate volituste kasutamine (rakendusaktide vastuvõtmine küberturvalisuse 2. direktiivi artikli 21 lõike 5 ja artikli 23 lõike 11 alusel)* – selle variandi kohaselt võetaks vastu rakendusaktid, kasutades olemasolevaid küberturvalisuse 2. direktiivis sätestatud volitusi, et tagada küberriskide juhtimise meetmete, intsidentidest teatamise künniste ning teabe liigi, vormi ja teatamise korra parem ühtlustamine. Samuti on kavandatud suuniste vastuvõtmine, et suurendada õiguskindlust ja ühtlustada rakendamist.

Variant C.2: *sihipärane sekkumine – asjaomase liidu küberturvalisuse õigusraamistiku järgimise edasine lihtsustamine* – see variant hõlmab piiratud sekkumist küberturvalisuse määruse ja küberturvalisuse 2. direktiivi muutmise kaudu, mille eesmärk on lihtsustada küberturvalisuse raamistiku konkreetseid aspekte, sh kohandada kohaldamisala, rakendusakte võimalikult palju ühtlustada, tõendada nõuete täitmist sertifitseerimise kaudu ja võtta vastu variandi C.1 all ette nähtud suunised.

Variant C.3: *liidu õiguses sätestatud küberturvalisuse meetmete ühtlustamine* – see variant põhineks variandil C.2 ja sellega eemaldataks kõik valdkondlikes õigusaktides sätestatud küberturvalisuse riskijuhtimismeetmed ja nende seotud volitused. Selle asemel muudetaks küberturvalisuse 2. direktiivi ökosüsteemi, et näha ette ühtlustatud nõuded igat liiki üksustele, tagades sel viisil suurema ühtlustamise.

IKT tarneahela turvalisusega seotud poliitikavariandid

Variant D.1: *pehme õiguse lähenemisviisi kasutamine IKT tarneahelate küberriskide käsitlemiseks* – see variant ei näeks ette ELi tasandi regulatiivset sekkumist. Selle asemel suurendaks komisjon koordineeritud riskihindamiste ja vabatahtlike abivahendite arvu.

Variant D.2: *sihtotstarbeline regulatiivne sekkumine, millega kodifitseeritakse 5G meetmepakett* – selle variandiga kodifitseeritaks 5G meetmepaketi meetmed. Sellega kehtestataks liikmesriikidele kohustus tagada, et võrgu olulistes varades ei kasutata suure riskiga tarnijate komponente.

Variant D.3: *terviklik ja horisontaalne raamistik IKT tarneahelate küberriskide käsitlemiseks* – selle variandiga loodaks IKT tarneahelates esinevate mittetehniliste küberriskide käsitlemiseks tehnoloogia- ja sektorineutraalne horisontaalne õigusraamistik.

Põhjaliku analüüsi tulemusel osutus eelistatud poliitikapaketiks järgmine poliitikavariantide kombinatsioon: variant A.2 (ENISA volituste reform), variant B.2 (Euroopa küberturvalisuse sertifitseerimise raamistiku reform, mille käigus vaadatakse läbi raamistiku menetlused ja laiendatakse selle kohaldamisala, et aidata lihtsustada õigusnormide järgimist), variant C.2 (sihipärane sekkumine – asjaomase liidu küberturvalisuse õigusraamistiku järgimise edasine lihtsustamine) ja variant D.3 (terviklik ja horisontaalne raamistik IKT tarneahelate küberriskide käsitlemiseks).

Need poliitikavariandid võimaldavad kindlakstehtud poliitikaprobleemidele tasakaalustatult reageerida ja suurendavad märkimisväärselt tulemuslikkust, tõhusust ja sidusust kogu liidus.

Eelistatud variantide rakendamisega õigusraamistikus kaasnevad kulud nii ENISA-le uute ülesannete täitmisel (hinnanguliselt kuni 161,3 miljonit eurot viie aasta jooksul) kui ka avaliku sektori asutustele kogu liidus järelevalve tegemisel (hinnanguliselt kuni 80 miljonit eurot viie aasta jooksul, võttes arvesse asjakohast kulude kokkuhoidu). Mis puudutab ettevõtjaid, siis suure riskiga seadmete järkjärguline kasutuselt kõrvaldamine võib tuua mobiilsideoperaatoritele viie aasta jooksul kaasa kulud suurusega 3,4–4,3 miljardit eurot

aastas ning investeeringud usaldusväärsetesse tarnijatesse võivad kasvada kuni 2 miljardile eurole aastas.

Samal ajal peaksid lihtsustatud ja vähendatud vastavuskohustused võimaldama ettevõtjatel viie aasta jooksul kokku hoida kuni 15,3 miljardit eurot. Lisaks tooks liidu üldise turvaoleku ja tehnoloogilise suveräänsuse parandamine ning innovatsiooni ja konkurentsivõime edendamine märkimisväärset kasu üldsusele, avaliku sektori asutustele ja ettevõtjatele. See peaks esialgsed kulutused pikas perspektiivis suures osas tasakaalustama.

Turu killustatuse vähendamisega ja regulatiivsete nõuete ühtlustamisega suurendatakse eelistatud variantidega konkurentsialast võrdsust liidus ning pakutakse ettevõtjatele selgemaid võimalusi nõuete täitmiseks ja innovatsiooniks.

Samuti aitaksid eelistatud variandid selgete suuniste ja integreeritud süsteemide kaudu kaasa lihtsustamisele, vähendades halduskoormust. Variandid on kooskõlas põhimõttega „üks sisse, üks välja“, kuna uute kohustuste tasakaalustamiseks vähendatakse mujal kohustusi.

- **Õigusnormide toimivus ja lihtsustamine**

Küberturvalisuse määruse läbivaatamine valitud poliitikavariantide A.2, B.2, C.2 ja D.3 rakendamisega aitab olulisel määral suurendada selgust, kaotada ebatõhusust ja ühtlustada menetlusi õigusraamistikes. Täpsemalt on variandis A.2 kavandatud ENISA volituste täielik reformimine, millega toetatakse tulemuslikult poliitika rakendamist ja liikmesriikide operatiivkoostööd. Selline konsolideerimine aitab ka vähendada tavade killustatust ning parandada koordineerimist ja vähendada samal ajal pikas perspektiivis nõuete täitmise ja tegevuskulusid. Variandiga B.2, mis hõlmab kehtiva küberturvalisuse määruse kehtetuks tunnistamist ja reformitud Euroopa küberturvalisuse sertifitseerimise raamistiku kasutuselevõttu, suurendatakse tõhusust tänu juhtimismudeli läbivaatamisele ning prognoositavamate, sidusamate ja kiiremate sertifitseerimismenetluste toetamisele. See võimaldab kavade kiiremat vastuvõtmist ja paremat vastavusse viimist valdkonnaüleste õigusaktidega, vähendades regulatiivset killustatust ning nii avaliku kui ka erasektori sidusrühmade koormust. Variandiga C.2 vähendatakse asjaomaste küberturvalisust käsitlevate liidu õigusaktide kohaldamisalasse kuuluvate üksuste nõuete täitmisega seotud kulusid, muutes küberturvalisuse raamistiku kohaldamisala ning võimaldades töötada küberturvalisuse 2. direktiivi ja muude õigusaktide kohaldamisalasse jäävate üksuste jaoks välja organisatsiooni küberturvalisuse sertifitseerimise kavasid. See lähenemisviis lihtsustab märkimisväärselt nende üksuste seadusest tulenevaid kohustusi, kelle suhtes kohaldatakse mitmeid nõudeid, ja tagab vahendite tõhusama kasutamise riiklikes asutustes. Variandiga D.3 luuakse ühtlustatud raamistik tegelemiseks IKT tarneahelaid mõjutavate mittetehniliste riskidega tegelemiseks ühtlustatud raamistik, millega vähendada liikmesriikide lähenemisviiside praegust killustatust. Need variandid kokku tähendavad liidu küberturvalisuse õigusraamistiku märkimisväärset lihtsustamist ja ajakohastamist, mis on täielikult kooskõlas õigusloome kvaliteedi ja tulemuslikkuse programmis sätestatud selguse, tõhususe ja digivalmiduse põhimõttega.

Ettepanek on kooskõlas digikontrolliga, kuna selle rõhuasetus ühtlustatud digitaalsetele protsessidele näitab liidu pühendumust lähenemisviisile „kõigepealt digitaalne“, mis tagab kiirema ja usaldusväärsema andmevahetuse ja otsuste tegemise. Variandil D.3 võib olla suur mõju ka digiüleminekule, kuna see toob kaasa küberturvalisuse seisukohast muret tekitavates kolmandates riikides asutatud üksuste või selliste üksuste kontrolli all olevate üksuste (suure riskiga tarnijad) komponentide asendamise.

- **Põhiõigused**

Seadusandliku ettepaneku hindamisel vaadeldi ettepaneku potentsiaali tugevdada või seada ohtu põhiõigusi ning edendada võrdõiguslikkust ja usaldust, pöörates erilist tähelepanu sotsiaalmõjule ja -õigustele, sh eraelu puutumatusele, andmekaitsele ning üksikisikute võimele mõista, kasutada ja panna maksma oma õigusi.

ENISA volituste laiendamine aitab suurendada küberkerksust kogu majanduses ja ühiskonnas üldiselt, mis toob kaasa inimeste eraelu puutumatuse ja isikuandmete parema kaitse. Ettepanekuga toetatakse ka küberturvalisuse alast haridust ja koolitust, kuna sellega muudetakse selgemaks ENISA roll küberturvalisuse valdkonna töötajate oskuste arendamisel.

Lisaks suurendab Euroopa küberturvalisuse sertifitseerimise raamistik ELi üldsuse ja ettevõtjate usaldust igapäevaelu toetavate sertifitseeritud IKT-lahenduste vastu. Seda mõju võimendaks täiendavate kavade kehtestamine.

Ettepanek aitab suurendada inimeste usaldust, innustades kriitilise tähtsusega sektorite üksusi hankima küberturvalisuse sertifikaate ja näitama seeläbi avalikult oma küberturvalisuse kõrget taset. Tagades ühtlustatud teatamise lunavaraintsidentidest ja nähes ette meetmed üleminekuks postkvantkrüptograafiale, aitab ettepanek suurendada üldsuse usku tundlike andmete kaitsesse kriitilise tähtsusega sektorites.

Tarneahela turvalisust käsitlevad sätted mõjutavad teataval määral põhiõiguste kaitset, piirates välissekkumist. Sellised tegevused nagu spionaaž ja jälgimine kahjustavad oluliselt kodanike põhiõigusi. Kõnealune horisontaalne raamistik võib suurendada usaldust, turvalisust ja eraelu puutumatust mitmesuguste tehnoloogiate ja digilahenduste puhul.

4. MÕJU EELARVELE

Euroopa Liidu Küberturvalisuse Ameti (ENISA) eelarveks, millega panustatakse ELi turvalisuse märkimisväärsesse suurendamisse, hinnati 341 miljonit eurot seitsme aasta jooksul, mis teeb keskmiseks aastaeelarveks 49 miljonit eurot (prognoos aastateks 2028–2034). See tähendab, et ameti 2025. aasta eelarvet suurendatakse 81,5 %. Kavandatud algatusest saadav kasu, mida on analüüsitud mõjuhinnangus, on märkimisväärne, kuna ettevõtjate kulud vähenevad kuni 14,6 miljardit eurot. Kuigi võimalikku kulude kokkuhoidu seoses liidu küberintsidentideks valmisoleku üldise paranemisega on keeruline kvantifitseerida, võib kiirema reageerimise ja küberintsidentide leviku aeglustamisega seotud kulude kokkuhoid viie aasta jooksul jääda hinnanguliselt vahemikku 3,7–4,4 miljardit eurot. Komisjon uurib tulevaste poliitikaalgatuste raames vahendite üldist jaotust küberturvalisuse valdkonnas tegutsevate Euroopa institutsioonide, organite ja asutuste vahel ja sees, et võimendada üldisi teadmisi ja eksperditeadmisi ning teha kindlaks ja arendada koostoimet.
ENISA tugevdamiseks kavandatud lisavahendid teisendatakse 118 täistööajale taandatud töötaja ametikohaks ja täiendavateks tegevuskuludeks ENISA ja komisjoni vaheliste kehtivate rahalist toetust käsitlevate lepingute jaoks, näiteks ühtse teatamisplatvormi haldamiseks, ELi küberreservi käitamise ja haldamisega tegelevate täistööajale taandatud töötajate jaoks ning olulisteks komisjoni algatusteks, nagu digivaldkonna koondpaketi ettepaneku kohase ühtse kontaktpunkti loomine. Tegevuskulud on seotud ka nõrkuste koordineeritud avalikustamise programmiga, küberohuteadmuse kogumise ja analüüsimisega, turvalise sidega ja ENISA küberturvalisuse küpsuse suurendamisega. Lisaks sisaldab see eelarve Euroopa küberturvalisuse sertifitseerimise kavade haldamise, küberturbeoskustega seotud lubade ja testimisvahendite teenustega seotud tegevuskulusid, ehkki nende kulude katmiseks kasutatakse tasude kaudu ka omafinantseerimist.

Ettepaneku oluline aspekt on kasutusele võetavad tasude mehhanismid, mis lisaks muudele poliitikaeesmärkidele toetavad kestlikku raharinglust ametis. Läbivaadatud küberturvalisuse määrus sisaldab kolme liiki tasusid, millega panustatakse ENISA eelarvesse, nimelt oskuste tõendamise lubade väljaandmise tasud, testimisvahendite teenustega seotud tasud ja Euroopa küberturvalisuse sertifitseerimise kavade haldamise toetamise tasud. Eeldatav kasu ELi eelarvele on hinnanguliselt 18,5 miljonit eurot seitsme aasta jooksul (2028–2034).

Komisjoni eelarvetaotlus hõlmab 50 täiendavat täistööajale taandatud töötaja ametikohta tarneahela raamistiku rakendamiseks, aga ka ülesandeid, mis on seotud muu hulgas tasude mehhanisme käsitlevate rakendusaktide koostamisega, sertifitseerimiskavade haldamisega, standardimisega ja operatiivkoostöö toetamisega. Komisjoni kulusid tarneahela raamistiku rakendamisel mõjutab eeldatavasti eriti see, kui palju teeb komisjon omandi ja kontrolli hindamisi. Samas aitavad nende hindamiste tulemused liikmesriikidel küberturvalisuse 2. direktiivi kohaldamisalasse kuuluvate üksuste suhtes raamistikuga kehtestatud leevendusmeetmete rakendamise ja kohustuste täitmise üle järelevalve tegemisel oluliselt kokku hoida. Liikmesriigid saavad kasutada omandi ja kontrolli hindamiste tulemusi, selle asemel et kulutada vahendeid samade hindamisvajaduste rahuldamiseks.

Üksikasjalikum teave on esitatud küberpaketile lisatud finantsselgituses.

5. MUU TEAVE

- **Rakenduskavad ning järelevalve, hindamise ja aruandluse kord**

Komisjon jälgib kavandatud määruse kohaldamist ning esitab iga viie aasta tagant Euroopa Parlamendile ja nõukogule aruande selle hindamise kohta. Need aruanded on avalikud ning neis kirjeldatakse üksikasjalikult määruse tegelikku kohaldamist ja täitmise tagamist.

- **Selgitavad dokumendid (direktiivide puhul)**

Ei kohaldata, kuna ettepanek on määrus.

- **Ettepaneku sätete üksikasjalik selgitus**

Ettepanekus selgitatakse ENISA rolli ning antakse ametile konkreetsed ülesanded, et toetada sidusrühmi, iseäranis liikmesriike, eelkõige liidu poliitika ja õigusaktide rakendamisel, operatiivkoostöö tegemisel, suutlikkuse suurendamisel, küberturvalisuse sertifitseerimisel ja standardimisel ning küberturvalisuse valdkonna tööjõu arendamisel ja selle liikuvuse parandamisel kogu liidus. Samuti püütakse ettepanekuga tugevdada ja tõhustada Euroopa küberturvalisuse sertifitseerimise raamistikku, et tõsta küberturvalisuse taset liidus ja võimaldada klientidel teha IKT-toodete, -teenuste ja -protsesside ning hallatud turbeteenuste puhul kogu siseturul teadlikke valikuid. Koos küberturvalisuse 2. direktiivi sihipäraste muudatuste tegemise direktiivi ettepanekuga on käesoleva ettepaneku eesmärk hõlbustada küberturvalisusega seotud kohustuste täitmist ja vabastada vahendeid, et tugevdada liidu kriitilise tähtsusega sektorite üksuste operatiivset küberturvalisuse alast valmisolekut. Lisaks käsitletakse ettepanekus vajadust muuta liidu majandus ja IKT tarneahel vastupidavamaks, et edendada liidu julgeolekut ja konkurentsivõimet. Üksikasjalikum kirjeldus on esitatud allpool.

I JAOTIS. ÜLDSÄTTED

Kavandatud määruse I jaotis sisaldab üldsätteid: reguleerimisese (artikkel 1) ja mõisted (artikkel 2), sh viited asjakohastele määratlustele muudes liidu õigusaktides, nagu direktiiv

(EL) 2022/2555[21] (küberturvalisuse 2. direktiiv), määrus (EÜ) nr 765/2008[22] ja määrus (EL) nr 1025/2012[23].

II JAOTIS. ENISA (EUROOPA LIIDU KÜBERTURVALISUSE AMET)

Kavandatud määruse II jaotis sisaldab ENISAga seotud põhisätteid.

I peatükis kirjeldatakse ENISA missiooni (artikkel 3) ja eesmärke (artikkel 4).

II peatükis kirjeldatakse kolmes jaos ENISA ülesandeid.

1. jagu sisaldab sätteid ülesannete kohta, mis on seotud liidu poliitikameetmete ja õiguse rakendamise toetamisega. Selles määratakse kindlaks, milliseid üksusi ja organisatsioone tuleb toetada ja kuidas seda tuleks teha (artikkel 5). Artiklis 6 piiritletakse ameti kohustused suutlikkuse suurendamisel, sh liikmesriikidele küberohtude ennetamiseks ja nendega tegelemiseks teadmiste ja eksperditeadmiste pakkumine, küberturvalisuse strateegiate ajakohastamine ja küberturvalisuse valdkonna töötajate arvu suurendamine. ENISA abistab liikmesriike ka nende teadlikkuse suurendamise alases tegevuses (artikkel 7), analüüsib peamisi turusuundumusi küberturvalisuse valdkonnas ning levitab tehnilisi nõuandeid ja analüüse (artikkel 8). Samuti toetab ja edendab ENISA rahvusvahelist koostööd küberturvalisusega seotud küsimustes, nagu kirjeldatakse artiklis 9.

2. jaos sätestatakse ENISA ülesanded seoses liikmesriikide, liidu üksuste ning liidu institutsioonide, organite ja asutuste küberturvalisuse teenistuse (CERT-EU), küberintsidentidele reageerimise üksuste (CSIRTide) võrgustiku, Euroopa küberkriisiga tegelevate kontaktasutuste võrgustiku (EU-CyCLONe) ja muude sidusrühmade vahelise operatiivkoostööga, sh suuniste andmine ja turvaliste sidevahendite rakendamine (artikkel 10). Samuti aitab ENISA parandada küberohtude ja -intsidentide alast olukorrateadlikkust, luues (muu hulgas) ühe või mitu küberohuteadmuse hoidlat, tehes analüüse ja esitades varajasi hoiatusi (artikkel 11). Varajasi hoiatusi (sisu, ajastust, kättetoimetamist) käsitlevad normid sätestatakse artiklis 12. Selleks et aidata elutähtsatel ja olulistel üksustel valmistuda lunavaraintsidentideks, neile reageerida ja neist taastuda, käitab ENISA ELi küberreservi, nagu selgitatakse artiklis 13, ning teeb vajaduse korral koostööd Europoli ja CSIRTide või muude pädevate asutustega. Artikkel 14 sisaldab sätteid ENISA rolli kohta liidu tasandi küberturvalisuse õppuste korraldamisel, sh nende õppuste iga-aastase jooksva programmi koostamisel. Lisaks neile ülesannetele peaks ENISA tagama vahendid ja platvormid, eelkõige määruse (EL) 2024/2847 artikli 16 lõike 1 kohaselt loodud ühtse teatamisplatvormi (artikkel 15). Samuti peab amet arendama liidu ühist suutlikkust nõrkusehalduse valdkonnas ja osutama nõrkusehalduse teenuseid (artikkel 16).

3. jaos küberturvalisuse sertifitseerimise ja standardimise kohta sätestatakse ENISA asjaomased ülesanded. Artiklis 17 kirjeldatakse ENISA rolli Euroopa küberturvalisuse sertifitseerimise raamistiku arendamisel ja rakendamisel, sh ameti juhtivat rolli kavade ettevalmistamisel ja nende haldamise tagamisel ning suutlikkuse suurendamisel. Artiklis 18 kirjeldatakse, kuidas ENISA peaks osalema tehniliste kirjelduste koostamises ning panustama standardimisse Euroopa ja rahvusvahelisel tasandil, sh krüptoalgoritmide valdkonnas.

---

21 http://data.europa.eu/eli/dir/2022/2555/oj.
22 http://data.europa.eu/eli/reg/2008/765/oj.
23 http://data.europa.eu/eli/reg/2012/1025/oj.

4. jaos kirjeldatakse üksikasjalikult ENISA ülesandeid seoses küberturbeoskuste akadeemiaga. Artikkel 19 sisaldab sätteid, mis puudutavad ENISA rolli Euroopa küberturbeoskuste raamistikus, artiklis 20 sätestatakse ENISA ülesanded seoses Euroopa individuaalsete küberturbeoskuste tõendamise kavade väljatöötamise ja haldamisega. Artiklis 21 sätestatakse nõuded, mis peavad olema täidetud volitatud tõendajaks saamiseks, ja artiklis 22 nõuded, mis on seotud taotluste menetlemisega. ENISA peab andma Euroopa küberturbeoskuste raamistiku ja individuaalsete küberturbeoskuste tõendite kohta avalikku teavet (artikkel 23).

III peatükis käsitletakse ENISA töökorraldust. Ameti haldus- ja juhtimisstruktuuri kuulub ka tegevdirektori asetäitja (artikkel 24). 1. jaos on sätted haldusnõukogu, selle koosseisu, esimehe, koosolekute, ülesannete ja hääletuskorra kohta (artiklid 25–29). 2. jao artiklis 30 sätestatakse, et haldusnõukogu abistab juhatus. 3. jagu sisaldab tegevdirektori ametisse nimetamise, ametist vabastamise ja ametiaja pikendamise korda (artikkel 31) ning tegevdirektori ülesandeid ja vastutust käsitlevaid norme (artikkel 32). Haldusnõukogu võib otsustada luua tegevdirektori abistamiseks tegevdirektori asetäitja ametikoha (4. jagu, artiklid 33 ja 34). Haldusnõukogu peab looma ENISA nõuanderühma, mis peab ENISAt nõustama vastavalt artiklis 35 sätestatud normidele. 6. jaos sätestatakse normid, mis käsitlevad apellatsiooninõukogu moodustamist ja koosseisu (artikkel 36) ja selle liikmeid (artikkel 37). Artiklis 38 määratakse kindlaks asjaolud, mille korral apellatsiooninõukogu liikmed peavad kaebuse menetlemisest hoiduma, ning esitatakse apellatsiooninõukogu liikme osalemise suhtes vastuväite esitamise põhjused. Apellatsiooninõukogule võib esitada kaebuse ENISA otsuse kohta või ENISA tegevusetuse korral (artikkel 39). Artikkel 40 sisaldab sätteid kaebeõigusega isikute, kaebetähtaja ja kaebuse vormi kohta. Artiklites 41–43 sätestatakse normid, mis käsitlevad esialgset läbivaatamist, kaebuste kohta tehtud otsuste läbivaatamist ja asja andmist Euroopa Kohtusse. Artiklis 44 kirjeldatakse ühtse programmdokumendiga seotud protsessi.

IV peatükis käsitletakse ENISA eelarve koostamist ja struktuuri ning selle esitamise ja täitmise norme (artiklid 45–55). Peatükk sisaldab ka sätteid, mis hõlbustavad võitlust pettuste, korruptsiooni ja muu ebaseadusliku tegevuse vastu (artikkel 51).

V peatükis käsitletakse ENISA personali. See sisaldab üldsätteid personalieeskirjade ja muude teenistujate teenistustingimuste kohta ning privileege ja immuniteete reguleerivaid norme (artiklid 56 ja 57). Samuti on selles sätted, mille kohaselt liikmesriigid peavad määrama riiklikud eksperdid, kes lähetatakse ENISAsse kontaktametnikeks, ning milles kirjeldatakse nende kontaktametnike rolli ametis (artikkel 58). Lisaks sisaldab peatükk sätteid, millega reguleeritakse riikide lähetatud ekspertide ja muude ametiväliste töötajate kasutamist (artikkel 59).

VI peatükk sisaldab ENISAga seotud üldsätteid. Selles kirjeldatakse ameti õiguslikku seisundit (artikkel 60) ja määratakse kindlaks ameti asukoht (artikkel 61) ning selles on sätted ameti peakorterilepingu ja tegutsemistingimuste ning ombudsmani tehtava halduskontrolli kohta (artiklid 62 ja 63). Peatükk sisaldab sätteid, millega reguleeritakse selliseid küsimusi nagu vastutus, keelekasutuse kord ja isikuandmete kaitse (artiklid 64–66), ning tundliku salastamata teabe ja salastatud teabe kaitset käsitlevaid turvanorme (artikkel 67). Selles sätestatakse normid koostöö tegemiseks liidu üksuste ja riiklike asutustega (artikkel 68) ning muude sidusrühmadega (artikkel 69). Selles on normid, mis reguleerivad ameti koostööd kolmandate riikide ja rahvusvaheliste organisatsioonidega (artikkel 70).

III JAOTIS. EUROOPA KÜBERTURVALISUSE SERTIFITSEERIMISE RAAMISTIK

Kavandatud määruse III jaotisega kehtestatakse Euroopa küberturvalisuse sertifitseerimise raamistik.

I peatükis tutvustatakse raamistiku eesmärke, kohaldamisala ja menetlusi. Raamistiku eesmärkideks on tugevdada küberturvalisust kogu liidus ning hõlbustada ühtlustatud lähenemisviisi IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ja üksuste turvaoleku sertifitseerimisele (artikkel 71). Samuti peaks raamistik kasutama sertifitseerimist, et lihtsustada kohaldatavate liidu õigusaktide järgimist nõuetele vastavuse eelduse kaudu, tänu millele väheneb ettevõtjate koormus (artikkel 78). Järgmisena kirjeldatakse I peatükis üksikasjalikult menetluslikke aspekte, mille hulka kuuluvad konsultatsioonid Euroopa küberturvalisuse sertifitseerimise strateegiliste prioriteetide üle, komisjoni antav avalik teave kavade väljatöötamise kohta ning uue Euroopa küberturvalisuse sertifitseerimise assamblee loomine (artikkel 72). Pärast komisjonilt üksikasjaliku taotluse saamist peaks ENISA esitama ettevalmistava kava 12 kuu jooksul (artikkel 73). Artiklis 74 sätestatakse Euroopa küberturvalisuse sertifitseerimise rühma arvamuse ja kava esitamise tähtajad, pidades silmas kava vastuvõtmist komisjonis. Artikliga 75 kehtestatakse selge kord olemasolevate kavade haldamiseks, mis võib kaasa tuua kava läbivaatamise (artikkel 76). Kava läbivaatamisel võib tugineda kava tulemuslikkuse ja ühtsele turule avaldatava mõju korrapärasele hindamisele. Artikliga 77 luuakse ENISA-le alus, et koostada Euroopa küberturvalisuse sertifitseerimise kavade väljatöötamise ja haldamise toetamiseks tehnilisi kirjeldusi. Komisjon võib viidata nendele tehnilistele kirjeldustele kava vastuvõtmisel või läbivaatamisel (artikkel 74). Erinevate menetluste abil tagatakse läbipaistvus ja tulemuste kvaliteet, kaasates sertifitseerimiskavade kavandamise, väljatöötamise, vastuvõtmise ja haldamise eri etappidesse eksperte ja üldisi sidusrühmi. Artikliga 79 nähakse ette ENISA spetsiaalne Euroopa küberturvalisuse sertifitseerimise kavade veebisait, mis peaks sisaldama teavet vastuvõetud kavade ning nende alusel välja antud Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide kohta.

II peatükis sätestatakse Euroopa küberturvalisuse sertifitseerimise kavade sisu käsitlevad üldeeskirjad.

Artiklis 80 esitatakse loetelu turbe-eesmärkidest, mille alusel ENISA kava koostab, ning sellega tagatakse kooskõla asjakohaste küberturvalisust käsitlevate õigusaktidega. Euroopa küberturvalisuse sertifitseerimise kava võib sisaldada artiklis 81 sätestatud elemente. Need elemendid peavad olema kooskõlas liidu õigusaktidega ja neid võib kavades ühtlustada, kasutades näidissätteid. Mõlemad artiklid tagavad vajaliku paindlikkuse eri liiki kavade jaoks. Järgmistes artiklites sätestatakse normid, mis on seotud usaldusväärsuse tasemetega (artikkel 82) ja vastavuse enesehindamisega (artikkel 83). Lisaks esitatakse selles peatükis loetelu täiendava teabe kohta, mille IKT-toodete, -teenuste või -protsesside tootja või pakkuja peab kättesaadavaks tegema (artikkel 84).

III peatükis, mis koosneb kolmest jaost, kehtestatakse Euroopa küberturvalisuse sertifitseerimise raamistiku juhtimist käsitlevad normid.

1. jagu sisaldab norme Euroopa küberturvalisuse sertifikaatide väljastamise kohta, muu hulgas kõrge usaldusväärsuse taseme korral (artikkel 85). Lisaks sätestatakse selles normid Euroopa küberturvalisuse sertifitseerimise kavade ühtlustamiseks riiklike küberturvalisuse sertifitseerimise kavade ja küberturvalisuse sertifikaatidega (artikkel 86) ning nähakse ette

võimalus Euroopa küberturvalisuse sertifikaatide rahvusvaheliseks tunnustamiseks samaväärsuse põhimõtte alusel (artikkel 87). Selles jaos kirjeldatakse ka riiklike küberturvalisuse sertifitseerimise asutuste rolli ja nende suhtes kohaldatavaid norme (artikkel 88) ning sätestatakse normid, mis käsitlevad nende asutuste vahelise vastastikuse hindamise mehhanismi, millega tagatakse samaväärsed standardid kogu liidus (artikkel 89), ning nende asutuste vahelist koostööd Euroopa küberturvalisuse sertifitseerimise rühmas (artikkel 90).

2. jaos sätestatakse i) vastavushindamisasutuste akrediteerimise ja nendele asutustele lubade andmise ühtlustatud eeskirjad (artiklid 91–92); ii) teavitamiseeskirjad, sh õigused, et tagada edasine kooskõla asjakohase liidu õiguse ja uue õigusraamistikuga (artikkel 93), ning iii) vaidlustamismenetlus, millega tagatakse vastavushindamisasutustele kehtestatud nõuete täitmine (artikkel 94).

3. jaos sätestatakse õigused ja õiguskaitsevahendid seoses sertifitseerimisotsustega (artikkel 96) ning nõutakse, et liikmesriigid kehtestaksid ja jõustaksid proportsionaalsed karistused õigusnormide rikkumiste eest.

IV JAOTIS

I peatüki artiklis 98 sätestatakse usaldusväärse IKT tarneahela raamistiku kohaldamisala. Raamistikus käsitletakse mittetehnilisi riske direktiivis (EL) 2022/2555 osutatud kriitilise tähtsusega sektorites ja muudes kriitilise tähtsusega sektorites. Selle mehhanismiga määratakse kindlaks kriitilise tähtsusega IKT tarneahelate olulised IKT-varad ning sätestatakse asjakohased ja proportsionaalsed leevendusmeetmed direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste jaoks. Raamistik põhineb komisjoni või vähemalt kolme liikmesriigi taotlusel korraldatavatel liidu tasandi koordineeritud turvariskide hindamistel. Artiklis 99 kirjeldatakse üksikasjalikult, kuidas neid riskihindamisi tehakse, ja nähakse ette, et nende raames tuleks välja pakkuda ka leevendusmeetmeid. Riskihindamine tuleks lõpule viia kuue kuu jooksul alates taotluse esitamisest. Komisjoni taotlusel võib võrgu- ja infoturbe koostöörühm nõustuda lühema tähtajaga. Raamistikuga nähakse ette võimalus rakendada kiirmenetlust, kui viivitamatu sekkumine on põhjendatud, et säilitada siseturu nõuetekohane toimimine, ja kui komisjonil on piisavalt põhjust arvata, et seoses kriitilise tähtsusega IKT tarneahelatega ähvardab liigu julgeolekut märkimisväärne küberoht. Sellisel juhul konsulteerib komisjon liikmesriikidega ühe või mitme leevendusmeetme võtmise vajaduse üle ja viib läbi riskihindamise. Artiklis 100 sätestatakse, et kui artiklis 99 osutatud riskihindamisest või muust allikast, näiteks liidu või liikmesriigi nimel tehtud avalikust avaldusest ilmneb, et kolmas riik põhjustab IKT tarneahelatele tõsiseid ja struktuurseid mittetehnilisi riske, kontrollib komisjon asjaomasest riigist tulenevat ohtu, võttes arvesse artiklis 100 loetletud elemente. Juhuks, kui komisjon jõuab järeldusele, et kolmas riik põhjustab IKT tarneahelatele tõsiseid ja struktuurseid mittetehnilisi riske, sätestatakse artiklis 100 menetlus, mille kohaselt komisjon nimetab asjaomase kolmanda riigi IKT tarneahelate küberturvalisuse seisukohast muret tekitavaks riigiks. Üksustel, mis on asutatud selle artikli kohaselt küberturvalisuse seisukohast muret tekitavaks nimetatud kolmandas riigis või on sellise kolmanda riigi, selles asutatud üksuse või selle kodaniku kontrolli all, ei ole lubatud tegeleda mitme selles artiklis kindlaks määratud tegevusega. Artikliga 101 nähakse ette üldine IKT tarneahela mehhanism, mille kohaselt võib komisjon pärast turvariski hindamist, mille on teinud artikli 99 kohaselt võrgu- ja infoturbe koostöörühm või komisjon ise, võtta artiklites 102 ja 103 sätestatud meetmeid.

Komisjon saab rakendusaktidega kindlaks määrata olulised IKT-varad, mida direktiivi (EL) 2022/2555 I ja II lisas osutatud üksused kasutavad toodete tootmiseks ja teenuste osutamiseks. Artiklis 102 kirjeldatakse üksikasjalikumalt elemente, mida tuleb arvesse võtta oluliste IKT-varade kindlaksmääramisel. Artikliga 103 kehtestatakse võimalikud leevendusmeetmed IKT tarneahelas. Komisjon võib võtta rakendusaktidega vastu otsuseid, et kriitilise tähtsusega sektorites ja muudes kriitilise tähtsusega sektorites tegutsevate üksuste suhtes tuleb kohaldada selles artiklis kirjeldatud konkreetseid leevendusmeetmeid.

Komisjon kehtestab rakendusaktidega loetelud suure riskiga tarnijatest, kelle suhtes kohaldatakse artikli 103 lõike 1 või 7 kohaselt vastu võetud rakendusaktides sätestatud keelde või artikli 110 lõikes 1 osutatud keeldu, olles hinnanud tarnijate tegutsemist ning omandi- ja kontrollistruktuure. Komisjon peaks konsulteerima asjaomaste tarnijate ja pädevate asutustega (artikkel 104).

Üksus, mis on asutatud artikli 100 kohaselt küberturvalisuse seisukohast muret tekitavaks nimetatud kolmandas riigis või on sellisest kolmandast riigist pärit üksuse kontrolli all, võib taotleda luba pakkuda direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste oluliste IKT-varade IKT-komponente ning osaleda selliste IKT-komponentidega seotud riigihangetes. Artiklis 105 täpsustatakse, mida selline taotlus peaks sisaldama ja milline on sellise erandi tegemise kord. Artiklis 106 sätestatakse kõnealuste üksuste kaitseõigus. Komisjon peab erandeid käsitlevate otsuste avalikku registrit (artikkel 107). Artiklites 108 ja 109 sätestatakse erandi tegemisega seotud konfidentsiaalsuseeskirjad ja tasud.

II peatükis nähakse ette usaldusväärse IKT tarneahela raamistiku kohaldamine elektroonilise side mobiili-, püsi- ja satelliitvõrkude suhtes, millega tagatakse kooskõla kavandatava digivõrkude õigusaktiga.

Elektroonilise side mobiili-, püsi- ja satelliitvõrkude olulised IKT-varad sätestatakse II lisas. Üleminekuperiood suure riskiga tarnijatelt mobiilivõrgu oluliste IKT-varade jaoks saadud IKT-komponentide järkjärguliseks kasutuselt kõrvaldamiseks ei tohi olla pikem kui 36 kuud alates käesoleva määruse jõustumisest. Üleminekuperioodid elektroonilise side püsi- ja satelliitvõrkude jaoks määrab komisjon kindlaks rakendusaktidega. Komisjonil on õigus võtta vastu delegeeritud õigusakte, et muuta kindlaksmääratud olulisi IKT-varasid ja üleminekuperioode, sh tulevaste mobiilsidepõlvkondade jaoks (artikkel 110). Artiklis 111 sätestatakse, et elektroonilise side mobiili-, püsi- ja satelliitvõrkude pakkujad ei tohi mingil kujul kasutada, paigaldada ega integreerida suure riskiga tarnijate IKT-komponente ning et neile ei saa anda üldist ega individuaalset luba.

Pädevad asutused, järelevalve ja täitmise tagamine, jurisdiktsioon, kaitseõigus (III peatükk)

III peatükis sätestatakse normid pädevate asutuste, järelevalve, täitmise tagamise ja jurisdiktsiooni kohta.

Artiklites 112–114 määratakse kindlaks liikmesriikide volitused, vahendid ja vastutus IV jaotise sätete rakendamise ja täitmise tagamisel. Liikmesriigid peavad määrama ühe või mitu pädevat asutust, millest tuleb komisjonile teatada. Artikliga 113 nähakse ette, et komisjon loob liikmesriikide pädevate asutuste ja komisjoni koostöövõrgustiku, et hõlbustada nõuete täitmist, ning artiklis 114 määratakse kindlaks järelevalve- ja täitemeetmed, mida pädevatel asutustel on õigus võtta. Artiklis 115 sätestatakse karistused IV jaotise sätete rikkumise eest. Artiklis 116 kirjeldatakse üksikasjalikult liikmesriikide võimalust üksteist abistada, kui üksuste tegevus on piiriülene või kui nende olulised IKT-varad asuvad mitmes liikmesriigis. Artiklis 117 sätestatakse kohtualluvust ja territoriaalsust käsitlevad normid.

VI JAOTIS. LÕPPSÄTTED

Kavandatud määruse VI jaotis sisaldab lõppsätteid, mis käsitlevad rakendusaktide ja delegeeritud õigusaktide vastuvõtmist, kavandatud määruse hindamist ning määruse (EL) 2019/881 kehtetuks tunnistamist ja jätkamist. Selles sätestatakse ka kavandatud määruse jõustumise kuupäev.

2026/0011 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

mis käsitleb Euroopa Liidu Küberturvalisuse Ametit (ENISA), Euroopa küberturvalisuse sertifitseerimise raamistikku ja IKT tarneahela turvalisust ning millega tunnistatakse kehtetuks määrus (EL) 2019/881 (küberturvalisuse 2. määrus)

(EMPs kohaldatav tekst)

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust[24],

võttes arvesse Regioonide Komitee arvamust[25],

toimides seadusandliku tavamenetluse kohaselt

ning arvestades järgmist:

(1) Pärast Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881[26] vastuvõtmist on geopoliitiline olukord ning tehnoloogia- ja poliitikamaastik märkimisväärselt muutunud. Küberintsidendid, olgu need põhjustatud süsteemirikkest, inimlikust eksimusest, pahatahtlikust tegevusest või loodusnähtustest, on järsult sagenenud ja küberründed on muutunud keerukamaks, kahjustades elutähtsaid üksusi, ettevõtjaid ja üldsust. Küberkuritegevuse ökosüsteem on laienenud, kusjuures selle keskmes on lunavararünded. Sagedamaks on muutunud ka tarneahelat kahjustavad intsidendid, mida põhjustavad kurjategijad rahalise kasu saamiseks või riiklikud osalejad häirete, spionaaži, desinformatsiooni või sõjategevuse huvides. Olles osa laiemast hübriidstrateegiast, levivad pahatahtlikust kübertegevusest ja süsteemiriketest tulenevad intsidendid kaugemale ning häirivad olulisi teenuseid, õõnestavad usaldust institutsioonide vastu ning mõjutavad liidu ühiskonna valmisolekut ja kaitsevalmidust. Sellised intsidendid on tõestanud oma potentsiaali mõjutada majandustegevust, finantsstabiilsust ja inimeste elu. Samal ajal seab elutähtsa tsiviiltaristu ja elutähtsate tsiviilsüsteemide haavatavus ohtu tsiviiltaristule ja -süsteemidele tugineva kaitsevõime.

---

24 ELT C […], lk […].

25 ELT C […], lk […].

26 Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (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) (ELT L 151, 7.6.2019, lk 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(2) Samaaegselt avaldavad küberturvalisusele ja küberkaitsele murrangulist mõju kujunemisjärgus tehnoloogiad, nagu tehisintellekt ja kvantarvutus. Need toovad kaasa kaitsevahendite ja vastaste taktika ümberkujundamise, seades niiviisi ohtu küberturvalisuse ja küberkaitse, ent pakuvad samuti võimalusi tehnoloogia arenguks. Kujunemisjärgus tehnoloogiad võivad aidata küberturvalisust parandada, tõhustades ohtude avastamist või automaatset reageerimist intsidentidele, kuid need suurendavad ka organisatsioonide üldist ründepinda, need võivad olla manipuleerimise sihtmärk ning need võivad kahjustada turbemeetmete, näiteks krüpteerimise pikaajalist elujõulisust.

(3) Selle arengu arvessevõtmiseks on liit tõhustanud oma õiguslikke ja poliitilisi vahendeid. Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2022/2555[27] tugevdatakse elutähtsa taristu küberturvalisust; füüsilise julgeoleku osas täiendab seda direktiivi Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2557[28]. Euroopa Parlamendi ja nõukogu määrusega (EL) 2024/2847[29] edendatakse digielemente sisaldavate toodete küberturvalisust. Euroopa Parlamendi ja nõukogu määrusega (EL) 2025/38[30] suurendatakse liidu ühist reageerimissuutlikkust ning nõukogu 6. juuni 2025. aasta soovitusega ELi küberkriiside ohjamise tegevuskava kohta[31] (edaspidi „kübervaldkonna tegevuskava käsitlev soovitus“) toetatakse liidu tasandi koostööd kriisiohje valdkonnas. 5G küberturvalisuse meetmepakett[32] on esimene samm liidu tasandi koordineeritud lähenemisviisi suunas 5G-võrkude turvalisuse tagamiseks. Komisjoni teatises küberturbeoskuste akadeemia kohta[33] käsitletakse küberturvalisuse valdkonna talendinappuse üha suuremat probleemi. Peale selle on küberturvalisuse raamistikku tõhustatud valdkondlike õigusaktidega, eelkõige Euroopa Parlamendi ja nõukogu määrusega (EL) 2022/2554[34] finantssektori puhul, komisjoni delegeeritud

---

27 Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

28 Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2557, mis käsitleb elutähtsa teenuse osutajate toimepidevust ja millega tunnistatakse kehtetuks nõukogu direktiiv 2008/114/EÜ (ELT L 333, 27.12.2022, lk 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

29 Euroopa Parlamendi ja nõukogu 23. oktoobri 2024. aasta määrus (EL) 2024/2847, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrusi (EL) nr 168/2013 ja (EL) 2019/1020 ning direktiivi (EL) 2020/1828 (küberkerksuse määrus) (ELT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

30 Euroopa Parlamendi ja nõukogu 19. detsembri 2024. aasta määrus (EL) 2025/38, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks, ning millega muudetakse määrust (EL) 2021/694 (kübersolidaarsuse määrus) (ELT L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

31 ELT C, C/2025/3445, 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3445/oj.

32 Võrgu- ja infoturbe koostöörühm, „Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures“ (5G-võrkude küberturvalisus – ELi riskimaandamismeetmete pakett), CG Publication 1/2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

33 Komisjoni 18. aprilli 2023. aasta teatis Euroopa Parlamendile ja nõukogule „Korvata küberturvalisuse valdkonna talendinappus edendamaks ELi konkurentsivõimet, majanduskasvu ja kerksust („Küberturbeoskuste akadeemia“), COM(2023) 207 final.

34 Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

määrusega (EL) 2024/1366[35] elektri allsektori puhul, komisjoni delegeeritud määrusega (EL) 2022/1645[36] ja komisjoni rakendusmäärusega (EL) 2023/203,[37] samuti asjakohaste lennundusjulgestusnormidega, mis on sätestatud komisjoni määruses (EL) 2019/1583[38] lennutranspordi allsektori jaoks, ning muude poliitikadokumentidega, nagu komisjoni teatis Euroopa haiglate ja tervishoiuteenuse osutajate küberturvalisuse tegevuskava kohta[39]. Liidu üksusi tugevdatakse ka Euroopa Parlamendi ja nõukogu määrusega (EL, Euratom) 2023/2841,[40] millega on nähtud ette meetmed, mille eesmärk on saavutada küberturvalisuse ühtlaselt kõrge tase liidu institutsioonides, organites ja asutustes. Selle küberturvalisust käsitleva tõhustatud õigusraamistikuga on veelgi täpsustatud ENISA ülesandeid.

(4) Sellega seoses – nagu on öeldud Euroopa sisejulgeoleku strateegias ProtectEU,[41] mis täiendab ELi kriisivalmiduse strateegiat,[42] – on liidu ühiskonna ja majanduse valmisoleku, turvalisuse ja vastupanuvõime tagamiseks vaja tugevat koordineerimist Euroopa tasandil, usaldust ja teabevahetust sidusrühmade vahel, tugevaid raamistikke IKT-toodete, -teenuste ja -protsesside ning hallatud turbeteenuste turvalisuse tagamiseks ning küberturvalisuse valdkonna tööjõu suurendamist ja tugevdamist. Strateegias kutsutakse ka üles tugevdama IKT tarneahelaid, tagades oluliste varade puhul Euroopa tehnoloogilise suveräänsuse, mis suurendaks liidu vastupanuvõimet ja

---

35 Komisjoni 11. märtsi 2024. aasta delegeeritud määrus (EL) 2024/1366, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2019/943 ning kehtestatakse võrgueeskiri piiriüleste elektrivoogude küberturvalisust käsitlevate sektoripõhiste normide kohta (ELT L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

36 Komisjoni 14. juuli 2022. aasta delegeeritud määrus (EL) 2022/1645, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139 rakendamise eeskirjad nõuete osas, mis on seotud selliste infoturvariskide juhtimisega, mis võivad mõjutada komisjoni määrustega (EL) nr 748/2012 ja (EL) nr 139/2014 hõlmatud organisatsioonide lennuohutust, ning muudetakse komisjoni määrusi (EL) nr 748/2012 ja (EL) nr 139/2014 (ELT L 248, 26.9.2022, lk 18–31, ELI: http://data.europa.eu/eli/reg_del/2022/1645/oj).

37 Komisjoni 27. oktoobri 2022. aasta rakendusmäärus (EL) 2023/203, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139 rakendamise eeskirjad nõuete osas, mis on seotud selliste infoturvariskide juhtimisega, mis võivad mõjutada lennuohutust ning mida kohaldatakse komisjoni määrustega (EL) nr 1321/2014, (EL) nr 965/2012, (EL) nr 1178/2011, (EL) 2015/340 ning komisjoni rakendusmäärustega (EL) 2017/373 ja (EL) 2021/664 hõlmatud organisatsioonide ning komisjoni määrustega (EL) nr 748/2012, (EL) nr 1321/2014, (EL) nr 965/2012, (EL) nr 1178/2011, (EL) 2015/340 ja (EL) nr 139/2014, komisjoni rakendusmäärustega (EL) 2017/373 ja (EL) 2021/664 hõlmatud pädevate asutuste suhtes, ning muudetakse komisjoni määrusi (EL) nr 1178/2011, (EL) nr 748/2012, (EL) nr 965/2012, (EL) nr 139/2014, (EL) nr 1321/2014, (EL) 2015/340 ning komisjoni rakendusmäärusi (EL) 2017/373 ja (EL) 2021/664 (ELT L 31, 2.2.2023, lk 1, ELI: http://data.europa.eu/eli/reg_impl/2023/203/oj).

38 Komisjoni 25. septembri 2019. aasta rakendusmäärus (EL) 2019/1583, millega muudetakse komisjoni rakendusmäärust (EL) 2015/1998 (millega nähakse ette lennundusjulgestuse ühiste põhistandardite rakendamise üksikasjalikud meetmed) küberkaitsemeetmete osas (ELT L 246, 26.9.2019, lk 15–18, ELI: http://data.europa.eu/eli/reg_impl/2019/1583/oj).

39 Komisjoni 15. jaanuari 2025. aasta teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Euroopa haiglate ja tervishoiuteenuse osutajate küberturvalisuse tegevuskava“, COM(2025) 10 final.

40 Euroopa Parlamendi ja nõukogu 13. detsembri 2023. aasta määrus (EL, Euratom) 2023/2841, millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes (ELT L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

41 Komisjoni 1. aprilli 2025. aasta teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Euroopa sisejulgeoleku strateegia ProtectEU“, COM(2025) 148 final.

42 Ühisteatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele ELi kriisivalmiduse strateegia kohta, JOIN(2025) 130 final.

millest võiks olla kasu küberkaitsealaste jõupingutuste tegemisel. Peale selle peetakse ELi majandusjulgeoleku tugevdamist käsitlevas teatises[43] esmatähtsaks vajadust takistada juurdepääsu tundlikule teabele ja andmetele, mis võib kahjustada ELi majandusjulgeolekut, ning ennetada ja leevendada ELi majandust mõjutavaid ELi elutähtsa taristu häireid. Teatises tunnistatakse, et selles mängivad olulist rolli tõhusad küberturvalisuse meetmed.

(5) Ulatuslikud küberintsidendid, mis kahjustavad elutähtsat taristut, digiteenuseid või olulisi ühiskondlikke funktsioone, võivad avaldada mõju elanikkonnale, mistõttu on vaja võtta liidu tasandil koordineeritud elanikkonnakaitse- ja kriisiohjemeetmeid. Kooskõlas kõiki ohte hõlmava lähenemisviisiga, mis on sätestatud Euroopa kriisivalmiduse strateegias ja liidu elanikkonnakaitse mehhanismi käsitlevas otsuses nr 1313/2013/EL, tuleks käesoleva määruse kohast olukorrateadlikkuse, intsidentidele reageerimise ja õppuste korda kasutada liidu kriisiohjes, eelkõige hädaolukordadele reageerimise koordineerimiskeskuse (ERCC) kaudu.

(6) Käesolev ettepanek on kooskõlas seda täiendava [ettepanekuga võtta vastu direktiiv, millega täiendatakse [määruse (EL) 2019/881 läbivaatamist] ja muudetakse direktiivi (EL) 2022/2555 seoses küberturvalisuse ühtlaselt kõrge taseme tagamise meetmete rakendamise lihtsustamisega kogu liidus] ning [ettepanekuga võtta vastu määrus digivaldkonna õigusaktide lihtsustamise kohta (digivaldkonna koondpakett)],[44] millega nähakse ette ENISA kohustus luua intsidentidest teatamise jaoks ühtne kontaktpunkt, mis võimaldab üksustel samaaegselt täita mitme õigusakti kohaseid intsidentidest teatamise kohustusi.

(7) ENISA loodi Euroopa Parlamendi ja nõukogu määrusega (EÜ) nr 460/2004[45] selleks, et aidata kaasa kõrgetasemelise ja toimiva võrgu- ja infoturbe tagamisele liidus ning arendada võrgu- ja infoturbekultuuri kodanike, tarbijate, ettevõtete ja ametiasutuste heaks. ENISA volitusi pikendati kolm korda, enne kui talle anti määrusega (EL) 2019/881 alalised volitused. Selleks et paremini rahuldada muutuval ohu- ja tehnoloogiamaastikul tekkivaid vajadusi, eelkõige mis puudutab operatiivkoostööd ja suurenenud vajadust küberturbespetsialistide järele, tuleks ENISA volitusi veelgi tugevdada. Õiguskindluse huvides tuleks määrus (EL) 2019/881 asendada.

(8) Muutuval ohumaastikul, kus küberintsidendid on üha märkimisväärsemad, on olulisem kui kunagi varem suurendada üksikisikute, avaliku sektori asutuste ja ettevõtjate usaldust igapäevaselt kasutatava tehnoloogia vastu. Usalduse suurendamisele saab kaasa aidata Euroopa küberturvalisuse sertifitseerimise raamistiku kohase kogu liitu hõlmava sertifitseerimise tõhustamisega, et tagada ühised küberturvalisuse nõuded ja hindamiskriteeriumid kõigi liikmesriikide turgudel ja kõigis sektorites. Uues raamistikus tuleks sätestada Euroopa küberturvalisuse sertifitseerimise kavade peamised horisontaalsed nõuded ning võimaldada tunnustada ja kasutada Euroopa küberturvalisuse sertifikaate ja ELi vastavusdeklaratsioone kõigis liikmesriikides. Sellega tuleks kehtestada menetlus ja juhtimisraamistik, mis võimaldab Euroopa küberturvalisuse sertifitseerimise kavade õigeaegset ja prognoositavat väljatöötamist ja haldamist. Euroopa küberturvalisuse sertifitseerimise kavu tuleks kohaldada

---

43 Ühisteatis Euroopa Parlamendile ja nõukogule „ELi majandusjulgeoleku tugevdamine“, JOIN(2025) 977 final.

44 COM(2025) 837 final.

45 Euroopa Parlamendi ja nõukogu 10. märtsi 2004. aasta määrus (EÜ) nr 460/2004, millega luuakse Euroopa Võrgu- ja Infoturbeamet (ELT L 77, 13.3.2004, lk 1, ELI: http://data.europa.eu/eli/reg/2004/460/oj).

kõikides liikmesriikides ühetaoliselt, et tagada küberturvalisuse nõuete ühtlustatud rakendamine, luua võrdsed tingimused ja vältida soodsama sertifitseerimise otsimist, mida põhjustaks nõuete erinev rangus liikmesriikides. ENISA-l peaks olema kavade väljatöötamisel keskne roll tänu tehnilistele kirjeldustele ja selle tagamisele, et kavad püsivad tehniliselt ajakohased. Selleks et rahuldada tulemuslikult turu vajadusi, tuleks raamistikuga näha lisaks ette võimalus sertifitseerida üksustele suunatud küberriskide juhtimise meetmeid ja hõlbustada küberturvalisuse valdkonnas kohaldatavate muude liidu õigusaktide järgimist. Kooskõla kehtiva liidu õigusega, näiteks määrusega (EL) 2024/2847 ja direktiiviga (EL) 2022/2555, on oluline selleks, et Euroopa küberturvalisuse sertifitseerimise kavad aitaksid vähendada ettevõtjate nõuete täitmisega seotud koormust, suurendada kavade atraktiivsust ja tugevdada liidu küberkerksust.

(9) ENISA missioon peaks olema toetada liikmesriike ja liidu üksusi, et saavutada liidus küberturvalisuse, vastupanuvõime ja usalduse kõrge tase. Selleks peaks ENISA tegutsema küberturvalisuse alast nõu ja eksperditeadmisi pakkuva kontaktüksusena ning keskenduma oma liidu tasandil tehtavas töös neljale küberturvalisuse põhivaldkonnale. Esiteks peaks ENISA toetama liikmesriike küberturvalisust käsitleva liidu poliitika ja õigusaktide järjekindlal rakendamisel ning abistama liikmesriike suutlikkuse suurendamise meetmete kaudu, et pidevalt parandada liikmesriikide valmisolekut, vastupanuvõimet ja reageerimissuutlikkust. Teiseks peaks ENISA aitama liidu tasandil kaasa liikmesriikide operatiivkoostööle ning küberohtude ja -intsidentide alase ühise olukorrateadlikkuse suurendamisele liikmesriikide ja liidu üksuste seas. Kolmas põhivaldkond peaks olema küberturvalisuse sertifitseerimine ja standardimine ning neljas küberturbeoskuste akadeemia rakendamine, mis peaks aitama kaasa liikmesriikide vahel ülekantavaid oskusi omava Euroopa küberturvalisuse valdkonna töötajaskonna jõudsale arengule.

(10) Määruses (EL, Euratom) 2023/2841, millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes, on sätestatud CERT-EU kui liidu institutsioonide, organite ja asutuste küberturvalisuse teenistuse volitused, et aidata kaasa liidu üksuste salastamata IKT-keskkonna turvalisusele, andes neile küberturvalisuse alast nõu, toetades neid intsidentide ennetamisel, avastamisel, käsitlemisel, leevendamisel, neile reageerimisel ja neist taastumisel ning tegutsedes nende küberturvalisuse alase teabevahetuse ja intsidentidele reageerimise koordineerimise keskusena. Peale selle on CERT-EU ülesanne pakkuda liidu üksustele asjakohaseid küberturbeteenuseid. Osana oma missioonist peaks ENISA toetama ka liidu üksusi. Eelkõige peaks ta selleks tegema CERT-EUga struktureeritud koostööd suutlikkuse suurendamise, operatiivkoostöö ja küberohtude pikaajalise strateegilise analüüsi valdkonnas. Kui see on asjakohane, võib ENISA struktureeritud koostööd CERT-EUga võimendada, et pakkuda oma küberturbeteenuseid või tuge, millel võib olla liidu üksuste jaoks lisaväärtus, tehes seda koordineeritud viisil, et tagada CERT-EU jõupingutuste koostoime.

(11) ENISA üks põhiülesandeid peaks olema toetada liikmesriike küberturvalisust käsitlevate liidu poliitikameetmete ja õiguse, eelkõige direktiivi (EL) 2022/2555, määruse (EL) 2024/2847 ja määruse (EL) 2025/38 järjekindlal rakendamisel. Selleks et aidata saavutada liidu küberturvalisuse *acquis*' järjekindel ja tõhus rakendamine, peaks ENISA avaldama tehnilisi suuniseid ja aruandeid, andma nõu ja jagama parimaid tavasid ning hõlbustama parimate tavade vahetamist pädevate asutuste vahel. Lisaks hindab ENISA küberturvalisuse olukorda liidus ja võtab selle kohta vastu aruande kooskõlas direktiivi (EL) 2022/2555 artikliga 18. Samuti peaks ENISA-l

olema võimalik reageerida liikmesriikide ja vajaduse korral liidu üksuste nõuande- ja abitaotlustele enda pädevusse kuuluvates küsimustes.

(12) Selleks et soodustada avaliku ja erasektori vahelist ning erasektori sisest koostööd, eelkõige eesmärgiga toetada elutähtsa taristu kaitset, peaks ENISA toetama teabe jagamist sektorite sees ja vahel, eriti mis puudutab direktiivi (EL) 2022/2555 I ja II lisas loetletud sektoreid, ning teabe jagamist määruse (EL) 2024/2847 kohaldamisalasse kuuluvate digielemente sisaldavate toodete kohta. Pakutav tugi võib seisneda olemasolevate vahendite ja menetlustega seotud parimate tavade ja suuniste jagamises ning suuniste andmises selle kohta, kuidas lahendada teabe jagamisega seotud regulatiivseid küsimusi näiteks hõlbustades valdkondlike teabe jagamise ja analüüsimise keskuste loomist.

(13) Strateegilise koostöö ja teabevahetuse toetamiseks ja lihtsustamiseks peaks ENISA aitama kaasa direktiiviga (EL) 2022/2555 loodud võrgu- ja infoturbe koostöörühma tööle, eelkõige pakkudes eksperditeadmisi ja andes nõu ning hõlbustades parimate tavade vahetamist riskide ja intsidentide kohta, muu hulgas seoses piiriüleste sõltuvustega. ENISA peaks aitama kaasa ka Euroopa Parlamendi ja nõukogu määrusega (EL) nr 910/2014[46] loodud Euroopa digiidentiteedi koostöörühma, Euroopa küberturvalisuse sertifitseerimise rühma ja määrusega (EL) 2024/2847 loodud halduskoostöörühma tööle.

(14) Avatud interneti avalik tuum, nimelt selle põhilised protokollid ja taristu, mis on üleilmne avalik hüve, tagab interneti kui terviku põhifunktsionaalsuse ja toetab selle tavapärast toimimist. ENISA peaks oma volituste piires toetama avatud interneti avaliku tuuma turvalisust ja kerksust ning selle toimimise stabiilsust, sh põhiprotokollide (eelkõige domeeninimede süsteem, piirilüüsi protokoll ja internetiprotokolli versioon 6) turvalist kasutuselevõttu ja käitamist ning domeeninimede süsteemi (nt kõigi tippdomeenide) käitamist, edendades parimaid tavasid, suuniseid ja koostööd kooskõlas väljakujunenud ülemaailmse mitut sidusrühma hõlmava interneti haldamise korraga ning asjaomaste rahvusvaheliste tehniliste ja operatiivasutuste vastavate rollide ja kohustustega.

(15) ENISA tegutseb küberturvalisuse alast nõu ja eksperditeadmisi pakkuva kontaktüksusena. Seepärast peaks ENISA komisjoni taotlusel abistama komisjoni eksperditeadmiste, tehnilise nõu, teabe, analüüside, sh teostatavusuuringute, arvamuste ja ettevalmistava tööga mis tahes konkreetses küberturvalisusega seotud küsimuses, et anda komisjonile teavet poliitika kujundamiseks ja hõlbustada komisjoni järelevalvet küberturvalisust käsitlevate liidu õigusaktide rakendamise üle.

(16) Samamoodi, võttes arvesse ENISA eksperditeadmisi, peaks ENISA abistama liikmesriike nende püüdlustes luua ja parandada suutlikkust ja valmisolekut ennetada ja avastada küberohte ja -intsidente ning neile reageerida, ning seoses võrgu- ja infosüsteemide turvalisusega. Eeskätt peaks ENISA toetama direktiiviga (EL) 2022/2555 ette nähtud küberintsidentidele reageerimise üksuste (CSIRTid) arendamist ja tõhustamist, et saavutada nende ühtmoodi kõrge küpsuse tase kogu liidus.

---

[46] Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.8.2014, lk 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(17) ENISA on toetanud ja peaks ka edaspidi toetama liikmesriike riiklikke küberturvalisuse strateegiaid käsitlevate suuniste koostamisel ja rakendamisel, aidates niiviisi kaasa nende strateegiate vastuvõtmisele ja rakendamisele kõigis liikmesriikides. ENISA peaks edendama kõnealuste strateegiate levitamist interaktiivse riiklike küberturvalisuse strateegiate kaardi kaudu ning peaks jätkuvalt jälgima strateegiate rakendamisel tehtavaid edusamme, sealhulgas toetama sellega seoses peamiste tulemusnäitajate väljatöötamist.

(18) Määrusega (EL, Euratom) 2023/2841 on antud institutsioonidevahelisele küberturvalisuse nõukojale ülesanne toetada liidu üksusi nende turvaoleku taseme tõstmisel ning CERT-EU-le ülesanne aidata kaasa kõigi liidu üksuste salastamata IKT-keskkonna turvalisusele. Tuginedes oma kogemustele küberturvalisuse valdkonnas, peaks ENISA seda nõukoda ja CERT-EUd nende ülesannete täitmisel toetama vastavalt määrusele (EL, Euratom) 2023/2841, sh aidates kaasa küberohtude analüüsile, olukorrateadlikkusele, küberturvalisuse õppustele, intsidentidele reageerimise koordineerimisele ning oskusteabe ja parimate tavade vahetamisele.

(19) Võttes arvesse ENISA eksperditeadmisi, peaks ENISA liikmesriikide ja liidu avaliku sektori asutuste suutlikkuse täiendamiseks pakkuma Euroopa küberturbeoskuste raamistikku kasutades koolitusi, eelkõige et toetada poliitikameetmete tulemuslikku rakendamist, operatiivkoostööd ja teadlikkuse suurendamist.

(20) Selleks et tagada koostoime küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskusega ning Euroopa Parlamendi ja nõukogu määruse (EL) 2021/887[47] kohaselt loodud riiklike koordineerimiskeskuste võrgustikuga, peaks ENISA neid toetama, jagades teavet praeguste ja tekkivate riskide ja küberohtude, sh info- ja kommunikatsioonitehnoloogiaga seotud riskide ja ohtude kohta.

(21) Kriisivalmiduse strateegias rõhutatakse, et selleks, et suurendada kodanike võimet panna vastu võimalikele kriisidele, on oluline digikirjaoskus, mis sõltub elementaarsete digioskuste omandamisest. Nagu on rõhutatud komisjoni teatises oskuste liidu kohta,[48] ei ole peaaegu pooltel täiskasvanutel paraku elementaarseid digioskusi, kuigi neid on vaja rohkem kui 90 % töökohtadest. Kandmaks hoolt selle eest, et praegustel ja potentsiaalsetel tulevastel töötajatel on kiiresti arenevas digikeskkonnas vajalikud oskused, ning aitamaks kaasa Euroopa küberturvalisuse talendireservi väljaarendamisele, peaks ENISA toetama küberturvalisuse alase teadlikkuse suurendamise meetmeid, nagu Euroopa küberturvalisuse võistlus, mille eesmärk on meelitada ligi talente ning aidata teavitada haridusest ja oskustest, mida küberturvalisusega seoses vaja läheb. Sellega seoses peaks ENISA koordineerima küberturvalisuse võistlusi, küberlahinguid ja sarnaseid praktilisi õppusi, et parandada küberturvalisusega seotud oskusi ja edendada suutlikkuse suurendamist kogu liidus. Teadlikkuse suurendamise meetmete võtmisel peaks ENISA tagama, et elluviidavad meetmed vastavad riikide ametiasutuste ja liidu üksuste, ent samuti ettevõtjate, eelkõige VKEde, ning haridus- ja koolitusasutuste vajadustele, pakkudes praktilisi

[47] Euroopa Parlamendi ja nõukogu 20. mai 2021. aasta määrus (EL) 2021/887, millega luuakse küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus ning riiklike koordineerimiskeskuste võrgustik (ELT L 202, 8.6.2021, lk 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[48] Komisjoni 5. märtsi 2025. aasta teatis Euroopa Parlamendile, Euroopa Ülemkogule, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Oskuste liit“, COM(2025) 90 final.

raamistikke ja koolitusi, nagu terviklikud teadlikkuse suurendamise töövahendid. ENISA peaks ka tulevikus koostama praktilisi ja rakendatavaid suuniseid, et toetada küberturvalisust käsitleva liidu poliitika ja õigusaktide rakendamist. Samuti peaks ENISA püüdma pakkuda asjakohast teavet kohaldatavate sertifitseerimiskavade kohta, näiteks andes suuniseid ja soovitusi.

(22) Selleks et toetada küberturvalisuse sektoris tegutsevaid ettevõtjaid ja küberturvalisuse lahenduste kasutajaid ning tagada käesoleva määruse III jaotise tõhus rakendamine, peaks ENISA välja töötama n-ö turuseirekeskuse ja seda alal hoidma, analüüsides korrapäraselt peamisi suundumusi nii küberturvalisuse turu nõudluse kui ka pakkumise poolel ja levitades selle kohta teavet. Peale selle peaks ENISA selleks, et toetada määruse (EL) 2025/38 kohaselt loodud ELi küberreservi kasutajad, koostama ülevaate selliste kasutajate jaoks vajalikest teenustest ja nende teenuste kättesaadavusest kooskõlas kõnealuse määrusega.

(23) Küberohud on üleilmne probleem. Küberturvalisuse parandamiseks, sh ühiste käitumisnormide ja lähenemisviiside kindlaksmääramiseks, on vaja tihedamat rahvusvahelist koostööd. Sellega seoses peaks ENISA toetama liidu koostööd kolmandate riikidega, keskendudes liidu kandidaatriikidele, ja rahvusvaheliste organisatsioonidega, näiteks NATOga, pakkudes vajaduse korral komisjonile ja asjaomastele liidu üksustele vajalikke eksperditeadmisi ja analüüse. ENISA tegevus rahvusvahelisel areenil peaks olema alati kooskõlas liidu prioriteetidega.

(24) Selleks et aidata saavutada küberturvalisuse kõrge tase liidus, peaks ENISA toetama operatiivkoostööd liikmesriikide seas (koostöös CERT-EUga) ning liidu üksuste ja sidusrühmade seas. Selleks tuleks ENISA rolli tugevdada. ENISAst peaks saama CSIRTide võrgustiku liige, kes aitab kaasa võrgustikus toimuvale teabevahetusele ja analüüsile. ENISA peaks veelgi edendama ja toetama asjaomaste CSIRTide vahelist koostööd CSIRTide hallatavates või kaitstavates võrgustikes või taristutes esinevate intsidentide, rünnete või häirete korral. ENISA aktiivne toetus CSIRTide võrgustiku ja Euroopa küberkriisiga tegelevate kontaktasutuste võrgustiku (EU-CyCLONe) tööle peaks võimaldama neil võrgustikel jätkata oma küpsustaseme tõstmist. ENISA roll sellise koostöö toetamisel hõlmab võitlust ohtude vastu, mis ähvardavad demokraatlike institutsioonide, valimiste ja muude protsesside turvalisust ja terviklikkust ning elutähtsat taristut, millest need sõltuvad, kooskõlas teatisega „Euroopa demokraatia kaitsekilp: tugevate ja vastupanuvõimeliste demokraatlike riikide võimestamine“[49].

(25) Selleks et toetada suutlikkuse suurendamist, operatiivkoostööd ja küberohtude pikaajalist strateegilist analüüsi, peaks ENISA kasutama struktureeritud koostöö raames, näiteks spetsiaalsete kokkulepete alusel, CERT-EU olemasolevaid tehnilisi ja operatiivseid eksperditeadmisi.

(26) Selleks et tugevdada küberturvalisust kogu liidus ning tagada kiire ja tulemuslik reageerimine küberohtudele, peaks ENISA pakkuma liikmesriikidele nende taotluse korral tuge, sh andma nõu, kuidas parandada liikmesriikide intsidentide ennetamise, avastamise, neile reageerimise ja neist taastumise suutlikkust, hõlbustama direktiivis (EL) 2022/2555 määratletud oluliste intsidentide tehnilist käsitlemist, eelkõige toetades tehniliste lahenduste vabatahtlikku jagamist liikmesriikide vahel, või tagama küberohtude ja -intsidentide analüüsimise. ENISA peaks samuti abistama EU-CyCLONe-t aruannete koostamisel liidu ja liikmesriikide poliitilise tasandi jaoks.

[49] JOIN(2025) 791 final.

(27) Selleks et vähendada avatust välistele sekkumistele, manipuleerimist tarneahelaga ja strateegiliste andmete väljaimbumist, peaks ENISA kasutama CSIRTide võrgustikus ja EU-CyCLONe-s turvalisi sidevahendeid. Kübervaldkonna tegevuskava käsitleva soovituse põhjal peaksid neid vahendeid pakkuma juriidilised isikud, kes on asutatud liidus või keda loetakse liidus asutatuks ja kes on liikmesriigi või selle kodanike kontrolli all.

(28) Selleks et parandada liidu tasandi valmisolekut ja reageerimist ulatuslike küberintsidentide ja kriiside korral, peaks ENISA võtma küberturvalisuse alase olukorrateadlikkusega seotud meetmeid.

(29) Juurdepääs kontrollitud ja usaldusväärsele küberohuteadmusele reaalaja on otsustava tähtsusega, et suurendada liidus ühist olukorrateadlikkust. ENISA, komisjon, CERT-EU ja Europoli juures tegutsev küberkuritegevuse vastase võitluse Euroopa keskus on juba loonud küberohuteadmuse hoidlad, lähtudes oma konkreetsetest vajadustest. ENISA ja muud asjaomased liidu üksused peaksid tegema vabatahtlikult koostööd, et arendada kontrollitud ja usaldusväärse reaalaja küberohuteadmuse hoidlaid, ning püüdma saavutada koostoimet, et tagada mastaabisääst ja tugevdada usaldusväärset finantsjuhtimist. Sellesse töösse tuleks kaasata ka liidu valdkondlikud üksused, nagu Euroopa Liidu Kosmoseprogrammi Amet. Üksused peaksid jagama ainult tuletatud analüüse ja suundumusi ning taktikaid, meetodeid ja menetlusi, mitte töötlemata andmeid, ning austada tuleks üksuste sõltumatust hallata oma küberohuteadmuse elutsüklit kooskõlas oma volituste ja teadmisvajadust käsitlevate eeskirjadega.

(30) Selleks et aidata kaasa õigeaegsele ja koordineeritud reageerimisele, peaks ENISA-l olema võimalik saata asjaomasele CSIRTile või asjaomastele CSIRTidele ning vajaduse korral CSIRTide võrgustikule ja EU-CyCLONe-le varajasi hoiatusi võimaliku või käimasoleva olulise või ulatusliku intsidendi või potentsiaalselt piiriülese küberohu kohta, eelkõige seoses direktiivi (EL) 2022/2555 I ja II lisas loetletud üksustega. Sellistes varajastes hoiatustes sisalduv teave võib hõlmata avalikult teadaolevaid nõrkusi ja teavet selle kohta, kas need nõrkused mõjutavad määruse (EL) 2024/2847 kohaldamisalasse kuuluvaid digielemente sisaldavaid tooteid, samuti meetodeid ja menetlusi, rikkeindikaatoreid, kahjulikke taktikaid, ohusubjektipõhist teavet ja soovitusi leevendusmeetmete kohta.

(31) Selleks et säilitada usaldus ja vältida teabe jagamise ohtu seadmist, on oluline, et ENISA kasutaks nähtavaid märgiseid, mis näitavad, millises ulatuses võib tema koostatud või saadud dokumenti või teavet edasi jagada. Samuti peaks ENISA oma tegevuse eluviimiseks saadud dokumente või teavet kasutades võtma arvesse nähtavast märgisest tulenevaid teabe edasise levitamise piiranguid.

(32) Selleks et aidata suurendada teadlikkust küberohu indikaatoritest ja soovitustest leevendusmeetmete kohta, peaks ENISA tegema direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorites tegutsevatele üksustele kättesaadavaks varajase hoiatamise teenuse. Sellised üldised vabatahtlikud varajased hoiatused peaksid tooma kasu eelkõige VKEdele ja need tuleks esitada üldsusele kättesaadavas masinloetavas vormingus. Selline vabatahtlik teenus on igal juhul eraldiseisev teenus, mis ei ole seotud ühegi ENISA loodava või juba loodud avaliku ja erasektori partnerlusega.

(33) Selleks et toetada liidu küberturvalisuse alast ühist olukorrateadlikkust, peaks ENISA koostama tihedas koostöös liikmesriikidega korrapäraselt ELi küberturvalisuse tehnilise olukorra põhjalikke aruandeid intsidentide ja küberohtude kohta, võttes aluseks avalikult kättesaadava teabe, omaenda tehtud analüüsid ja aruanded, mida on temaga jaganud liikmesriikide CSIRTid või direktiivis (EL) 2022/2555 ettenähtud

riiklikud võrgu- ja infosüsteemide turbe ühtsed kontaktpunktid (mõlemad vabatahtlikkuse alusel), Europol ja CERT-EU. Koostatud aruanne tuleks teha kättesaadavaks nõukogule, Euroopa välisteenistusele, EU-CyCLONe-le, CSIRTide võrgustikule, komisjonile ja Europolile.

(34) Selleks et suurendada sidusrühmade seas küberohtude ja -intsidentide alast ühist olukorrateadlikkust, peaks ENISA analüüsima küberohtude ja -intsidentidega seotud suundumusi. See peaks hõlmama korrapärast analüüsi, milles vaadeldakse direktiivi (EL) 2022/2555 I ja II lisas loetletud kriitilise tähtsusega sektoreid ja muid kriitilise tähtsusega sektoreid, sh tervishoiu-, energia- ja transpordisektorit. Muu hulgas tuleks analüüsida sektorite küpsuse taset ja teha kindlaks konkreetsele sektorile omased võimalikud probleemid. Kui see on asjakohane, tuleks analüüsis käsitleda määruse (EL) 2024/2847 kohaldamisalasse kuuluvate tootekategooriatega seotud küberohte ja suundumusi, et teha kindlaks mõju tarneahelale. ENISA peaks arendama eksperditeadmisi taristute küberturvalisuse ja kriitilise tähtsusega tarneahela sõltuvuse valdkonnas, eelkõige et toetada direktiivi (EL) 2022/2555 I ja II isas loetletud sektoreid ning määruse (EL) 2024/2847 rakendamist. Selleks peaks ENISA tegema asjakohasel juhul koostööd teiste asjaomaste liidu üksustega.

(35) Selleks et paremini mõista küberturvalisuse valdkonnas esinevaid probleeme, peab ENISA lisaks analüüsima olemasolevaid ja kujunemisjärgus tehnoloogiaid ning andma teemakohaseid hinnanguid küberturvalisuse valdkonna tehnoloogiliste uuenduste eeldatava ühiskondliku, õigusliku, majandusliku ja regulatiivse mõju kohta. Selleks et tagada üldsuse lihtsam juurdepääs teabele küberriskide ja võimalike vastumeetmete kohta, võib ENISA esitada oma veebisaidil asjakohast teavet kasutajasõbralikul ja hästi struktureeritud viisil.

(36) ENISA tugevdatud roll olukorrateadlikkuse parandamisel, ohtude analüüsimisel ja tehnilise nõu andmisel aitab suurendada ühiseid jõupingutusi digielemente sisaldavate toodete küberturvalisuse valdkonnas ja toetab määruse (EL) 2024/2847 rakendamist. Vastavalt määrusele (EL) 2024/2847 võib ENISA teha turujärelevalveasutustele ettepanekuid ühismeetmete kohta, et kontrollida digielemente sisaldavate toodete nõuetelevastavust ja määrata kindlaks digielemente sisaldavate toodete kategooriad, mille puhul võib korraldada lauskontrolle. Küberohtude analüüsist ja varajastest hoiatustest saadav teave peaks tugevdama ENISA poolt neile asutustele pakutavat toetust ning aitama tagada määruse (EL) 2024/2847 tulemusliku täitmise, et ennetada küberrünnete mõju tarneahelale kogu siseturul ja suurendada liidu üldist valmisolekut.

(37) Märkimisväärne küberoht liidus on lunavararünded. Selleks et edendada liidu küberturvalisust ja võidelda lunavara vastu, peaks ENISA suurendama olukorrateadlikkuse alast suutlikkust ning intsidentidele reageerimiseks ja neist taastumiseks pakutavat tuge. Aidates individuaalsetel elutähtsatel ja olulistel üksustel lunavararünnetele reageerida ja neist taastuda, peaks ENISA tegema tihedat koostööd Europoli ja vastavalt vajadusele CSIRTide või pädevate asutustega, et kasutada ära Europoli kogemusi lunavarakuritegude vastu võitlemisel. Selline abi peaks täiendama CSIRTide tegevust, millega toetatakse intsidentidele reageerimist. Lunavaravastases töös koostoime saavutamiseks peaks ENISA looma kasutajatoe, mille jaoks võiks ta koondada asjakohase suutlikkuse ja lunavaravastased teenused ning teha kergesti kättesaadavaks teabe, suunised ja vahendid, mis võivad aidata elutähtsatel ja olulistel üksustel lunavaraintsidentidele reageerida ja neist taastuda.

(38) ENISA peaks pakkuma komisjonile tehnilisi eksperditeadmisi ja tuge liidu tasandi küberturvalisuse õppuste iga-aastase jooksva programmi koostamisel kooskõlas

kübervaldkonna tegevuskava käsitleva soovitusega, et valmistuda küberkriisideks, testida sellistel õppustel osalevate üksuste küberturvalisuse taset ja minimeerida jõupingutuste dubleerimist. ENISA peaks näiteks andma nõu õppuste asjakohase liigi kohta (lauaõppus, hübriidõppus või täismahus reaalajas õppus), aga ka eesmärkide, stsenaariumide ja osalemise kohta.

(39) Küberturvalisuse kõrge taseme tagamiseks siseturul on hädavajalikud juurdepääs korrektsele ja õigeaegsele teabele nõrkuste kohta ning usaldusväärne nõrkusehaldus. Seetõttu peaks ENISA pidama Euroopa nõrkuste andmebaasi vastavalt direktiivile (EL) 2022/2555 ja looma liidu ühise nõrkusehalduse teenuste alase suutlikkuse, tagades vastupidava ja kestliku teenuste taseme ning vähendades häirete riski. Selleks peaks ENISA uurima võimalusi süvendada struktureeritud koostööd Euroopa nõrkuste andmebaasiga sarnaste programmide, registrite või andmebaaside haldajatega, et vältida jõupingutuste dubleerimist ja püüda asjakohasel juhul saavutada vastastikune täiendavus rahvusvahelisel tasandil. Peale selle peaks ENISA toetama mitut osapoolt puudutavate nõrkuste koordineeritud avalikustamist liidu tasandil ja pakkuma lisaväärtusega teenuseid, nagu nõrkustega seotud nõustamine, raskusastme hindamine ja toodete loetelud, ning pakkuma Euroopa teadaolevate ärakasutatavate nõrkuste täiustatud kataloogi, et aidata üksustel hallata oma nõrkusi.

(40) ENISA volituste üks põhiaspekte peaks olema tema roll Euroopa küberturvalisuse sertifitseerimise raamistiku arendamisel. ENISA peaks pakkuma tehnilisi eksperditeadmisi kogu Euroopa küberturvalisuse sertifitseerimise kavade elutsükli vältel. ENISA peaks kindlaks tegema olemasolevad standardid või tehnilised kirjeldused, mida saab aluseks võtta tulevaste kavade väljatöötamisel, ja vajaduse korral koostama tehnilised kirjeldused, millele neis kavades viidata. ENISA peaks juhtima ettevalmistava kava koostamist pärast komisjon sellekohast taotlust. ENISA peaks vastutama olemasolevate kavade haldamise eest. Seda tehes peaks ENISA aitama kujundada ja arendada sellist sertifitseerimise ökosüsteemi, kus küsitakse liikmesriikidelt ja erasektori sidusrühmadelt tagasisidet ning suurendatakse nende sertifitseerimissuutlikkust. See peaks hõlmama spetsiaalse sertifitseerimise veebisaiti, kus on vabalt ja avalikult kättesaadav asjakohane teave vastuvõetud kavade, sh sertifikaatide ja vastavusdeklaratsioonide kohta.

(41) ENISA peaks kujundama küberturvalisuse valdkonna tehnika taset, pakkudes tehnilisi kirjeldusi, et toetada asjakohaste liidu õigusaktide rakendamist, muu hulgas selleks, et neile saaks viidata Euroopa küberturvalisuse sertifitseerimise kavades. Samuti peaks ENISA jälgima standardite loomist ja arendamist asjaomastes standardiorganisatsioonides, et olla kursis standardimissuundumustega Euroopa ja ülemaailmsel tasandil ning vajaduse korral asjaomaseid standardeid kujundada, osaledes standardiorganisatsioonide töös, muu hulgas sisendite koostamisega, ja juhtides nende tegevust. Seda tehes peaks ENISA jääma erapooletuks. Näiteks võib tekkida olukordi, kus ENISA peaks loobuma osalemisest standardiorganisatsiooni asjaomases tegevuses, kui tal palutakse hinnata Euroopa standardeid, mida komisjon on taotlenud liidu õigusaktide toetamiseks. ENISA ei tohiks kaasa aidata selliste standardite koostamisele, mille hindamise eest ta vastutab.

(42) Selleks et toetada liidu poliitikameetmete rakendamist ja potentsiaalse standardimise ettevalmistamist, peaks ENISA aitama kaasa krüptoalgoritmide väljatöötamisele ja hindamisele, eelkõige kvanttehnoloogiajärgse krüptograafia valdkonnas. Sellega seoses võib ENISA kehtestada komisjoni taotlusel ja Euroopa Parlamendi ja nõukogu

määruses (EL, Euratom) 2024/2509[50] määratletud rahalist toetust käsitleva lepingu alusel protsessi, et küsida asjaomastelt sidusrühmadelt, eelkõige krüptograafia-, akadeemilistelt ja teadusringkondadelt, samuti tootjatelt, CSIRTidelt, riiklikelt küberturvalisuse sertifitseerimise asutustelt ja direktiivis (EL) 2022/2555 määratletud pädevatelt asutustelt krüptoalgoritmide jaoks algoritme ja neid hinnata. Kui ENISA osaleb selliste protsesside kehtestamises, peaks ta edendama koostööd asjaomaste sidusrühmade vahel ja rakendama korralduslikke aspekte. Protsess peaks olema ametlik, avatud, läbipaistev ja kaasav, hõlmates konsulteerimist asjaomaste sidusrühmadega kavandatavate miinimumnõuete ning hindamisprotsessi ja -kriteeriumide üle, eelkõige hindamise turvalisuse ja teostamise huvides.

(43) Selleks et toetada Euroopa küberturvalisuse sertifitseerimise kavade ja muude asjakohaste liidu õigusaktide kohast vastavushindamist, võib ENISA pakkuda liikmesriikide, ettevõtjate ja vastavushindamisasutuste hindamistegevuse toetamiseks asjakohaseid tehnilisi testimisvahendeid. Nende vahenditega tuleks püüda tagada liidu tasandil koostoime ja vastavushindamismenetluste tõhus toimimine, et rahuldada liikmesriikide ja turu vajadusi. Sellised vajadused võivad tekkida näiteks sisseprojekteeritud turbe valdkonnas, et toetada ettevõtjaid, sh VKEsid, töös, mida nad teevad määruse (EL) 2024/2847 rakendamiseks. Seoses sellega peaks ENISA nõudma tasu, et katta kulud, mis on seotud selliste testimisvahendite jaoks vajaliku tark- ja riistvara projekteerimise, väljatöötamise, arendamise, hooldamise ja ajakohastamisega.

(44) Selleks et toetada liikmesriike nende püüdlustes vähendada küberturbespetsialistide nappust ning rahuldada kasvavat vajadust kvalifitseeritud, mitmekesise (sh soolise tasakaalu vaatenurgast) ja paindliku tööjõu järele ning võimaldada tööjõu liikuvust ja valmisolekut kõigis liikmesriikides, peaks ENISA arendama edasi küberturbeoskuste akadeemia põhimõtteid ja tööd. Eelkõige peaks ENISA looma Euroopa küberturbeoskuste raamistiku kui küberturvalisuse valdkonna rollikirjelduste ühise raamistiku. Peale sellel peaks ENISA toetama liikmesriike küberturvalisusega seotud rollide soolise ebavõrdsuse vähendamisel. See lähenemisviis on kooskõlas oskuste liitu käsitlevas komisjoni teatises esitatud visiooniga ja aitaks kaasa selle eesmärkide saavutamisele. Lisaks tuleks edasi tegeleda Euroopa individuaalsete küberturbeoskuste tõendi kvaliteedimärgisega.

(45) Euroopa küberturbeoskuste raamistik peaks olema vabatahtlikkuse alusel kasutatav praktiline ja paindlik vahend, mis tagab ühise terminoloogia ja arusaama küberturvalisusega seotud rollidest ja nendega seotud ülesannetest ning enamasti vajaminevatest oskustest ja teadmistest, et toetada töötajate kriitilise tähtsusega oskuste, sh valdkonnaüleste oskuste kindlaksmääramist, võimaldada koolitajatel, sh ettevõtjatel, kõrgharidusasutustel ning kutsehariduse ja -õppe pakkujatel kavandada programme ning aidata poliitikakujundajatel töötada välja algatusi oskuste nappuse leevendamiseks. Kuna Euroopa küberturbeoskuste raamistikku võidakse kasutada võrdlusraamistikuna oskuste tunnustamisel, peaks see olema koostalitlusvõimeline oskuste, kompetentside, kvalifikatsioonide ja ametite Euroopa klassifikaatoriga (ESCO), et aidata personaliosakondadel mõista küberturvalisuse vajadusi toetava vahendite planeerimise, värbamise ja karjääri arendamise nõudeid. Kui Euroopa kodanike digipädevuse raamistikus (DigComp 3.0) kirjeldatakse teadmisi, oskusi ja hoiakuid, mida on vaja, et olla igapäevaelu, ühiskonnaelus osalemise, töötamise ja

[50] Euroopa Parlamendi ja nõukogu 23. septembri 2024. aasta määrus (EL, Euratom) 2024/2509, mis käsitleb liidu üldeelarve suhtes kohaldatavaid finantsreegleid (ELT L, 2024/2509, 26.09.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

õppimise jaoks digitaalselt pädev, ning seda saavad kasutada nii täiskasvanud kui ka lapsed, siis Euroopa küberturbeoskuste raamistik on lihtne raamistik, milles määratakse kindlaks küberturvalisusega seotud rollid, nendega seotud ülesanded ning nende täitmiseks vajalikud teadmised ja oskused. Seega on see mõeldud küberturvalisusele spetsialiseerunud sihtrühmadele alates olemasolevatest või potentsiaalsetest küberturbespetsialistidest ja haridusasutustest kuni tööandjateni. Euroopa küberturbeoskuste raamistik peaks olema toeks ka Euroopa individuaalsete küberturbeoskuste tõendamise arendamisel kui asjaomaste kavade väljatöötamise oluline vahend, mis võimaldab uute turuosaliste esilekerkimist ja toetab turukonkurentsi ühises raamistikus. Raamistikku tuleks korrapäraselt hinnata ja ajakohastada, kandmaks hoolt selle eest, et see kajastab asjakohaselt küberturvalisuse tööturu vajadusi ning tehnoloogia ja poliitika arengut. ENISA peaks toetama Euroopa küberturbeoskuste raamistiku kasutuselevõttu liikmesriikide ja liidu üksuste poolt ja nende sees ning pakkuma piisavat tuge, kui seda vajatakse.

(46) Küberturvalisuse alased oskused ja kvalifikatsioonid tuleks muuta võrreldavaks, läbipaistvaks ja usaldusväärseks kogu siseturul. Sel eesmärgil peaksid Euroopa individuaalsete küberturbeoskuste tõendid[51] aitama tööandjatel, sh VKEdel ja idufirmadel, liikmesriikides ja eri liikmesriikide vahel tulemuslikult värvata olemasolevaid või potentsiaalseid küberturbespetsialiste kooskõlas oskuste liitu käsitlevas teatises sätestatud eesmärkidega. Selleks et tagada järjekindel rakendamine kõigis liikmesriikides, peaksid Euroopa individuaalsete küberturbeoskuste tõendid põhinema liidu tasandi ühisel arusaamal nende eesmärkide saavutamiseks vajalikest oskustest ning tõendeid peaksid väljastama ENISA poolt ühiste kriteeriumide alusel volitatud tõendajad. See lähenemisviis peaks olema kooskõlas tulevase oskuste ülekantavuse algatuse eesmärkidega ja aitama neid eesmärke saavutada.

(47) Euroopa individuaalsete küberturbeoskuste tõendamise kavade väljatöötamisega tuleks täiendada liikmesriikide meetmeid, pakkudes avaliku sektori asutustele ja ettevõtjatele võimalust kasutada Euroopa tõendamismehhanismi kooskõlas liidu toetava pädevusega hariduse ja kutseõppe valdkonnas, millele on osutatud ELi toimimise lepingu artikli 6 punktis e, artikli 165 lõikes 1 ja artikli 166 lõikes 1. Kõnealused kavad koos küberturbeoskuste akadeemia tööga võivad olla aluseks ka kõrgharidusprogrammidele, nagu valdkondlikud Euroopa kraadid, ja mikrokvalifikatsioonide arendamisel. Seepärast ei tuleks Euroopa individuaalsete küberturbeoskuste tõendamise kavadega püüda ühtlustada liikmesriikide õigusnorme, vaid neid tuleks pigem pidada võimaluseks, mida liikmesriigid ja ettevõtjad võivad soovida kasutada ja edendada.

(48) ENISA peaks tagama, et Euroopa individuaalsete küberturbeoskuste tõendamise kavad järgivad turu vajadusi ning tuginevad nii avaliku kui ka erasektori individuaalsete tõendite väljaandjate, sh liikmesriikide, kõrgharidusasutuste, kutseharidus- ja -õppeasutuste ning ettevõtjate kogemustele. ENISA peaks konsulteerima Euroopa individuaalsete küberturbeoskuste tõendamise kavade prioriseerimise küsimuses komisjoniga, võttes nõuetekohaselt arvesse poliitika rakendamist ja turu vajadusi.

---

[51] Euroopa individuaalsete küberturbeoskuste tõendid peaksid järgima sarnast lähenemisviisi kui küberturvalisuse sertifikaadid. Selleks et vältida segiajamist Euroopa küberturvalisuse sertifitseerimise raamistikuga, eelistatakse väljendit „tõendamine“, mida on juba kasutatud küberturbeoskuste akadeemiat käsitlevas teatises.

(49) Selleks et tagada kooskõla Euroopa küberturbeoskuste raamistiku ja Euroopa individuaalsete küberturbeoskuste tõendamise kavade vahel, peaks Euroopa küberturbeoskuste raamistiku rollikirjelduse muutmine tooma automaatselt kaasa asjaomas(t)e Euroopa individuaalsete küberturbeoskuste tõendamise kava(de) sobivuse hindamise, mis võib viia kava läbivaatamiseni.

(50) Võttes arvesse küberturvalisusega seotud rollide ning nendega seotud ülesannete, oskuste ja teadmiste mitmekesisust, võib juhtuda, et üksikisikute hindamist ja hindamismeetodeid on vaja igas Euroopa individuaalsete küberturbeoskuste tõendamise kavas kohandada. Iga kava peaks tagama, et isikult nõutavate oskuste hindamist õpitulemuste, sh vajaduse korral oskuste taseme osas hinnatakse süstemaatiliselt Euroopa küberturbeoskuste raamistiku rollikirjelduse või selle osa põhjal. Hindamismeetodid võivad hõlmata teoreetiliste teadmiste kontrolli, praktilist eksamit, eeltingimusi ja vastastikust hindamist. Üksikisikute kogemusi tuleks nõuetekohaselt arvesse võtta.

(51) Selleks et tagada Euroopa individuaalsete küberturbeoskuste tõendamise kavade järjepidev rakendamine, eelkõige üksikisikute hindamise osas, peaks ENISA pakkuma üksikisikute hindamise eest vastutavatele töötajatele kohustuslikku koolitust. Sellistel töötajatel peaks olema küberturvalisuse valdkonnas kogemus, mida saab tõendada Euroopa individuaalsete küberturbeoskuste tõendiga, mis kinnitab hindaja vastavust selle rolli kirjeldusele, mida ta hindab, ja oskuste taset, mis on vähemalt samaväärne hinnatava isiku oskuste tasemega.

(52) Volitatud tõendaja ülesanne on tõendada ja anda tööandjatele kogu liidus kindlus, et isikul on teadmised ja pädevus, mis võimaldavad tal täita Euroopa küberturbeoskuste raamistikus kindlaks määratud rolli. Kuna kinnitusele Euroopa individuaalsete küberturbeoskuste tõendi saanud isikute oskuste ja pädevuse kvaliteedi kohta pööravad tähelepanu ka liidu elutähtsat taristut käitavad tööandjad, peaksid oskuste ja pädevuse taset tõendavad volitatud tõendajad olema küberturvalisuse seisukohast usaldusväärsed ning neid ei tohiks lubamatult mõjutada kolmas riik, kelle puhul on põhjust muret tunda küberturvalisuse pärast. Seepärast ei tohiks üksused, mis on asutatud käesoleva määruse kohaselt küberturvalisuse seisukohast muret tekitavaks nimetatud kolmandas riigis või on sellise kolmanda riigi, selles asutatud üksuse või selle kodaniku kontrolli all (suure riskiga tarnijad), saada volitatud tõendajaks, kes annab välja II jaotise 4. jao kohaseid Euroopa individuaalsete küberturbeoskuste tõendeid.

(53) Tagamaks, et isikud, kellel on Euroopa küberturbeoskuste tõend, saaksid seda tunnistust hõlpsasti kasutada ja jagada kõigis liikmesriikides, peaksid volitatud tõendajad tagama, et asjaomase isiku taotlusel väljastatakse Euroopa individuaalsete küberturbeoskuste tõend elektroonilisel kujul määrusega (EL) nr 910/2014 loodud Euroopa digiidentiteedikukrusse. Volitatud tõendajaid tuleks käsitada usaldusteenuse osutajatena ning nende suhtes tuleks kohaldada määruses (EL) nr 910/2014 sätestatud järelevalve- ja vastutuskorda. Komisjoni rakendusmääruse (EL) 2025/1569[52] kohaselt kasutatav atribuutide tõendamise kava tuleks registreerida selles rakendusmääruses sätestatud atribuutide tõendamise kavade kataloogis.

---

52 Rakendusmäärus – EL – 2025/1569.

(54) Selleks et aidata kaasa küberturvalisuse valdkonna tööjõu arendamisele ja oskuste ülekantavusele kogu liidus, peaks ENISA tegema Euroopa individuaalsete küberturbeoskuste tõendamise kavad ja volitatud tõendajate loetelu üldsusele kättesaadavaks spetsiaalse veebisaidi kaudu.

(55) ENISA juhtimisel ja tegevuses tuleks arvesse võtta 19. juulil 2012 Euroopa Parlamendi, nõukogu ja komisjoni poolt vastu võetud liidu detsentraliseeritud asutusi käsitleva ühise lähenemisviisi[53] põhimõtteid. Samuti peaksid ühises lähenemisviisis sisalduvad soovitused asjakohaselt kajastuma ENISA tööprogrammides, hindamistes ning aruandlus- ja haldustavades.

(56) Selleks et haldusnõukogu saaks tõhusalt oma ülesandeid täita, eelkõige ENISA tegevuse üldisel suunamisel ja strateegiliste prioriteetide seadmisel, on oluline, et haldusnõukogu koosneks liikmesriikide ja komisjoni kõrgetasemelistest esindajatest. Seega peaks iga liikmesriik nimetama haldusnõukogu liikmeks direktiivi (EL) 2022/2555 artikli 8 lõike 1 kohaselt määratud küberturvalisuse eest vastutava riikliku pädeva asutuse juhi.

(57) Tagamaks, et haldusnõukogu asendusliikmed saavad nõuetekohaselt oma rolli täita, peaksid liikmesriigid nimetama asendusliikmed, kellel on asjakohased eksperditeadmised ja kogemused. Komisjon ja liikmesriigid peaksid püüdma asendusliikmete puhul saavutada meeste ja naiste tasakaalustatud esindatuse haldusnõukogus ning piirama liikmete vahetumist, et tagada haldusnõukogu töö järjepidevus.

(58) Selleks et ENISA saaks tulemuslikult oma missiooni täita, peaks liikmesriikide ja komisjoni esindajatest koosnev haldusnõukogu määrama kindlaks ENISA tegevuse üldsuuna, sh strateegilised prioriteedid, ning tagama, et ENISA täidab oma ülesandeid vastavalt käesolevale määrusele. Haldusnõukogule tuleks anda õigus koostada ENISA eelarve ja kontrollida selle täitmist, võtta vastu asjakohased finantsreeglid, kehtestada ENISA otsuste tegemiseks läbipaistev kord, võtta vastu ENISA ühtne programmdokument, võtta vastu oma kodukord, nimetada ametisse tegevdirektor, otsustada tegevdirektori ametiaja pikendamise ja lõpetamise üle ning otsustada tegevdirektori asetäitja ametikoha loomise üle ning selle loomise korral tegevdirektori asetäitja ametisse nimetamise ning tema ametiaja pikendamise ja lõpetamise üle. Seega peaks iga isiku, kellel on ENISAs täidesaatev funktsioon, nimetama ametisse haldusnõukogu. Haldusnõukogu peaks vastutama ka apellatsiooninõukogu liikmete ametisse nimetamise ja ametist vabastamise eest ning nende liikmete huvide konfliktide ennetamise ja lahendamise eeskirjade kehtestamise eest.

(59) Selleks et aidata tagada, et ENISA määrab kindlaks oma strateegilised prioriteedid ja hoiab neid ajakohasena, peaks haldusnõukogu pidama aastas vähemalt ühe koosoleku, kus keskendutakse ENISA strateegilistele prioriteetidele. Haldusnõukogu koosolekute tulemuslikkuse ja haldusnõukogu liikmete informeerituse tagamiseks võib haldusnõukogu kutsuda oma koosolekule arvamusi, eksperditeadmisi või nõu jagama mis tahes isiku, kelle seisukoht võib olla arutatavate teemade vaatenurgast oluline ja huvipakkuv. Selline isik on hääleõiguseta ajutine vaatleja.

---

[53] Ühine lähenemisviis, mis on lisatud 19. juulil 2012 vastu võetud Euroopa Parlamendi, Euroopa Liidu Nõukogu ja Euroopa Komisjoni ühisavaldusele detsentraliseeritud asutuste kohta, https://european-union.europa.eu/document/download/d4199ff4-1e3d-45e6-af7e-90cf1a7b10bc_en?filename=joint_statement_on_decentralised_agencies_en.pdf.

(60) Haldusnõukogu peaks võtma otsused vastu oma hääleõiguslike liikmete absoluutse häälteenamusega, kui käesolevas määruses ei ole sätestatud teisiti. Otsused eelarve- ja personaliküsimuste kohta, eelkõige aastaeelarve, iga-aastase tegevusaruande, pettustevastase strateegia, personalieeskirjade rakenduseeskirjade, tegevdirektori, tegevdirektori asetäitja ja peaarvepidaja ametisse nimetamise, Euroopa Pettustevastase Ameti (OLAF) ja Euroopa Prokuratuuri järelduste järelmeetmete ning ENISA finantseeskirjade vastuvõtmisega seotud küsimustes, peaks haldusnõukogu nende küsimuste olulisuse tõttu vastu võtma üksnes juhul, kui komisjoni esindaja hääletab otsuse poolt. Lõpliku ühtse programmdokumendi vastuvõtmise otsuse tegemisel pärast komisjoni arvamuse arvessevõtmist on komisjoni esindaja poolthääl vajalik ainult nende otsuse elementide puhul, mis ei ole seotud ENISA iga-aastase ja mitmeaastase tööprogrammiga.

(61) Juhatus peaks aitama kaasa haldusnõukogu tõhusale toimimisele. Osana haldusnõukogu otsustega seotud ettevalmistustööst peaks juhatus põhjalikult analüüsima asjakohast teavet ja olemasolevaid võimalusi ning pakkuma nõu ja lahendusi haldusnõukogu asjakohaste otsuste ettevalmistamiseks. Samuti peaks ta abistama ja nõustama tegevdirektorit haldusnõukogu otsuste rakendamisel.

(62) ENISA sujuvaks toimimiseks on tarvis, et tegevdirektori ametisse nimetamisel lähtutakse tema teenetest, dokumenteeritud haldamis- ja juhtimisoskusest ning küberturvalisuse alastest teadmistest ja kogemustest. Tegevdirektori ülesandeid tuleks täita täiesti sõltumatult. Haldusnõukogu peaks nimetama tegevdirektori komisjoni koostatud kandidaatide nimekirjast, järgides avatud ja läbipaistvat menetlust, kus austatakse soolise tasakaalu põhimõtet.

(63) Tegevdirektor peaks pärast komisjoniga konsulteerimist koostama ettepaneku ENISA ühtse programmdokumendi kohta ning võtma kõik vajalikud meetmed, et tagada programmdokumendi nõuetekohane rakendamine. Tegevdirektor peaks koostama haldusnõukogule esitatava aastaaruande ENISA iga-aastase tööprogrammi rakendamise kohta, koostama ENISA tulude ja kulude kalkulatsiooni eelnõu ning vastutama eelarve täitmise eest. Lisaks peaks tegevdirektoril olema võimalik moodustada ajutisi töörühmi, et käsitleda konkreetseid, eeskätt teaduslikku, tehnilist, õiguslikku või sotsiaal-majanduslikku laadi küsimusi. Ajutise töörühma moodustamist peetakse vajalikuks eelkõige seoses Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava koostamisega. Ajutise töörühma moodustamine võib olla vajalik ka konkreetsete vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade haldamiseks. Ajutised töörühmad tuleks moodustada ka selleks, et koostada ja hallata Euroopa individuaalsete küberturbeoskuste tõendamise kavasid ning abistada ENISAt Euroopa küberturbeoskuste raamistiku juhtimisel, rakendamisel ja arendamisel. Tegevdirektor peaks tagama, et ajutiste töörühmade liikmed valitakse kõige põhjalikumate eksperditeadmiste põhjal, püüdes tagada soolise tasakaalu ning selle, et seal oleksid (konkreetse küsimuse puhul asjakohasel viisil) tasakaalustatult esindatud liikmesriikide ametiasutused, liidu üksused ning erasektor, sh tööstusharu, kasutajad ning võrgu- ja infoturbe valdkonna ja digielemente sisaldavate toodete valdkonna teaduseksperdid.

(64) Haldusnõukogu võib otsustada luua tegevdirektori abistamiseks tegevdirektori asetäitja ametikoha, kui ta leiab, et selline ametikoht on vajalik, et tagada või säilitada ENISA sujuv toimimine. Selle ametikoha loomise üle otsustamisel võib haldusnõukogu võtta arvesse tegevdirektori arvamust.

(65) ENISA-l peaks olema nõuanderühm, et tagada korrapärane dialoog erasektori, tarbijaorganisatsioonide ja teiste asjaomaste sidusrühmadega. ENISA nõuanderühm, mille moodustab tegevdirektori ettepanekul haldusnõukogu, peaks keskenduma sidusrühmade jaoks olulistele küsimustele ja juhtima nendele küsimustele ENISA tähelepanu. Eelkõige tuleks ENISA nõuanderühmaga konsulteerida ENISA iga-aastase tööprogrammi kavandi üle. ENISA nõuanderühma koosseis ja ülesanded peaksid tagama sidusrühmade piisava esindatuse ENISA töös. ENISA nõuanderühmas peaksid olema esindatud liikmesriikide ja liidu õiguskaitse-, andmekaitse- ja turujärelevalveasutuste esindajad.

(66) Isikutel, kes soovivad saada volitatud tõendajateks või oma volitust uuendada, peaks olema neid mõjutava ENISA otsuse korral juurdepääs vajalikele õiguskaitsevahenditele. Seepärast tuleks luua asjakohane edasikaebamismehhanism, et ENISA asjakohaseid otsuseid saaks vaidlustada apellatsiooninõukogus, kelle otsuseid on omakorda võimalik edasi kaevata Euroopa Liidu Kohtusse kooskõlas aluslepingutega. Nõue kasutada enne asja Euroopa Liidu Kohtusse andmist ENISA-sisest kaebemenetlust on kohaldatav üksnes isikutele, kellel on apellatsiooninõukogus kaebeõigus.

(67) Selleks et tagada ENISA täielik autonoomia ja sõltumatus ning võimaldada tal täita oma ülesandeid, tuleks ENISA-le eraldada piisav ja autonoomne eelarve, mida rahastatakse peamiselt liidu rahalisest toetusest, ent samuti ENISA töös osalevate kolmandate riikide rahalisest osalusest ning tasudest, mida maksavad kavades osalevad ning Euroopa küberturvalisuse sertifikaate ja ELi vastavusdeklaratsioone välja andvad volitatud tõendajad ja vastavushindamisasutused. Asukohaliikmesriigil ja mis tahes muul liikmesriigil peaks olema lubatud teha ENISA eelarvesse vabatahtlikult sissemakseid. Liikmesriikidelt, kolmandatelt riikidelt või teistelt üksustelt või isikutelt saadud rahalised või mitterahalised panused ei tohiks kahjustada ENISA sõltumatust ja erapooletust. Liidu rahalise toetuse ja muude liidu üldeelarvest makstavate toetuste suhtes tuleks kohaldada liidu eelarvemenetlust. Kontrollikoda peaks auditeerima ENISA raamatupidamisarvestust, et tagada läbipaistvus ja vastutus. Selleks et võimaldada ENISA-l osaleda kõigis asjakohastes tulevastes projektides, peaks tal olema võimalik saada toetusi.

(68) Selleks et tagada ENISA suutlikkus rahuldada oma tegevusega seotud nõudlust, eelkõige seoses otsustega, millega antakse luba väljastada Euroopa individuaalsete küberturbeoskuste tõendeid, ning seoses Euroopa küberturvalisuse sertifitseerimise kavade ja testimisvahendite haldamisega, tuleks ENISA-le anda õigus nõuda tasu. Volitatud tõendajaks saamise taotluste menetlemisega seotud tasud tuleks kindlaks määrata nii, et need aitaksid piisaval määral katta prognoositud kulusid, mis on seotud Euroopa individuaalsete küberturbeoskuste tõendamise kavade väljatöötamise ja haldamisega ning selle hindamisega, kas volitatud tõendajaks saamise ja sellena tegutsemise nõuded ja kohustused on (jätkuvalt) täidetud. Tasud, mis on seotud volitatud tõendajatele lubade väljaandmise ja nende lubade uuendamise kuludega, peaksid hõlmama ENISA läbiviidavate või tema järelevalve all tehtavate hindamiste kulusid. Tasud, mis on seotud Euroopa küberturvalisuse sertifitseerimise kavades osalemisega ja nende kavade alusel sertifikaatide välja andmisega, tuleks kindlaks määrata nii, et need aitaksid piisavalt kaasa nende kavade haldamise prognoositud kulude katmisele. Tasude maksmine peaks võimaldama teatatud vastavushindamisasutustel ja asjakohasel juhul kava kohaste sertifikaatide omanikel osaleda kõnealuses tegevuses ning asjakohases suutlikkuse suurendamises ja

edendustegevuses, et edendada parimate tavade vahetamist ning kavade ja sertifitseeritud lahenduste kasutuselevõttu.

(69) Proportsionaalsuse, läbipaistvuse ja õiguskindluse tagamiseks tuleks tasud kehtestada läbipaistvalt ja õiglaselt. Neis kuludes peaksid kajastuma kõik ENISA kulud, mis on seotud tasulistes toimingutes osalevate töötajatega, eelkõige tööandja proportsionaalsed maksed pensioniskeemi, ja kulud, mis on seotud apellatsiooninõukoguga. Tasud ei tohi põhjustada taotlejatele tarbetut finants- või halduskoormust. Tasude maksmiseks tuleks kehtestada mõistlikud tähtajad.

(70) On vaja kehtestada näitajad, et mõõta ameti töökoormust, tulemuslikkust ja tõhusust tasudest rahastatavate toimingute tegemisel. Neid näitajaid silmas pidades peaks ENISA kohandama oma personaliplaneerimist ja tasudega seotud vahendite haldamist, et oleks võimalik asjakohaselt reageerida asjaomasele nõudlusele ja tasudest saadava tulu kõikumisele.

(71) Selleks et teha kindlaks tegelike ja tajutavate huvide konflikti risk ja seda riski nõuetekohaselt juhtida, peaksid ENISA-l olema eeskirjad huvide konfliktide ärahoidmise ja kõrvaldamise kohta. ENISA peaks kohaldama ka dokumentidele juurdepääsu käsitlevaid norme, mis on sätestatud Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 1049/2001[54]. ENISA peaks töötlema isikuandmeid kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2018/1725[55]. ENISA peaks järgima teabe, eelkõige tundliku salastamata teabe ja Euroopa Liidu salastatud teabe käitlemisel liidu üksuste suhtes kohaldatavaid sätteid ja liikmesriikide õigusakte.

(72) ENISA-l võib olla oma ülesannete täitmisel juurdepääs tundlikule teabele, näiteks teabele küberohtude ja -intsidentide kohta. Seetõttu on oluline, et ENISA säilitaks käideldava teabe konfidentsiaalsuse. Eelkõige, kooskõlas ELi toimimise lepingu artikliga 339, ei tohiks ENISA ametnikud ja muud teenistujad isegi pärast oma ametikohustuste lõppemist avalikustada ametisaladuse pidamise kohustuse alla kuuluvat teavet, iseäranis teavet ettevõtjate, nende ärisuhete või nende kulukomponentide kohta.

(73) Tagamaks, et ENISA saavutab oma eesmärgid täies ulatuses, peaks ta suhtlema asjaomaste liidu järelevalve- ja muude pädevate asutustega, asjaomaste liidu üksustega, kelle hulka kuuluvad CERT-EU, Europoli juures tegutsev küberkuritegevuse vastase võitluse Euroopa keskus (ECCC), küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus, Euroopa Kaitseagentuur (EDA), Euroopa Liidu Kosmoseprogrammi Amet (EUSPA), elektroonilise side Euroopa reguleerivate asutuste amet (BEREC), Vabadusel, Turvalisusel ja Õigusel Rajaneva Ala Suuremahuliste IT-süsteemide Operatiivjuhtimise Euroopa Liidu Amet (eu-LISA), Euroopa Keskpank (EKP), Euroopa Pangandusjärelevalve (EBA), Euroopa Andmekaitsenõukogu, Euroopa Liidu Energeetikasektorit Reguleerivate Asutuste Koostöö Amet (ACER), Euroopa Liidu Lennundusohutusamet (EASA) ja muud liidu üksused, kes tegelevad küberturvalisusega. Samuti peaks ENISA suhtlema direktiivi (EL) 2022/2555 kohaste

[54] Euroopa Parlamendi ja nõukogu 30. mai 2001. aasta määrus (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele (EÜT L 145, 31.5.2001, lk 43, ELI: http://data.europa.eu/eli/reg/2001/1049/oj).

[55] Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

pädevate asutustega, turujärelevalveasutustega ja andmekaitsega tegelevate ametiasutustega, et vahetada oskusteavet ja parimaid tavasid ning anda nõu küberturvalisuse küsimustes, mis võivad mõjutada nende asutuste tööd.

(74) Europolil on oluline roll küberkuritegevuse, sh võrgu- ja infoturbeintsidentidega seotud küberkuritegevuse ennetamisel ja nende vastu võitlemisel. Selleks et luua koostoime Europoli ja ENISA vastavate ülesannete vahel, peaks ENISA tegema Europoliga koostööd, eelkõige jagama teavet lunavararünnete meetodite, nõuete ja mõju kohta. See koostöö võib hõlmata direktiivi (EL) 2022/2555 I ja II lisas loetletud üksuste vastu suunatud kõige levinumate lunavaratüvede kindlakstegemist, et toetada elutähtsaid ja olulisi üksusi intsidentidele reageerimisel ja neist taastumisel.

(75) Selleks et toetada operatiivkoostööd ning küberohtude ja -intsidentide alast ühist olukorrateadlikkust, on oluline, et ENISA teeks koostööd sidusrühmadega, eelkõige erasektori ettevõtjate ja organisatsioonidega, kellega ENISA võib luua avaliku ja erasektori partnerlusi.

(76) Selleks et saavutada tulemuslikult käesolevas määruses sätestatud eesmärgid, võib ENISA teha koostööd eeskätt selliste akadeemiliste asutustega, kes viivad asjaomastes valdkondades ellu teadusalgatusi, ning luua kanalid, mis võimaldavad saada sisendit tarbijaorganisatsioonidelt- ja muudelt organisatsioonidelt.

(77) Küberohud ja -intsidendid ei hooli riigipiiridest, mistõttu võib liidu üksusi mõjutada kolmandate riikide küberturvalisuse ja valmisoleku tase. Seepärast peaks ENISA-l olema võimalik pakkuda kolmandatele riikidele suutlikkuse suurendamise meetmeid, sh koolitust, suutlikkuse suurendamist ja mestimist, ning eelkõige kohandatud suutlikkuse suurendamise meetmeid liidu kandidaatriikidele või muudele partnerriikidele kooskõlas liidu prioriteetidega. Neid meetmeid tuleks võtta, kui esitatakse konkreetne taotlus, et pakutaks asjakohast tuge, võttes arvesse liidu prioriteete, ning neid tuleks rakendada konkreetsete kokkulepete, sh määruses (EL, Euratom) 2024/2509 osutatud rahalist toetust käsitlevate lepingute kaudu. Euroopa küberturvalisuse sertifitseerimise raamistiku eesmärk on kaitsta küberohtude eest, nagu pahatahtlikult ärakasutatavad küberturvalisusega seotud nõrkused või küberintsidendid, mis mõjutavad IKT-toodete, -teenuste ja -protsesside ning hallatud turbeteenuste funktsionaalsust (disainilahendust ja toimimist) või üksuste turvaolekut. Keskendudes IKT-toodete, -teenuste ja -protsesside, hallatud turbeteenuste ning üksuste turvaolekuga seotud tehnilistele riskidele, peaks Euroopa küberturvalisuse sertifitseerimise raamistik täiendama IKT tarneahelate turvalisuse raamistikku, mille eesmärk on tagada liidu tasandi ühtlustatud lähenemisviis tegelemiseks mittetehniliste riskidega kriitilise tähtsusega sektorites ja muudes kriitilise tähtsusega sektorites.

(78) Liikmesriikidel peaks olema võimalik kasutada Euroopa küberturvalisuse sertifitseerimist riigihangete kontekstis kooskõlas Euroopa Parlamendi ja nõukogu direktiiviga 2014/24/EL[56].

(79) Selleks et oleks hõlpsam üksuste jaoks nõuete täitmist lihtsustada, tuleks Euroopa küberturvalisuse sertifitseerimise raamistikus ette näha üksuste turvaoleku sertifitseerimise võimalus. Üksustel, eelkõige neil, kes osutavad mitut liiki teenuseid mitmes liikmesriigis, võivad olla erinevad küberturvalisuse ja andmeturbega seotud

[56] Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/24/EL riigihangete kohta ja direktiivi 2004/18/EÜ kehtetuks tunnistamise kohta (ELT L 94, 28.3.2014, lk 65, ELI: http://data.europa.eu/eli/dir/2014/24/oj).

kohustused, mis tulenevad horisontaalsetest õigusaktidest, nagu Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679[57] ja Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555,[58] aga ka valdkondlikest õigusaktidest. Selleks et ühtlustada üldise küberturvalisuse õigusraamistiku rakendamist ja lihtsustada selle järgimist, peaks olema võimalik anda üksustele liidu õigusaktiga võimalus tõendada küberriskide juhtimise nõuete täitmist Euroopa küberturvalisuse sertifitseerimise sertifikaadi abil. Asjakohane kava võiks aidata ühtlustada eri õigusaktidest tulenevaid vastavusnõudeid, piiramata neis sätestatud sertifitseerimisnõudeid. Sellised lihtsustamismeetmed võivad aidata vähendada halduskoormust ning vabastada vahendeid, et tugevdada liidu kriitilise tähtsusega sektorite üksuste operatiivset küberturvalisuse alast valmisolekut.

(80) Euroopa küberturvalisuse sertifitseerimise raamistikus väljatöötatud küberriskide juhtimise nõuete Euroopa sertifitseerimine peaks võimaldama üksustel tõendada asjakohastes liidu õigusaktides sätestatud nõuete täitmist, kui sertifitseerimiskava hõlmab selles õigusaktis sätestatud õigusnõudeid ja õigusaktiga on taoline võimalus ette nähtud. Selle põhjal võib liidu õigusaktiga ette näha neile nõuetele vastavuse eelduse. Sellised kavad võiksid aidata parandada liidu õigusaktides sätestatud küberturvalisuse nõuete sidusat rakendamist, et tagada kõigis liikmesriikides võrdsed tingimused ja vähendada nõuete täitmisega seotud koormust.

(81) Euroopa küberturvalisuse sertifitseerimise raamistikus tuleks näha ette võimalus sertifitseerida IKT-protsesse, mis on määratletud kui IKT-toote või -teenuse projekteerimiseks, arendamiseks, tarnimiseks või hooldamiseks tehtavate toimingute kogum. Näiteks komisjoni rakendusmääruses (EL) 2024/482[59] määratletud kaitseprofiil on IKT-protsess. Teise IKT-protsessi näitena võib nimetada toiminguid, mida tootja teeb IKT-toote turvaliseks projekteerimiseks ja arendamiseks, sh füüsilised, loogilised, menetluslikud, personaliga seotud ja muud turbemeetmed, mis on vajalikud IKT-toote disainilahenduse ja rakendamise konfidentsiaalsuse ja tervikluse kaitsmiseks selle arenduskeskkonnas. Sellise tegevuse sertifitseerimist nimetatakse komisjoni rakendusmääruse (EL) 2024/482 kohase sertifitseerimisprotsessi kontekstis sageli tegevuskoha sertifitseerimiseks.

(82) Käesolevas määruses sätestatud mõiste „hallatud turbeteenused“ määratlus peaks olema kooskõlas direktiivis (EL) 2022/2555 kasutatud mõiste „hallatud turbeteenuse osutaja“ määratlusega. Kõnealused teenused seisnevad klientide küberriskide juhtimisega seotud tegevuse korraldamises või toetamises ning need on muutunud intsidentide ennetamisel ja leevendamisel üha olulisemaks. Seega käsitatakse selliste teenuste osutajaid elutähtsate või oluliste üksustena, mis kuuluvad direktiivi (EL) 2022/2555 kohaselt kriitilise tähtsusega sektorisse. Sellistes valdkondades nagu

---

57 Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

58 Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

59 Komisjoni 31. jaanuari 2024. aasta rakendusmäärus (EL) 2024/482, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega (ELT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

intsidentidele reageerimine, läbistustestimine, turvaaudit ja konsultatsioonid on hallatud turbeteenuse osutajatel eriti oluline roll, et aidata üksustel intsidente ennetada, avastada, lahendada ja neist taastuda. Paraku on hallatud turbeteenuse osutajad olnud ka ise küberrünnete sihtmärgiks ja kuna nad on tihedalt lõimitud oma klientide tegevusse, kujutavad nad endast erilist riski. Seepärast on vajalik, et elutähtsad ja olulised üksused direktiivi (EL) 2022/2555 tähenduses oleksid hallatud turbeteenuse osutajate valimisel iseäranis hoolikad.

(83) Euroopa küberturvalisuse sertifitseerimise kavad on olulised paljude sidusrühmade jaoks, nagu IKT-lahenduste pakkujad, vastavushindamisasutused ja kasutajad. Sidusrühmade laialdase kaasamise edendamiseks tuleks vähemalt kord aastas kokku kutsuda Euroopa küberturvalisuse sertifitseerimise assamblee, et edendada koostööd komisjoni, ENISA, liikmesriikide ja asjaomaste sidusrühmade vahel. Assambleel on keskne roll uute küberturvalisuse probleemide ja sertifitseerimise strateegiliste prioriteetide kindlakstegemisel ja käsitlemisel ning selle tagamisel, et sertifitseerimiskavad hõlbustavad digitehnoloogia turvalist integreerimist ja vastavad kasutajate vajadustele. Assamblee peaks tugevdama liidu juhtpositsiooni sertifitseerimistegevuses ning aitama säilitada sertifitseerimisraamistiku usaldusväärsuse ettevõtjate, avaliku sektori asutuste ja üldsuse silmis.

(84) Komisjon peaks haldama spetsiaalset veebisaiti, et tagada läbipaistvus, avaldades ajakohastatud teavet Euroopa küberturvalisuse sertifitseerimise raamistiku rakendamisel tehtud edusammude kohta. Veebisait peaks sisaldama teavet koostamisel olevate sertifitseerimiskavade kohta, tulevaste sertifitseerimiskavade strateegilisi prioriteete, ENISA-le esitatud ettevalmistavate sertifitseerimiskavade koostamise taotlusi ja teavet sertifitseerimiskavade vastuvõtmise kohta. Komisjoni veebisait täiendab ENISA hallatavat Euroopa küberturvalisuse sertifitseerimise kavade veebisaiti, mis peaks sisaldama üksikasjalikku teavet ettevalmistavate kavade tehnilise ettevalmistamise ja kavade haldamise kohta, keskendudes välja antud Euroopa küberturvalisuse sertifikaatidele ja ELi vastavusdeklaratsioonidele.

(85) Selleks et tõhustada dialoogi liidu institutsioonide vahel ning aidata kaasa ametlikule, avatud, läbipaistvale ja kaasavale konsultatsiooniprotsessile, peaks komisjon võtma käesoleva määruse hindamisel arvesse Euroopa Parlamendi, nõukogu ja Euroopa küberturvalisuse sertifitseerimise assamblee väljendatud seisukohti.

(86) ENISA tehtud teostatavusuuringud peaksid aitama teha ettevalmistusi küberturvalisuse sertifitseerimise kavade ettevalmistamiseks ja väljatöötamiseks. Uuringud peaksid hõlmama asjaomaste sidusrühmade vaatenurki ja nende abil tuleks viia tulevased sertifitseerimiskavad kooskõlla käimasoleva teadus- ja arendustegevusega ning tehnoloogia hindamisega, võttes arvesse eelkõige liidu ja liikmesriikide teadusalgatuste panust. Sellised uuringud võivad aidata kindlaks teha olemasolevaid standardeid ja tehnilisi kirjeldusi. Neid tuleks teha komisjoni taotlusel või kooskõlas liidu strateegiliste prioriteetidega, et tagada areneva tehnoloogiamaastiku ja muutuvate küberturvalisuse vajaduste piisav käsitlemine ja kajastamine kavade taotlemisel ja väljatöötamisel.

(87) Ettevalmistava kava ülesehitus ning turvaeesmärkide ja -elementide hõlmatus peaks olema vastavuses sertifitseerimisobjekti sisu ja ulatusega. Seega võib näiteks pilvteenuste sertifitseerimise kavas käsitleda turvaeesmärke, mis on asjakohased IKT-teenuste ja organisatsiooni turvalisuse seisukohast. Teise näitena võib märkida, et IKT-protsesside sertifitseerimisel ei ole tõenäoliselt asjakohane turvaeesmärk, mis on seotud teadaolevate ärakasutatavate nõrkuste väljajätmisega.

(88) Selleks et tagada Euroopa küberturvalisuse sertifitseerimise kavade ühtlustatud rakendamine kõigis liikmesriikides, on vaja ette näha eeskirjad nende kavade haldamise kohta. Kavade haldamine on vajalik muu hulgas selleks, et tagada kavade ja neile lisatud dokumentide ajakohasus, eelkõige küberturvalisuse valdkonnas, kus ohud ja tehnoloogia pidevalt muutuvad. Seepärast peaks sertifitseerimiskavade kavandamine ja haldamine toimuma viisil, millega välditakse ohtu, et kava aegub kiiresti. Kavade haldamine peaks üldjuhul hõlmama lisadokumentide, sh tehniliste kirjelduste ja suuniste koostamist ja ajakohastamist ning asjakohaste standardite või tehniliste kirjelduste kindlakstegemist. Samuti tuleks kava haldamise raames analüüsida kava toimimist, selle võimalikke puudusi ja vajalikke täiustusi. Lisaks peaks haldamine hõlmama liikmesriikidevahelist teabevahetust kavade rakendamise kohta ning panustamist vastastikustesse eksperdihinnangutesse ja vastastikuse hindamise mehhanismidesse.

(89) Kuna tegemist on laadilt tehnilise tegevusega, peaks ENISA haldama kavu koostöös komisjoniga ning teda peaksid toetama Euroopa küberturvalisuse sertifitseerimise rühm ja selle kavade haldamise allrühm. Kõnealuse kavade hindamise allrühma loomine võimaldab koguda liikmesriikidelt lähenemisviiside ühtlustamiseks tehnilist teavet ja seisukohti.

(90) Kavade haldamise raames tuleks suhelda asjaomaste sidusrühmadega, et tagada muu hulgas tehnilise panuse jagamise ja vastuvõtmise kaudu, et kavad vastavad jätkuvalt turu vajadustele ja on ajakohased. Nendeks sidusrühmadeks võivad olla standardiorganisatsioonid, vastavushindamisasutused, müüjad, kasutajad, avaliku sektori asutused või kutseorganisatsioonid. Iga kava, sh asjaomaste tehniliste foorumite ja tööstusharude iseärasuste tõttu peaks olema võimalik koguda tehnilisi panuseid eri kavade puhul erinevalt. Mõne kava puhul peaks ENISA saama tugineda ajutisele töörühmale, mis koondab liikmesriikide ametiasutuste, liidu üksuste ja erasektori eksperte. Tehnilise panuse võivad anda ka teabe jagamise ja analüüsimise keskused ja standardiorganisatsioonid. ENISA peaks analüüsima, milline vorm on iga kava jaoks kõige sobivam, ja sätestama igas ettevalmistavas kavas kava haldamise strateegia.

(91) Euroopa küberturvalisuse sertifitseerimise kavad peaksid tuginema standarditele või tehnilistele kirjeldustele, eelkõige turvanõuete ja hindamismetoodika kindlaksmääramise osas. ENISA-le tuleks anda võimalus koostada tehnilisi kirjeldusi, et toetada kavade väljatöötamist ja haldamist, eelkõige juhul, kui standardiorganisatsioonide koostatud dokumendid puuduvad või ei sobi need kava eesmärkide saavutamiseks. Teksti koostamisel peaks ENISAt toetama Euroopa küberturvalisuse sertifitseerimise rühm ja vajaduse korral asjaomase kava jaoks loodud ajutine töörühm. ENISA peaks küsima sisendit ka sidusrühmadelt. Lisaks peaks ENISA kaaluma, kas tehniline kirjeldus on turule vastuvõetav, ning võtma arvesse Euroopa ja rahvusvahelisi standardeid. Arvestades tehniliste kirjelduste kvaliteeti ja kava eesmärke, peaks komisjonil olema võimalik viidata Euroopa küberturvalisuse sertifitseerimise kavas ENISA koostatud tehnilistele kirjeldustele.

(92) ENISA koostatud ja kavas viidatud tehnilised kirjeldused tuleks teha kättesaadavaks ENISA hallataval Euroopa küberturvalisuse sertifitseerimise kavade veebisaidil, et neile pääseksid ligi kõik huvitatud isikud. Mõnel konkreetsel juhul võib veebisaidil avaldamine seada ohtu sertifitseeritud IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste küberturvalisuse või üksuste turvaoleku ja seega ka avaliku julgeoleku. Näiteks võivad tehnilised kirjeldused sisaldada täpset teavet uute ründevektorite kohta ja selle teabe avalik kättesaadavus võimaldaks pahatahtlikel isikutel neid kasutada.

Sellist teavet tuleks levitada piiratult ja teadmisvajaduse alusel asjaomastele sidusrühmadele, nagu riiklikud küberturvalisuse sertifitseerimise asutused, vastavushindamisasutused ja sertifitseeritavad müüjad. Seoses piiratud levitamisega ei tohiks Euroopa küberturvalisuse sertifitseerimise kavades sellistele tehnilistele kirjeldustele viidata, mistõttu peaksid need kirjeldused olema mittesiduvad.

(93) Turvaoleku sertifitseerimise kavad tuleks üles ehitada modulaarselt, et oleks võimalik tõendada nõuete täitmist ja eeldada vastavust muudes liidu õigusaktides sätestatud asjakohastele küberturvalisuse nõuetele, kui asjaomase õigusaktiga on selline võimalus ette nähtud. Seega saab muus õigusaktis sätestatud nõuetele vastavuse eeldust kasutada nõuete täitmise tõendamiseks vaid siis, kui asjaomane õigusakt seda võimaldab. Turvaoleku sertifitseerimise Sellise kava üksikasjad, nimelt otstarve, eesmärk või elemendid, erinevad tõenäoliselt teiste kavade üksikasjadest. Eeskätt tuleks turvaoleku sertifitseerimise kavad välja töötada selleks, et oleks võimalik hinnata, kas üksus järgib järjekindlalt liidu õigusakte. Seetõttu ei ole vaja, et üksuste turvaoleku sertifitseerimise kavad hõlmaksid kõiki Euroopa küberturvalisuse sertifitseerimise kavade elemente, näiteks usaldusväärsuse tasemeid, ning see peaks kajastuma ka neid kavu käsitlevates õigusnormides.

(94) Raamistik turvaoleku sertifitseerimiseks Euroopa küberturvalisuse sertifitseerimise raamistikus võimaldab töötada välja kava, mis annab mitmes liikmesriigis teenuseid osutavatele üksustele võimaluse tõendada Euroopa Parlamendi ja nõukogu direktiivis (EL) 2022/2555 sätestatud küberriskide juhtimise kohustuste täitmist. See võimalus tõendada nõuetelevastavust tähendab üksuste jaoks sidusamat ja vähem koormavat järelevalvet kogu siseturul. Sellise sertifitseerimiskava väljatöötamist tuleks hõlbustada rakendusaktide vastuvõtmisega direktiivi (EL) 2022/2555 alusel. Tänu laiendusprofiilidele võimaldab turvaoleku sertifitseerimise kava tõendada nõuetelevastavust olukorras, kus liikmesriik on kooskõlas direktiiviga (EL) 2022/2555 vastu võtnud või jätnud kehtima sätted, millega tagatakse küberturvalisuse kõrgem tase. Üksus, kes osutab teenuseid mitmes liikmesriigis, saab tõendada ühtse Euroopa küberturvalisuse sertifikaadi abil vastavust kõigile asjakohastele laiendusprofiilidele.

(95) Euroopa küberturvalisuse sertifitseerimise kavades sätestatud turvaeesmärgid ja -nõuded, mis on seotud toodete turvalisusega, peaksid olema kooskõlas määruse (EL) 2024/2847 I lisas sätestatud oluliste küberturvalisuse nõuetega. See sidusus on vajalik selle tagamiseks, et tootjate suhtes, kelle tooted kuuluvad määruse (EL) 2024/2847 kohaldamisalasse, ei kohaldata üksteisele vastukäivaid nõudeid, kui nende tooteid sertifitseeritakse Euroopa küberturvalisuse sertifitseerimise kava alusel. Lisaks hõlbustab nõuete järjepidevus nõuetele vastavuse eeldamist kooskõlas määruse (EL) 2024/2847 artikliga 27, mille kohaselt võidakse tootjate puhul, kes toodavad Euroopa küberturvalisuse sertifitseerimise kava alusel sertifitseeritud digielemente sisaldavaid tooteid, teatavatel tingimustel eeldada kõnealuse määruse I lisas sätestatud oluliste küberturvalisuse nõuete täitmist.

(96) Euroopa küberturvalisuse sertifitseerimise kavas peaks olema võimalik määrata kindlaks laiendusprofiil, nähes kasutusjuhtude jaoks ette lisa- või erinõuded, sh lisasuutlikkus, nagu täiustatud tooteomadused, eriteenuste pakkumine või eriotstarbelised varad, optimeeritud protsessid ja täiustatud turbemeetmed. Kuna laiendusprofiilid ei vasta konkreetsele usaldusväärsuse tasemele, tuleks neis üksikasjalikult kirjeldada taotletavat eesmärki, sh käsitletavaid küberohte. Laiendusprofiilid on mõeldud eeskätt selleks, et tõendada vastavust konkreetsetele standarditele ja regulatiivsetele nõuetele, sh vajaduse korral vastavust nõuetele, mis on seotud küberriskide juhtimise meetmetega, mille liikmesriik on täiendavalt

kehtestanud, järgides kooskõlas direktiiviga (EL) 2022/2555 minimaalse ühtlustamise põhimõtet.

(97) Ilma et see piiraks üldist vastastikuse hindamise süsteemi, mis kehtestatakse Euroopa küberturvalisuse sertifitseerimise raamistiku raames kõigis riiklikes küberturvalisuse sertifitseerimise asutustes, peaks olema võimalik lisada Euroopa küberturvalisuse sertifitseerimise kavadesse vastastikuse hindamise mehhanism asutustele, kes väljastavad IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku kohta Euroopa küberturvalisuse sertifikaate, eelkõige neile asutustele, kes annavad selliste kavade alusel välja sertifikaate kõrge usaldusväärsuse taseme kohta. Nende asutuste hulka peaksid kuuluma ka kõrge usaldusväärse taseme kohta sertifikaate välja andvad riiklikud küberturvalisuse sertifitseerimise asutused. Selliste vastastikuse hindamise mehhanismide rakendamist peaks toetama Euroopa küberturvalisuse sertifitseerimise rühm. Vastastikuse hindamise käigus tuleks hinnata eeskätt seda, kas asjaomased asutused täidavad oma ülesandeid ühtlustatud viisil, ja see võib hõlmata edasikaebamise mehhanisme.

(98) Sertifitseerimistegevusele võivad avaldada kahjulikku mõju kriisid, näiteks sõjad, loodusõnnetused ja pandeemiad. Sellises kriisiolukorras ei pruugi taristu hävimise, küberrünnete, töötajate kättesaamatuse või tegevuskoha ligipääsmatuse tõttu olla võimalik tagada näiteks tegevuskoha turvalisust. Seepärast tuleks Euroopa küberturvalisuse sertifitseerimise kavas sätestada ajutised eeskirjad sertifitseerimistegevuse järjepidevuse tagamiseks selliste stsenaariumide korral.

(99) Tehniliste ettevalmistavate kavade muutmine rakendusaktideks nõuab põhjalikke tehnilisi ja juriidilisi teadmisi ning võib tekitada märkimisväärse halduskoormuse. Lisaks on Euroopa küberturvalisuse sertifitseerimise kavade teatavad elemendid, nagu nõrkusehaldus või märkide või märgistuste kasutamise tingimused, valdkondadevahelised ja nende puhul võiksid olla kasulikud ühtlustatud viitamissätted. Selleks et tagada vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade kvaliteet ja vähendada ettevõtjate jaoks nõuete täitmisega seotud koormust, peaks komisjonil olema õigus võtta vastu sertifitseerimiskavade teatavaid elemente käsitlevad näidissätted.

(100) Euroopa küberturvalisuse sertifitseerimise raamistiku järjepidevuse tagamiseks peaks Euroopa küberturvalisuse sertifitseerimise kavas saama täpsustada asjaomase kava alusel välja antavate Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide usaldusväärsuse tasemed. Euroopa küberturvalisuse sertifikaat peaks osutama ühele usaldusväärsuse tasemele: usaldusväärsuse baastasemele, märkimisväärsele usaldusväärsuse tasemele või kõrgele usaldusväärsuse tasemele, ELi vastavusdeklaratsioon aga üksnes baastasemele. Usaldusväärsuse tasemed peaksid kajastama IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või turvaoleku hindamise rangust ja põhjalikkust ning nende kirjeldamisel tuleks viidata asjaomastele tehnilistele kirjeldustele, standarditele ja menetlustele, sh tehnilistele kontrollidele, mille eesmärk on vähendada või ennetada intsidente. Iga usaldusväärsuse tase peaks olema järjepidev eri valdkondade lõikes, kus sertifitseerimist kohaldatakse.

(101) Euroopa küberturvalisuse sertifikaadi kasutajad peaksid valima asjakohase sertifitseerimise ja seonduvad turvanõuded, lähtudes IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste kasutamisega seotud riskide või üksuste sertifitseerimise konteksti analüüsist. Seega peaks usaldusväärsuse tase vastama riskitasemele, mida seostatakse IKT-toote, -teenuse, -protsessi või hallatud

turbeteenuse kavandatud kasutamisega või selle üksuse tegevuskeskkonna ja laadiga, kelle turvaolekut sertifitseeritakse.

(102) Usaldusväärsuse baastaseme hindamisel tuleks juhinduda vähemalt järgmistest usaldusväärsuse komponentidest: hindamine peaks sisaldama vähemalt seda, et vastavushindamisasutus vaatab läbi IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuse turvaoleku tehnilise dokumentatsiooni. Kui sertifitseerimine hõlmab IKT-protsesse, peaks tehnilist läbivaatamist kohaldama ka protsesside suhtes, mida on kasutatud IKT-toote, -teenuse, hallatud turbeteenuse või üksuse turvaoleku projekteerimiseks, arendamiseks ja hooldamiseks. Kui Euroopa küberturvalisuse sertifitseerimise kavaga on ette nähtud vastavuse enesehindamine, peaks piisama sellest, kui IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja või üksus, kelle turvaolekut sertifitseeritakse, on viinud läbi enesehindamise, et hinnata oma IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuse turvaoleku vastavust sertifitseerimiskavale.

(103) Märkimisväärse usaldusväärsuse taseme jaoks tuleks hindamisel lisaks usaldusväärsuse baastaseme puhul ette nähtule kontrollida vähemalt IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuse turvaoleku turvafunktsioonide vastavust asjaomasele tehnilisele dokumentatsioonile.

(104) Kõrge usaldusväärsuse taseme jaoks tuleks hindamisel lisaks märkimisväärse usaldusväärsuse taseme puhul nõutule teha vähemalt tõhususe kontroll, mille käigus hinnatakse turvafunktsioonide võimet panna vastu küberrünnetele, mida panevad toime isikud, kellel on selleks märkimisväärsed oskused ja vahendid. Kõrge usaldusväärsuse taseme jaoks või juhul, kui kava eesmärk on tõendada vastavust ja anda alus eeldada vastavust muudele liidu õigusaktidele, tuleks vastavushindamine teha Euroopa Majanduspiirkonnas. Seda nõuet õigustab asjaolu, et väljaspool Euroopa Majanduspiirkonda tehtavad hindamistoimingud põhjustavad küberturvalisusele, eelkõige hinnatavate IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste intellektuaalomandile, täiendavaid ohte. Näiteks võidakse kolmanda riigi piiri ületamisel kontrollida IKT-toote lähtekoodi, mis kujutab endast riski intellektuaalomandile. Lisaks ei tegutse kolmandates riikides asutatud katselaborid keskkonnas, mille suhtes kohaldatakse ELi õigusaktidega, näiteks direktiiviga (EL) 2022/2555 või määrusega (EL) 2024/2847 ette nähtud küberturvalisuse meetmeid. Näiteks võib katselabor kasutada kolmandast isikust pilvteenuse osutajat, kes ei täida direktiivis (EL) 2022/2555 sätestatud küberturvalisuse nõudeid. Sellegipoolest peaks olema lubatud näha sertifitseerimiskavas ette mehhanism erandite tegemiseks, näiteks tegevuskoha sertifitseerimisel või muudel juhtudel, kui vastavushindamist ei ole võimalik mõistlikult teha Euroopa Majanduspiirkonnas.

(105) Mõnel juhul võib konkreetse usaldusväärsuse taseme turvaeesmärkide saavutamiseks olla vaja erinevaid lähenemisviise, et võtta arvesse IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuse turvaoleku spetsiifikat. Üksikasjalikuma lähenemisviisi võimaldamiseks peaks olema võimalik määrata Euroopa küberturvalisuse sertifitseerimise kavas kindlaks üks või mitu ühele usaldusväärsuse tasemele vastavat hindamistaset. See võimaldaks koostada kavu, kus konkreetse usaldusväärsuse tasemega seotud turvalisuse tasemele vastavad mitu eri eesmärgil kavandatud hindamistaset.

(106) Euroopa küberturvalisuse sertifitseerimise kavas peaks olema lubatud näha ette vastavushindamise läbiviimine nii, et selle eest vastutab vaid IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja või üksus, kelle turvaolekut

sertifitseeritakse („vastavuse enesehindamine“). Sellistel juhtudel peaks selle tagamiseks, et IKT-toode, -teenus, -protsess, hallatud turbeteenus või üksuse turvaolek vastab Euroopa küberturvalisuse sertifitseerimise kavale, piisama sellest, kui tootja, pakkuja või üksus, kelle turvaolekut sertifitseeritakse, teeb ise kõik kontrollid. Vastavuse enesehindamist tuleks pidada asjakohaseks IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ja üksuse turvaoleku puhul, mis on vähekeerukad, kujutavad endast avalikkusele väikest riski ning on lihtsa disainilahenduse või tootmismehhanismiga.

(107) Kui Euroopa küberturvalisuse sertifitseerimise kava võimaldab nii IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ja üksuste turvaoleku vastavuse enesehindamist kui ka sertifitseerimist, tuleks sertifitseerimiskavas ette näha selged ja arusaadavad vahendid, mille abil saaksid tarbijad või muud kasutajad teha vahet tootja või pakkuja enda hinnatud ja kolmanda isiku sertifitseeritud IKT-toodetel, -teenustel, -protsessidel, hallatud turbeteenustel ja üksuste turvaolekul.

(108) IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja või üksus, kelle turvaolekut sertifitseeritakse, peaks saama vastavushindamismenetluse raames väljastada ja allkirjastada ELi vastavusdeklaratsiooni. ELi vastavusdeklaratsioon on dokument, mis kinnitab, et konkreetne IKT-toode, -teenus, -protsess, hallatud turbeteenus või üksuse turvaolek vastab Euroopa küberturvalisuse sertifitseerimise kavas esitatud nõuetele. ELi vastavusdeklaratsiooni väljastamise ja allkirjastamisega võtab IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja või üksus, kelle turvaolekut sertifitseeritakse, endale vastutuse selle eest, et IKT-toode, -teenus, -protsess, hallatud turbeteenus või turvaolek vastab Euroopa küberturvalisuse sertifitseerimise kavas sätestatud turvanõuetele. ELi vastavusdeklaratsiooni koopia tuleks esitada riiklikule küberturvalisuse sertifitseerimise asutusele ja ENISA-le.

(109) IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootjad ja pakkujad ning üksused, kelle turvaolekut sertifitseeritakse, peaksid tegema ELi vastavusdeklaratsiooni, tehnilise dokumentatsiooni ja kogu muu teabe, mis puudutab vastavust Euroopa küberturvalisuse sertifitseerimise kavale, pädevale riiklikule küberturvalisuse sertifitseerimise asutusele kättesaadavaks asjaomases sertifitseerimiskavas kindlaks määratud tähtaja jooksul kooskõlas kohaldatavate liidu õigusaktidega. Tehnilistes dokumentides tuleks kindlaks määrata kava kohaselt kohaldatavad nõuded, mis on vastavuse enesehindamise seisukohast asjakohased. Tehnilised dokumendid peaksid olema koostatud nii, et need võimaldavad hinnata IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuse turvaoleku vastavust kava kohaselt kohaldatavatele nõuetele.

(110) Euroopa küberturvalisuse sertifikaadid ja ELi vastavusdeklaratsioonid peaksid aitama kasutajatel teha teadlikke valikuid. Seepärast tuleks asjakohane teave avaldada ENISA hallataval veebisaidil. Lisaks tuleks koos sertifitseeritud või ELi vastavusdeklaratsiooni saanud IKT-toodete, -teenuste ja -protsessidega esitada struktureeritud teave, mis on kohandatud kavandatud kasutaja eeldatavale tehnilisele tasemele. Kõigil kasutajatel peaks olema juurdepääs sellisele teabele nagu sertifitseerimiskava viitenumber, sertifikaadi välja andnud asutus või organ ja asjakohasel juhul usaldusväärsuse tase, või neil peaks olema võimalus saada Euroopa küberturvalisuse sertifikaadi koopia. Seda teavet tuleks korrapäraselt ajakohastada ja see peaks olema kättesaadav spetsiaalsel Euroopa küberturvalisuse sertifitseerimise kavade veebisaidil. Selleks et tagada teabe pidev kättesaadavus, tuleks tootjatelt ja

pakkujatelt nõuda, et nad teavitaksid asjaomast sertifitseerimisasutust, kui veebis esitatud või asjakohasel juhul füüsilise teabe asukoht muutub.

(111) Vastavushindamine on protseduur, mille käigus hinnatakse, kas IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksusega seotud konkreetsed nõuded on täidetud. Selle protseduuri teostab sõltumatu kolmas isik, kes ei ole sertifitseeritava IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse tootja ega pakkuja ega üksus, kelle turvaolekut hinnatakse. IKT-tootele, -teenusele, -protsessile, hallatud turbeteenusele või üksuse turvaolekule positiivse hinnangu andmise tulemusel tuleks välja anda Euroopa küberturvalisuse sertifikaat. Euroopa küberturvalisuse sertifikaati tuleks käsitada kinnitusena selle kohta, et hindamine on toimunud nõuetekohaselt.

(112) Selleks et vältida moonutusi ja häireid, mis võivad tekkida olukordades, kus turujärelevalvet teostav üksus ka ise sama turul konkureerib, on väga oluline hoida järelevalve- ja sertifitseerimistegevus rangelt lahus. Tegevusi, mida ellu viies riiklik küberturvalisuse sertifitseerimise asutus üksnes täidab oma järelevalverolli (nt annab eelneva heakskiidu sertifikaadi väljaandmiseks), ei peaks olema vaja täiendavalt eraldada muust järelevalvetegevusest. Nende tegevuste hulka kuulub ka see, kui riiklik küberturvalisuse sertifitseerimise asutus kogub eraõigusliku vastavushindamisasutuse läbiviidava protsessi jooksul aktiivselt teavet ja esitab seejärel oma arvamuse selle kohta, kas vastavushindamisasutus peaks sertifikaadi välja andma (edaspidi „eelneva heakskiidu mudel“).

(113) Euroopa küberturvalisuse sertifitseerimise kavades tuleks kindlaks määrata tingimused, mille korral võib tekkida vajadus sertifitseerida IKT-toode, -teenus, -protsess, hallatud turbeteenus või üksuse turvaolek uuesti või vähendada konkreetse Euroopa küberturvalisuse sertifikaadi kohaldamisala. Lisaks tuleks Euroopa küberturvalisuse sertifitseerimise kavades arvesse võtta sertifitseeritud IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuse turvaolekuga seotud hiljem avastatud nõrkuse või mittevastavuse võimalikku kahjulikku mõju vastavusele asjaomase sertifikaadi turvanõuetega.

(114) Range küberturvalisuse tagamiseks ja ettevõtjate turulepääsu parandamiseks on tähtis ühtlustamine. Killustatus ja sertifikaatide vastastikune mittetunnustamine takistavad märkimisväärselt andmete sujuvat liikumist, suurendades seeläbi liidu tootmisharu tegevuskulusid. Nende probleemide leevendamiseks on oluline vältida kogu liidus killustatust nii turvakontrollimeetmete kohaldamisala kui ka vastavushindamismeetodite puhul.

(115) Liikmesriigid peaksid teavitama komisjoni ja Euroopa küberturvalisuse sertifitseerimise rühma piisavalt aegsasti enne uue riikliku küberturvalisuse sertifitseerimise kava vastuvõtmist IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku jaoks, et aidata komisjonil ja sel rühmal hinnata uue riikliku kava mõju siseturu nõuetekohasele toimimisele ning pidades silmas mis tahes strateegilist huvi taotleda Euroopa küberturvalisuse sertifitseerimise kava.

(116) Liikmesriikide õigusaktides sisalduvad viited riiklikele standarditele, mida Euroopa küberturvalisuse sertifitseerimise kava jõustumise tõttu enam ei kohaldata, võivad põhjustada segadust. Seetõttu peaksid liikmesriigid asjakohasel juhul kajastama Euroopa küberturvalisuse sertifitseerimise kava vastuvõtmist oma siseriiklikes õigusaktides.

(117) Selleks et hõlbustada usaldusväärse siseturu kasvu ja luua samal ajal partnerlusi kolmandate riikidega, tuleks Euroopa küberturvalisuse sertifitseerimise raamistikus

kehtestatud sertifitseerimismenetlust rakendada viisil, mis hõlbustab rahvusvahelist ja vastastikust tunnustamist ning kooskõlastamist rahvusvaheliste standarditega.

(118) Selleks et veelgi enam lihtsustada kaubandust ja tunnistades, et IKT tarneahelad on rahvusvahelised, võib liit sõlmida kooskõlas ELi toimimise lepingu artikliga 218 Euroopa küberturvalisuse sertifikaatide vastastikuse tunnustamise lepinguid. Komisjonil peaks olema õigus võtta vastu rakendusakte, et ühepoolselt tunnistada kolmandate riikide sertifikaatide samaväärsust Euroopa küberturvalisuse sertifikaatidega. Kolmandate riikide sertifikaatide selliseks tunnustamiseks peaks olema võimalik kehtestada eritingimused.

(119) Selleks et saavutada raamistiku samaväärne rakendamine kogu liidus, hõlbustada vastastikust tunnustamist ning edendada Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide üldist aktsepteerimist, tuleb kehtestada riiklike küberturvalisuse sertifitseerimise asutuste vaheline vastastikuse hindamise süsteem. Vastastikune hindamine peaks hõlmama menetlusi, et kontrollida, kas IKT-tooted, -teenused, -protsessid, hallatud turbeteenused ja üksuste turvaolek vastavad Euroopa küberturvalisuse sertifikaadi nõuetele, teha vastavuse enesehindamist läbiviivatee IKT-toodete, -teenuste, -protsesside ja hallatud turbeteenuste tootjate ja pakkujate ja sertifitseeritud üksuste kohustuste järelevalvet, vastavushindamisasutuste järelevalvet ning kontrollida, kas kõrge usaldusväärsuse taseme kohta sertifikaate väljaandvate asutuste töötajatel on sobivad eksperditeadmised. ENISA peaks osalema vastastikuses hindamises vaatlejana ning toetama vastastikuse hindamise mehhanismi rakendamist ja vastastikuse hindamise korraldamist, sh töötama koostöös komisjoni ja Euroopa küberturvalisuse sertifitseerimise rühmaga välja asjakohased juhenddokumendid ja vormid. Samuti peaks ENISA tegema enda hallataval Euroopa küberturvalisuse sertifitseerimise kavade veebisaidil üldsusele kättesaadavaks teabe vastastikuste hindamiste ajakava kohta ja loetelu vastastikuse hindamise läbinud riiklikest küberturvalisuse sertifitseerimise asutustest, kes peavad selle ajakava ellu viima. Vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavades kasutatav vastastikuse hindamise kava on kehtestatud määruse (EL) 2019/881 alusel vastu võetud komisjoni rakendusmäärusega (EL) 2025/2540[60]. On vaja tagada vastastikuse hindamise jätkumine. Komisjonil peaks siiski olema võimalik vajaduse korral kehtestada rakendusaktiga vähemalt viieaastane uus vastastikuse hindamise kava ning sätestada vastastikuse hindamise süsteemi töö kriteeriumid ja metoodikad.

(120) Kui Euroopa küberturvalisuse sertifitseerimise kava vastu võetakse, siis peaks IKT-toodete, -teenuste, -protsesside ja hallatud turbeteenuste tootjatel või pakkujatel või üksustel, kelle turvaolekut sertifitseeritakse, olema võimalik esitada oma IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või turvaoleku sertifitseerimise taotlusi nende valitud vastavushindamisasutusele kõikjal liidus. Vastavushindamisasutused peaks akrediteerima riiklik akrediteerimisasutus, kui nad vastavad käesolevas määruses sätestatud nõuetele ja, kui see on kohaldatav, käesoleva määruse kohaselt komisjoni kindlaks määratud nõuetele. Käesolevas määruses kindlaks määratud

[60] Komisjoni 9. detsembri 2025. aasta rakendusmäärus (EL) 2025/2540, milles sätestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses vastastikuse hindamise kava koostamisega (ELT L, 2025/2540, 12.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2540/oj).

süsteemi peaks täiendama Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 765/2008[61] sätestatud akrediteerimissüsteem.

(121) Vastavushindamisasutused, mis on akrediteeritud või millest on teatatud kehtivate liidu õigusaktide alusel, eelkõige määruse (EL) 2024/2847 või rakendusmääruse (EL) 2024/482 alusel, võivad omada uute vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade jaoks asjakohast pädevust. Põhjendamatu finants- ja halduskoormuse vältimiseks on asjakohane luua koosmõju käesoleva määruse alusel vastavushindamisasutuste akrediteerimiseks. Seetõttu tuleks kehtestada kavade akrediteerimise nõuded selliselt, et tagada võimalikult suures ulatuses vastavus määruses (EL) 2024/2847 sätestatud nõuetele, mis puudutavad teada antud asutusi, ning rakendusmääruses (EL) 2024/482 sätestatud akrediteerimisnõuetele. Lisaks sellele peaks käesoleva määruse alusel akrediteerimisprotsessi läbinud vastavushindamisasutustel olema võimalik tugineda nende pädevuse hindamise varasematele tulemustele, mis on saadud muude liidu õigusaktide alusel, kui akrediteerimisnõuded kattuvad.

(122) Liidus ühtlustatud vastavushindamisteenuste soodustamiseks peaks olema võimalik määrata Euroopa küberturvalisuse sertifitseerimise kavas vastavushindamisasutuste jaoks lisa- või erinõudeid. Sertifitseerimise kontekstis tuleks luba käsitada riikliku küberturvalisuse sertifitseerimise asutuse otsusena, mille kohaselt vastab vastavushindamisasutus Euroopa küberturvalisuse sertifitseerimise kava lisa- või erinõuetele konkreetse vastavushindamistoimingu elluviimiseks.

(123) Kui Euroopa küberturvalisuse sertifitseerimise kavas on kooskõlas käesoleva määrusega sätestatud lisa- või erinõuded, peaks riiklikud küberturvalisuse sertifitseerimise asutused andma vastavushindamisasutustele loa sellise kava alusel ülesannete täitmiseks. Mitmekordse lubade andmise vältimiseks, loa andmise otsuste aktsepteerimise ja tunnustamise lihtsustamiseks ning loa saanud vastavushindamisasutuste tulemuslikuks järelevalveks peaksid vastavushindamisasutused taotlema asukohaliikmesriigi riikliku küberturvalisuse sertifitseerimise asutuse luba. Sellegipoolest tuleb tagada, et vastavushindamisasutusel oleks võimalik taotleda luba teises liikmesriigis, juhul kui tema asukohaliikmesriigis ei ole riiklikku küberturvalisuse sertifitseerimise asutust või kui riiklik küberturvalisuse sertifitseerimise asutus ei ole taotletava loa andmise teenuste osutamiseks pädev. Sellisteks juhtudeks tuleks tagada riiklike küberturvalisuse sertifitseerimise asutuste asjakohane koostöö ja teabevahetus. Komisjonil peaks olema volitus võtta vastu rakendusakte, millega kehtestatakse loa andmise menetlused, sh loa andmisega seotud piiriülese koostöö jaoks.

(124) IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuse turvaoleku vajaliku kaitsetaseme tagamiseks on hädavajalik, et vastavushindamise alltöövõtjatelt ja tütarettevõtjatelt nõutakse vastavushindamise ülesannete täitmise puhul samade nõuete täitmist kui teada antud vastavushindamisasutustelt. Seega peaks vastavushindamisasutusel olema sobilik pädevus ja ta peaks suutma kontrollida, et tema alltöövõtjad täidavad kohaldatavaid nõudeid.

(125) Teavitav ametiasutus peaks nõuetekohaselt hindama seda, kui suures ulatuses kavatseb vastavushindamisasutus kasutada väljaspool liitu asuvaid alltöövõtjaid või mil määral

[61] Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määrus (EÜ) nr 765/2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 (ELT L 218, 13.8.2008, lk 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

tal on juurdepääs väljaspool liikmesriiki asuvatele töötajatele või rajatistele. Liikmesriigi avaliku sektori asutusel peaks olema võimalik otsustada, et ta ei saa võtta riikliku küberturvalisuse sertifitseerimise asutusena üldist vastutust kõnealuse korralduse eest, ning teatamisest keelduda või selle ulatust piirata.

(126) IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuste turvaoleku küberturvalisuse nõuete hindamiseks peaksid riiklikud küberturvalisuse sertifitseerimise asutused teatama komisjonile ja teistele liikmesriikidele akrediteeritud vastavushindamisasutustest. Akrediteeritud ja, kui see on kohaldatav, loa saanud vastavushindamisasutustest teatamine näitab, et neid asutusi saab usaldada käesoleva määruse ja Euroopa küberturvalisuse sertifitseerimise kava kohaste hindamis- ja sertifitseerimistegevuse elluviimisel, millega panustatakse Euroopa küberturvalisuse sertifitseerimise üldisesse mainesse. Seetõttu on hädavajalik tagada, et vastavushindamisasutused, millest on teatatud, täidavad nende suhtes kehtivaid nõudeid ja kohustusi pidevalt ning et teatatud vastavushindamisasutuste loetelu hoitakse ajakohasena.

(127) Määruse (EL) 2019/881 kohaselt vastu võetud komisjoni rakendusmäärusega (EL) 2024/3143[62] on ette nähtud teadete esitamise asjaolud, vormingud ja menetlused, mida kasutatakse vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavades. Seetõttu on vaja tagada teavitamistegevuse jätkumine. Sellest hoolimata tuleks komisjonile anda volitus võtta vastu rakendusakte, et kohandada neid asjaolusid, menetlusi ja vorminguid vastavushindamisasutuste teavitamise otstarbel. Selles kontekstis peaks komisjon tuginema olemasolevate kavade käigus omandatud kogemustele ja proovima tagada vastavuse muudele asjakohastele liidu õigusaktidele ja raamistikele, eelkõige määrusele (EL) 2024/2847 ning uuele õigusraamistikule, et vähendada eri õigusaktide alusel tegutsevate vastavushindamisasutuste regulatiivset koormust.

(128) Info- ja kommunikatsioonitehnoloogia (edaspidi „IKT“) tarneahelad koosnevad ettevõtjatevaheliste ressursside ja protsesside omavahel seotud kogumist. IKT tarneahelatel on ülioluline roll sotsiaalse stabiilsuse säilitamisel ja majandustegevuse edendamisel kogu liidus. Ühtlasi on neil on kriitilise tähtsusega roll liidu digitaristu võimaldamisel ning need on liidu ühiskonna ja majanduse toimimise alus. IKT tarneahelad võimaldavad mitmesuguste kriitilise ja eriti kriitilise tähtsusega sektorite (sh tervishoid, rahandus, transport, telekommunikatsioon, energeetika ja toll) aluseks olevate IKT-teenuste, -süsteemide ja -toodete valmistamist, tootmist, levitamist ja hooldamist. Nende kriitilise tähtsusega sektorite IKT tarneahelate turvalisus võib mõjutada ka kaitse- ja sõjalise taristu turvalisust, kui kõnealune taristu tugineb tsiviilvaldkonna kriitilise tähtsusega sektoritele ja nende IKT tarneahelatele. ENISA välja antud küberohtude olukorda käsitleva aruande (edaspidi „ENISA ohtude kaardistamise aruanne 2025“)[63] kohaselt on ründed tarneahelate vastu siiski üks viiest peamisest küberturvalisust ähvardavast ohust, mis näitab, et ründajad kasutavad aktiivselt kaudseid mõjuahelaid kolmandast isikust teenuseosutajate ja sõltuvuste kaudu. IKT tarneahelate häirimine võib tõkestada majandustegevust siseturul,

---

62 Komisjoni 18. detsembri 2024. aasta rakendusmäärus (EL) 2024/3143, millega nähakse ette teadete esitamise asjaolud, vormingud ja menetlused vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 (mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist) artikli 61 lõikele 5 (ELT L, 2024/3143, 19.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

63 ENISA ohtude kaardistamise aruanne 2025, oktoober 2025.

põhjustada rahalist kahju, õõnestada kasutajate usaldust ning tekitada suurt kahju liidu majandusele ja ühiskonnale. Seetõttu on küberturvalisuse alane valmisolek ja tõhusus siseturu tõrgeteta toimimiseks olulisem kui kunagi varem.

(129) Lisaks tehnilistele riskidele, mida maandatakse Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2022/55,[64] Euroopa Parlamendi ja nõukogu määrusega (EL) 2024/2847[65] ning määrusega (EL) 2019/881 loodud Euroopa küberturvalisuse sertifitseerimise raamistikuga, on IKT tarneahelad üha enam avatud mittetehnilise olemusega riskidele. Kõnealused mittetehnilised riskid võivad muu hulgas olla seotud teatavate komponentide tarnija suhtes kohaldatava jurisdiktsiooniga, eelkõige kui kolmas riik või sellest riigist kontrollitavad ohusubjektid tegelevad majandusspionaažiga, viivad ellu pahatahtlikku kübertegevust või -kampaaniaid liidu või selle liikmesriikide vastu või käituvad riigina küberruumis vastutustundetult. Mittetehnilised riskid võivad samuti olla seotud varjatud nõrkuste, tagauste või võimalike süsteemsete tarnehäiretega, eelkõige tehnoloogilise kinnistumise või tarnijatest sõltuvuse puhul. Näiteks võidakse kasutada hädaseiskamislüliteid, et negatiivselt mõjutada side- ja elektrivõrkude kättesaadavust.

(130) Ühisteatises ELi majandusjulgeoleku tugevdamise kohta[66] rõhutati riski, et kolmandad riigid saavad juurdepääsu liidu või selle liikmesriikide tundlikule teabele ja andmetele kas tööstusspionaaži või teatavates toodetes kasutatava riist- või tarkvara tarnimise tulemusena või seetõttu, et nad on omandanud ja kontrollivad teatavaid tundlikku teavet ja andmeid omavaid ettevõtteid. Selles toodi samuti esile risk, et välismaised osalejad põhjustavad häiringuid ELi elutähtsas taristus (sh elutähtis transporditaristu, kosmosesüsteemid, energia- ja sidetaristu, eelkõige need, mida käsitletakse sõjalise liikuvuse seisukohast strateegilisena), mis võib tekitada ahelmõju liidu majandusele. Häired võivad tekkida füüsiliste või hübriidrünnakute või küberrünnete tulemusena, sh tervete rajatiste või nende osade või alakomponentide sabotaaži tõttu. Need võivad olla seotud ka IKT tarneahelatega, millel põhinevad elutähtsa taristu ülitähtsad komponendid või teenused.

(131) Selleks, et reageerida IKT tarneahela turvalisuse probleemidele, mille on põhjustanud mittetehnilised riskid, on teatavad liikmesriigid võtnud regulatiivseid meetmeid, sh määranud suure riskiga tarnijad, ning teiste liikmesriikide puhul on nende meetmete võtmine tõenäoline. See võib põhjustada riiklike lähenemisviiside üha suuremat lahknevust ja kokkuvõttes teatavate liikmesriikide suuremat nõrkust, mille ülekanduv mõju võib avalduda kogu liidus. Seetõttu on vaja ühtlustada teatavaid aspekte, mis on seotud IKT tarneahelale avalduvate mittetehniliste küberriskidega. Kõnealune sekkumine liidu tasandil on samuti põhjendatud, võttes arvesse vajadust tagada küberturvalisuse kõrge tase kogu liidus. IKT tarneahela turvalisust käsitlevate sätete eesmärk on kõrvaldada kõnealused suured erinevused liikmesriikide vahel, eelkõige

---

64 Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152, ELI: https://eur-lex.europa.eu/eli/dir/2022/2555/oj).

65 Euroopa Parlamendi ja nõukogu 23. oktoobri 2024. aasta määrus (EL) 2024/2847, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrusi (EL) nr 168/2013 ja (EL) 2019/1020 ning direktiivi (EL) 2020/1828 (küberkerksuse määrus) (ELT L, 2024/2847, 20.11.2024, ELI: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/est).

66 Ühisteatis Euroopa Parlamendile ja nõukogule „ELi majandusjulgeoleku tugevdamine“, 3. detsember 2025, JOIN(2025) 977 final.

kehtestades liidu tasandil IKT tarneahela turvalisuse riskide hindamise mehhanisme käsitlevad normid ning IKT tarneahela riskide eest kaitsmise miinimumnõuded.

(132) Kriitiliste sõltuvuste ja nõrkuste vähendamiseks on vaja luua usaldusväärne IKT tarneahela raamistik, mis peaks aitama lahendada suure riskiga tarnijate ja sõltuvustega seotud mittetehnilisi riske kriitilise tähtsusega sektorites ja muudes kriitilise tähtsusega sektorites. Seega on vaja tagada liidu tasandil objektiivne, riskipõhine, tulevikukindel ja tehnoloogianeutraalne raamistik, et määrata kindlaks olulised IKT-varad ning näha riskide vähendamiseks ette proportsionaalsete leevendusmeetmete kogum.

(133) Küberriske, sh riske, mis on seotud sõltuvusega suure riskiga tarnijatest, võib täheldada mitmes kriitilise tähtsusega IKT tarneahelas liidus, sh tuvastamisseadmed, ühendatud ja automatiseeritud sõidukid, elektrivarustuse süsteemid ja elektri salvestamine, veevarustuse süsteemid, mehitamata õhusõidukid ja mehitamata õhusõidukite vastased süsteemid, pilvandmetöötlusteenused, meditsiiniseadmed, jälgimisseadmed, kosmoseteenused ja pooljuhid. Näiteks nõrkused turvaseadmetes võivad anda juurdepääsu IKT-süsteemidele, mis võimaldavad kuritahtlikel osalejatel manipuleerida skannereid viisil, mis võimaldab tuua keelatud objekte läbi turvakontrolli ilma neid avastamata, mille tagajärjed võivad olla katastroofilised.

(134) Käesolev määrus ei tohiks takistada liikmesriike vastu võtmast või kehtima jätmast sätteid, millega tagatakse IKT tarneahela küberturvalisuse kõrgem tase, tingimusel et sellised sätted on kooskõlas liikmesriikide kohustustega, mis on sätestatud liidu õiguses. Kõnealused sätted võivad näiteks hõlmata oluliste IKT-varade puhul rangemate leevendusmeetmete kehtestamist.

(135) Konkreetseid IKT tarneahelaid mõjutavate võimalike küberriskide kindlaks tegemiseks võib direktiivi (EL) 2022/2555 artikliga 14 loodud koostöörühm (edaspidi „võrgu- ja infoturbe koostöörühm“) hinnata konkreetseid IKT tarneahelaid liidu tasandi koordineeritud turvariski hindamiste teel. Liidu tasandi koordineeritud turvariski hindamiste käigus tuleks muu hulgas kontrollida peamisi ohusubjekte, peamisi ohte ja nõrkusi, mis mõjutavad olulisi IKT-varasid. Liidu tasandi koordineeritud turvariski hindamiste käigus tuleks koostada riskistsenaariumide loetelu ja riskide maandamise meetmete loetelu. Liidu tasandi koordineeritud turvariski hindamised tuleks läbi viia kuue kuu jooksul. Eriti kiireloomulistes olukordades peaks olema võimalik tähtaegu lühendada.

(136) Kui komisjonil on piisavalt põhjust olla seisukohal, et seoses elutähtsate IKT tarneahelatega ähvardab liidu julgeolekut märkimisväärne küberoht ning siseturu nõuetekohase toimimise säilitamiseks võib olla vaja võtta meetmeid, peaks komisjon viivitamata konsulteerima liikmesriikidega leevendusmeetmete võtmise vajaduse asjus ning viima läbi turvariski hindamise, võttes arvesse liikmesriikidega konsulteerimist.

(137) Kui võrgu- ja infoturbe koostöörühma või komisjoni läbiviidud turvariski hindamise tulemusena nähtub, et konkreetne kolmas riik põhjustab IKT tarneahelatele tõsiseid ja struktuurseid mittetehnilisi küberriske, siis peaks komisjon kontrollima selle riigi põhjustatud ohtu. Komisjon võib selle kontrolli algatada ka muude allikate alusel, nagu liidu või liikmesriigi nimel tehtud avaldus, millega reageeritakse küberruumis riigi vastutustundetule käitumisele, mis on põhjustanud küberintsidendi. Ohutaseme hindamiseks peaks komisjon võtma arvesse selliseid elemente nagu see, kas kolmandas riigis on õigusakte või tavasid, millega nõutakse nende jurisdiktsiooni kuuluvatelt üksustelt teabe esitamist tark- või riistvara nõrkuste kohta kõnealuse kolmanda riigi asutustele, enne kui on teada, et kõnealuseid nõrkusi on ära kasutatud.

Teine oluline element on tulemuslike õiguskaitsevahendite ning sõltumatute ja demokraatlike kontrollimehhanismide puudumine, mis aitavad turvalisuse probleeme lahendada, sh kehtivate tavade puhul, põhjendatud teave kõnealuse riigi territooriumil tegutsevate ning kuritahtlikku kübertegevust või -kampaaniaid ellu viivate ohusubjektidega seotud intsidentide kohta ning kolmanda riigi võime või valmiduse puudumine teha komisjoni või liikmesriikidega koostööd kõnealuste ohusubjektide tegevusest tuleneva riski maandamiseks. Komisjon peaks samuti võtma arvesse teavet, mis tuleneb liidu tasandi koordineeritud turvariski hindamistest või liikmesriikide või rahvusvaheliste organisatsioonide (nt NATO) esitatud aruannetest.

(138) Käesoleva määruse kohaldamisel tuleks käsitada kontrolli võimena avaldada otsustava tähtsusega mõju juriidilisele isikule kas otseselt või kaudselt ühe või enama vahendava juriidilise isiku kaudu. Küberturvalisuse seisukohast muret tekitavate kolmandate riikide üksuste kontroll tuleks kehtestada ka olukordades, kus kõnealusel üksusel tegutsevad selles riigis juhatuse struktuurid.

(139) Liit ei tohiks rahastada suure riskiga tarnijaid hõlmavaid projekte, mis ohustaksid liidu turvalisust ning õõnestaksid liidu huve ja usaldusväärsust. Käesoleva määruse alusel kindlaks määratud suure riskiga tarnijatel ei tohiks seega olla õigust osaleda üheski liidu rahastamisprogrammis ja -vahendis, mida rakendatakse eelarve otsese ja kaudse täitmise alusel kooskõlas määruse (EL/Euratom) 2024/2509 artikliga 136 ja liidu sektoripõhiste normidega, ega üheski eelarve jagatud täitmise alusel rakendatavas liidu rahastamistegevuses, sh järgmise mitmeaastase finantsraamistiku alusel seoses selliste IKT-komponentide või IKT-komponente sisaldavate komponentide pakkumisega, mida hakatakse kasutama kindlaksmääratud olulistes IKT-varades. Liidu rakenduspartnerid, nagu Euroopa Investeerimispanga Grupp ja riiklikud tugipangad ja -asutused ei tohiks toetada eespool märgituga vastuolus olevaid projekte, sh omal vastutusel toimuva tegevuse puhul.

(140) Riigihanked võivad olla tugev vahend, mille abil avaliku sektori asutused saavad panustada innovatiivsemasse, kestlikumasse ja konkurentsivõimelisemasse majandusse, ning mis aitab riigi raha strateegiliselt kasutada. IKT tarneahelatega seotud riigihankeid ei tohiks kasutada liidu elutähtsa taristu turvalisust ohustavate tarnijate huvides. Käesoleva määruse alusel kindlaks määratud suure riskiga tarnijatel ei tohiks seega olla õigust osaleda kindlaks määratud olulistes IKT-varades kasutatavate IKT-komponentide või IKT-komponente sisaldavate komponentide tarnimise riigihangetes.

(141) Küberturvalisuse sertifitseerimisel on roll üldise turvalisuse suurendamisel ja küberohtude tõkestamisel ning seega on see usalduse näitaja. Kõnealune usaldus võib väheneda, kui küberturbeoskuste tõendeid väljastavad suure riskiga tarnijad, kellel ei tohiks seega olla õigust kandideerida liidu individuaalsete küberturbeoskuste volitatud tõendajaks saamiseks. Samal moel on asjakohane välistada suure riskiga tarnijate puhul küberturvalisuse sertifikaadi saamine Euroopa küberturvalisuse sertifitseerimise raamistiku alusel ja kõnealuseid sertifikaate väljastavaks akrediteeritud vastavushindamisasutuseks saamine.

(142) Küberturvalisuse standarditel on ülioluline roll digitaristu turvalisuse ja usaldusväärsuse tagamisel. On vaja võtta sobilikke meetmeid, et tagada standardimine küberturvalisuse valdkonnas. Kui osalevad üksused, mis on asutatud riikides või mida kontrollivad riigid, mis on kooskõlas käesoleva määrusega tehtud kindlaks IKT tarneahelale küberturvalisuse seisukohast muret tekitavate riikidena, võib see

mõjutada küberturvalisuse standardeid nende turvalisust ja usaldusväärsust õõnestaval viisil.

(143) Komisjon võib määrata turvariski hindamise tulemuste põhjal rakendusaktidega kindlaks, milliseid IKT-varasid tuleks nende kriitilise tähtsuse tõttu käsitada oluliste IKT-varadena, mille suhtes kohaldatakse konkreetseid leevendusmeetmeid. Juba puhtalt vara ühendamisvõimaluse olemasolu peaks olema piisav alus küberriski hindamiseks.

(144) Kui see on liidus küberturvalisuse, küberkerksuse ja usalduse kõrge taseme tagamiseks vajalik, siis võidakse üksuste suhtes kohaldada leevendusmeetmeid nende IKT tarneahela puhul ja eelkõige kindlaks tehtud oluliste IKT-varade puhul. Väljapakutud leevendusmeetmed peaksid põhinema kõnealuste meetmete võimalike riskide ja sõltuvuste, sh kriitilise tähtsusega või muudes kriitilise tähtsusega sektorites tegutsevatele üksustele ning eelkõige VKEdele avalduva võimaliku majandusliku ja sotsiaalse mõju hindamisel. Majandusliku mõju puhul tuleks analüüsida leevendusmeetmete rakendamise kulusid, sh oluliste IKT-varade asjaomaste komponentide elutsükli kestust juhul, kui meetmed hõlmavad tarnijate asendamist. Samuti tuleks hinnata alternatiivsete tarnijate kättesaadavust turul, et tagada teenuste jätkuv osutamine.

(145) Kuna leevendusmeetmed võivad avaldada piiravat mõju rahvusvahelisele kaubandusele ja teenuskaubandusele, peaksid need olema proportsionaalsed ja sihipärased, et saavutada õiguspärane eesmärk, milleks on tagada IKT tarneahelate küberturvalisus direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste puhul kooskõlas liidu rahvusvaheliste kohustustega.

(146) Suure riskiga tarnijate pakutud komponentide kasutamine, paigaldamine või muud liiki integreerimine oluliste IKT-varade käitamisse võib olla seotud riskiga, et andmed edastatakse hiljem kolmandasse riiki. Eelkõige võib riske tekitada kolmandas riigis andmetele pakutava kaitse ebapiisav tase, näiteks põhiõiguste, intellektuaalomandi või ärisaladuste kaitse puhul, või ebaseaduslik juurdepääs andmetele ja nende ebaseaduslik kasutamine võimalikeks tulevasteks tarneahela häireteks ning spionaaži eesmärgil. Selliste riskide maandamiseks võib konkreetset liiki andmete kolmandatesse riikidesse edastamise suhtes kohaldada piiranguid.

(147) Märkimisväärsed nõrkused tulenevad direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste kasutatavate seadmete ebapiisavast mitmekesisusest. Kui tuginetakse ühele tarnijale, siis tekib sõltuvus konkreetsetest seadmetest või lahendustest. Kui ei ole piisavalt erinevaid tarnijaid, siis suureneb elutähtsa taristu üldine nõrkus, eriti kui üksused hangivad oma tundlikes IKT-varades kasutatavaid IKT-komponente suure riskiga tarnijalt. Sõltuvus mõjutab märkimisväärselt ka riikide ja kogu ELi kerksust ning tekitab nõrku lülisid. Selliste riskide maandamiseks võidakse kohaldada nõuet kasutada konkreetsete oluliste IKT-varade jaoks rohkem kui ühte tarnijat.

(148) Käesolevas määruses määratletud olulisi varasid võivad kasutada ka liidu üksused. Seega tuleks käesolevas määruses sätestatud norme, mis käsitlevad IKT tarneahela turvalisust, kohaldada ka nende suhtes. Selleks et võtta arvesse liidu üksuste iseärasusi, on oluline võtta liidu tasandi koordineeritud turvariski hindamisel arvesse liidu üksustele tekkivaid mittetehnilisi riske, mis tulenevad IKT tarneahelatest.

(149) Erandlike asjaolude korral, kui siseturu nõuetekohase toimimise säilitamiseks on põhjendatud viivitamatu sekkumine ning kui on selgeid tõendeid, mis annavad komisjonile piisava põhjuse olla seisukohal, et konkreetselt tarnijalt pärit IKT-

komponentide või IKT-komponente sisaldavate komponentide kasutamine põhjustab märkimisväärse küberohu vähemalt kolme liikmesriigi majanduslikule või ühiskondlikule tegevusele, võib komisjon teha tihedalt liikmesriikidega konsulteerides ettepaneku keelata direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksustel kasutada, paigaldada või kaasata selliseid komponente, mis pärinevad kõnealuselt tarnijalt.

(150) Kohaldatavate meetmete proportsionaalsuse tagamiseks võivad üksused, mis on asutatud käesoleva määruse kohaselt küberturvalisuse seisukohast muret tekitavaks nimetatud kolmandas riigis või mida kontrollib kõnealune kolmas riik, sellises kolmandas riigis asutatud üksus või sellise kolmanda riigi kodanik, esitada taotluse, et neile tehtaks erand keelust pakkuda direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksustele IKT-komponente või IKT-komponente sisaldavaid komponente, et kõnealune üksus saaks neid oma olulistes IKT-varades kasutada, neid sinna paigaldada või integreerida, ning et neil oleks õigus osaleda riigihankemenetlustes, mis on korraldatud kooskõlas Euroopa Parlamendi ja nõukogu direktiivide 2014/24/EL[67] ja 2014/25/EL[68] ülevõtmise õigusaktidega ning mis käsitlevad IKT-komponentide või IKT-komponente sisaldavate komponentide pakkumist kindlaks määratud olulistes IKT-varades kasutamise otstarbel. Selleks peaks üksus selgete tõendite alusel näitama, et ta kohaldab tulemuslikke meetmeid mittetehniliste riskide maandamiseks ning tagab, et küberturvalisuse seisukohast muret tekitav kolmas riik ei avalda talle mingit sobimatut mõju.

(151) Elektroonilise side võrgud on aluseks väga mitmesugustele teenustele, mis on olulised siseturu toimimiseks ning ühiskonna ja majanduse eluliselt tähtsate funktsioonide (nt energeetika, transport, pangandus, tervishoid, kaitsevaldkond ja tööstuslikud juhtimissüsteemid) haldamiseks ja toimimiseks. Seetõttu on need väga kriitilise tähtsusega võrgud atraktiivsed sihtmärgid igasuguste küberrünnete ja hübriidohtude, häirete, spionaaži, luureandmete kogumise ning samuti pettuste ja finantskuritegude jaoks. Võrgu- ja infoturbe koostöörühma läbiviidud Euroopa sidetaristu ja -võrkude küberturvalisuse ja -kerksuse riskihindamise tulemusena tehti kindlaks mitu liidu seisukohast strateegilise olulisusega riski ja ohtu, näiteks pühkur/lunavara, ründed, tarneahela ründed, võrkutungid ja hajusad teenusetõkestusründed.

(152) Võttes arvesse eri riikide elektroonilise side võrkude omavahelist ühendatust ja sõltuvust, on vaja, et kõik liikmesriigid võtaksid sobilikke meetmeid oma võrkude turvalisuse tagamiseks. Samadel põhjustel on vaja võtta liidu tasandil kasutusele tulemuslik õigusraamistik, mis aitab käsitleda ka mittetehnilisi riske ning tagada omavahel ühendatud elektroonilise side võrkude tervikliku turvalisuse.

(153) Eeskätt 5G võrkude küberturvalisus on liidu jaoks strateegilise olulisusega, kuna need võrgud on mitmesuguste siseturu toimimise jaoks määrava tähtsusega teenuste alus ning samuti määrava tähtsusega kaitsevalmiduse tagamiseks, sh sõjalise liikuvuse puhul. 5G-võrkude kaudu saab pakkuda usaldusväärset ja ülikiiret ühenduvust näiteks

---

67 Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/24/EL riigihangete kohta ja direktiivi 2004/18/EÜ kehtetuks tunnistamise kohta (ELT L 94, 28.3.2014, lk 65–242, ELI: https://eur-lex.europa.eu/eli/dir/2014/24/oj/est).

68 Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/25/EL, milles käsitletakse vee-, energeetika-, transpordi- ja postiteenuste sektoris tegutsevate üksuste riigihankeid ja millega tunnistatakse kehtetuks direktiiv 2004/17/EÜ (ELT L 94, 28.3.2014, lk 243–374, ELI: https://eur-lex.europa.eu/eli/dir/2014/25/oj).

andmete ja teabe jagamiseks, mehitamata õhusõidukite avastamiseks ning lahinguvälja koordineerimiseks reaalajas.

(154) 5G kasutuselevõtt hõlmab peamiselt mitteeraldiseisvaid võrke, mille puhul täiustatakse 5G-tehnoloogiaga ainult raadio juurdepääsuvõrku, kuid ülejäänud võrk tugineb jätkuvalt olemasolevale 4G-tuumikvõrgule. Mitteeraldiseisvad 5G-võrgud tuginevad peamiselt juba kasutusel olevale taristule, mis tähendab, et tulevaste 5G-võrkude turvalisuse määravad teatavas ulatuses kindlaks juba kasutusel olevad võrguseadmed ja selliste seadmete seadistus. Seetõttu peaksid leevendusmeetmed hõlmama ka 4G-võrke, millele 5G kasutuselevõtt tugineb.

(155) 5G-võrkude oluliste turvaprobleemide lahendamiseks viisid liikmesriigid võrgu- ja infoturbe koostöörühma raames koos komisjoni ja ENISAga läbi 5G-võrkude liidu tasandi koordineeritud turvariski hindamise, analüüsides nii tehnilisi kui ka mittetehnilisi riske. Selle hindamise käigus tehti kindlaks mitu riski, sh kolmandate riikide või kolmandate riikide osalejate potentsiaalsed sekkumised tarneahela kaudu, ning liigitati varad lähtuvalt nende olulisusest. Sellest hindamisest tuleks lähtuda 5G sidevõrkude jaoks oluliste IKT-varade kindlaksmääramisel.

(156) 5G-võrkude liidu tasandi koordineeritud turvariski hindamise käigus kindlaks tehtud riskide maandamiseks võttis võrgu- ja infoturbe koostöörühm kasutusele 5G küberturvalisuse ELi meetmepaketi, milles on kindlaks määratud strateegilised ja tehnilised meetmed. Kuigi enamikul liikmesriikidest on õigusraamistikud, mis võimaldavad suure riskiga tarnijate piiranguid või välistamist, nagu on soovitatud 5G meetmepaketis, ei ole neid raamistikke ühtselt rakendatud. Seetõttu varustavad märkimisväärset osa 5G objektidest liidus suure riskiga tarnijad, nagu on osutatud komisjoni teatises 5G meetmepaketi rakendamise kohta[69]. See olukord tekitab nõrkusi, sh strateegilist sõltuvust ja võimalikku avatust kolmandate riikide sekkumisele, mis võib samuti mõjutada olemasolevatele 5G-võrkudele rajatavat tulevast 6G-taristut. 5G meetmepaketi soovitatud meetmete killustatud rakendamine, eelkõige suure riskiga tarnijate piirangute kohaldamisala puhul, on põhjustanud liikmesriikidevahelisi erinevusi, millest tulenevad ebavõrdsed tingimused, mis jaotavad siseturu osadeks ja õõnestavad võrkude üldist turvalisust. Euroopa Kontrollikoda on toonud esile kõnealused erinevused ja hoiatanud et kooskõlastatud lähenemisviisi puudumine õõnestab siseturu toimimist. Püsiv sõltuvus suure riskiga tarnijatest tekitab märkimisväärseid riske liidu elutähtsa taristu turvalisusele ning võib õõnestada usaldust siseturul, kuna erinevad turvalisuse tasemed võivad ajendada tarbijaid ja ettevõtteid hoiduma 5G-l põhinevatele toodetele ja teenustele tuginemisest kogu liidus. Seetõttu on hädavajalik kehtestada liidu tasandi meetmed, et tagada ühtlustatud lähenemisviis 5G-võrkude turvalisusele.

(157) Elektroonilise side püsi- ja satelliitvõrkude oluliste IKT-varade järkjärgulise kasutuselt kõrvaldamise ajavahemiku kehtestamiseks peaks komisjon viima läbi hindamise, võttes nõuetekohaselt arvesse püsi- ja satelliitvõrkude iga konkreetse olulise IKT-varaga seotud turvariskide ulatust, asjakohaste komponentide kasutusaega ja majanduslikku mõju, mida kõnealuste komponentide kõrvaldamine asjaomastele ettevõtjatele avaldaks. Kõnealuse hindamise tulemuste põhjal võib komisjon kaaluda erinevate järkjärgulise kasutuselt kõrvaldamise ajavahemike kehtestamist konkreetsetele olulistele IKT-varadele ja nende lahutamatutele osadele.

---

[69] Komisjoni teatis 5G küberturvalisuse meetmepaketi rakendamise kohta, 15. juuni 2023, C(2023) 4049 final.

(158) Elektroonilise side mobiili-, püsi- ja satelliitvõrkude pakkujaid puudutavate kohustuste tulemusliku järelevalve ja täitmise tagamise otstarbel peaksid asjaomased käesoleva määruse kohaselt pädevad asutused tagama tiheda koostöö [digivõrkude õigusakti ettepaneku] kohaselt pädevate asutustega. Käesoleva määruse kohaselt määratud pädeva asutuse taotluse korral peaksid riigi reguleerivad asutused või muud raadiospektri pädevad asutused tunnistama vajaduse korral kehtetuks [digivõrkude õigusakti ettepaneku] artiklis 9 ja artiklis 20 osutatud õigused, kui üldkasutatavate elektroonilise side võrkude pakkuja ei täida käesolevast määrusest tulenevaid kohustusi, sh kui pakkuja ei kõrvalda järk-järgult kasutuselt suure riskiga tarnijatelt pärinevaid IKT-komponente või IKT-komponente sisaldavaid komponente, mida kasutatakse oluliste IKT-varade käitamiseks, käesolevas määruses kindlaks määratud ajavahemiku jooksul.

(159) Võttes arvesse riiklike juhtimisstruktuuride erinevusi, peaksid liikmesriigid määrama või asutama pädeva(d) asutuse(d), mis vastutab või vastutavad käesoleva määruse kohaste järelevalve- ja täitemeetmete eest.

(160) Pädevad asutused peaksid toetama direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksusi käesolevast määrusest tulenevate kohustuste täitmisel. Sel otstarbel peaks komisjon hindama, kas tarnijad, keda konkreetsed keelud võivad mõjutada, on asutatud küberturvalisuse seisukohast muret tekitavas kolmandas riigis või on kõnealuse kolmanda riigi või kõnealuses kolmandas riigis asutatud üksuse või selle kodaniku kontrolli all. Pädevad asutused peaksid tegema tihedat koostööd komisjoni ja muude pädevate asutustega käesoleva määruse alusel loodud võrgustikus. Pädevad asutused peaksid komisjoni hindamise põhjal jagama suure riskiga tarnijaid käsitlevat asjakohast teavet direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki asjaomaste üksustega. Üksustelt ei eeldata selle kontrollimist, kas tarnija on välisriigi kontrolli all, vaid nad võivad täielikult tugineda pädevatelt asutustelt saadud teabele. Pädevad asutused peaksid tagama, et kõnealustele üksustele ei tekitata põhjendamatut halduskoormust.

(161) Tulemusliku nõuete täitmise tagamiseks tuleks käesolevas määruses ette näha järelevalve- ja täitemeetmed, mille abil pädevad asutused saavad teha direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste järelevalvet. Kui pädevad asutused täidavad kõnealuste üksuste puhul oma järelevalve- ja nõuete täitmise tagamise kohustusi, siis ei tohiks nad minna kaugemale sellest, mis on kindlaks tehtud riskide jaoks vajalik ja proportsionaalne.

(162) Selleks et muuta nõuete täitmise tagamine liidus tulemuslikuks ja järjepidevaks, on vaja ette näha nõuete täitmise tagamise volitused, mida pädevad asutused saavad kasutada käesolevas määruses sätestatud kohustuste rikkumise korral. Kõnealuste nõuete täitmise tagamise volituste rakendamisel peaksid pädevad asutused võtma nõuetekohaselt arvesse mitmesuguseid tegureid, sh rikkumise laadi, tõsidust ja kestust, põhjustatud varalist või mittevaralist kahju, seda, kas rikkumine oli tahtlik või tingitud hooletusest, varalise või mittevaralise kahju vältimiseks või leevendamiseks võetud meetmeid, vastutuse taset ja varasemaid asjaomaseid rikkumisi, pädeva asutusega tehtud koostöö ulatust ning muid raskendavaid või leevendavaid tegureid. Sellised täitemeetmed, sh karistused, peaksid olema proportsionaalsed ja nende määramise suhtes tuleks kooskõlas liidu õiguse üldpõhimõtete ja Euroopa Liidu põhiõiguste hartaga kohaldada asjakohaseid menetluslikke kaitsemeetmeid, sh õigust tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, süütuse presumptsiooni ja kaitseõigust.

(163) Samuti on oluline näha ette õigus määrata sunniraha, mille eesmärk on sundida direktiivi (EL) 2022/2555 I või II lisas osutatud liiki üksust käesoleva määruse rikkumist lõpetama, kooskõlas pädeva asutuse eelneva otsusega.

(164) Selleks et tagada käesolevas määruses sätestatud kohustuste tulemuslik täitmine, peaks igal pädeval asutusel olema õigus karistusi määrata või nende määramist taotleda.

(165) Kui karistusi määratakse direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksusele, mis on ettevõtja, siis käsitatakse ettevõtjana ettevõtjat kooskõlas Euroopa Liidu toimimise lepingu artiklitega 101 ja 102. Kui trahv määratakse isikule, kes ei ole ettevõtja, peaks pädev asutus karistuse sobiva suuruse määramisel arvesse võtma üldist sissetulekutaset selles liikmesriigis ja isiku majanduslikku olukorda. See, kas ja kui palju tuleks avaliku sektori asutustele karistusi määrata, peaks olema liikmesriikide otsustada. Karistuse määramine ei tohiks mõjutada pädevate asutuste muude volituste kohaldamist.

(166) Selleks et tagada ühtsed tingimused käesoleva määruse rakendamiseks, tuleks anda komisjonile rakendamisvolitused, et võtta vastu rakendusaktid, millega kehtestatakse üksikasjalikud normid ENISA nõutavate tasude kohta, rakendusaktid, millega nähakse IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku jaoks ette Euroopa küberturvalisuse sertifitseerimise kava, rakendusaktid, millega kehtestatakse ühised põhimõtted ja viitamissätted, mille eesmärk on näha ette Euroopa küberturvalisuse sertifitseerimise kavade elemendid, rakendusaktid, millega täpsustatakse eelneva heakskiidu või üldise delegeerimise mudelite menetlused, rakendusaktid, mis käsitlevad kolmanda riigi või rahvusvahelise organisatsiooni küberturvalisuse sertifikaatide tunnustamist Euroopa küberturvalisuse sertifikaatidega võrdväärsena, rakendusaktid, millega kehtestatakse vastastikuste eksperdihinnangute kava, rakendusaktid, millega kehtestatakse menetlused, sh piiriülese koostöö menetlused vastavushindamisasutustele lubade väljastamiseks, rakendusaktid, millega määratakse kindlaks vastavushindamisasutustest teatamise asjaolud, vormingud ja menetlused, rakendusaktid, millega nimetatakse kolmas riik IKT tarneahelate küberturvalisuse seisukohast muret tekitaks riigiks, rakendusaktid, millega määratakse kindlaks direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste poolt toodete valmistamiseks või teenuste osutamiseks kasutatavad olulised IKT-varad, rakendusaktid, millega määratakse kindlaks, et kriitilise tähtsusega sektorites ja muudes kriitilise tähtsusega sektorites tegutsevate üksuste suhtes kohaldatakse konkreetseid leevendusmeetmeid, ning millega määratakse kindlaks suure riskiga tarnijate tarnitavate IKT-komponentide või IKT-komponente sisaldavate komponentide järkjärgulise kasutuselt kõrvaldamise ajavahemikud, rakendusaktid, millega täpsustatakse küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud üksustele või sellisest riigist pärit üksuste kontrolli all olevate üksustele erandi tegemise tingimused, ning samuti rakendusaktid, millega kehtestatakse üksikasjalikud normid komisjoni nõutavate tasude kohta. Neid volitusi tuleks rakendada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011 ning kasutada tuleks kontrollimenetlust. Käesoleva määruse rakendamisel ühtsete tingimuste tagamiseks tuleks komisjonile samuti anda rakendusvolitused, et koostada suure riskiga tarnijate loetelu, mis on asjakohane teatavate käesolevas määruses sätestatud meetmete puhul.

(167) Euroopa küberturvalisuse sertifitseerimise kavad peavad kajastama tehnoloogia uusimaid arengusuundi, uusi asjakohaseid ohte ja uute liidu õigusaktide vastuvõtmist, millega kehtestatakse Euroopa küberturvalisuse sertifitseerimise kaudu vastavuse

tõendamine ja nõuetele vastavuse eeldus kõnealuste õigusaktide asjakohaste küberturvalisuse nõuete puhul. Neil põhjustel tuleks komisjonile delegeerida õigus võtta kooskõlas ELi toimimise lepingu artikliga 290vastu õigusakte, et lisada või muuta Euroopa küberturvalisuse sertifitseerimise kavade turvaeesmärke. Samal moel tuleks usaldusväärse IKT tarneahela raamistiku huvides delegeerida komisjonile õigus võtta kooskõlas ELi toimimise lepingu artikliga 290 vastu õigusakte, et muuta käesoleva määruse II lisa selle kohandamiseks tehnoloogia arenguga. On eriti oluline, et komisjon viiks oma ettevalmistava töö käigus läbi asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil, ja et kõnealused konsultatsioonid viidaks läbi kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetega. Eelkõige selleks, et tagada delegeeritud õigusaktide ettevalmistamises võrdne osalemine, peaksid Euroopa Parlament ja nõukogu saama kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel peaks olema pidev juurdepääs komisjoni eksperdirühmade koosolekutele, millel arutatakse delegeeritud õigusaktide ettevalmistamist.

(168) ENISA tööd tuleks hinnata korrapäraselt ja sõltumatult. Hindamisel tuleks pidada silmas ENISA eesmärke ja ülesannete asjakohasust, eelkõige seoses liidu tasandil operatiivkoostööga seotud ülesannetega. Läbivaatamise korral peaks komisjon hindama seda, kuidas on võimalik tugevdada ENISA rolli nõu ja eksperditeadmisi pakkuva kontaktüksusena.

(169) Komisjoni rakendusmääruses (EL) 2024/482 on sätestatud normid Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava vastuvõtmiseks. Euroopa ühiskriteeriumidel põhinev küberturvalisuse sertifitseerimise kava on esimene ja ainus määruse (EL) 2019/881 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava. See käsitleb IKT-toodete sertifitseerimist, sh tehnilistesse valdkondadesse „Kiipkaardid ja samalaadsed seadmed“ ning „Turvaümbrisega riistvaraseadmed“ kuuluvate toodete ning kaitseprofiilide (kui IKT-protsesside) puhul. Seetõttu on vaja tagada sertifitseerimistegevuse ja ameti tegevuse jätkumine.

(170) Vastavalt määruse (EL) 2018/1725[70] artikli 42 lõikele 2 on konsulteeritud Euroopa Andmekaitseinspektori ja Euroopa Andmekaitsenõukoguga, kes esitasid oma ühisarvamuse [kuupäev].

(171) Määrus (EL) 2019/881 tuleks kehtetuks tunnistada.

(172) Kuna käesoleva määruse eesmärke ei suuda liikmesriigid piisavalt saavutada, küll aga saab neid meetme ulatuse ja toime tõttu paremini saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu (edaspidi „ELi leping“) artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärkide saavutamiseks vajalikust kaugemale,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I JAOTIS
ÜLDSÄTTED

[70] Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artikkel 1
Reguleerimisese ja kohaldamisala

1. Käesolevas määruses sätestatakse järgmine:

   a) Euroopa Liidu Küberturvalisuse Ameti (edaspidi „ENISA“) missioon, eesmärgid, ülesanded ja organisatsioonilised aspektid,

   b) Euroopa küberturvalisuse sertifitseerimise kavade kehtestamise raamistik, et kindlustada liidus IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku piisav küberturvalisuse tase ning vältida siseturu killustatust seoses küberturvalisuse sertifitseerimise kavadega liidus, ning

   c) usaldusväärse IKT tarneahela raamistik.

2. Lõike 1 punktis b osutatud raamistiku kohaldamine ei piira muude liidu õigusaktide erinormide kohaldamist, mis käsitlevad vabatahtlikku või kohustuslikku sertifitseerimist.

3. Lõike 1 punktis c osutatud raamistikku kohaldatakse direktiivi (EL) 2022/2555 I või II lisas osutatud liiki avaliku või erasektori üksuste suhtes, mis osutavad oma teenuseid või viivad ellu oma tegevust liidus.

4. Käesolev määrus ei piira liikmesriikide põhifunktsioone riigina, sealhulgas riigi territoriaalse terviklikkuse tagamist, avaliku korra säilitamist ja riigi julgeoleku kaitsmist. Eelkõige jääb riigi julgeolek iga liikmesriigi ainuvastutusse.

Artikkel 2
Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „küberturvalisus“ – tegevused, mis on vajalikud selleks, et kaitsta võrgu- ja infosüsteeme, selliste süsteemide kasutajaid ja muid küberohtudest mõjutatud isikuid;

2) „liidu üksused“ – direktiivi (EL) 2023/2841 artikli 3 punktis 1 määratletud üksused;

3) „volitatud tõendaja“ – avaliku või erasektori üksus, mille kohta ENISA on teinud otsuse, millega on kõnealune üksus volitatud andma Euroopa individuaalsete küberturbeoskuste tõendeid, nagu on sätestatud Euroopa individuaalsete küberturbeoskuste tõendamise kavas;

4) „Euroopa individuaalsete küberturbeoskuste tõend“ – digitaalne või füüsiline kirje, mis tõendab, et üksikisik teab, mõistab ja on suuteline täitma ülesandeid, mis on seotud Euroopa küberturbeoskuste raamistiku ametikirjelduse või ametikirjelduste alamkogumiga, pärast Euroopa individuaalsete küberturbeoskuste tõendamise kavas sätestatud hindamist;

5) „Euroopa individuaalsete küberturbeoskuste tõendamise kava“ – terviklik normide, nõuete, standardite ja menetluste komplekt, mille on kehtestanud ENISA ja mis on seotud Euroopa küberturbeoskuste raamistiku ametikirjelduse või selle alamkogumiga ja mida kohaldatakse volitatud tõendajate suhtes ja mida kohaldavad volitatud tõendajad;

6) „võrgu- ja infosüsteem“ – direktiivi (EL) 2022/2555 artikli 6 punktis 1 määratletud võrgu- ja infosüsteem;

7) „riiklik küberturvalisuse strateegia“ – direktiivi (EL) 2022/2555 artikli 6 punktis 4 määratletud riiklik küberturvalisuse strateegia;

8) „intsident“ – direktiivi (EL) 2022/2555 artikli 6 punktis 6 määratletud intsident;

9) „ulatuslik küberintsident“ – direktiivi (EL) 2022/2555 artikli 6 punktis 7 määratletud ulatuslik küberintsident;

10) „intsidendi käsitlemine“ – direktiivi (EL) 2022/2555 artikli 8 punktis 6 määratletud intsidendi käsitlemine;

11) „küberoht“ – võimalik asjaolu, sündmus või tegevus, mis võib kahjustada või häirida võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid või neile muul viisil halba mõju avaldada;

12) „Euroopa küberturvalisuse sertifitseerimise kava“ – liidu tasandil kindlaks määratud reeglite, tehniliste nõuete, standardite ja menetluste põhjalik kogum, mida kasutatakse konkreetsete IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku sertifitseerimiseks või nende vastavuse hindamiseks;

13) „riiklik küberturvalisuse sertifitseerimise kava“ – riigi ametiasutuse välja töötatud ja kehtestatud reeglite, tehniliste nõuete, standardite ja menetluste põhjalik kogum, mida kasutatakse konkreetse kava kohaldamisalasse kuuluvate IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku sertifitseerimiseks või nende vastavuse hindamiseks;

14) „Euroopa küberturvalisuse sertifikaat“ – asjakohase asutuse välja antud dokument, mis kinnitab, et hinnatud on asjaomase IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuse turvaoleku vastavust Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud turvalisuse erinõuetele;

15) „ELi vastavusdeklaratsioon“ – dokument, mille on väljastanud IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse tootja või pakkuja või üksus, kelle turvaolekut sertifitseeritakse, ja milles on märgitud, et vastavuse enesehindamise teel on tõendatud nõuete täitmist, mis vastavad usaldusväärsuse baastasemele, mis on sätestatud Euroopa küberturvalisuse sertifitseerimise kavas;

16) „IKT-toode“ – võrgu- või infosüsteemi element või elementide rühm;

17) „IKT-teenus“ – teenus, mis koosneb täielikult või peamiselt võrgu- ja infosüsteemide kaudu teabe edastamisest, säilitamisest, väljavõtmisest või töötlemisest;

18) „IKT-protsess“ – tegevused, mille käigus projekteeritakse või töötatakse välja IKT-toode või -teenus, seda tarnitakse või hooldatakse;

19) „hallatud turbeteenus“ – kolmandale isikule osutatav teenus, mis seisneb küberriskide juhtimisega seotud tegevuse, näiteks intsidentide käsitlemise, läbistustestimise, turvaauditite ja tehnilise toega seotud konsultatsioonide, sh eksperdinõu pakkumise korraldamises või nende korraldamiseks toe pakkumises;

20) „akrediteerimine“ – määruse (EÜ) nr 765/2008 artikli 2 punktis 10 määratletud akrediteerimine;

21) „riiklik akrediteerimisasutus“ – määruse (EÜ) nr 765/2008 artikli 2 punktis 11 määratletud riiklik akrediteerimisasutus;

22) „vastavushindamine“ – määruse (EÜ) nr 765/2008 artikli 2 punktis 12 määratletud vastavushindamine;

23) „vastavushindamisasutus“ – määruse (EÜ) nr 765/2008 artikli 2 punktis 13 määratletud vastavushindamisasutus;

24) „standard“ – Euroopa Parlamendi ja nõukogu määruse (EL) nr 1025/2012[71] artikli 2 punktis 1 määratletud standard;

25) „tehniline kirjeldus“ – määruse (EL) nr 1025/2012 artikli 2 punktis 4 määratletud tehniline kirjeldus;

26) „harmoneeritud standard“ – määruse (EL) nr 1025/2012 artikli 2 punkti 1 alapunktis c määratletud harmoneeritud standard;

27) „usaldusväärsuse tase“ – alus kindlustundele, et IKT-toode, -teenus, -protsess, hallatud turbeteenus või üksuse turvaolek vastab konkreetse Euroopa küberturvalisuse sertifitseerimise kava turvanõuetele, näidates ühtlasi, millisel tasemel on seda hinnatud, aga usaldusväärsuse tase ei mõõda IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuse turvaoleku enda turvalisust;

28) „vastavuse enesehindamine“ – IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuse tootja või pakkuja või sertifitseeritava turvaolekuga üksuse läbiviidav tegevus, mille käigus hinnatakse nende IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku vastavust teatavatele Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud nõuetele;

29) „üksuste turvaolek“ – üksuste küberturvalisuse tase turvalisuse erinõuete puhul;

30) „eelneva heakskiidu mudel“ – mudel, mille alusel võib vastavushindamisasutus väljastada Euroopa küberturvalisuse sertifikaadi lähtuvalt riikliku küberturvalisuse sertifitseerimise asutuse hindamisest, mis on läbi viidud asjaomase kava konkreetse sertifitseerimisprotsessi kontekstis;

31) „üldise delegeerimise mudel“ – mudel, mille alusel võib vastavushindamisasutus väljastada Euroopa küberturvalisuse sertifikaadi, mis põhineb riikliku küberturvalisuse sertifitseerimise asutuse delegeeritud sertifitseerimistegevusel;

32) „küberintsidentidele reageerimise üksus“ ehk „CSIRT“ – küberintsidentidele reageerimise üksus (edaspidi „CSIRT“), mis on määratud või asutatud vastavalt direktiivi (EL) 2022/2555 artiklile 10;

33) „IKT-komponendid“ – IKT-tooted, -teenused või -protsessid, mida võidakse kasutada IKT-varade käitamiseks;

34) „IKT-varad“ – võrgu- ja infosüsteemide tark- ja riistvara, mida kasutab direktiivi (EL) 2022/2555 I või II lisas osutatud üksus;

35) „olulised IKT-varad“ – artiklis 102 määratletud IKT-varad;

36) „elektroonilise side võrk“ – määruse (EL) XX/XXXX [digivõrkude õigusakti ettepanek] artikli 2 punktis 1 määratletud elektroonilise side võrk;

---

[71] Euroopa Parlamendi ja nõukogu 25. oktoobri 2012. aasta määrus (EL) nr 1025/2012, mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ (ELT L 316, 14.11.2012, lk 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

37) „kontroll“ – võime otsustavalt mõjutada õigussubjekti kas otse või kaudselt ühe või mitme vahepealse õigussubjekti kaudu;

38) „tegutsemine“ – tegevuse tegelik elluviimine püsivate korralduste alusel riigis, kus asub üksuse keskne haldusasutus või peamine tegevuskoht;

39) „suure riskiga tarnija“ – üks järgmistest:

a) üksus, mis tegutseb kolmandas riigis, mis on nimetatud küberturvalisuse seisukohast muret tekitavaks riigiks vastavalt artiklile 100, või on kõnealuse kolmanda riigi või kõnealuses kolmandas riigis asutatud üksuse või kõnealuse kolmanda riigi kodaniku kontrolli all;

b) kooskõlas artikli 103 lõikega 7 määratud üksus ja kõnealuse üksuse kontrolli all olevad üksused;

40) „IKT tarneahel“ – IKT-teenuste, -toodete ja -protsesside kogum, mis hõlmab kõigi turul kättesaadavaks tehtava toote või osutatava teenuse eelneva etapi tegevusi ja osalejaid;

41) „kolmas riik“ – Euroopa Parlamendi ja nõukogu määruse (EL) 2023/2675[72] artikli 3 punktis 4 määratletud kolmas riik;

42) „mittetehniline risk“ – tõenäosus, et tarnija on kolmanda riigi mõju all, mis võib põhjustada osutatava teenuse kaotamise või häirimise või kahjustada üksuse valmistatud toodet või põhjustada andmete väljatoimetamise, sh spionaaži või tulu saamise eesmärgil;

43) „oluline mittetehniline küberrisk“ – mittetehniline küberrisk, mille puhul võib eeldada suurt tõenäosust sellise intsidendi tekkeks, mis võib põhjustada tõsist negatiivset mõju, muu hulgas olulist varalist või mittevaralist kahju või häiret;

44) „elektroonilise side mobiilivõrkude tuumikvõrgu funktsioonid“ – elektroonilise side mobiilivõrkude arhitektuuri keskne element, mis ühendab peamisi võrgusõlmi internetiga ja haldab olulisi süsteemifunktsioone, mis hõlmab kasutaja seadmete autentimist, seadusliku infopüügi funktsioone, turvalüüse (SeGW) võrgu serval, signaalimise turvafunktsioone, rändluse ja seansihaldust, kasutaja ja juhttasandi andmeedastust, juurdepääsupoliitika haldamist, võrguteenuste registreerimist ja lubade väljastamist, lõppkasutaja ja võrguandmete salvestamist, kriitilise tähtsusega võrguteenuseid, sh domeeninimede süsteemi (DNS), omavahelist ühendamist kolmandate isikute mobiilivõrkudega, tuumikvõrgu funktsioonide avatus välisrakendustele ning tükeldatud võrguosade valimist ja haldamist;

45) „elektroonilise side mobiilivõrkude võrgufunktsioonide virtualiseerimine (NFV) ning haldamine ja võrgu orkestreerimine (MANO)“ – tarkvara- ja arhitektuuriraamistik, millega tagatakse virtualiseeritud võrgufunktsioonide (VNF) ja pilvepõhiste võrgufunktsioonide (CNF) elutsükli haldamine, orkestreerimine ja automatiseerimine ning tükeldatud võrguosade valimine ja haldamine elektroonilise side mobiilivõrkudes;

46) „elektroonilise side mobiilivõrkude raadio juurdepääsuvõrk (RAN)“ – võrk, mis ühendab mobiilikasutaja seadmeid tuumikvõrguga, sh tugijaamad (eNodeB 4G

[72] Euroopa Parlamendi ja nõukogu 22. novembri 2023. aasta määrus (EL) 2023/2675, mis käsitleb liidu ja selle liikmesriikide kaitset kolmandatest riikidest tuleneva majandusliku survestamise eest (ELT L, 2023/2675, 7.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2675/oj).

puhul, gNodeB 5G puhul), kaugtransiiverid (RRH) ja põhiribaseadmed (BBU), aktiivsed antennisüsteemid (AAS) ning, kui see on kohaldatav, eraldiseisvad raadio juurdepääsuvõrgu komponendid, nagu kesküksused (CU) ja hajusüksused (DU) ning raadio juurdepääsuvõrgu arukas kontroller (RIC);

47) „elektroonilise side püsivõrkude tuumikvõrgu funktsioonid“ – võrgu tuumandmed, mis ühendavad peamisi sõlmi ja täidavad mitmesuguseid olulisi funktsioone, sh kasutajate autentimine ja volitamine (AAA), seadusliku infopüügi (LI) funktsioonid, domeeninimede süsteem (DNS) ning IP-aadresside määramise teenused (DHCP), juurdepääsupoliitika haldamine, lõppkasutaja ja võrguandmete salvestamine, IP kommutatsioon ja IP marsruutimine ning rahvusvahelised netilüüsid (IIG);

48) „elektroonilise side püsivõrkude haldamise süsteem“ – kõik keskplatvormid ja tarkvarakomponendid, mis on vajalikud võrgu käitamiseks, haldamiseks, hooldamiseks ja tagamiseks (OAM&P) ning võrguga seotud teabe seireks;

49) „elektroonilise side püsivõrkude edastus- ja ülekandefunktsioonid“ – kõik komponendid, mis on vajalikud võrguliikluse tagasiühenduse ja agregeerimise jaoks, sh optilised edastusseadmed, mikrolaineühendused, ning merekaablisüsteemid, mis hõlmavad veealuseid seadmeid ning veelause liini lõppseadmeid (SLTE) ja füüsilise maabumispunkti rajatisi;

50) „elektroonilise side püsivõrgu juurdepääsuvõrk“ – võrk, mis ühendab lõppkasutaja ruume agregeerimis- või tuumikvõrguga, sh kiudoptiliste võrkude optilise liini terminal (OLT) ja optilise võrgu terminal (ONT); koaksiaalkaabelmodemi terminalisüsteem (CMTS) ja kaabelmodemid koaksiaalkaabelvõrkude jaoks ning traadita püsijuurdepääsu komponendid, kui neid kasutatakse püsivõrgu liini asendajana.

II JAOTIS
EUROOPA LIIDU KÜBERTURVALISUSE AMET

I peatükk
Missioon ja eesmärgid

Artikkel 3
ENISA missioon

1. ENISA missioon on toetada liikmesriike ja liidu üksusi liidus küberturvalisuse, küberkerksuse ja usalduse kõrge taseme saavutamisel.

2. ENISA tegutseb küberturvalisuse vallas liikmesriikidele ja liidu muudele sidusrühmadele nõu ja eksperditeadmisi pakkuva kontaktüksusena.

3. ENISA aitab käesoleva määrusega talle pandud ülesannete täitmisega kaasa siseturu killustatuse vähendamisele.

4. ENISA täidab talle liidu õigusaktidega määratud ülesandeid.

5. ENISA arendab oma võimekusi, sh tehnilist ja inimvõimekust ning oskusi, mis on vajalikud käesoleva määrusega talle pandud ülesannete täitmiseks.

Artikkel 4
ENISA eesmärgid

1. ENISA on küberturvalisuse alaste eksperditeadmiste keskus tänu oma sõltumatusele, antava nõu, panuse ja abi ning levitatava teabe teaduslikule ja tehnilisele kvaliteedile, töökorra läbipaistvusele, töömeetoditele ja oma ülesannete hoolikale täitmisele.

2. ENISA aitab liikmesriike ja vajaduse korral liidu üksusi küberturvalisusega seotud horisontaalsete ja valdkondlike liidu poliitikameetmete ja õigusaktide rakendamisel, sh turujärelevalve tegevuse puhul.

3. ENISA pakub oma eksperditeadmisi ja aitab komisjonil välja töötada liidu küberturvalisusega seotud poliitikat ja õigusakte.

4. ENISA toetab suutlikkuse suurendamist ja valmisolekut liidus, aidates liikmesriikidel ja liidu üksustel määruse (EL, Euratom) 2023/2841 IV peatükis osutatud liidu institutsioonide, organite ja asutuste küberturvalisuse teenistuse (edaspidi „CERT-EU“) kaudu ning avaliku ja erasektori sidusrühmadel suurendada nende võrgu- ja infosüsteemide kaitset ning arendada ja täiustada küberkerksust ja reageerimisvõimekust.

5. ENISA aitab rakendada küberturbeoskuste akadeemiat ja suurendada küberturvalisuse valdkonna töötajate arvu liidus, toetades jõupingutusi liidus oskuste ülekantavuse arendamiseks, sh Euroopa küberturbeoskuste raamistiku haldamise ja kasutuselevõtu teel ning Euroopa individuaalsete küberturbeoskuste tõendamise kavade väljatöötamise, haldamise ja kasutuselevõtu teel kooskõlas käesoleva jaotise 4. jao II peatükiga ning tagades koolituste pakkumise kooskõlas artikli 6 punktiga 8.

6. ENISA edendab liidu tasandil küberturvalisusega seotud küsimuste alast koostööd, sh teabe jagamist ning koordineerimist liikmesriikide ja liidu üksuste seas kooskõlas määrusega (EL, Euratom) 2023/2841 ning asjaomaste era- ja avaliku sektori sidusrühmade seas.

7. ENISA aitab kaasa küberturvalisuse alase suutlikkuse suurendamisele liidu tasandil, et toetada liikmesriikide tegevust küberohtude ennetamisel ja neile reageerimisel.

8. ENISA toetab operatiivkoostööd liidu tasandil, sh panustades küberohtude ja intsidentide maastiku alasesse ühisesse olukorrateadlikusse liikmesriikide hulgas ning koos CERT-EUga liidu üksuste hulgas.

9. ENISA teeb tihedat koostööd Europoli, CSIRTide ja muude asjaomaste riiklike asutustega, et parandada küberturvalisuse alast valmisolekut ja reageerimist lunavara intsidentidele.

10. ENISA aitab luua ja kasutusel hoida Euroopa küberturvalisuse sertifitseerimise raamistikku kooskõlas käesoleva määruse III jaotisega. ENISA propageerib Euroopa küberturvalisuse sertifitseerimise kasutamist, et vältida siseturu killustatust.

11. ENISA aitab ühtlustada digitaalset ühtset turgu, osaledes standardimistegevuses, mis on küberturvalisusega seotud liidu poliitika seisukohast oluline, ning töötades välja tehnilisi kirjeldusi.

12. ENISA edendab küberturvalisusealase teadlikkuse kõrget taset organisatsioonide ja ettevõtete hulgas.

II peatükk
Ülesanded

1. jagu
Liidu poliitikameetmete ja õiguse rakendamise toetamine

Artikkel 5
Liidu poliitikameetmete ja õiguse rakendamise toetamine

1. ENISA aitab liidu poliitikameetmete ja õiguse rakendamisele kaasa järgmiselt:

   a) aitab liikmesriikidel järjekindlalt rakendada küberturvalisusega seotud liidu poliitikameetmeid ja õigust, sh väljastades tehnilisi suuniseid ja aruandeid, andes nõu ja jagades parimaid tavasid ning soodustades parimate tavade vahetamist pädevate asutuste vahel seoses sellega;

   b) toetab teabe jagamist sektorite piires ja vahel, eelkõige direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorite puhul ning määruse (EL) 2024/2847 kohaldamisalasse kuuluvate digielemente sisaldavate toodete puhul, pakkudes parimaid tavasid ja suuniseid kättesaadavate vahendite ja menetluste kohta;

   c) aitab komisjoni taotluse korral liikmesriike, andes toetust, nt tehnilisi suuniseid muu hulgas küberriski juhtimise meetmete kohta, vahendeid küberturvalisuse küpsustaseme hindamiseks ning küberintsidentidele reageerimise käsiraamatuid, mis on kohandatud direktiivi (EL) 2022/2555 I ja II lisas loetletud sektoritele, või toetades digielemente sisaldavate toodete sisseprojekteeritud turbe rakendamist kooskõlas määrusega (EL) 2024/2847, et edendada küberturvalisuse küpsustaseme parandamist ning küberturvalisuse valdkonnas liidu õiguse järgimist;

   d) panustab direktiivi (EL) 2022/2555 artikli 14 lõike 1 kohaselt loodud koostöörühma (edaspidi „võrgu- ja infoturbe koostöörühm“), määruse (EL) nr 910/2014 artikli 46e lõike 1 kohaselt loodud Euroopa digiidentiteedi koostöörühma, käesoleva määruse artiklis 90 osutatud Euroopa küberturvalisuse sertifitseerimise rühma ning määruse (EL) 2024/2847 artikli 52 lõike 15 kohaselt loodud halduskoostöörühma tegevusse;

   e) aitab liikmesriikidel ja asjaomastel liidu üksustel välja töötada ja edendada küberturvalisuse alaseid poliitikameetmeid, mis on seotud interneti avaliku tuuma üldise kättesaadavuse ja terviklikkuse säilitamisega;

   f) annab liikmesriikidele ja komisjonile kõnealuse määruse rakendamisega seotud küsimustes tehnilist nõu ja toetust kooskõlas määrusega (EL) 2024/2847;

   g) aitab liikmesriikidel anda vastastikust abi ning edendada elutähtsate ja oluliste üksuste koostööprotsesse kooskõlas [direktiivi (EL) 2022/2555 artikliga 37a];

   h) annab Euroopa Andmekaitsenõukogu taotlusel nõu liidu poliitikameetmete ja õiguse konkreetsete küberturvalisuse aspektide rakendamise kohta andmekaitse ja privaatsuse valdkonnas.

2. ENISA panustab liidu tasandi küberriski koordineeritud hindamistesse, sh kui neid viiakse ellu kooskõlas direktiivi (EL) 2022/2555 artikliga 22.

3. ENISA väljastab suunised teabe jagamiseks kasutatavate võrgu- ja infosüsteemide koostalitlusvõime kohta, sh määruse (EL) 2025/38 artikli 6 lõikes 3 osutatud piiriüleste küberkeskustega.

4. ENISA on direktiivi (EL) 2022/2555 artikli 14 lõike 3 kohaselt loodud võrgu- ja infoturbe koostöörühma liige.

5. ENISA pakub komisjoni taotlusel eksperditeadmisi, tehnilist nõu, teavet ja analüüsitulemusi või teeb ettevalmistavat tööd konkreetsetes küberturvalisuse küsimustes, et komisjon saaks neist lähtuda poliitikakujundamisel ja liidu õigusaktide rakendamise järelevalves.

Artikkel 6
Suutlikkuse suurendamine

ENISA abistab:

1) liikmesriike nende tegevuses, et parandada küberohtude ja intsidentide ennetamist, avastamist, analüüsimist ja neile reageerimise suutlikkust, pakkudes liikmesriikidele üldisi ja eksperditeadmisi;

2) liikmesriike nende taotlusel turvanõrkuste avalikustamise poliitikameetmete vabatahtlikkuse alusel loomisel ja rakendamisel;

3) kooskõlas määrusega (EL, Euratom) 2023/2841 CERT-EUd ja institutsioonidevahelist küberturvalisuse nõukoda, kui nad toetavad liidu üksusi, et suurendada nende küberturvalisust, täiustada küberohtude ja intsidentide ennetamist, avastamist ja analüüsimist ning suurendada nende võimekust reageerida kõnealustele küberohtudele ja intsidentidele;

4) liikmesriike riiklike CSIRTide väljatöötamisel, kui nad seda taotlevad vastavalt direktiivi (EL) 2022/2555 artikli 10 lõikele 10;

5) liikmesriike riikliku küberturvalisuse strateegia ja kõnealuse strateegia hindamiseks kasutatavate peamiste tulemusnäitajate väljatöötamisel või ajakohastamisel, kui nad seda taotlevad vastavalt direktiivi (EL) 2022/2555 artikli 7 lõikele 4, ning edendab nimetatud strateegiate levitamist ja sedastab nende rakendamisel tehtavad edusammud kogu liidus, et edendada parimaid tavasid;

6) liidu institutsioone, kui nad seda taotlevad, liidu küberturvalisuse alaste strateegiate väljatöötamisel ja läbivaatamisel, nende levitamisel ning nende rakendamisel tehtavate edusammude jälgimisel;

7) riiklikke CSIRTe nende suutlikkuse arendamisel, muu hulgas edendades dialoogi ja teabevahetust tagamaks vastavalt tehnika tasemele, et iga CSIRTi võimekus vastab ühistele miinimumsuutlikkuse nõuetele ning et iga CSIRT toimib kooskõlas parimate tavadega;

8) liikmesriike, liidu üksusi ning avaliku ja erasektori sidusrühmi, kui nad hindavad küberturvalisuse valdkonna töötajaid, suurendavad nende arvu ja täiustavad nende oskusi, sh arendades asjakohaseid vahendeid, nagu Euroopa küberturbeoskuste raamistik ja Euroopa individuaalsete küberturbeoskuste tõendamise kavad, hallates neid ja edendades nende kasutuselevõttu kooskõlas käesoleva peatüki 4. jaotisega;

9) asjaomaseid avaliku sektori asutusi ja erasektori sidusrühmi sihtotstarbeliste koolituste korraldamisel, kui see on asjakohane, siis koostöös sidusrühmadega;

10) võrgu- ja infoturbe koostöörühma parimate tavade ja teabe vahetamisel, eelkõige direktiivi (EL) 2022/2555 rakendamise kohta kooskõlas kõnealuse direktiivi artikli 14 lõike 4 punktiga c;

11) määruse (EL) 2024/2847 kohaselt määratud turujärelevalveasutusi tegevuses, mille eesmärk on tagada kõnealuse määruse tulemuslik rakendamine, sh toetada suuniseid ja tehnilisi nõuandeid ettevõtjatele, toetada nõuetele vastavuse kontrolle, riskide hindamist, ühismeetmeid ning lauskontrolle nagu on sätestatud määruses (EL) 2024/2847;

12) Euroopa küberturvalisuse sertifitseerimise rühma liikmeid parimate tavade vahetamisel ning individuaalsete liikmesriikide taotluse korral abistab riiklikke küberturvalisuse sertifitseerimise asutusi Euroopa küberturvalisuse sertifitseerimise kavade rakendamisel riiklikul tasandil;

13) avaliku sektori asutusi ja erasektori sidusrühmi vastavushindamisel ja hindamistegevuses, sh vastavushindamisasutusi ning väikeseid ja keskmise suurusega ettevõtjaid, et toetada kindlat, konkurentsivõimelist, kaasavat ja ühtlustatud vastavushindamise ökosüsteemi, mis toetab määruse (EL) 2024/2847 ja Euroopa küberturvalisuse sertifitseerimise raamistiku rakendamist;

14) küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskust ja riiklike koordineerimiskeskuste võrgustikku, mis on loodud määruse (EL) 2021/887 kohaselt, jagades teavet praeguste ja tekkivate riskide ning küberohtude kohta, sh uue ning esilekerkiva info- ja kommunikatsioonitehnoloogia puhul;

15) liikmesriike, pakkudes tehnilist tuge, sh küberturvalisuse valdkonnas regulatiivliivakastide loomiseks ja käitamiseks kooskõlas asjakohaste liidu õigusaktidega.

Artikkel 7
Teadlikkuse suurendamine ja talendireserv

ENISA abistab liikmesriike, kui nad suurendavad teadlikkust liidu poliitikameetmetest ja õigusaktidest küberturvalisuse valdkonnas ning edendavad nende märgatavust, töötades välja rakendatavaid vahendeid ja suuniseid. ENISA toetab algatusi, mille eesmärk on suurendada Euroopa küberturvalisuse alast talendireservi, eelkõige koordineerides konkursse.

Artikkel 8
Turuteadmised ja -analüüsid

1. ENISA viib läbi peamiste turusuundumuste analüüse küberturvalisuse turu nõudluse ja pakkumise poolel ning levitab nende tulemusi, eelkõige valdkondades, mille puhul on kasutusele võetud või kavas Euroopa küberturvalisuse sertifitseerimise kavad, direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorites ning määrusega (EL) 2024/2847, sh selle määruse III ja IV lisaga hõlmatud tootekategooriate puhul.

2. ENISA viib läbi tehnoloogiliste küberturvalisuse suundumuste analüüse ja levitab nende tulemusi, eelkõige direktiivi (EL) 2022/2555 kohaldamisalasse kuuluvate

tegevuste ja üksuste ning määruse (EL) 2024/2847 kohaldamisalasse kuuluvate digielementidega toodete puhul.

3. ENISA kogub teadmisi ning levitab tehnilisi nõuandeid ja analüüse tipptasemel küberturvalisuse vahendite, raamistike, standardite ja parimate tavade kohta.

Artikkel 9
Rahvusvaheline koostöö

ENISA annab panuse liidu jõupingutustesse teha koostööd kolmandate riikide ja rahvusvaheliste organisatsioonidega ning asjaomastes rahvusvahelistes koostööraamistikes, et edendada rahvusvahelist koostööd küberturvalisusega seotud küsimustes, sh:

a) osaleb asjakohasel juhul vaatlejana rahvusvaheliste õppuste korraldamises ning analüüsib selliste õppuste tulemusi ja annab nende kohta aru haldusnõukogule;

b) soodustab komisjoni taotluse korral parimate tavade vahetamist kolmandate riikide ja rahvusvaheliste organisatsioonidega;

c) pakub komisjonile taotluse korral eksperditeadmisi;

d) annab komisjonile eksperdinõuandeid ja toetust Euroopa küberturvalisuse sertifikaatide rahvusvahelise tunnustamise küsimustes kooskõlas artikliga 87;

e) annab komisjonile eksperdinõuandeid ja pakub komisjonile toetust küsimustes, mis käsitlevad rahvusvahelist standardimist ja rahvusvaheliste standardiorganisatsioonidega suhtlemist, vajaduse korral koostöös artikli 90 kohaselt moodustatud Euroopa küberturvalisuse sertifitseerimise rühmaga.

2. jagu

Operatiivkoostöö

Artikkel 10
Operatiivkoostöö liidu tasandil

1. ENISA toetab operatiivkoostööd liikmesriikide, CERT-EU kaudu liidu üksuste ning muude sidusrühmade vahel.

2. ENISA on direktiivi (EL) 2022/2555 artikli 15 lõike 1 kohaselt loodud riiklike CSIRTide võrgustiku liige ning tagab CSIRTide võrgustiku sekretariaaditeenused kooskõlas direktiivi (EL) 2022/2555 artikli 15 lõikega 2.

3. ENISA tagab Euroopa küberkriisiga tegelevate kontaktasutuste võrgustiku (edaspidi „EU-CyCLONe“) sekretariaaditeenused kooskõlas direktiivi (EL) 2022/2555 artikli 16 lõike 2 teise lõiguga.

4. ENISA toetab liikmesriikide tehnilist ja operatiivkoostööd, eelkõige CSIRTide võrgustiku ja EU-CyCLONe kaudu. Kõnealune toetus hõlmab järgmist:

   a) nõuandeid intsidentide ennetamise, avastamise, neile reageerimise ja neist taastumise võimekuste suurendamise kohta;

   b) ühe või mitme liikmesriigi taotluse korral nõuannete andmist konkreetse võimaliku või käimasoleva intsidendi või võimaliku või avalduva küberohu kohta ning nende hindamist, sh pakkudes eksperditeadmisi ja edendades

kõnealuste intsidentide tehnilist käsitlemist, ning toetades asjakohase teabe ja tehniliste lahenduste vabatahtlikku jagamist liikmesriikide vahel;

c) nõrkuste, ohtude ja intsidentide analüüsimist;

d) ühe või mitme liikmesriigi taotluse korral direktiivi (EL) 2022/2555 artikli 23 lõike 3 tähenduses oluliste intsidentide tehnilise järeluurimise toetamist;

e) ulatuslike küberintsidentide ja kriiside koordineeritud haldamise toetamist operatiivtasandil, eelkõige aidates EU-CyCLONe-t poliitilise tasandi jaoks aruannete koostamisel ning edendades õigeaegset teabe jagamist CSIRTide võrgustiku ja EU-CyCLONe vahel.

5. ENISA toetab liikmesriigi või liidu üksuse taotlusel koostöös CERT-EUga järjepidevat avalikku suhtlust intsidendi või küberohu asjus.

6. ENISA toetab liikmesriikide ja CERT-EU kaudu liidu üksuste koostööd turvaliste sidevahendite kasutuselevõtu valdkonnas. ENISA kasutab CSIRTide võrgustikus ja EU-CyCLONes turvalisi sidevahendeid, mida pakuvad juriidilised isikud, mis on asutatud liidus või mida loetakse liidus asutatuks ja mis on liikmesriigi või selle kodanike kontrolli all.

Artikkel 11
Küberturvalisuse alane ühine olukorrateadlikkus

1. ENISA teeb liikmesriikide ja liidu üksuste hulgas küberohtude ja intsidentide olukorra alase suurema ühise olukorrateadlikkuse tagamiseks järgmist:

a) töötab koostöös EU-CyCLONe, CSIRTide võrgustiku, komisjoni, CERT-EU, Europoli ja muude asjaomaste liidu üksustega välja kontrollitud ja usaldusväärse küberohuteadmuse hoidlad, mis sisaldavad teavet intsidentide suundumuste, taktika, meetodite ja menetluste kohta;

b) esitab kooskõlas artikliga 12 varajasi hoiatusi potentsiaalsete või käimasolevate oluliste või ulatuslike intsidentide või potentsiaalse piiriülese olemusega küberohu kohta, eelkõige direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorite puhul;

c) esitab CSIRTide võrgustiku, EU-CyCLONe või komisjoni taotluse korral aegsasti vajaduspõhised analüüsid intsidentide uute suundumuste kohta;

d) esitab liikmesriikide või komisjoni taotluse korral analüüsi või muu teabe tegeliku või tajutud küberriski või -ohu kohta;

e) esitab digielementidega toodete küberriski analüüsi ja annab nende kohta tehnilist nõu, sh turujärelevalve toetamiseks ning koostades iga kahe aasta tagant esitatava tehnilise aruande uute suundumuste kohta kooskõlas määruse (EL) 2024/2847 artikli 17 lõikega 3;

f) koostab korrapäraselt põhjaliku ELi küberturvalisuse tehnilise olukorra aruande intsidentide ja küberohtude kohta ning teeb aruande kättesaadavaks nõukogule, EU-CyCLONe-le, CSIRTide võrgustikule, komisjonile, Euroopa välisteenistusele ja Europolile;

g) jälgib lunavararünnete meetodite, nõudmiste ja mõju suundumusi ning esitab teabe kõnealuste suundumuste kohta komisjonile, CSIRTide võrgustikule, EU-CyCLONe-le ja Europolile.

2. ENISA teeb sidusrühmade hulgas küberohtude ja intsidentide keskkonna kohta suurema ühise olukorrateadlikkuse tagamiseks järgmist:

a) teeb küberohtude, intsidentide, suundumuste, kujunemisjärgus tehnoloogia ja nende mõju analüüse, sh korrapäraseid analüüse direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorite ning määrusega (EL) 2024/2847 hõlmatud asjaomaste tootekategooriate kohta;

b) väljastab koostöös komisjoni ja vajaduse korral CSIRTide võrgustikuga nõuandeid, suuniseid ja parimaid tavasid võrgu- ja infosüsteemide turvalisuse kohta, eelkõige direktiivi (EL) 2022/2555 I ja II lisas loetletud sektoreid toetava taristu turvalisuse kohta;

c) koostab pikaajalisi strateegilisi analüüse küberohtude ja intsidentide kohta, et teha kindlaks uued suundumused ja aidata ennetada intsidente.

3. ENISA võib avalikustada lõikes 2 osutatud analüüse, nõuandeid, suuniseid, parimaid tavasid ja aruandeid kokkuleppel nendesse panustanud üksustega, millele on osutatud lõikes 2.

4. ENISA kasutab lõike 1 punktides a–d ja f ja lõikes 2 osutatud tegevuse elluviimisel enda analüüse ja vajaduse korral oma ülesannete täitmisel saadud teavet, sh:

a) üldsusele kättesaadavates allikates esitatud teave, sh IKT-toodete või -teenuste üldsusele teadaolevad nõrkused, mis on saadaval direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt koostatud Euroopa nõrkuste andmebaasis;

b) liikmesriikide, liidu üksuste, CERT-EU, erasektori või valitsusväliste partnerite, kolmandate riikide ja rahvusvaheliste organisatsioonide jagatud teave mis tahes piirangutega kõnealuse teabe edasi jagamiseks, mis on silmapaistval viisil märgistatud.

5. ENISA teeb lõike 1 punktis e osutatud ELi küberturvalisuse tehnilise olukorra aruande koostamisel tihedat koostööd liikmesriikidega. See aruanne põhineb üldsusele kättesaadaval teabel, ENISA enda tehtud analüüsil ja aruannetel, mida jagavad muu hulgas liikmesriikide CSIRTid või direktiivi (EL) 2022/2555 kohaselt loodud ühtsed kontaktpunktid (mõlemad vabatahtlikkuse alusel), ning küberkuritegevuse vastase võitluse Euroopa keskus ja CERT-EU. ENISA võib panustanud üksustega kokkuleppel teha aruande koondversiooni üldsusele kättesaadavaks.

Artikkel 12
Varajased hoiatused

1. Käesoleva määruse artikli 11 lõike 1 esimese lõigu punktis b osutatud varajased hoiatused sisaldavad asjakohast teavet potentsiaalsete või käimasolevate oluliste või ulatuslike intsidentide või potentsiaalse piiriülese olemusega küberohu kohta direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorite puhul. Kõnealune teave võib hõlmata üldsusele teadaolevaid nõrkusi ja seda, kas need mõjutavad määrusega (EL) 2024/2847 hõlmatud digielemente sisaldavaid tooteid, meetodeid ja menetlusi, turvarikke indikaatoreid, kahjulikke võtteid, konkreetsete ohusubjektidega seotud teavet ja soovitusi leevendusmeetmete kohta.

2. Artikli 11 lõike 1 esimese lõigu punktis b osutatud varajased hoiatused esitatakse esimesel võimalusel asjaomas(t)ele CSIRTi(de)le ning vajaduse korral CSIRTide võrgustikule ja EU-CyCLONe-le.

3. ENISA pakub varajase hoiatuse teenust direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorites tegutsevatele üksustele.

4. Lõikes 3 osutatud teenust osutatakse üksuse taotluse korral ja see tehakse masinloetavas vormingus üldsusele kättesaadavaks. See teenus hõlmab teabe jagamist küberohu indikaatorite kohta ja soovitusi leevendusmeetmete kohta.

5. ENISA kehtestab menetluse varajaste hoiatuste levitamiseks lõikes 3 osutatud üksustele.

Artikkel 13
Intsidentidele reageerimise ja nende läbivaatamise toetus

1. ENISA käitab ja haldab kas täielikult või osaliselt ELi küberreservi kooskõlas määrusega (EL) 2025/38.

2. ENISA vaatab komisjoni või EU-CyCLONe taotlusel, CSIRTide võrgustiku toetusel ja asjaomaste liikmesriikide heakskiidul läbi olulised küberintsidendid või ulatuslikud küberintsidendid ning hindab neid kooskõlas määruse (EL) 2025/38 artikliga 21.

3. ENISA aitab koostöös Europoli ja CSIRTide või muude pädevate asutustega, nagu on kohaldatav, direktiivi (EL) 2022/2555 I ja II lisas loetletud individuaalseid elutähtsaid ja olulisi üksusi lunavaraintsidentideks valmistumisel, neile reageerimisel ja nendest taastumisel. Sel otstarbel loob ENISA kasutajatoe ja eelkõige kasutab täiustatud küberohu ja intsidentide keskkonna alast ühist olukorrateadlikkust kooskõlas käesoleva määruse artikli 11 lõike 1 esimese lõigu punktidega a ja g.

Artikkel 14
Küberturvalisuse õppused liidu tasandil

1. ENISA toetab komisjoni liidu tasandi küberturvalisuse õppuste iga-aastase jooksva programmi koostamisel.

2. ENISA haldab lõikes 1 osutatud õppustest omandatud kogemuste andmehoidlat ning annab liikmesriikidele ja vajaduse korral liidu üksustele soovitusi saadud õppetundide tulemusliku ja tõhusa rakendamise kohta.

3. EU-CyCLONe ja komisjoni taotlusel korraldab ENISA liidu tasandil küberturvalisuse õppusi või panustab nende korraldamisse, sh testib valmisolekut reageerida ulatuslikele küberintsidentidele ja kriisidele liidu tasandil.

4. Liikmesriikide taotlusel toetab ENISA neid riiklike küberturvalisuse õppuste korraldamisel.

5. CERT-EU taotlusel panustab ENISA selliste küberturvalisuse õppuste korraldamisse, mille CERT-EU korraldab kooskõlas määruse (EL, Euratom) 2023/2841 artikli 13 lõikega 7.

Artikkel 15
Vahendite ja platvormide pakkumine

1. ENISA loob operatiivsed tehnilised vahendid, sh liidu tasandil küberturvalisusega seotud platvormid, eelkõige määruse (EL) 2024/2847 artikli 16 lõike 1 kohaselt loodud ühtse teatamisplatvormi [ja direktiivi (EL) 2022/2555 artikli 23a kohaselt loodud intsidentidest teatamise ühtse kontaktpunkti] ning testimisvahendid, et

toetada vastavushindamismenetluste rakendamist kooskõlas asjakohaste liidu õigusaktidega, pakub ja käitab neid, hoiab neid kasutuses ja ajakohastab neid vastavalt vajaduse.

2. Kui see on lõike 1 kohaldamiseks asjakohane, teeb ENISA koostööd ja vahetab teavet CSIRTide võrgustikuga ning, kui see on kohaldatav, turujärelevalveasutustega.

Artikkel 16
Nõrkusehalduse teenused

ENISA töötab välja liidu ühise nõrkusehalduse teenuse võimekuse ja pakub sidusrühmadele nõrkusehalduse teenuseid järgmiselt:

a) pidades direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasi;

b) pakkudes sidusrühmadele nõrkusehalduse teenuseid, tuginedes Euroopa nõrkuste andmebaasile ja kasutades ENISA-le kättesaadavat asjakohast teavet;

c) kui see on asjakohane, siis tehes struktureeritud koostööd Euroopa nõrkuste andmebaasile sarnaseid programme, registreid või andmebaase pakkuvate organisatsioonidega;

d) toetades aktiivselt CSIRTe, mis on määratud koordineerijateks kooskõlas direktiivi (EL) 2022/2555 artikli 12 lõikega 1, selliste nõrkuste koordineeritud avalikustamise haldamisel, millel võib olla märkimisväärne mõju rohkem kui ühe liikmesriigi üksustele;

e) töötades välja ja hoides kasutuses metoodikaid ning juhtimismehhanisme nõrkuste kindlaksmääramiseks ja koordineeritud avalikustamiseks koostöös riiklike pädevate asutuste, CSIRTide, tööstuse ja teaduskogukonnaga.

3. jagu

Küberturvalisuse sertifitseerimine ja standardimine

Artikkel 17
Küberturvalisuse sertifitseerimine

1. ENISA panustab liidu küberturvalisuse sertifitseerimise poliitika väljatöötamisse ja rakendamisse ning edendab seda, nagu on märgitud käesoleva määruse III jaotises. ENISA vastutab järgmise eest:

   a) Euroopa küberturvalisuse sertifitseerimise ettevalmistavate kavade (edaspidi „ettevalmistavad kavad“) koostamine IKT-toodetele, -teenustele, -protsessidele, hallatud turbeteenustele ja üksuste turvaolekule kooskõlas artikliga 74 ning, kui see on kohaldatav, tehniliste kirjelduste koostamine kooskõlas artikliga 77;

   b) vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade haldamine kooskõlas artikliga 75, sh võttes arvesse vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade võimalikku läbivaatamist kooskõlas artikliga 76;

   c) vastuvõetud kavade kasutuselevõtu edendamine ning sihtotstarbelise veebisaidi haldamine, millel esitatakse teavet Euroopa küberturvalisuse sertifitseerimise

kavade, Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide kohta kooskõlas artikliga 79 ning tutvustatakse neid;

d) sertifitseerimisprotsesside, hindamistegevuste, vastastikuste eksperdihinnangute ja vastastikuste hindamiste alase suutlikkuse suurendamise korraldamine, sh toetades liikmesriike, kui nad esitavad vastava taotluse, kooskõlas artikli 6 punktiga 12.

2. ENISA toetab komisjoni järgmises tegevuses:

a) Euroopa küberturvalisuse sertifitseerimise rühma juhtimine kooskõlas artikliga 90;

b) Euroopa küberturvalisuse sertifitseerimise assamblee korraldamine kooskõlas artikli 72 lõikega 1;

c) Euroopa küberturvalisuse sertifikaatide rahvusvaheline tunnustamine kooskõlas artikliga 87;

d) vastastikuste eksperdihinnangute korraldamine kooskõlas artikliga 89;

e) näidissätete koostamine, millele osutatakse IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ja üksuste turvaoleku Euroopa küberturvalisuse sertifitseerimise kavades kooskõlas artikli 81 lõikega 5.

Artikkel 18
Standardimine, tehnilised kirjeldused ja suunised

1. ENISA koostab tehnilised kirjeldused ja suunised, et toetada liidu õigusaktide rakendamist küberturvalisuse valdkonnas. Kõnealuste tehniliste kirjelduste koostamisel võtab ENISA arvesse kehtivaid Euroopa ja rahvusvahelisi standardeid ning muid asjakohaseid tehnilisi kirjeldusi. ENISA tagab oma tehniliste kirjelduste ja suuniste järjekindluse.

2. ENISA seirab liidu tasandil ning kooskõlas artikliga 9 rahvusvahelisel tasandil standardite koostamise tegevust ning vajaduse korral osaleb selles ja juhib seda, et toetada küberturvalisusega seotud liidu poliitikat.

3. ENISA toetab krüptoalgoritmide väljatöötamist ja hindamist. Kui ENISA annab krüptoalgoritmile positiivse hinnangu, teeb ENISA kooskõlas määrusega (EL) nr 1025/2012 koostööd Euroopa standardiorganisatsioonidega, et toetada selle standardimist.

4. ENISA annab komisjonile ja vajaduse korral liikmesriikidele tehnilist nõu liidu küberturvalisuse poliitikat toetavate asjakohaste standardite või tehniliste kirjelduste kohta, sh küberturvalisuse valdkonna liidu ühtlustamisõigusaktide, eelkõige määruse (EL) 2024/2847, direktiivi (EL) 2022/2555 artikli 25 kohaldamise tehniliste valdkondade ning artikli 81 lõike 1 punkti d kohaste Euroopa küberturvalisuse sertifitseerimise kavade osas.

5. ENISA abistab komisjoni harmoneeritud standardite projektide hindamisel, et toetada liidu ühtlustamisõigusaktide rakendamist küberturvalisuse valdkonnas.

6. ENISA edendab küberturvalisuse valdkonna Euroopa ja rahvusvaheliste standardite kasutuselevõttu.

7. ENISA täidab lõigetes 1–6 osutatud ülesandeid usaldusväärselt, sõltumatult ja konfidentsiaalselt, sh lõpetades või peatades oma osalemise konkreetsetes tehnilistes

organites, kui kõnealune osalemine on vastuolus muude ülesannete või eesmärkidega.

4. jagu
Küberturbeoskuste akadeemia rakendamine

Artikkel 19
Euroopa küberturbeoskuste raamistik

1. ENISA töötab välja ja teeb üldsusele kättesaadavaks Euroopa küberturbeoskuste raamistiku. ENISA konsulteerib komisjoniga enne Euroopa küberturbeoskuste raamistiku üldsusele kättesaadavaks tegemist või ajakohastamist kooskõlas lõikega 4.
2. Euroopa küberturbeoskuste raamistikus määratakse kindlaks küberturvalisuse spetsialistide ametikirjeldused ning konkreetse ametikirjeldusega seotud konkreetsed ülesanded, oskused ja teadmised. Euroopa küberturbeoskuste raamistiku kasutamine on avaliku ja erasektori üksustele vabatahtlik.
3. ENISA võib konsulteerida Euroopa küberturbeoskuste raamistiku väljatöötamise ja kasutuselevõtu asjus sidusrühmadega.
4. ENISA hindab Euroopa küberturbeoskuste raamistiku ajakohastamise vajadust korrapäraselt ning vajaduse korral ajakohastab seda.

Artikkel 20
Euroopa individuaalsete küberturbeoskuste tõendamise kavade väljatöötamine, vastuvõtmine ja haldamine

1. ENISA töötab välja, võtab vastu ja haldab Euroopa individuaalsete küberturbeoskuste tõendamise kavasid. Euroopa individuaalsete küberturbeoskuste tõendamise kavade kasutamine on riiklikele avaliku sektori asutustele ja erasektori üksustele vabatahtlik, kui liikmesriigi õiguses ei ole määratud teisiti.
2. ENISA konsulteerib enne uue Euroopa individuaalsete küberturbeoskuste tõendamise kava algatamist komisjoniga. ENISA võtab sellise kava vastu ainult juhul, kui komisjon on esitanud selle kohta positiivse arvamuse. ENISA võib Euroopa individuaalsete küberturbeoskuste tõendamise kavade koostamisel konsulteerida asjaomaste sidusrühmadega.
3. Euroopa individuaalsete küberturbeoskuste tõendamise kava hõlmab järgmist:
   a) tõendamise kava reguleerimisese ja kohaldamisala kooskõlas Euroopa küberturbeoskuste raamistiku ametikirjelduste ja nende alamkogumitega;
   b) hindamisi tegema koolitatud üksikisikute (edaspidi „hindajad“) suhtes kohaldatavad nõuded kooskõlas artikliga 21, vajalikud oskused, teadmised ja kogemused ning koolitusmeetodid;
   c) iga tõendamiskava põhine turul kasutuselevõtu analüüs;
   d) õppetulemused, hindamismeetodid ja tingimused, mida volitatud tõendajad kasutavad, et hinnata seda, kuidas üksikisik tõendab nõutavaid oskusi kooskõlas artikliga 21;
   e) asjakohasel juhul üks või mitu pädevustaset;

f) normid, mis käsitlevad aruannete säilitamist volitatud tõendajate poolt;

g) Euroopa individuaalsete küberturbeoskuste tõendite sisu ja vorm, võttes nõuetekohaselt arvesse artikli 21 lõike 5 punkti e;

h) tõendamiskava kohaselt välja antud Euroopa individuaalsete küberturbeoskuste tõendi maksimaalne kehtivusaeg.

4. Euroopa individuaalsete küberturbeoskuste tõendamise kava võib sisaldada Euroopa individuaalsete küberturbeoskuste tõendi hinnangulist maksumust.

5. ENISA tagab Euroopa individuaalsete küberturbeoskuste tõendamise kavade koostamise vältel tiheda koostöö liikmesriikidega.

6. Euroopa individuaalsete küberturbeoskuste tõendamise kava muutmine ei mõjuta artikli 22 lõike 3 punkti a kohaselt väljastatud tõendeid, mis jäävad kehtima kogu ajavahemikuks, milleks need on antud.

Artikkel 21
Volitatud tõendajad

1. Volitatud tõendajad hindavad, kas üksikisikud vastavad Euroopa individuaalsete küberturbeoskuste tõendamise kava nõuetele ning, kui need nõuded on täidetud, siis väljastavad Euroopa individuaalsete küberturbeoskuste tõendi. Tõendajal võib olla mitu volitust, neist igaüks ühe Euroopa individuaalsete küberturbeoskuste tõendamise kava jaoks.

2. ENISA annab hindajatele suuniseid ja korraldab nende kohustusliku koolitamise Euroopa individuaalsete küberturbeoskuste tõendamise kavas sisalduvate nõuete ja hindamismeetodite kohta, nagu on osutatud artikli 20 lõike 3 punktis b.

3. Üksused, kes soovivad saada volitatud tõendajaks või oma volitust uuendada (edaspidi „taotluse esitajad“) esitavad ENISA-le taotluse. Nad peavad vastama järgmistele nõuetele:

a) nad on juriidilised isikud;

b) nad on suutelised täitma käesolevas määruses seoses Euroopa individuaalsete küberturbeoskuste tõenditega sätestatud ülesandeid olenemata sellest, kas hindamise teeb volitatud tõendaja ise või tehakse see tema nimel ja tema vastutuse all;

c) neil on Euroopa individuaalsete küberturbeoskuste tõendamise kavaga seotud tehniliste ja haldusülesannete nõuetekohaseks täitmiseks vajalikud vahendid ning juurdepääs kõigile vajalikele seadmetele ja vahenditele.

Esimese lõigu punkti b kohaldamiseks peab alltöövõtt ja konsulteerimine asutuseväliste töötajatega olema nõuetekohaselt dokumenteeritud ja toimuma ilma vahendajateta ning selle kohta tuleb sõlmida kirjalik leping, milles käsitletakse muu hulgas konfidentsiaalsust ja huvide konflikti küsimusi.

4. Taotluse esitajad ei tohi olla suure riskiga tarnijad.

5. Volitatud tõendajad peavad täitma järgmisi kohustusi:

a) iga Euroopa individuaalsete küberturbeoskuste tõendamise kava rakendamisel:

i) peavad neil olema vajalikud hindajad ja töötajad nende tegevuse elluviimiseks kõnealuses kavas märgitud viisil ja õigeaegselt;

ii) peavad nad tagama, et hindajad järgivad ametisaladuse hoidmise nõuet, nad on erapooletud ja viivad oma tegevust läbi sõltumatult ning suurima erialase kohusetundega;

iii) peavad neil olema kirjalikud menetlused oma tegevuse elluviimiseks selle kava alusel, milleks nad on volitatud;

b) nad ei hinda oma hindajaid ega väljasta neile Euroopa individuaalsete küberturbeoskuste tõendeid;

c) nad tagavad vajaduse korral nõuetekohaste kaitsemeetmete kasutuselevõtu teel, et nende hindajad saavad teha oma tööd sõltumatult, eelkõige kui kõnealused üksikisikud kuuluvad nende enda struktuuri või on kõnealuse struktuuri töötajad või õppijad;

d) nad ei osale tegevuses, mis võib olla vastuolus nende hindajate otsuste sõltumatuse või usaldusväärsusega;

e) nad tagavad, et Euroopa individuaalsete küberturbeoskuste elektrooniline tõend väljastatakse üksikisiku taotlusel elektroonilise tõendina sellises vormingus, mille saab salvestada määruses (EL) nr 910/2014 sätestatud Euroopa digiidentiteedikukrusse.

6. Volitatud tõendajad teavitavad ENISAt viivitamata, kui mõni lõigetes 3 ja 4 loetletud nõuetest või lõikes 5 loetletud kohustustest ei ole enam täidetud või kui tekib kahtlus, et kõnealused nõuded või kohustused ei ole täidetud, sh hindajate sõltumatuse osas.

7. Volitatud tõendajad võivad küsida üksikisikutelt hindamise ja Euroopa individuaalsete küberturbeoskuste tõendi väljastamise eest tasu, võttes arvesse Euroopa individuaalsete küberturbeoskuste tõendite hinnangulist maksumust kooskõlas artikli 20 lõikega 4, ning avalikustada selle sihtotstarbelisel veebisaidil kooskõlas artikli 23 punktiga d.

8. Taotluse esitajad ja volitatud tõendajad lubavad ENISA-l teha taotlusprotsessi või loa säilitamise raames hindamisi ning jagavad kogu asjakohast teavet, et tagada lõigetes 3 ja 4 sätestatud nõuete või lõikes 5 sätestatud kohustuste täitmine või jätkuv täitmine kooskõlas artikli 22 lõikega 2.

Artikkel 22

Volitatud tõendajaks saamise taotluste läbivaatamine ja lubade säilitamine

1. Taotluse esitajad maksavad oma taotluse läbivaatamise eest ENISA-le tasu. Volitatud tõendajad maksavad oma volituse säilitamise eest ENISA-le tasu.

2. ENISA hindab, kas taotluse esitaja või volitatud tõendaja täidab või täidab jätkuvalt artikli 21 lõigetes 3 ja 4 sätestatud nõudeid ning artikli 21 lõikes 5 sätestatud kohustusi.

3. Pärast seda, kui ENISA on taotluse artikli 21 lõigetes 3 ja 4 osutatud nõuete alusel läbi vaadanud, võib ta teha ühe järgmistest otsustest:

a) anda taotluse esitajale volitatud tõendaja õigused või neid õigusi uuendada;

b) lükata volitatud tõendajaks saamise taotluse tagasi või volitatud tõendaja õigusi mitte uuendada;

c) lõpetada taotluse menetlemise ENISA lisateabe nõudele järgnenud taotluse esitaja tegevusetuse tõttu.

ENISA võib kõnealuseid otsuseid muuta, need peatada või tühistada artikli 22 lõike 2 kohase hindamise põhjal või artikli 21 lõikes 6 osutatud juhul.

4. ENISA teeb lõikes 3 osutatud otsuse kolme kuu jooksul alates artikli 21 lõike 3 kohaselt taotluse esitamise kuupäevast. Kui ENISA on nõudnud taotluse esitajalt lisateavet, siis teeb ENISA lõikes 3 osutatud otsuse ühe kuu jooksul alates lisateabe saamisest.

5. Lõike 3 punktis a osutatud otsuse maksimumkestus on kolm aastat ja selles märgitakse volituse iga-aastase säilitamisega seotud tasu.

6. ENISA tagab, et tema tegevus, mis on seotud Euroopa individuaalsete küberturbeoskuste tõendamise kavade väljatöötamise ja vastuvõtmisega, nagu on sätestatud artiklis 20, on rangelt eraldatud käesoleva artikli lõigetes 2 ja 3 sätestatud taotluste läbivaatamise ja hindamise tegevusest ning seda viiakse ellu sellest sõltumatult.

Artikkel 23
Avalik teave

ENISA haldab ja ajakohastab korrapäraselt sihtotstarbelist veebisaiti, millel on esitatud avalik teave järgmise kohta:

a) Euroopa küberturbeoskuste raamistik, sh selle ajakohastamise struktuur ja ajakava;

b) Euroopa individuaalsete küberturbeoskuste tõendamise kavad, nende kulg ja nende väljatöötamise ajakava;

c) iga käesoleva määruse artikli 47 kohaselt vastu võetud Euroopa individuaalsete küberturbeoskuste tõendamise kavaga seotud tasud;

d) Euroopa individuaalsete küberturbeoskuste tõendi hinnanguline maksumus kooskõlas artikli 20 lõikega 4;

e) volitatud tõendajate loetelu.

III peatükk
ENISA töökorraldus

Artikkel 24
ENISA haldus- ja juhtimisstruktuur

ENISA haldus- ja juhtumisstruktuuri kuuluvad:

a) haldusnõukogu, mis täidab artiklis 28 sätestatud ülesandeid;

b) juhatus, mis täidab artiklis 30 sätestatud ülesandeid;

c) tegevdirektor, kes täidab artiklis 32 sätestatud kohustusi;

d) tegevdirektori asetäitja, kes täidab artiklis 34 sätestatud kohustusi;

e) ENISA nõuanderühm;

f) apellatsiooninõukogu, kes täidab artiklites 39–42 sätestatud ülesandeid.

1. jagu
Haldusnõukogu

Artikkel 25
Haldusnõukogu koosseis

1. Haldusnõukogusse kuulub igast liikmesriigist üks liige, kelle on määranud liikmesriik, ning kaks liiget, kelle on määranud komisjon. Kõigil liikmetel on hääleõigus.

2. Igal haldusnõukogu liikmel on asendusliige. Asendusliikmed esindavad täisliikmeid nende puudumise korral.

3. Iga liikmesriik määrab haldusnõukogu liikmeks direktiivi (EL) 2022/2555 artikli 8 lõike 1 kohaselt määratud riikliku pädeva asutuse juhataja. Kui see ei ole teostatav, siis määravad liikmesriigid haldusnõukogu liikmeks direktiivi (EL) 2022/2555 artikli 8 lõike 1 kohaselt määratud riikliku pädeva asutuse kõrgetasemelise esindaja.

4. Komisjoni määratud liikmed ja haldusnõukogu asendusliikmed nimetatakse ametisse lähtuvalt nende teadmistest küberturvalisuse valdkonnas, võttes arvesse asjakohaseid juhtimis-, haldus- ja eelarvealaseid oskusi. Komisjon ja liikmesriigid püüavad asendusliikmete puhul saavutada meeste ja naiste tasakaalustatud esindatuse haldusnõukogus ning teevad jõupingutusi nende vahetumise piiramiseks, et tagada haldusnõukogu töö järjepidevus.

5. Liikmesriikide määratud liikmete ametiaeg on võrdväärne nende ülesannete kestusega, millele on osutatud lõikes 3.

6. Komisjoni määratud liikmete ja asendusliikmete ametiaeg on neli aastat. Neid võib ametisse tagasi nimetada.

Artikkel 26
Haldusnõukogu esimees

1. Haldusnõukogu valib oma hääleõiguslike liikmete hulgast esimehe ja aseesimehe. Esimees ja aseesimees valitakse haldusnõukogu hääleõiguslike liikmete kahekolmandikulise häälteenamusega.

2. Kui esimees ei saa oma ülesandeid täita, asendab teda automaatselt aseesimees.

3. Esimehe ja aseesimehe ametiaeg on neli aastat ja seda võib üks kord pikendada. Kui nende liikmesus haldusnõukogus lõpeb mis tahes ajal nende ametiaja jooksul, lõpeb nende ametiaeg automaatselt samal päeval.

Artikkel 27
Haldusnõukogu koosolekud

1. Haldusnõukogu koosolekud kutsub kokku esimees.

2. Tegevdirektor osaleb haldusnõukogu koosolekutel hääleõiguseta.

3. Haldusnõukogul on aastas vähemalt kaks korralist koosolekut. Lisaks sellele tuleb haldusnõukogu kokku esimehe algatusel, komisjoni taotlusel või vähemalt ühe kolmandiku liikmete taotlusel.

4. Määrusega (EL) 2021/887 loodud küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse esindaja on haldusnõukogu koosolekutel ilma hääleõiguseta alaline vaatleja.

5. Haldusnõukogu võib kooskõlas haldusnõukogu kodukorraga kutsuda koosolekul või selle osal ilma hääleõiguseta sihtotstarbelise vaatlejana osalema mis tahes isikut, kelle arvamus võib huvi pakkuda.

6. Haldusnõukogu liikmed ja nende asendusliikmed võivad vastavalt haldusnõukogu kodukorrale kasutada haldusnõukogu koosolekutel nõustajate või ekspertide abi.

Artikkel 28
Haldusnõukogu ülesanded

1. Haldusnõukogu teeb järgmist:

a) määrab kindlaks ENISA tegevuse üldise suuna ja tagab, et ENISA tegutseb kooskõlas käesolevas määruses sätestatud normide ja põhimõtetega; samuti tagab haldusnõukogu, et ENISA tegevus on kooskõlas liikmesriikide ja liidu tasandi tegevusega;

b) võtab vastu artiklis 44 osutatud ENISA ühtse programmdokumendi kavandi, enne kui see esitatakse arvamuse saamiseks komisjonile;

c) võtab komisjoni arvamust arvesse võttes vastu ENISA ühtse programmdokumendi kooskõlas artikli 29 lõike 2 punktiga a;

d) teeb järelevalvet ühtses programmdokumendis sisalduva iga-aastase ja mitmeaastase programmi rakendamise üle;

e) võtab kooskõlas artikli 29 lõike 2 punktiga b vastu ENISA aastaeelarve ja täidab muid ENISA eelarvega seotud ülesandeid vastavalt IV peatükile;

f) annab hinnangu konsolideeritud aastaaruandele ENISA tegevuse kohta, mis hõlmab raamatupidamisaruannet ja milles kirjeldatakse, kuidas ENISA on täitnud oma tulemuslikkuse näitajaid, ja võtab selle vastu; esitab nii aastaaruande kui ka sellele antud hinnangu järgmise aasta 1. juuliks Euroopa Parlamendile, nõukogule, komisjonile ja Euroopa Kontrollikojale; teeb aastaaruande üldsusele kättesaadavaks;

g) võtab vastavalt artiklile 50 vastu ENISA suhtes kohaldatavad finantsreeglid;

h) võtab vastu pettustevastase strateegia, mis on proportsionaalses vastavuses pettuste riskiga, pidades silmas rakendatavate meetmete kulude-tulude analüüsi;

i) tagab, et sise- või välisauditi aruannetest ja hindamistest ning Euroopa Pettustevastase Ameti (edaspidi „OLAF“) ja Euroopa Prokuratuuri (edaspidi „EPPO“) uurimistest tulenevate järelduste ja soovituste põhjal võetakse piisavaid järelmeetmeid;

j) võtab vastu oma kodukorra, milles muu hulgas käsitletakse esialgsete otsuste tegemist konkreetsete ülesannete delegeerimise kohta vastavalt artikli 30 lõikele 7;

k) kasutab kooskõlas käesoleva artikli lõikega 2 ENISA töötajate suhtes volitusi, mis on antud ametisse nimetavale asutusele või ametiisikule nõukogu määruses (EMÜ, Euratom, ESTÜ) nr 259/68[73] sätestatud Euroopa Liidu ametnike personalieeskirjadega (edaspidi „personalieeskirjad“) ja töölepingute

[73] EÜT L 56, 4.3.1968, lk 1, ELI: http://data.europa.eu/eli/reg/1968/259(1)/oj.

sõlmimiseks volitatud asutusele Euroopa Liidu muude teenistujate teenistustingimustega (edaspidi „teenistustingimused“) (edaspidi „ametisse nimetava asutuse või ametiisiku volitused“);

l) võtab vastu personalieeskirjade ja teenistustingimuste rakendusnormid kooskõlas personalieeskirjade artikli 110 lõikega 2;

m) määrab tegevdirektori ja, kui ta otsustab luua tegevdirektori asetäitja ametikoha, siis tegevdirektori asetäitja, ning vajaduse korral pikendab nende ametiaega või vabastab nad ametist kooskõlas artikliga 31;

n) nimetab vastavalt personalieeskirjadele ning teenistustingimustele ametisse peaarvepidaja, kes on oma ülesannete täitmisel täiesti sõltumatu;

o) teeb kõik otsused ENISA sisestruktuuri kehtestamise ja vajaduse korral selle muutmise kohta, võttes arvesse ENISA tegevusega seotud vajadusi ja usaldusväärset eelarvehaldust;

p) annab loa leppida kokku koostöökorras seoses artikliga 68;

q) annab loa leppida kokku koostöökorrasseoses artikliga 70;

r) määrab apellatsiooninõukogu liikmed ja vabastab nad ametist kooskõlas artikli 29 lõike 2 punktiga d;

s) võtab vastu normid apellatsiooninõukogu liikmete huvide konfliktide vältimiseks ja lahendamiseks.

2. Haldusnõukogu võtab kooskõlas personalieeskirjade artikli 110 lõikega 2 vastu personalieeskirjade artikli 2 lõikel 1 ja muude teenistujate teenistustingimuste artiklil 6 põhineva otsuse, millega delegeeritakse asjakohased ametisse nimetava asutuse volitused tegevdirektorile ja määratakse kindlaks tingimused, mille alusel võib volituste delegeerimise peatada. Tegevdirektoril on õigus need volitused edasi delegeerida.

3. Erandlike asjaolude korral võib haldusnõukogu võtta vastu otsuse, millega ajutiselt peatatakse tegevdirektorile delegeeritud ja tema poolt edasi delegeeritud ametisse nimetava asutuse või ametiisiku volitused ning täidetakse kõnealuseid volitusi ise või delegeeritakse need ühele oma liikmetest või mõnele töötajale, välja arvatud tegevdirektorile.

Artikkel 29
Haldusnõukogu hääletuskord

1. Haldusnõukogu võtab otsused vastu oma hääleõiguslike liikmete absoluutse häälteenamusega, kui käesolevas määruses ei ole sätestatud teisiti.

2. Haldusnõukogu hääleõigusega liikmete kahekolmandikulist häälteenamust nõutakse järgmistel juhtudel:

a) artikli 28 lõike 1 punktis c osutatud ühtse programmdokumendi vastuvõtmine;

b) artikli 28 lõike 1 punktis e osutatud aastaeelarve vastuvõtmine;

c) tegevdirektori ja tegevdirektori asetäitja määramine, ametiaja pikendamine või ametist vabastamine, nagu on osutatud artiklites 31 ja 33;

d) apellatsiooninõukogu liikmete määramine ja ametist vabastamine, nagu on osutatud artiklis 36.

3. Eelarvet või personali käsitlevad otsused, eelkõige artikli 28 lõike 1 punktides c, e, f, g, h, i, k, l, m ja n osutatud küsimustes, võetakse vastu ainult juhul, kui komisjoni esindajad hääletavad otsuse poolt. Artikli 28 lõike 1 punktis c osutatud ENISA ühtset programmdokumenti käsitlevate otsuste vastuvõtmiseks nõutakse komisjoni esindajate poolthäält ainult otsuse nende elementide puhul, mis ei ole seotud ENISA iga-aastaste tööprogrammide ja mitmeaastase tööprogrammiga.

4. Igal hääleõiguslikul liikmel on üks hääl. Hääleõigusliku liikme puudumise korral võib tema eest hääletada tema asendusliige.

5. Haldusnõukogu esimees osaleb hääletamisel.

6. Tegevdirektor ei osale hääletamisel.

7. Haldusnõukogu kodukorraga kehtestatakse üksikasjalikum hääletamiskord, eelkõige tingimused, mille korral üks liige võib tegutseda teise liikme nimel.

2. jagu
Juhatus

Artikkel 30
Juhatus

1. Haldusnõukogu abistab juhatus.

2. Juhatus:

   a) valmistab ette haldusnõukogus vastu võetavad otsused;

   b) tagab koos haldusnõukoguga auditeerimise sise- ja välisaruannetest ja -hinnangutest, samuti OLAFi ja EPPO uurimistest tulenevate järelduste ja soovituste põhjal piisavate järelmeetmete võtmise;

   c) abistab ja nõustab tegevdirektorit haldusnõukogu otsuste rakendamisel eesmärgiga tugevdada haldus- ja eelarvejuhtimise järelevalvet, ilma et see piiraks tegevdirektori kohustuste täitmist, mis on sätestatud artiklis 32.

3. Juhatuse koosseisu kuuluvad haldusnõukogu esimees, üks komisjoni esindaja haldusnõukogus ning kolm muud liiget, kelle määrab haldusnõukogu oma hääleõigusega liikmete hulgast. Haldusnõukogu esimees on ühtlasi juhatuse esimees. Juhatuse liikmete ametisse nimetamisel püütakse saavutada tasakaalustatud sooline esindatus juhatuses. Tegevdirektor osaleb juhatuse koosolekutel hääleõiguseta.

4. Juhatuse liikmete ametiaeg on neli aastat. Neid võib ametisse tagasi nimetada. Juhatuse liikme ametiaeg lõpeb samal ajal tema liikmesuse lõppemisega haldusnõukogus.

5. Juhatus peab vähemalt ühe korralise koosoleku kvartalis. Lisaks toimuvad juhatuse koosolekud kas selle esimehe algatusel või liikmete taotlusel.

6. Haldusnõukogu kehtestab juhatuse kodukorra.

7. Kiireloomulistel juhtudel võib juhatus vajaduse korral teha haldusnõukogu nimel teatavaid esialgseid otsuseid, eeskätt halduskü simustes, sh ametisse nimetava asutuse volituste delegeerimise peatamise ja eelarveküsimuste kohta. Haldusnõukogu teavitatakse sellistest esialgsetest otsustest viivitamata. Haldusnõukogu otsustab seejärel hiljemalt kolme kuu möödumisel pärast esialgse otsuse tegemist, kas see heaks kiita või tagasi lükata. Juhatus ei tee haldusnõukogu nimel otsuseid, mille

tegemiseks on vaja haldusnõukogu hääleõigusega liikmete kahekolmandikulist häälteenamust.

3. jagu
Tegevdirektor

Artikkel 31
Ametisse nimetamine, ametist vabastamine ja ametiaja pikendamine

1. Tegevdirektori nimetab ametisse haldusnõukogu pädevuse ja oskuste alusel komisjoni esitatud kandidaatide nimekirjast pärast avatud ja läbipaistvat valikumenetlust.
2. Enne ametisse nimetamist kutsutakse haldusnõukogu valitud kandidaat esinema Euroopa Parlamendi pädeva komisjoni ette ja vastama parlamendiliikmete küsimustele.
3. Tegevdirektor võetakse tööle ENISA ajutise teenistujana vastavalt teenistustingimuste artikli 2 punktile a.
4. Tegevdirektoriga lepingu sõlmimisel on ENISA esindajaks haldusnõukogu esimees.
5. Tegevdirektori ametiaeg on viis aastat. Enne selle ajavahemiku lõppu koostab komisjon aegsasti hinnangu, milles võetakse arvesse tegevdirektori tegevusele antud hinnangut ning ENISA edasisi ülesandeid ja lahendamist vajavaid küsimusi.
6. Komisjoni ettepanekul, milles võetakse arvesse lõikes 5 osutatud hinnangut, võib haldusnõukogu pikendada tegevdirektori ametiaega ühe korra kuni viieks aastaks.
7. Tegevdirektor, kelle ametiaega on pikendatud, ei või oma teise ametiaja lõpus osaleda uues sama ametikoha täitmiseks korraldatud valikumenetluses.
8. Haldusnõukogu teavitab Euroopa Parlamenti kavatsusest pikendada tegevdirektori ametiaega kooskõlas lõikega 6. Kolme kuu jooksul enne ametiaja pikendamist esineb tegevdirektor Euroopa Parlamendi pädeva komisjoni kutsel selle ees ja vastab parlamendiliikmete küsimustele.
9. Tegevdirektori võib ametist tagandada üksnes otsusega, mille haldusnõukogu teeb komisjoni ettepanekul.

Artikkel 32
Tegevdirektori ülesanded ja kohustused

1. Tegevdirektor juhib ENISAt ja annab aru haldusnõukogule.
2. Tegevdirektor on oma ametikohustuste täitmisel sõltumatu ning ei küsi ega saa juhiseid üheltki valitsuselt ega muult organilt.
3. Tegevdirektor annab Euroopa Parlamendile oma ülesannete täitmisest aru, kui temalt seda palutakse. Nõukogu võib tegevdirektorilt tema ülesannete täitmise kohta aru pärida.
4. Tegevdirektor on ENISA seaduslik esindaja.
5. Tegevdirektor vastutab käesoleva määrusega ENISA-le pandud ülesannete täitmise eest. Eelkõige teeb tegevdirektor järgmist:
   a) tagab ENISA igapäevase töö juhtimise;

b) rakendab haldusnõukogu otsuseid;

c) tagab ENISA finantsreeglite täitmise;

d) koostab ühtse programmdokumendi kavandi ja esitab selle heakskiitmiseks haldusnõukogule enne, kui see esitatakse komisjonile arvamuse saamiseks;

e) rakendab ühtset programmdokumenti ja annab haldusnõukogule aru selle rakendamise kohta;

f) koostab ENISA konsolideeritud iga-aastase tegevusaruande, sh ENISA iga-aastase tööprogrammi rakendamise kohta, ning esitab selle hindamiseks ja vastuvõtmiseks haldusnõukogule;

g) koostab artiklis 121 osutatud ENISA järelhindamise järelduste põhjal võetavaid järelmeetmeid sisaldava tegevuskava ning esitab iga kahe aasta järel komisjonile aruande edusammude kohta;

h) koostab tegevuskava sise- või välisauditiaruannete ja hindamiste ning OLAFi ja EPPO juurdluste järelduste põhjal järelmeetmete võtmiseks ning annab komisjonile kaks korda aastas ja haldusnõukogule korrapäraselt aru tehtud edusammude kohta;

i) koostab artiklis 50 osutatud ENISA suhtes kohaldatavate finantsreeglite kavandi;

j) koostab ENISA tulude ja kulude eelarvestuse projekti ning täidab ENISA eelarvet;

k) kaitseb liidu finantshuve, rakendades pettuste, korruptsiooni ja muu ebaseadusliku tegevuse vastu võitlemiseks ennetusmeetmeid, ilma et see piiraks OLAFi ja EPPO juurdluspädevust, tehes tulemuslikke kontrolle, nõudes õigusnormide rikkumise avastamise korral sisse alusetult makstud summad ning rakendades vajaduse korral mõjusaid, proportsionaalseid ja hoiatavaid haldus- ja rahalisi karistusi;

l) koostab ENISA pettustevastase võitluse strateegia, tõhususe kasvu ja koostoime strateegia, kolmandate riikide ja rahvusvaheliste organisatsioonidega tehtava koostöö strateegia ning organisatsiooni juhtimise ja sisekontrollisüsteemide strateegia ning esitab need haldusnõukogule heakskiitmiseks;

m) arendab ja hoiab kontakte äriringkondade ja tarbijaorganisatsioonidega, et tagada korrapärane dialoog asjaomaste sidusrühmadega;

n) vahetab korrapäraselt arvamusi ja teavet asjaomaste liidu üksustega nende tegevuse kohta, mis on seotud küberturvalisusega, et tagada selles valdkonnas liidu poliitika rakendamise sidusus;

o) edendab mitmekesisust ja soolist tasakaalu ENISA töötajate värbamisel;

p) võtab vastu Euroopa individuaalsete küberturbeoskuste tõendamise kavad, nagu on osutatud artikli 20 lõikes 1;

q) võtab vastu otsused, mille alusel taotluse esitajad saavad volitatud tõendajaks, või uuendab nende volitusi, nagu on osutatud artikli 22 lõikes 3;

r) täidab muid käesoleva määrusega tegevdirektorile pandud ülesandeid.

6. Vajaduse korral ning kooskõlas ENISA eesmärkide ja ülesannetega võib tegevdirektor moodustada ajutisi töörühmi, kuhu kuuluvad eksperdid, sealhulgas liikmesriikide pädevate asutuste eksperdid. Tegevdirektor teavitab sellest eelnevalt haldusnõukogu. ENISA sise-eeskirjas sätestatakse eeskätt töörühmade koosseisu, tegevdirektori poolt töörühmade ekspertide määramist ja töörühmade tegevust käsitlev kord.

7. Vajaduse korral ja kohasele kulude-tulude analüüsile tuginedes võib tegevdirektor otsustada ENISA ülesannete tõhusaks ja tulemuslikuks täitmiseks asutada ühes või mitmes liikmesriigis kohaliku(d) kontori(d). Enne kui tegevdirektor otsustab asutada kohaliku kontori, peab ta küsima asjaomaste liikmesriikide, sh ENISA asukohaliikmesriigi arvamust ning saama komisjonilt ja haldusnõukogult eelneva nõusoleku. Kui konsulteerimise käigus lähevad tegevdirektori ja asjaomaste liikmesriikide arvamused lahku, esitatakse küsimus arutamiseks nõukogule. Töötajate koguarv kõigis kohalikes kontorites peab olema minimaalne ega tohi moodustada kokku rohkem kui 40 % ENISA asukohaliikmesriigis asuvate ENISA töötajate koguarvust. Ühegi kohaliku kontori puhul ei tohi töötajate arv olla suurem kui 10 % ENISA asukohaliikmesriigis asuvate ENISA töötajate koguarvust.

8. Kohaliku kontori asutamise otsuses määratakse kindlaks kohaliku kontori tegevuse ulatus, et vältida tarbetuid kulusid ja ENISA haldusülesannete dubleerimist.

4. jagu
Tegevdirektori asetäitja

Artikkel 33
Tegevdirektori asetäitja

1. Haldusnõukogu võib otsustada luua tegevdirektorit tema töös abistava asetäitja ametikoha.

2. Kui haldusnõukogu otsustab luua tegevdirektori asetäitja ametikoha, kohaldatakse tegevdirektori asetäitja suhtes artikli 31 sätteid.

Artikkel 34
Tegevdirektori asetäitja ülesanded ja kohustused

Tegevdirektori asetäitja abistab tegevdirektorit ENISA juhtimisel ja artiklis 32 osutatud ülesannete täitmisel. Kui tegevdirektor ei ole kohal või ei saa oma kohustusi täita või ametikoht on vaba, täidab tema puudumise ajal või kuni ametikoha täitmiseni tema ülesandeid tegevdirektori asetäitja.

5. jagu
ENISA nõuanderühm

Artikkel 35
ENISA nõuanderühm

1. Haldusnõukogu loob tegevdirektori ettepanekul läbipaistval viisil ENISA nõuanderühma. ENISA nõuanderühm koosneb tunnustatud ekspertidest, kes esindavad asjaomaseid sidusrühmi, nagu küberturvalisuse tööstus, IKT-tööstus,

VKEd, direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorites tegutsevad üksused, digielemente sisaldavate toodete valmistajad ja avatud lähtekoodiga tarkvara korraldajad määruse (EL) 2024/2847 tähenduses, vastavushindamisasutused, millest on teavitatud artiklis 93 osutatud Euroopa küberturvalisuse sertifitseerimise raamistiku ja määruse (EL) 2024/2847 alusel, e-identimise vahendite valdkonnas tegutsevad üksused, tarbijarühmad, küberturvalisuse valdkonna akadeemilised eksperdid, Euroopa standardiorganisatsioonid ning samuti õiguskaitse ja andmekaitse järelevalveasutused. Kõnealused tunnustatud eksperdid peavad olema liikmesriikide kodanikud. Haldusnõukogu eesmärk on tagada asjakohane sooline ja geograafiline tasakaal ning tasakaal erinevate sidusrühmade vahel.

2. ENISA sise-eeskirjas sätestatakse eeskätt ENISA nõuanderühma koosseisu, lõikes 1 osutatud tegevdirektori ettepanekut, liikmete arvu ja nimetamist ning ENISA nõuanderühma tegevust käsitlev kord ning see avalikustatakse.

3. ENISA nõuanderühma juhatab tegevdirektor või isik, kelle tegevdirektor nimetab igal üksikjuhul eraldi.

4. ENISA nõuanderühma liikmete ametiaeg on kaks ja pool aastat ja seda saab ühe korra pikendada. Haldusnõukogu liige ei või olla ENISA nõuanderühma liige. Komisjoni ja liikmesriikide ekspertidel on õigus viibida ENISA nõuanderühma koosolekutel ning osaleda selle töös. Tegevdirektor võib kutsuda ENISA nõuanderühma koosolekutel ning selle töös osalema teiste asutuste esindajaid, kes ei ole ENISA nõuanderühma liikmed.

5. ENISA nõuanderühm nõustab ENISAt tema ülesannete täitmisel, välja arvatud seoses käesoleva määruse III, IV ja V jaotise kohaldamisega. Eelkõige annab ENISA nõuanderühm tegevdirektorile nõu ENISA iga-aastase tööprogrammi ettepaneku koostamise kohta ning teabevahetuse tagamise kohta asjaomaste sidusrühmadega iga-aastase tööprogrammiga seotud küsimustes.

6. ENISA nõuanderühm teavitab korrapäraselt haldusnõukogu oma tegevusest.

7. ENISA annab ENISA nõuanderühmale vajalikku logistilist abi ning tagab koosolekuteks sekretariaaditeenused.

6. jagu
Apellatsiooninõukogu

Artikkel 36
Apellatsiooninõukogu moodustamine ja koosseis

1. ENISA asutab haldusnõukogu otsusega apellatsiooninõukogu.

2. Apellatsiooninõukogu koosneb esimehest ja kolmest liikmest. Igal apellatsiooninõukogu liikmel on asendusliige. Asendusliige esindab täisliiget tema puudumise korral.

3. Haldusnõukogu nimetab esimehe, ülejäänud liikmed ja nende asendusliikmed komisjoni esitatud kvalifitseeritud kandidaatide nimekirjast. Kvalifitseeritud kandidaatide nimekiri kehtib neli aastat. Haldusnõukogu võib komisjoni ettepaneku alusel pikendada nimekirja kehtivust täiendavate nelja-aastaste ajavahemike kaupa.

4. Kui apellatsiooninõukogu peab menetletava kaebuse puhul seda vajalikuks, võib ta haldusnõukogu taotluse korral nimetada asjaomase juhtumi menetlemiseks lõikes 3 osutatud nimekirjast veel kaks liiget ja nende asendusliikmed.

5. Apellatsiooninõukogu võtab vastu ja avalikustab oma kodukorra.

Artikkel 37
Apellatsiooninõukogu liikmed

1. Apellatsiooninõukogu liikmete ja asendusliikmete ametiaeg on neli aastat. Haldusnõukogu võib nende ametiaega komisjoni ettepaneku alusel pikendada täiendavate nelja-aastaste ajavahemike kaupa.

2. Apellatsiooninõukogu liikmed on sõltumatud ega täida ENISAs ühtki muud ülesannet. Otsuste tegemisel ei või nad taotleda ega vastu võtta juhiseid üheltki valitsuselt, muult organilt ega erasektori üksuselt.

3. Apellatsiooninõukogu liikmeid ei või nende ametiaja jooksul ametist tagasi kutsuda ega kvalifitseeritud kandidaatide nimekirjast kustutada, välja arvatud juhul, kui selleks on mõjuvad põhjused ja kui haldusnõukogu teeb komisjoni soovituse alusel sellekohase otsuse.

Artikkel 38
Väljaarvamine ja vastuväidete esitamine

1. Apellatsiooninõukogu liikmed ei osale kaebemenetluses, kui neil on menetlusega seotud isiklikud huvid, kui nad on olnud varem menetluse ühe osalise esindajad või kui nad on osalenud edasikaevatud otsuse vastuvõtmises.

2. Kui apellatsiooninõukogu liige leiab ühel lõikes 1 loetletud põhjusel või mis tahes muul põhjusel, et ta ei peaks osalema kaebuse menetlemises, teatab ta sellest apellatsiooninõukogule.

3. Kaebemenetluse osaline võib taotleda apellatsiooninõukogu liikme taandamist kõikidel lõikes 1 osutatud põhjustel või juhul, kui liiget kahtlustatakse erapoolikuses. Sellist taandamistaotlust ei võeta vastu, kui kaebemenetluse osaline on juba alustanud menetlust, olles samas teadlik taandamistaotluse põhjusest. Vastuväited ei tohi põhineda apellatsiooninõukogu liikmete kodakondsusel.

4. Apellatsiooninõukogu teeb otsuse lõigetes 2 ja 3 sätestatud juhtudel võetavate meetmete kohta ilma asjaomase liikme osavõtuta. Asjaomane liige asendatakse selle otsuse tegemiseks apellatsiooninõukogus tema asendajaga.

Artikkel 39
Otsuste ja tegevusetuse peale kaebamine

1. Apellatsiooninõukogule võidakse esitada kaebus:

   a) otsuste kohta, mille ENISA on vastu võtnud vastavalt artikli 22 lõikele 3;

   b) ENISA suutmatuse kohta tegutseda artikli 22 lõikes 4 sätestatud kohaldatava tähtaja jooksul.

2. Lõike 1 kohaselt esitatud kaebus kuulub kooskõlas artikliga 41 esialgsele läbivaatamisele, enne kui see esitatakse apellatsiooninõukogule läbivaatamiseks.

3. Lõike 1 kohaselt esitatud kaebus ei peata otsuse täitmist.

Artikkel 40
Kaebeõigusega isikud, kaebetähtaeg ja kaebuse vorm

1. Taotluse esitajad artikli 21 lõike 3 tähenduses võivad esitada kaebuse järgmise kohta:

   a) artikli 22 lõike 3 kohaselt neile adresseeritud ENISA otsus;

   b) ENISA suutmatus tegutseda nende poolt ENISA-le esitatud taotluse suhtes artikli 22 lõikes 4 sätestatud kohaldatava tähtaja jooksul.

2. Lõike 1 punktis a osutatud juhul esitatakse kaebus koos selle põhjendustega kirjalikult kooskõlas artikli 36 lõikes 5 osutatud kodukorraga kahe kuu jooksul alates otsuses asjaomasele taotluse esitajale teatavaks tegemisest või selle puudumise korral päevast, kui taotluse esitaja sai otsusest teada.

3. Lõike 1 punktis b osutatud juhul esitatakse kaebus ENISA-le kirjalikult kooskõlas artikli 36 lõikes 5 osutatud kodukorraga kahe kuu jooksul alates artikli 22 lõikes 4 sätestatud tähtaja möödumise kuupäevast.

Artikkel 41
Esialgne läbivaatamine

1. Kui ENISA leiab, et kaebus on vastuvõetav ja põhjendatud, parandab ta artikli 40 lõikes 1 viidatud otsust või tegevusetust.

2. Kui ENISA ei paranda otsust ühe kuu jooksul alates kaebuse laekumisest, otsustab ta viivitamata, kas peatada otsuse kohaldamine, ning edastab kaebuse edasiseks lahendamiseks apellatsiooninõukogule.

Artikkel 42
Kaebuste kohta tehtud otsuste läbivaatamine

1. Apellatsiooninõukogu otsustab kolme kuu jooksul pärast kaebuse esitamist, kas rahuldada kaebus või lükata see tagasi. Kaebuse läbivaatamisel tegutseb apellatsiooninõukogu selle kodukorras sätestatud tähtaegade piires. Ta kutsub nii sageli kui vajalik kaebemenetluse osalisi esitama kindlaksmääratud aja jooksul märkusi enda saadetud teadete või teiste kaebemenetluse osaliste avalduste kohta. Apellatsioonimenetluse osalistel on õigus anda suulisi seletusi.

2. Kui apellatsiooninõukogu leiab, et kaebus on põhjendatud, saadab ta juhtumi tagasi ENISA-le. ENISA teeb kooskõlas apellatsiooninõukogu järeldustega oma lõpliku otsuse ja põhjendab seda. ENISA teavitab asjakohaselt kaebemenetluse osalisi.

Artikkel 43
Asja andmine Euroopa Liidu Kohtusse

1. Artikli 22 lõike 3 kohaselt vastu võetud ENISA otsuste tühistamist või artikli 22 lõike 4 kohaselt kohaldatavate tähtaegade jooksul tegevuse puudumist käsitlevad hagid võib esitada Euroopa Liidu Kohtusse pärast artiklites 39–42 sätestatud ENISA apellatsioonimenetluse lõppu või kui artikli 41 lõike 2 kohaselt ei ole tegutsetud kohaldatava tähtaja piires.

2. ENISA võtab kõik vajalikud meetmed Euroopa Liidu Kohtu otsuse täitmiseks.

7. jagu
Tegevus

Artikkel 44
Ühtne programmdokument

1. ENISA tegutseb kooskõlas ühtse programmdokumendiga, mis sisaldab ENISA iga-aastast ja mitmeaastast tööprogrammi ning mis hõlmab kõiki ENISA kavandatud tegevusi.

2. Tegevdirektor koostab igal aastal lõikes 1 osutatud ühtse programmdokumendi kavandi ning sellele vastava finants- ja inimressursside kavandamise kooskõlas komisjoni delegeeritud määruse (EL) nr 2019/715[74] artikliga 32, võttes arvesse komisjoni kehtestatud suuniseid.

3. Haldusnõukogu võtab lõikes 1 osutatud ühtse programmdokumendi vastu iga aasta 30. novembriks, võttes arvesse delegeeritud määruse (EL) 2019/715 artikli 32 lõikes 7 osutatud komisjoni arvamust. Kui haldusnõukogu otsustab komisjoni arvamuse mis tahes aspekti mitte arvesse võtta, peab ta seda otsust põhjalikult põhjendama. Haldusnõukogu saadab ühtse programmdokumendi Euroopa Parlamendile, nõukogule ja komisjonile hiljemalt järgmise aasta 31. jaanuariks ja edastab neile ka kõik selle hilisemad ajakohastatud versioonid.

4. Ühtne programmdokument muutub lõplikuks pärast liidu üldeelarve lõplikku vastuvõtmist ja vajaduse korral kohandatakse seda vastavalt.

5. Iga-aastane tööprogramm sisaldab üksikasjalikke eesmärke ja eeldatavaid tulemusi, sh tulemusnäitajaid. Samuti sisaldab see rahastatavate meetmete kirjeldust koos igale meetmele eraldatavate rahaliste vahendite ja inimressurssidega vastavalt tegevuspõhise eelarvestamise ja juhtimise põhimõtetele. Iga-aastane tööprogramm peab olema kooskõlas lõikes 7 osutatud mitmeaastase tööprogrammiga. Selles näidatakse selgelt ära ülesanded, mis võrreldes eelmise eelarveaastaga on lisatud või välja jäetud või mida on muudetud.

6. Kui ENISA-le pannakse uus ülesanne, muudab haldusnõukogu vastuvõetud iga-aastast tööprogrammi. Kõik iga-aastase tööprogrammi olulised muudatused võetakse vastu sama korra kohaselt nagu algne iga-aastane tööprogramm. Haldusnõukogu võib delegeerida tegevdirektorile õiguse teha iga-aastases tööprogrammis vähetähtsaid muudatusi.

7. Mitmeaastases tööprogrammis esitatakse üldine strateegiline programm, sh eesmärgid, oodatavad tulemused ja tulemusnäitajad. Selles esitatakse ka vahendite eraldamise programm, mis hõlmab muu hulgas mitmeaastast eelarvet ja personali.

8. Vahendite eraldamise programmi ajakohastatakse igal aastal. Strateegilist programmi ajakohastatakse, kui selle järele on vajadus, eeskätt artiklis 120 osutatud hindamise tulemuste arvesse võtmiseks.

---

[74] Komisjoni 18. detsembri 2018. aasta delegeeritud määrus (EL) 2019/715 raamfinantsmääruse kohta asutustele, mis on asutatud Euroopa Liidu toimimise lepingu ja Euroopa Aatomienergiaühenduse asutamislepingu alusel ning millele osutatakse Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) 2018/1046 artiklis 70 (ELT L 122, 10.5.2019, lk 1, ELI: http://data.europa.eu/eli/reg_del/2019/715/oj).

IV PEATÜKK
ENISA eelarve koostamine ja struktuur

Artikkel 45
ENISA eelarve koostamine

1. Tegevdirektor koostab igal aastal ENISA järgmise eelarveaasta tulude ja kulude esialgse eelarvestuse projekti, mis sisaldab ametikohtade loetelu, ning edastab selle haldusnõukogule.
2. Esialgne eelarvestuse projekt põhineb iga-aastase tööprogrammi eesmärkidel ja oodatavatel tulemustel ning selles võetakse arvesse nende eesmärkide ja oodatavate tulemuste saavutamiseks vajalikke rahalisi vahendeid, järgides usaldusväärse finantsjuhtimise põhimõtet ja tulemuspõhisust.
3. Esialgse eelarvestuse projekti põhjal võtab haldusnõukogu vastu ENISA järgmise eelarveaasta tulude ja kulude eelarvestuse projekti ning saadab selle komisjonile iga aasta 31. jaanuariks.
4. Komisjon edastab eelarvestuse projekti eelarvepädevatele institutsioonidele koos liidu üldeelarve projektiga. Eelarvestuse projekt tehakse kättesaadavaks ka ENISA-le.
5. Selle eelarvestuse projekti põhjal kannab komisjon liidu üldeelarve projekti kalkulatsioonid, mida ta peab ametikohtade loetelu põhjal vajalikuks, ning liidu üldeelarvest eraldatava toetuse summa, ning esitab selle kooskõlas ELi toimimise lepingu artiklitega 313 ja 314 eelarvepädevatele institutsioonidele.
6. Eelarvepädevad institutsioonid kinnitavad liidu üldeelarvest ENISA toetuseks eraldatavad assigneeringud.
7. Eelarvepädevad institutsioonid võtavad vastu ENISA ametikohtade loetelu.
8. Haldusnõukogu võtab vastu ENISA eelarve. See muutub lõplikuks pärast liidu üldeelarve lõplikku vastuvõtmist ja kui see on vajalik, tehakse selles vastavad kohandused.
9. Hoonetega seotud projektide suhtes, mis võivad märkimisväärselt mõjutada ENISA eelarvet, kohaldatakse delegeeritud määrust (EL) 2019/715.

Artikkel 46
ENISA eelarve struktuur

1. Igal eelarveaastal koostatakse ENISA kõikide tulude ja kulude eelarvestus, mis esitatakse ENISA eelarves. Eelarveaasta vastab kalendriaastale.
2. ENISA eelarve tulud ja kulud peavad olema tasakaalus.
3. Ilma et see piiraks muid sissetulekuallikaid, koosnevad ENISA tulud järgmistest vahenditest:
   a) liidu osamaks, mis on kantud liidu üldeelarvesse;
   b) tulu, mis on ette nähtud konkreetsete kuluartiklite rahastamiseks kooskõlas artiklis 50 osutatud finantsreeglitega;
   c) liidu rahalised vahendid rahalise toetuse andmise kokkulepete või sihtotstarbeliste toetuste vormis kooskõlas artiklis 50 osutatud ENISA

finantsreeglite ja liidu poliitikavaldkondade toetamiseks mõeldud rahastamisvahendeid käsitlevate asjaomaste sätetega;

d) artikli 22 lõikes 1 osutatud Euroopa individuaalsete küberturbeoskuste tõendamise kavadega seotud tegevuse eest taotluse esitajatelt nõutavad tasud;

e) tasud, mida nõutakse vastavushindamisasutustelt artikli 47 lõikes 2 osutatud Euroopa küberturvalisuse sertifitseerimise kavas osalemise ja selle alusel Euroopa küberturvalisuse sertifikaatide väljastamise eest;

f) avaliku või erasektori asutustelt artikli 47 lõikes 3 osutatud testimisvahendite eest nõutavad tasud;

g) ENISA töös osalevate kolmandate riikide osamaksed vastavalt artikli 70 lõikele 4;

h) liikmesriikide vabatahtlikud rahalised või mitterahalised osamaksed.

4. Lõike 3 punktis g osutatud vabatahtlikke osamakseid tegevatel liikmesriikidel ei ole õigust nõuda sellest tulenevalt konkreetseid õigusi või teenuseid.

5. ENISA kulud hõlmavad personali töötasu, haldus- ja taristukulusid ning tegevuskulusid.

Artikkel 47
Tasud

1. Iga artikli 22 lõikes 1 osutatud Euroopa tõendamiskava tegevuse puhul nõutakse artikli 21 lõike 3 tähenduses taotluse esitajatelt või volitatud tõendajatelt järgmisi tasusid, et katta ENISA tehtud toimingute täielikud kulud:

a) lubade andmine pärast artikli 21 lõigetes 3 ja 4 sätestatud nõuete läbivaatamist, sh hindamine;

b) lubade iga-aastane säilitamine;

c) Euroopa individuaalsete küberturbeoskuste tõendajate volituste uuendamine, sh hindamine.

2. Sertifitseerimise puhul nõutakse vastavushindamisasutustelt Euroopa küberturvalisuse sertifikaatide väljastamise aluseks olevate Euroopa küberturvalisuse sertifitseerimise kavade haldamise eest järgmisi tasusid:

a) Euroopa küberturvalisuse sertifitseerimise kavas osalemise iga-aastane tasu;

b) tasu Euroopa küberturvalisuse sertifitseerimise kavade alusel Euroopa küberturvalisuse sertifikaatide väljastamise eest.

Punktis b osutatud tasusid nõutakse, kui vastavushindamisasutus esitab Euroopa küberturvalisuse sertifikaadid ENISA-le tema veebisaidil avaldamiseks kooskõlas artikliga 79.

3. Artikli 15 lõikes 1 osutatud testimisvahendite puhul nõutakse nende kasutamise eest tasu mis tahes avaliku või erasektori asutuselt.

4. Tasud esitatakse ja tasutakse eurodes.

5. Komisjon võtab vastu rakendusaktid, millega kehtestatakse üksikasjalikud normid ENISA nõutavate tasude kindlaksmääramiseks, määrates eelkõige kindlaks lõigete 1, 2 ja 3 kohaselt maksmisele kuuluvate tasude igale elemendile omistatavad

hinnangulised kulud ja maksmisele kuuluvad individuaalsed tasusummad ning tasude maksmise viisid ja tingimused. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega. Komisjon konsulteerib kõnealuste rakendusaktide eelnõude koostamisel ENISAga.

6. Lõikes 5 osutatud rakendusaktidega kindlaks määratud tasud määratakse eelnevalt kindlaks, et need oleksid proportsionaalsed elluviidava tegevuse või osutatavate teenuste hinnanguliste kuludega, mis on määratud kindlaks kulutõhusal viisil ja on piisavad kõnealuste kulude katmiseks. Kõik ENISA kulud, mis on omistatavad lõigetes 1, 2 ja 3 osutatud tegevuses osalevatele töötajatele, kajastatakse kaetavates kuludes. Tasud kehtestatakse sellisel tasemel, millega hoitakse ära ENISA eelarve puudujääk või märkimisväärse ülejäägi tekkimine. Tasude läbi tekkinud eelarveülejääk kantakse üle, et rahastada ENISA tegevust, eelkõige tasudega seotud tulevast tegevust, või tekkinud kahju katmiseks. Kui tasudega hõlmatud tegevusest tulenev märkimisväärne positiivne eelarvesaldo muutub korduvaks, või kui tasudega kaetud teenuste osutamisest tuleneb märkimisväärne negatiivne saldo, siis muudab komisjon lõikes 5 osutatud rakendusakte, et korrigeerida kõnealuste tasude arvutamise meetodit kooskõlas artikli 118 lõikega 2.

   Lõikes 1 osutatud ülesannete tasude summa määratakse kindlaks sellisel tasemel, et tagada nendest tekkiva tulu abil Euroopa individuaalsete tõendamiskavade koostamise ja haldamisega seotud tegevuse kulude piisav katmine, taotluste menetlemine ning lubade väljastamine ja uuendamine ning ENISA vajalik järelevalvetegevus.

   Lõikes 2 osutatud ülesannete tasude summa määratakse kindlaks sellisel tasemel, et tagada nende tulu abil artiklis 75 sätestatud Euroopa küberturvalisuse sertifitseerimise kavade haldamisega soetud tegevuse täielike kulude piisav katmine.

   Lõikes 3 osutatud ülesannete tasude summa määratakse kindlaks sellisel tasemel, et tagada nendest tekkiva tulu abil artikli 15 lõikes 1 sätestatud testimisvahendite pakkumisega seotud tegevuse kulude piisav katmine.

7. ENISA esitab aruande nõutavate tasude ja neist eelarvele tekkiva mõju kohta osana artiklis 50 sätestatud raamatupidamisarvestuse esitamise menetlusest.

8. ENISA võtab kasutusele näitajate komplekti, et mõõta tasudest rahastatava tegevusega seotud töökoormust, tulemuslikkust ja tõhusust. ENISA kohandab oma personali kavandamist ja ressursside haldamist seoses tasudega vastavalt, et ta suudaks piisavalt reageerida kõnealusele nõudlusele ning tasudest saadava tulu mis tahes kõikumistele. ENISA jagab komisjoniga aruannet, mida komisjon võib kasutada artikli 120 lõikes 1 osutatud hindamise otstarbel.

Artikkel 48
ENISA eelarve täitmine

1. ENISA eelarve täitmise eest vastutab tegevdirektor, kes tegutseb ka eelarvevahendite käsutajana.

2. Komisjoni siseaudiitoril on ENISA suhtes samad volitused kui komisjoni talituste suhtes.

3. Tegevdirektor saadab eelarvepädevatele institutsioonidele igal aastal kogu asjaomase teabe kõigi hindamismenetluste tulemuste kohta.

Artikkel 49

Raamatupidamisaruannete esitamine ja eelarve täitmisele heakskiidu andmine

1. ENISA peaarvepidaja saadab eelarveaasta (aasta N) esialgse raamatupidamise aastaaruande komisjoni peaarvepidajale ja kontrollikojale järgmise eelarveaasta (aasta N + 1) 1. märtsiks.

2. ENISA peaarvepidaja esitab konsolideerimise otstarbel vajaliku raamatupidamisteabe aasta N + 1 1. märtsiks nõutaval viisil ja nõutavas vormingus komisjoni peaarvepidajale.

3. ENISA saadab aasta N eelarvehalduse ja finantsjuhtimise aruande Euroopa Parlamendile, nõukogule ja kontrollikojale 31. märtsiks aastal N + 1.

4. Kui on laekunud kontrollikoja märkused aasta N ENISA esialgsete raamatupidamise aastaaruannete kohta, siis koostab ENISA peaarvepidaja omal vastutusel ENISA lõpliku raamatupidamise aastaaruande. Tegevdirektor esitab selle haldusnõukogule arvamuse saamiseks.

5. Haldusnõukogu esitab ENISA lõpliku raamatupidamise aasta N aruande kohta arvamuse.

6. ENISA peaarvepidaja saadab aasta N + 1 1. juuliks aasta N lõpliku raamatupidamise aastaaruande ja haldusnõukogu arvamuse Euroopa Parlamendile, nõukogule, komisjonile ja kontrollikojale.

7. Link ENISA lõplikku raamatupidamise aastaaruannet sisaldavatele veebilehtedele avaldatakse *Euroopa Liidu Teatajas* aasta N + 1 15. novembriks.

8. Tegevdirektor saadab kontrollikojale vastuse kontrollikoja aastaaruandes esitatud tähelepanekute kohta 30. septembriks aastal N + 1. Tegevdirektor saadab kõnealuse vastuse ka haldusnõukogule ja komisjonile.

9. Tegevdirektor esitab Euroopa Parlamendi taotluse korral parlamendile kogu teabe, mida on vaja aasta N eelarve täitmisele heakskiidu andmise menetluse tõrgeteta kohaldamiseks vastavalt Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) 2024/2509 artikli 267 lõikele 3.

10. Kvalifitseeritud häälteenamusega otsuse teinud nõukogu soovituse põhjal annab Euroopa Parlament enne 15. maid aastal N + 2 heakskiidu tegevdirektori tegevusele aasta N eelarve täitmisel.

Artikkel 50

Finantsreeglid

1. Haldusnõukogu võtab pärast komisjoniga konsulteerimist vastu ENISA suhtes kohaldatavad finantsreeglid. Need ei või lahkneda delegeeritud määrusest (EL) 2019/715, välja arvatud juhul, kui see on konkreetselt vajalik ENISA toimimiseks ja komisjon on selleks eelnevalt nõusoleku andnud.

2. ENISA koostab oma eelarve ja täidab seda kooskõlas oma finantsreeglite ja määrusega (EL, Euratom) 2024/2509.

Artikkel 51
Pettustevastane võitlus

1. Pettuste, korruptsiooni ja muude õigusvastaste tegude vastu võitlemiseks kohaldatakse ENISA tegevuse suhtes piiranguteta Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) nr 883/2013[75].

2. ENISA ühineb 25. mai 1999. aasta institutsioonidevahelise kokkuleppega Euroopa Parlamendi, Euroopa Liidu Nõukogu ja Euroopa Ühenduste Komisjoni vahel, mis käsitleb Euroopa Pettustevastase Ameti (OLAF) sisejuurdlust,[76] kuue kuu jooksul alates [*Väljaannete Talitus: palun lisada artiklis 127 osutatud täpne kuupäev*] ja võtab kõnealuse kokkuleppe lisas esitatud vormis viivitamata vastu kõigi tema töötajate suhtes kohaldatavad asjakohased sätted.

3. Kontrollikojal on õigus auditeerida nii dokumentide alusel kui ka kontrollida kohapeal kõiki toetusesaajaid, töövõtjaid ja alltöövõtjaid, keda ENISA on rahastanud liidu vahenditest.

4. OLAF võib määruses (EL, Euratom) nr 883/2013 ja nõukogu määruses (Euratom, EÜ) nr 2185/96[77] sätestatud korra kohaselt läbi viia uurimisi, sh kohapealseid kontrolle ja inspekteerimisi, et teha kindlaks, kas seoses ENISA rahastatud toetuse või lepinguga on esinenud pettust, korruptsiooni või muud liidu finantshuve kahjustavat ebaseaduslikku tegevust.

5. Ilma et see piiraks lõigete 1–4 kohaldamist, sisaldavad ENISA ning kolmandate riikide ja rahvusvaheliste organisatsioonide vahelised töökokkulepped ning ENISA lepingud, toetuslepingud ja toetuse määramise otsused sätteid, mis annavad kontrollikojale ja OLAFile sõnaselgelt õiguse korraldada oma vastava pädevuse piires sellist auditeerimist ja uurimist.

6. Vastavalt nõukogu määrusele (EL) 2017/1939 võib EPPO uurida pettusi ja muid ebaseaduslikke toiminguid, mis mõjutavad liidu finantshuve, ja esitada nende kohta süüdistusi, nagu on ette nähtud Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2017/1371[78].

Artikkel 52
Huvide deklaratsioon

1. Haldusnõukogu liikmed, tegevdirektor, tegevdirektori asetäitja ja liikmesriikide poolt ajutiselt lähetatud ametnikud esitavad kohustuste deklaratsiooni ning deklaratsiooni, milles nad kinnitavad, et neil puudub või on olemas otsene või kaudne huvi, mida

---

75 Euroopa Parlamendi ja nõukogu 11. septembri 2013. aasta määrus (EL, Euratom) nr 883/2013, mis käsitleb Euroopa Pettustevastase Ameti (OLAF) juurdlusi ning millega tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1073/1999 ja nõukogu määrus (Euratom) nr 1074/1999 (ELT L 248, 18.9.2013, lk 1, ELI: http://data.europa.eu/eli/reg/2013/883/oj).

76 EÜT L 136, 31.5.1999, lk 15, ELI: http://data.europa.eu/eli/agree_interinstit/1999/531/oj.

77 Nõukogu 11. novembri 1996. aasta määrus (Euratom, EÜ) nr 2185/96, mis käsitleb komisjoni tehtavat kohapealset kontrolli ja inspekteerimist, et kaitsta Euroopa ühenduste finantshuve pettuste ja igasuguse muu eeskirjade eiramiste eest (EÜT L 292, 15.11.1996, lk 2, ELI: http://data.europa.eu/eli/reg/1996/2185/oj).

78 Euroopa Parlamendi ja nõukogu 5. juuli 2017. aasta direktiiv (EL) 2017/1371, mis käsitleb võitlust liidu finantshuve kahjustavate pettuste vastu kriminaalõiguse abil (ELT L 198, 28.7.2017, lk 29, ELI: http://data.europa.eu/eli/dir/2017/1371/oj).

võib pidada nende sõltumatust kahjustavaks. Deklaratsioon peab olema täpne ja täielik, see esitatakse kirjalikult kord aastas ja vajaduse korral seda ajakohastatakse.

2. Haldusnõukogu liikmed, tegevdirektor, tegevdirektori asetäitja ning ajutistes töörühmades osalevad väliseksperdid esitavad hiljemalt iga koosoleku alguses täpse ja täieliku deklaratsiooni oma huvide kohta, mida võib pidada päevakorraküsimusega seoses nende sõltumatust kahjustavaks, ning nad ei võta osa selliste küsimuste arutamisest ega hääletusest.

3. ENISA sätestab oma sise-eeskirjas lõigetes 1 ja 2 osutatud huvide deklaratsioone käsitlevate normide rakendamise praktilise korra.

Artikkel 53
Läbipaistvus

1. ENISA viib oma tegevust läbi maksimaalselt läbipaistvalt ning kooskõlas artikliga 55.

2. ENISA tagab üldsusele ja huvitatud isikutele asjakohase, objektiivse, usaldusväärse ja kergesti juurdepääsetava teabe andmise, eelkõige ENISA töötulemuste kohta. Samuti teeb ENISA avalikkusele kättesaadavaks artikli 52 kohaselt esitatud huvide deklaratsioonid.

3. Haldusnõukogu võib tegevdirektori ettepanekul lubada huvitatud isikutel jälgida ENISA mõne tegevusega seotud menetlust.

4. ENISA sätestab oma sise-eeskirjas lõigetes 1 ja 2 osutatud läbipaistvusnormide rakendamise praktilise korra.

Artikkel 54
Konfidentsiaalsus ENISAs

1. Ilma et see piiraks artikli 55 kohaldamist, ei avalikusta ENISA kolmandatele isikutele teavet, mida ta töötleb või mille on saanud ja mille kohta on esitatud põhjendatud taotlus käsitleda seda teavet konfidentsiaalsena.

2. Haldusnõukogu liikmed, tegevdirektor, tegevdirektori asetäitja, ENISA nõuanderühma liikmed, ajutistes töörühmades osalevad väliseksperdid ja ENISA töötajad, sh liikmesriikide poolt ajutiselt lähetatud ametnikud järgivad ELi toimimise lepingu artiklis 339 sätestatud konfidentsiaalsuse nõudeid, ning seda ka pärast nende töökohustuste lõppemist.

3. ENISA sätestab oma sise-eeskirjas lõigetes 1 ja 2 osutatud konfidentsiaalsuse nõuete rakendamise praktilise korra.

Artikkel 55
Juurdepääs dokumentidele

1. ENISA valduses olevate dokumentide suhtes kohaldatakse määrust (EÜ) nr 1049/2001.

2. Haldusnõukogu võtab vastu määruse (EÜ) nr 1049/2001 rakenduskorra.

3. Määruse (EÜ) nr 1049/2001 artikli 8 kohaselt vastu võetud ENISA otsuste peale võib esitada vastavalt ELi toimimise lepingu artiklile 228 kaebuse Euroopa ombudsmanile või pöörduda vastavalt ELi toimimise lepingu artiklile 263 Euroopa Liidu Kohtusse.

V PEATÜKK
Töötajad ja kontaktametnikud

Artikkel 56
Üldsätted

1. ENISA töötajate suhtes kohaldatakse personalieeskirju ja muude teenistujate teenistustingimusi ning personalieeskirjade ja muude teenistujate teenistustingimuste täitmiseks liidu institutsioonide kokkuleppel vastu võetud sätteid.
2. ENISA töötajad, kontaktametnikud ja ENISAsse lähetatud riiklikud eksperdid läbivad nõuetekohase julgeolekukontrolli.

Artikkel 57
Privileegid ja immuniteedid

ENISA ja selle töötajate suhtes kohaldatakse ELi toimimise lepingule lisatud protokolli nr 7 Euroopa Liidu privileegide ja immuniteetide kohta.

Artikkel 58
Kontaktametnikud

1. Iga liikmesriik määrab direktiivi (EL) 2022/2555 artikli 8 lõike 1 kohaselt määratud riiklikust pädevast asutusest vähemalt kaks kontaktametnikku, kes lähetatakse riiklike ekspertidena ENISAsse ning kes töötavad selle tegevuskohas või kohalikus büroos kooskõlas artikli 59 lõikega 2. Komisjon võib samuti määrata kontaktametniku.
2. Kontaktametnikud panustavad ENISA ülesannete täitmisesse, sh edendades operatiivkoostööd ja teabevahetust, nagu on osutatud artiklis 11. Kontaktametnikud toetavad ENISAt selle tegevuse, järelduste ja soovituste kohta teabe levitamisel asjakohastele sidusrühmadele liidus. Nad tegelevad riiklike kontaktpunktidena ka oma liikmesriigist saabunud küsimuste või liikmesriiki käsitlevate küsimustega, vastates kõnealustele küsimustele kas otse või suheldes riiklike haldusasutustega.
3. Nende liikmesriigi määratud kontaktametnikel on õigus küsida ja saada oma liikmesriigist käesoleva määruse kohaldamisalas kogu asjakohast teavet täielikus kooskõlas oma liikmesriigi õiguse või tavadega, eelkõige andmekaitse ja konfidentsiaalsuse osas.

Artikkel 59
Lähetatud riiklikud eksperdid ja muud töötajad

1. ENISA võib kasutada lähetatud riiklikke eksperte või muid ENISA-väliseid töötajaid kõigis oma tegevusvaldkondades. Nimetatud töötajate suhtes ei kohaldata personalieeskirju ega teenistustingimusi.
2. Haldusnõukogu võtab vastu otsuse, milles sätestatakse riiklike ekspertide, sh kontaktametnike ENISAsse lähetamist käsitlevad normid.

VI PEATÜKK
ENISAt KÄSITLEVAD ÜLDSÄTTED

Artikkel 60
ENISA õiguslik seisund

1. ENISA on liidu asutus ja juriidiline isik.
2. ENISA-l on igas liikmesriigis kõige laialdasem õigusvõime, mis vastavalt selle liikmesriigi õigusele on juriidilistel isikutel. Eelkõige võib ta omandada ja võõrandada vallas- ja kinnisvara ning olla kohtus hagejaks ja kostjaks.
3. ENISAt esindab tegevdirektor.

Artikkel 61
Tegevuskoht

ENISA tegevuskoht on Kreekas Ateenas.

Artikkel 62
Peakorterileping ja tegutsemistingimused

1. Vajalikud kokkulepped, milles käsitletakse ENISA-le vastuvõtvas liikmesriigis antavaid ruume ja pakutavat taristut ning vastuvõtvas liikmesriigis tegevdirektori, haldusnõukogu liikmete, ENISA töötajate ja nende pereliikmete suhtes kohaldatavaid erinorme, sätestatakse ENISA ja vastuvõtva liikmesriigi vahelises peakorterilepingus, mis sõlmitakse pärast haldusnõukogu heakskiidu saamist.
2. ENISA vastuvõttev liikmesriik tagab ENISA-le parimad võimalikud tegutsemistingimused, et tagada ENISA nõuetekohane toimimine, võttes arvesse asukoha ligipääsetavust, sobivate haridusasutuste olemasolu töötajate laste jaoks ning töötajate laste ja abikaasade piisavat juurdepääsu tööturule, sotsiaalkindlustusele ja arstiabile.

Artikkel 63
Halduskontroll

ENISA tegevuse üle teeb järelevalvet Euroopa ombudsman ELi toimimise lepingu artikli 228 kohaselt.

Artikkel 64
ENISA vastutus

1. ENISA lepingulist vastutust reguleerib asjaomase lepingu suhtes kohaldatav õigus.
2. ENISA sõlmitud lepingus sisalduva vahekohtuklausli alusel kohtuotsuste tegemine kuulub Euroopa Liidu Kohtu pädevusse.
3. Lepinguvälise vastutuse korral heastab ENISA vastavalt liikmesriikide õiguse ühistele üldpõhimõtetele kõik kahjud, mida ENISA või tema töötajad on oma ülesannete täitmisel tekitanud.
4. Lõikes 3 osutatud kahju ülemäärase hüvitamisega seotud vaidluste lahendamine kuulub Euroopa Liidu Kohtu pädevusse.
5. Töötajate isiklik vastutus ENISA ees on reguleeritud nende suhtes kohaldatavate personalieeskirjade või teenistustingimustega.

Artikkel 65
Kasutatavad keeled

1. ENISA suhtes kohaldatakse nõukogu määrust nr 1[79]. Liikmesriigid ja nende poolt määratud asutused võivad pöörduda ENISA poole ja saada vastuse nende poolt valitud liidu institutsioonide ametlikus keeles.

2. ENISA tegevuseks vajalikke tõlke- ja muid keeleteenuseid, välja arvatud suuline tõlge, osutab Euroopa Liidu Asutuste Tõlkekeskus.

Artikkel 66
Isikuandmete kaitse

1. ENISA kohaldab isikuandmete töötlemise suhtes määrust (EL) 2018/1725.

2. Haldusnõukogu võtab vastu määruse (EL) 2018/1725 artikli 45 lõikes 3 osutatud rakenduseeskirjad. Haldusnõukogu võib võtta vastu täiendavaid meetmeid, mida on vaja ENISA poolt määruse (EL) 2018/1725 kohaldamiseks.

Artikkel 67
Julgeolekunormid salastamata tundliku teabe ja salastatud teabe kaitse kohta

Kokkuleppel komisjoniga võtab ENISA vastu julgeolekunormid, mille abil kohaldatakse julgeolekupõhimõtteid, mis sisalduvad komisjoni julgeolekunormides, mis käsitlevad salastamata tundliku teabe ja ELi salastatud teabe kaitset, nagu on sätestatud otsustes (EL, Euratom) 2015/443[80] ja 2015/444[81]. Nimetatud julgeolekunormid hõlmavad kõnealuse teabe vahetust, töötlemist ja säilitamist käsitlevaid sätteid.

Artikkel 68
Koostöö liidu üksuste ja riikide ametiasutustega

1. Järjepidevuse tagamiseks, koosmõju tekitamiseks ja ühiste probleemide lahendamiseks teeb ENISA küberturvalisusega seotud küsimustes koostööd CERT-EU ja asjaomaste liidu üksustega, sh Europoliga, määruse (EL) 2021/887 kohaselt loodud küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse ja määruse (EL) 2016/679 artikli 68 lõike 1 kohaselt loodud Euroopa Andmekaitsenõukoguga.

2. Lõikes 1 osutatud koostöö võidakse tagada järgmiselt:

   a) oskusteabe ja parimate tavade vahetamine;

   b) nõu ja suuniste andmine küberturvalisusega seotud küsimustes;

   c) konkreetsete ülesannete täitmise praktilise korra kehtestamine pärast komisjoniga konsulteerimist.

---

79 Nõukogu määrus nr 1, millega määratakse kindlaks Euroopa Majandusühenduses kasutatavad keeled (EÜT 17, 6.10.1958, lk 385, ELI: http://data.europa.eu/eli/reg/1958/1(1)/oj).

80 Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/443 komisjoni julgeoleku kohta (ELT L 72, 17.3.2015, lk 41, ELI: http://data.europa.eu/eli/dec/2015/443/oj).

81 Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/444 ELi salastatud teabe kaitseks vajalike julgeolekunormide kohta (ELT L 72, 17.3.2015, lk 53, ELI: http://data.europa.eu/eli/dec/2015/444/oj).

3. ENISA osaleb struktureeritud koostöös CERT-EUga, eelkõige küberohtudega seotud suutlikkuse suurendamise, operatiivkoostöö ja pikaajaliste strateegiliste analüüside valdkonnas.

4. ENISA teeb koostööd ja vahetab teavet asjaomaste turujärelevalve- ja järelevalveasutustega, mis on määratud küberturvalisuse valdkonna liidu õigusaktide, sh määruse (EL) 2024/2847 alusel.

Artikkel 69
Koostöö sidusrühmadega

1. Kui see on vajalik käesoleva määruse eesmärkide saavutamiseks, teeb ENISA koostööd asjaomaste sidusrühmadega, nagu küberturvalisuse tööstus, IKT-tööstus, VKEd, direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorites tegutsevad üksused, digielemente sisaldavate toodete tootjad, importijad või turustajad määruse (EL) 2024/2847 tähenduses, vastavushindamisasutused, millest on teavitatud Euroopa küberturvalisuse sertifitseerimise raamistiku ja määruse (EL) 2024/2847 alusel, e-identimise vahendite valdkonnas tegutsevad üksused, tarbijarühmad ning küberturvalisuse valdkonna akadeemilised eksperdid. Selleks võib ENISA luua avaliku ja erasektori partnerlused.

2. ENISA toetab komisjoniga konsulteerides koostööd teada antud vastavushindamisasutuste vahel kooskõlas artikliga 93. Eelkõige võib ta luua teada antud vastavushindamisasutuste rühma parimate tavade jagamiseks, luues koosmõju muude asjakohaste liidu õigusaktidega, eelkõige määrusega (EL) 2024/2847.

Artikkel 70
Koostöö kolmandate riikide ja rahvusvaheliste organisatsioonidega

1. Niivõrd kui see on vajalik käesoleva määruse eesmärkide saavutamiseks, võib ENISA teha koostööd kolmandate riikide pädevate asutuste või rahvusvaheliste organisatsioonide või mõlemaga kooskõlas liidu prioriteetidega. Selleks võib ENISA komisjoni eelneval nõusolekul leppida kolmandate riikide asutuste ja rahvusvaheliste organisatsioonidega kokku koostöökorras. See koostöökord ei too liidule ega selle liikmesriikidele kaasa õiguslikke kohustusi.

2. Haldusnõukogu võtab vastu strateegia, mis käsitleb suhteid kolmandate riikide ja rahvusvaheliste organisatsioonidega ENISA pädevusse kuuluvates küsimustes kooskõlas lõikes 1 osutatud prioriteetidega. Komisjon tagab, et ENISA tegutseb oma volituste piires ja olemasolevas institutsioonilises raamistikus, leppides tegevdirektoriga kokku asjakohases töökorras.

3. Kolmandate riikidega tehtava koostöö toetamiseks, eelkõige liiduga ühinemise kandidaatriikide puhul, võib ENISA jagada oma suutlikkuse suurendamise oskusteavet, eelkõige järgmistes valdkondades:

   a) küberturvalisuse võimekuse ja ressursside küpsustaseme hindamine;

   b) küberturvalisuse valdkonna tööjõu suurenemine ja täiustamine, sh edendades Euroopa küberturbeoskuste raamistikku ja Euroopa individuaalsete küberturbeoskuste tõendamise kavasid ning pakkudes õppe- ja koolitustegevust;

   c) küberturvalisuse õppuste kavandamise ja elluviimise toetamine.

4. ENISA on selle töös osalemiseks avatud nendele kolmandatele riikidele, kes on sõlminud liiduga vastavad lepingud. Kolmandate riikide ja liidu vahel sõlmitud lepingute asjakohaste sätete alusel lepitakse komisjoni eelneva nõusoleku alusel kokku koostöökorras, milles täpsustatakse eelkõige nende kolmandate riikide poolt ENISA töös osalemise olemus, ulatus ja viis, sh sätted, mis käsitlevad ENISA käivitatud algatustes osalemist, rahalist osalust ja töötajaid. Personaliküsimustes peab kõnealune koostöökord olema igal juhul kooskõlas personalieeskirjade ja muude teenistujate teenistustingimustega.

5. ENISA annab nõukogule ja komisjonile korrapäraselt aru lõigetes 1 ja 4 osutatud koostöökorra rakendamisest.

III JAOTIS

EUROOPA KÜBERTURVALISUSE SERTIFITSEERIMISE RAAMISTIK

I PEATÜKK
Eesmärgid, kohaldamisala ja menetlused

Artikkel 71

Euroopa küberturvalisuse sertifitseerimise raamistiku eesmärgid ja kohaldamisala

1. Euroopa küberturvalisuse sertifitseerimise raamistik kehtestatakse eesmärgiga luua IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ja üksuste digitaalne ühtne turg. Selleks suurendab raamistik liidus küberturvalisuse taset ja võimaldab Euroopa küberturvalisuse sertifitseerimise kavade ühtlustatud lähenemisviisi ning kasutab sertifitseerimist, et edendada vastavust kohaldatavatele liidu õigusaktidele.

2. Euroopa küberturvalisuse sertifitseerimise raamistik tagab mehhanismi Euroopa küberturvalisuse sertifitseerimise kavade loomiseks ja järgmise tõendamiseks:

   a) et selliste kavade kohaselt hinnatud IKT-tooted, -teenused ja -protsessid vastavad kindlaksmääratud turvanõuetele eesmärgiga kaitsta salvestatud, edastatud või töödeldud andmete või kõnealuste toodete, protsesside ja teenuste funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust kogu nende elutsükli kestel;

   b) et kooskõlas selliste kavadega hinnatud hallatud turbeteenused vastavad kindlaksmääratud turvanõuetele, mille eesmärk on kaitsta hallatud turbeteenuste pakkumisega seoses juurdepääsetavate, töödeldavate, salvestatavate või edastatavate andmete käideldavust, autentsust, terviklust ja konfidentsiaalsust, ning et neid hallatud turbeteenuseid pakuvad pidevalt vajaliku pädevuse, erialateadmiste ja kogemustega töötajad, kellel on piisaval ja sobival tasemel tehnilised teadmised ning erialane kohusetunne;

   c) et kõnealuste kavade kohaselt hinnatud üksuse turvaolek vastab kindlaks määratud küberturvalisuse nõuetele.

3. Euroopa küberturvalisuse sertifitseerimine on vabatahtlik, kui liidu või liikmesriikide õiguses ei ole sätestatud teisiti.

4. Kõik liikmesriigid peavad automaatselt tunnustama Euroopa küberturvalisuse sertifitseerimise raamistiku alusel väljastatud Euroopa küberturvalisuse sertifikaati ja ELi vastavusdeklaratsiooni.

Artikkel 72
Üldsuse teavitamine ja konsulteerimine

1. Komisjon korraldab ENISA toetusel vähemalt kord aastas Euroopa küberturvalisuse sertifitseerimise assamblee, kuhu ta kutsub Euroopa küberturvalisuse sertifitseerimise rühma liikmed ja muud asjaomased eksperdid liikmesriikidest, asjaomased eksperdid liidu üksustest ning asjaomased sidusrühmad, et arutada küberturvalisuse sertifitseerimise valdkonnas ühtlustamise strateegilisi prioriteete.

2. Komisjon haldab ja ajakohastab korrapäraselt sihtotstarbelist veebisaiti, millel esitatakse teavet järgmiste aspektide kohta:

   a) Euroopa küberturvalisuse sertifitseerimise kavad, mille loomise taotlus on esitatud kooskõlas artikliga 73;

   b) strateegilised prioriteedid IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste, üksuste turvaoleku või liidu õigusaktides sätestatud turvanõuete ühtlustamiseks, sh võimalikud valdkonnad, mille tarbeks võidakse taotleda Euroopa küberturvalisuse sertifitseerimise kava.

3. Komisjon teeb käesoleva artikli lõikes 2 osutatud veebisaidil üldsusele kättesaadavaks teabe taotluse kohta, mille ta on esitanud ENISA-le artiklis 73 osutatud ettevalmistava kava koostamiseks, ja oma otsuse kohta kiita ENISA edastatud ettevalmistav kava heaks, lükata see tagasi või lõpetada selle kohaldamine kooskõlas artikli 74 lõikega 7.

4. Selle aja jooksul, mil ENISA koostab artikli 74 kohast ettevalmistavat kava, võivad Euroopa Parlament ja nõukogu taotleda komisjonilt kui Euroopa küberturvalisuse sertifitseerimise rühma juhatajalt ja ENISA-lt asjakohase teabe esitamist ettevalmistava kava projekti kohta. ENISA võib Euroopa Parlamendi või nõukogu taotlusel ja kokkuleppel komisjoniga ning ilma et see piiraks artikli 54 kohaldamist, teha Euroopa Parlamendile ja nõukogule kättesaadavaks ettevalmistava kava projekti asjakohased osad nõutava konfidentsiaalsusega kooskõlas oleval ja asjakohasel juhul piiratud viisil.

5. Euroopa Parlament ja nõukogu võivad kutsuda komisjoni ja ENISAt arutama IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku Euroopa küberturvalisuse sertifitseerimise kavade rakendamisega seotud küsimusi.

Artikkel 73
Euroopa küberturvalisuse sertifitseerimise kava taotlemine

1. Komisjon võib taotleda ENISA-lt IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava koostamist.

2. Nõuetekohaselt põhjendatud juhtudel võib Euroopa küberturvalisuse sertifitseerimise rühm soovitada komisjonil esitada lõikes 1 osutatud taotluse.

3. Lõikes 1 osutatud taotluses kirjeldatakse artiklites 80 ja 81 sätestatud asjakohaste turvaeesmärkide otstarvet, kohaldamisala ja saavutamise viise. Taotluses

täpsustatakse ka Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava plaan ja kavas osutatavad või kindlaks määratavad asjakohased tehnilised kirjeldused.

4. Lõikes 1 osutatud taotluse koostamisel konsulteerib komisjon nõuetekohaselt ENISA ja Euroopa küberturvalisuse sertifitseerimise rühmaga ning võtab arvesse kõigi asjaomaste sidusrühmade ja liidu üksuste seisukohti, sh (kui see on kohaldatav) neid, mis on asjakohased liidu õigusaktide alusel, millele vastavust Euroopa küberturvalisuse sertifitseerimise kava tõendab ja mille vastavuseelduse see tagab.

Artikkel 74

Euroopa küberturvalisuse sertifitseerimise kavade koostamine ja vastuvõtmine

1. Hiljemalt 12 kuud pärast komisjonilt artikli 73 kohase taotluse saamist koostab ENISA Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava, mis vastab artiklites 80 ja 81 sätestatud nõuetele, kui taotluses ei ole teisiti märgitud.

2. Iga ettevalmistava kava koostamise puhul moodustab ENISA kooskõlas artikli 32 lõikega 6 ajutise töörühma, et pakkuda ENISA-le spetsiifilist nõu ja oskusteavet.

3. ENISA teeb ettevalmistava kava koostamisel tihedat koostööd Euroopa küberturvalisuse sertifitseerimise rühmaga. Euroopa küberturvalisuse sertifitseerimise rühm pakub ENISA-le abi ja eksperdinõu seoses ettevalmistava kava ning vajaduse korral sellele lisatavate tehniliste kirjelduste koostamisega.

4. Ettevalmistavat kava, sh vajaduse korral sellele lisatavaid tehnilisi kirjeldusi koostades konsulteerib ENISA aegsasti sidusrühmadega ametliku, avatud, läbipaistva ja kaasava konsulteerimisprotsessi raames. ENISA teeb samuti koostööd asjaomaste avaliku sektori asutustega liikmesriikides, et saada neilt eksperdinõuandeid ettevalmistava kava ja vajaduse korral sellele lisatavate tehniliste kirjelduste koostamise kohta. Kui ENISA edastab lõike 6 kohaselt komisjonile ettevalmistava kava, kirjeldab ta seda, mil viisil ta on käesolevat lõiget järginud.

5. Enne ettevalmistava kava ja vajaduse korral lisatavate tehniliste kirjelduste komisjonile edastamist küsib ENISA Euroopa küberturvalisuse sertifitseerimise rühma liikmetelt kirjalikke arvamusi ettevalmistava kava kohta. Arvamused esitatakse taotluse esitamise kuupäevast hiljemalt 30 päeva jooksul. ENISA võtab Euroopa küberturvalisuse sertifitseerimise rühma arvamusi võimalikult suurel määral arvesse. Kui selliseid arvamusi ei esitata, ei takista see ENISA-l ettevalmistava kava komisjonile saatmist.

6. ENISA edastab ettevalmistava kava komisjonile hiljemalt 60 päeva jooksul alates lõikes 5 osutatud taotluse esitamise kuupäevast.

7. Kui komisjon saab ettevalmistava kava kätte, siis ta hindab, kas kava vastab artikli 73 kohaselt esitatud taotlusele. Komisjon käitub 30 päeva jooksul alates kõnealuse ettevalmistava kava edastamise kuupäevast ühel järgmisel viisil:

   a) kiidab ettevalmistava kava heaks;

   b) saadab ettevalmistava kava ENISA-le muutmiseks tagasi koos tagasisaatmise põhjendusega ja kuni 90päevase tähtajaga, mille jooksul ENISA peab esitama muudetud ettevalmistava kava;

   c) lõpetab ettevalmistava kava kohaldamise.

8. Kui komisjon saadab ettevalmistava kava kooskõlas lõike 7 punktiga b ENISA-le muutmiseks tagasi, siis kohaldatakse vastavalt lõikeid 4, 5 ja 7.

9. Komisjonil on ENISA koostatud ettevalmistava kava alusel, mille komisjon on heaks kiitnud, volitus võtta vastu rakendusakte, millega sätestatakse IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku Euroopa küberturvalisuse sertifitseerimise kava, mis vastab artiklites 80 ja 81 sätestatud nõuetele. Nimetatud rakendusakt võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.

10. Komisjon võib käesoleva artikli lõikes 9 osutatud rakendusaktides osutada ENISA koostatud tehnilistele kirjeldustele kooskõlas artiklitega 18 ja 77.

11. Komisjon võib täpsustada käesoleva artikli lõikes 9 osutatud rakendusaktides Euroopa küberturvalisuse sertifikaatide rahvusvahelise tunnustamise tingimused kooskõlas artikliga 87.

Artikkel 75
Euroopa küberturvalisuse sertifitseerimise kava haldamine

1. Igas Euroopa küberturvalisuse sertifitseerimise kavas määratakse kindlaks haldamise strateegia. Haldamise strateegias kirjeldatakse haldamistegevusega seotud ootusi, eelkõige kui need on seotud kavas osutatud standardite või tehniliste kirjeldustega, ning mõju asjaomastele sidusrühmadele.

2. ENISA tagab koostöös komisjoniga ning Euroopa küberturvalisuse sertifitseerimise rühma ja selle vastava haldamise alamrühma toetusel Euroopa küberturvalisuse sertifitseerimise kavade haldamise, võttes muu hulgas arvesse kõnealuste kavade võimalikku läbivaatamist komisjoni poolt. ENISA teeb haldamisega seoses koostööd ja vahetab teavet asjaomaste liidu üksuste ja rühmadega.

3. ENISA võib korraldada erasektori kaasamise kava haldamisse ajutise töörühma kujul kooskõlas lõikes 1 osutatud haldamise strateegiaga.

4. Euroopa küberturvalisuse sertifitseerimise kavade haldamise tegevus hõlmab järgmist:

   a) tehniliste kirjelduste ja suuniste koostamine, ajakohastamine ja toetamine eesmärgiga toetada kavade ühtlustatud ja ühtset rakendamist;

   b) kava jaoks asjakohaste standardite või tehniliste kirjelduste kindlaks tegemine;

   c) suhtlus ja vajaduse korral suhete loomine asjaomaste sidusrühmadega, sh Euroopa või rahvusvaheliste standardiorganisatsioonidega, muu hulgas tehnilise panuse tegemise või saamise eesmärgil;

   d) komisjonile soovituste esitamine kavade vajalike täienduste ja ajakohastuste kohta, sh kavade võimaliku läbivaatamise eesmärgil;

   e) liikmesriikide teabevahetus kavade tegelikkuses rakendamise kohta;

   f) panused vastastikustesse eksperdihinnangutesse ja vastastikuse hindamise mehhanismidesse ning kõnealuste hindamiste tulemuste analüüsid, et parandada kavade toimimist ning toetada nende võimalikku läbivaatamist.

5. Euroopa küberturvalisuse sertifitseerimise rühm võib esitada Euroopa küberturvalisuse sertifitseerimise kavade haldamise kohta arvamuse.

Artikkel 76

Euroopa küberturvalisuse sertifitseerimise kavade hindamine, läbivaatamine ja kehtetuks tunnistamine

1. ENISA hindab vähemalt iga nelja aasta tagant pärast Euroopa küberturvalisuse sertifitseerimise kava kohaldamise algust kõnealuse kava mõju ja tulemuslikkust koostöös Euroopa küberturvalisuse sertifitseerimise rühma asjaomase haldamise allrühmaga ning võttes arvesse sidusrühmadelt saadud tagasisidet. ENISA viib hindamise läbi, tehes turuanalüüsi kooskõlas artikli 8 lõikega 1.

2. Komisjon võib pärast lõikes 1 osutatud hindamist vaadata läbi või tunnistada kehtetuks rakendusaktid, millega nähakse ette Euroopa küberturvalisuse sertifitseerimise kava kooskõlas artikli 74 lõikega 9.

3. Komisjon konsulteerib Euroopa küberturvalisuse sertifitseerimise kavade läbivaatamisel või kehtetuks tunnistamisel ENISA, Euroopa küberturvalisuse sertifitseerimise rühma ja selle asjaomase haldamise allrühmaga ning võtab arvesse asjaomaste sidusrühmade ja muude liidu üksuste seisukohti.

4. Euroopa küberturvalisuse sertifitseerimise rühm võib esitada Euroopa küberturvalisuse sertifitseerimise kava läbivaatamise või kehtetuks tunnistamise kohta arvamuse. Komisjon võtab seda Euroopa küberturvalisuse sertifitseerimise kava läbivaatamisel või kehtetuks tunnistamisel nõuetekohaselt arvesse.

Artikkel 77

Euroopa küberturvalisuse sertifitseerimise kavades esitatud tehnilised kirjeldused

1. ENISA võib koostada tulevase Euroopa küberturvalisuse sertifitseerimise kava eesmärgil või Euroopa küberturvalisuse sertifitseerimise kava haldamise toetamiseks tehnilised kirjeldused.

2. Käesoleva artikli lõikes 1 osutatud tehnilised kirjeldused koostatakse aegsasti Euroopa küberturvalisuse sertifitseerimise rühma ja selle haldamise allrühmade ning vajaduse korral artikli 75 lõikes 3 osutatud vastava ajutise töörühma toetusel. Sel otstarbel küsib ENISA samuti sisendeid asjaomastelt sidusrühmadelt, võttes arvesse artikli 75 lõikes 1 osutatud haldamise strateegiat.

3. Kui Euroopa küberturvalisuse sertifitseerimise kavas osutatakse tehnilistele kirjeldustele, nagu on märgitud artikli 74 lõikes 10, siis tehakse need kättesaadavaks artiklis 79 osutatud veebisaidil.

4. Nõuetekohaselt põhjendatud juhtudel, eelkõige kui tehnilised kirjeldused sisaldavad teavet, mis võib kahjustada sertifitseeritud IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku turvalisust, jaotatakse need ainult sidusrühmadele, kelle suhtes kava nõudeid kohaldatakse. Sellistele tehnilistele kirjeldustele ei osutata Euroopa küberturvalisuse sertifitseerimise kavas, nagu on märgitud artikli 74 lõikes 10.

Artikkel 78

Liidu õigusaktidele vastavuse hõlbustamine

1. Kui konkreetses liidu õigusaktis on nii sätestatud, näitab Euroopa küberturvalisuse sertifitseerimise kava kohaselt välja antud sertifikaat vastavust selles õigusaktis sätestatud asjakohastele nõuetele ja tagab sellele nõuetele vastavuse eelduse.

2. Euroopa küberturvalisuse sertifitseerimise kava kohane hindamine peab olema kooskõlas liidu vastava õigusaktiga, milles määratakse kindlaks vastavuse tõendamine ja nõuetele vastavuse eeldus. Kui vastavas liidu õigusaktis ei ole seda hindamist käsitletud, siis käsitletakse seda kavas. Liidu õigusaktide nõuetele vastavuse eelduse tagava sertifikaadi vastavushindamise viib läbi kolmandast isikust asutus.

3. Liidu ühtlustatud õigusaktide puudumisel võidakse liikmesriigi õiguses sätestada, et Euroopa küberturvalisuse sertifitseerimise kava võib kasutada selleks, et tõendada vastavust ja tagada nõuetele vastavuse eeldus liikmesriigi õiguses sätestatud õiguslikele erinõuetele.

Artikkel 79
Euroopa küberturvalisuse sertifitseerimise kavade kasutuselevõtt, ENISA veebisait ja sertifikaatide avaldamine

1. ENISA korraldab tegevuse, et edendada vastu võetud Euroopa küberturvalisuse sertifitseerimise kavade kasutuselevõttu, muu hulgas hallates käesoleva artikli lõikes 2 osutatud veebisaiti.

2. ENISA haldab ja ajakohastab korrapäraselt sihtotstarbelist veebisaiti, millel on esitatud avalik teave järgmise kohta:

   a) Euroopa küberturvalisuse sertifitseerimise kavad;

   b) iga Euroopa küberturvalisuse sertifitseerimise kava haldamisega seotud tasud;

   c) asjakohased ENISA tehnilised kirjeldused;

   d) Euroopa küberturvalisuse sertifikaadid ja ELi vastavusdeklaratsioonid, sh teave selliste sertifikaatide ja deklaratsioonide kohta, mis enam ei kehti, mis on peatatud, kehtetuks tunnistatud või aegunud;

   e) asjakohane täiendav küberturvalisuse teave, mis on esitatud kooskõlas artikliga 84;

   f) vastastikuste eksperdihinnangute kokkuvõtted kooskõlas artikli 89 lõikega 7;

   g) Euroopa küberturvalisuse sertifitseerimise kavas märgitud tehnilised kirjeldused kooskõlas artikli 74 lõikega 10.

3. Kui see on asjakohane, märgitakse lõikes 2 osutatud veebisaidil ära ka riiklikud küberturvalisuse sertifitseerimise kavad, mis on asendatud Euroopa küberturvalisuse sertifitseerimise kavaga.

II PEATÜKK
Euroopa küberturvalisuse sertifitseerimise kavade sisu

Artikkel 80
Euroopa küberturvalisuse sertifitseerimise kavade turvalisusega seotud eesmärgid

1. Euroopa küberturvalisuse sertifitseerimise kaval on kohaldataval juhul järgmised turvalisusega seotud eesmärgid:

   a) tagada, et IKT-tooted, -teenused ja -protsessid ning hallatud turbeteenused on vaikimisi ja sisseprojekteeritult turvalised;

b) kaitsta salvestatud, edastatud või muul moel töödeldud andmeid juhusliku või volitamata salvestamise, töötlemise, juurdepääsu või avalikustamise eest, kasutades sobilikke tehnilisi vahendid ning võttes arvesse IKT-toote, -teenuse või -protsessi kogu elutsüklit;

c) kaitsta salvestatud, edastatud või muul moel töödeldud andmete (isikuandmed või muud andmed), käskude, programmide ja konfiguratsioonide terviklust mis tahes manipuleerimise või muutmise eest, milleks kasutaja ei ole luba andnud, ja teatada rikkumistest, võttes arvesse IKT-toote, -teenuse või -protsessi kogu elutsüklit;

d) tagada asjakohaste kontrollimehhanismide (sh, aga mitte ainult autentimis-, identimis- või juurdepääsu haldamise süsteemide) abil kaitse loata juurdepääsu eest ning teatada võimalikust loata juurdepääsust;

e) teha kindlaks ja dokumenteerida komponendid ja nõrkused, sh vajaduse korral koostades tarkvaramaterjalide loetelu, mis hõlmab vähemalt kõrgeima taseme sõltuvusi;

f) anda turvalisusega seotud teavet, registreerides ja seirates asjaomaseid sisetoiminguid, sh juurdepääsu andmetele, teenustele või funktsioonidele või nende muutmist, kui see on kohaldatav siis koos loobumismehhanismiga kasutajate jaoks;

g) kontrollida, et IKT-toodetel, -teenustel ja -protsessidel ei ole teadaolevaid ärakasutatavaid turvanõrkuseid;

h) kaitsta oluliste ja põhifunktsioonide kättesaadavust, seda ka pärast intsidenti, muu hulgas ummistusrünnete vastu suunatud vastupidavus- ja leevendusmeetmetega;

i) minimeerida negatiivset mõju muude võrkude ja seadmete osutatavate teenuste kättesaadavusele füüsilise või tehnilise intsidendi korral;

j) tagada, et IKT-tooteid, -teenuseid ja -protsesse testitakse korrapäraselt ja nende turvalisus vaadatakse läbi;

k) tagada, et nõrkusi võetakse arvesse ja need kõrvaldatakse viivitamata, sh turvauuendite abil, ja et teavet kõrvaldatud nõrkuste kohta jagatakse ja see avalikustatakse, v.a juhul, kui avaldamise riskid on turvalisusele saadavast kasust kaalukamad;

l) tagada, et kasutusel on poliitika nõrkuste kohta teabe kooskõlastatud avalikustamiseks;

m) hõlbustada teabe jagamist IKT-toodete, -teenuste ja -protsesside võimalike nõrkuste kohta;

n) tagada, et kui kindlaks tehtud turvaprobleemide lahendamiseks on saadaval turvauuendid, siis levitatakse neid turvauuendeid viivitamata;

o) tagada, et hallatud turbeteenuseid pakutakse vajalikul tasemel pädevuse, erialateadmiste ja kogemustega; muu hulgas peavad töötajatel, kelle ülesanne on kõnealuseid teenuseid pakkuda, olema asjaomases valdkonnas piisaval ja sobival tasemel tehnilised teadmised ja pädevus ning piisav ja asjakohane kogemus ning suurim erialane kohusetunne;

p) tagada, et hallatud turbeteenuste pakkumisel kasutatud IKT-tooted, -teenused ja -protsessid on sisseprojekteeritult ja vaikimisi turvalised ning kohaldataval juhul on neile paigaldatud kõige värskem turvauuend ja need ei sisalda avalikult teadaolevaid nõrkusi;

q) tagada, et sertifitseeritud üksusel on kasutusel sobivad sisemenetlused, mis tagavad, et teenuseid pakutakse igal ajal piisava ja sobiva kvaliteediga;

r) tagada, et sertifitseeritud üksus suudab intsidente kindlaks teha, nende vastu kaitsta, neid avastada, neile reageerida ja neist taastuda;

s) tagada, et sertifitseeritud üksus suudab juhtida riske, mis ohustavad üksuse tegevuses või teenuste osutamisel kasutatavate võrgu- ja infosüsteemide turvalisust, ning ennetada või minimeerida intsidentide mõju üksuse teenuste saajatele ja muudele teenustele;

t) tagada, et sertifitseeritud üksus suudab luua, tagada ja vaadata läbi oma tegevuse terviklikkust ja usaldusväärsust, tagades kas otseselt või kaudselt kolmandast isikust IKT-teenuste osutajate pakutavate teenuste kasutamise kaudu kogu IKTga seotud suutlikkuse, mida on vaja selliste võrgu- ja infosüsteemide turvalisuse käsitlemiseks, mida üksus kasutab ning mis toetavad teenuste jätkuvat osutamist ja nende kvaliteeti, sealhulgas katkestuste vältel;

u) tagada, et sertifitseeritud üksus suudab rakendada ja säilitada infoturbe halduse süsteemi;

v) panna vastu mis tahes sündmusele, mis võib ohustada üksuse salvestatud, edastatud või töödeldud andmete või tema pakutud või tema kasutatava võrgu- ja infosüsteemi kaudu kättesaadavate andmete käideldavust, autentsust, terviklust või konfidentsiaalsust ning tagada teenuste jätkuva osutamise ja nende kvaliteedi, sh katkestuste vältel;

w) tagada, et üksus suudab tagada isikuandmete töötlemise turvalisuse.

2. Komisjonil on õigus võtta kooskõlas artikliga 119 vastu delegeeritud õigusakte, et muuta käesoleva artikli lõiget 1, lisades turvalisuse eesmärke või muutes neid eesmärgiga tagada, et need kajastavad uusimat tehnoloogia arengut ja sellega seotud uusi ohte ning uute liidu õigusaktide vastuvõtmist, millega määratakse Euroopa küberturvalisuse sertifitseerimise kaudu kindlaks vastavuse tõendamine ja nõuetele vastavuse eeldus kõnealuste õigusaktide asjakohaste küberturvalisuse nõuetega.

3. Euroopa küberturvalisuse sertifitseerimise kava, mis käsitleb määruse (EL) 2024/2847 artikli 3 punktis 1 määratletud digielemente sisaldavaid tooteid, koostatakse kooskõlas kõnealuse määruse I lisas sätestatud oluliste küberturvalisuse nõuetega ja selle puhul võetakse arvesse olemasolevaid harmoneeritud standardeid.

Artikkel 81
Euroopa küberturvalisuse sertifitseerimise kavade elemendid

1. Euroopa küberturvalisuse sertifitseerimise kava sisaldab vähemalt järgmisi elemente:

a) sertifitseerimiskava reguleerimisese ja kohaldamisala, sh sertifitseerimisega hõlmatud IKT-toodete, -teenuste ja -protsesside, hallatud turbeteenuste või üksuse varade, teenuste ja funktsioonide liik või kategooria;

b) kava eesmärgi selge kirjeldus ja, kui see on kohaldatav, siis nende liidu õigusaktide kindlaks määramine, milles on märgitud nõuded, millele vastavust Euroopa küberturvalisuse sertifikaadid tõendavad ja mille nõuetele vastavuse eelduse need tagavad;

c) haldamise strateegia, milles määratakse kindlaks artiklis 75 sätestatud haldamistegevuse lähenemisviis;

d) küberturvalisuse erinõuded, hindamiskriteeriumid ja -meetodid, mida kasutatakse IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku hindamiseks, ning viited rahvusvahelisetele Euroopa või riiklikele standarditele, mida kohaldatakse IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku hindamiseks, või kui kõnealused standardid ei ole saadaval või asjakohased, siis viited tehnilistele kirjeldustele, mille ENISA on koostanud kooskõlas artikliga 77, või kui kõnealused kirjeldused ei ole saadaval, siis muudele tehnilistele kirjeldustele;

e) kava kohaselt välja antud Euroopa küberturvalisuse sertifikaatide maksimaalne kehtivusaeg.

2. Euroopa küberturvalisuse sertifitseerimise kava sisaldab vähemalt järgmist käsitlevaid norme ja tingimusi:

a) IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku Euroopa küberturvalisuse sertifikaatide nõuetele või ELi vastavusdeklaratsiooni nõuetele vastavuse järelevalve, sh mehhanismid, millega kinnitatakse kindlaksmääratud küberturvalisuse nõuete jätkuvat täitmist;

b) Euroopa küberturvalisuse sertifikaatide väljastamine, kinnitamine, kehtetuks tunnistamine ja uuendamine, sertifikaatide kohaldamisala suurendamine või vähendamine ja taassertifitseerimine;

c) tagajärjed sertifitseeritud või ELi vastavusdeklaratsiooni saanud IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste puhul, mis ei järgi kõnealuse kava nõudeid;

d) kuidas tuleks IKT-toodete, -teenuste ja -protsesside varem avastamata küberturvalisuse nõrkustest teada anda ja kuidas neid menetleda;

e) väljaantavate Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide sisu ja vorming;

f) ELi vastavusdeklaratsiooni, tehnilise dokumentatsiooni ning IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja või sertifitseeritava turvaolekuga üksuse poolt kättesaadavaks tehtava kogu muu asjaomase teabe kättesaadavuse tähtaeg;

g) kava alusel artikli 85 lõikes 4 käsitletud Euroopa küberturvalisuse sertifikaate väljastavatele ametitele või asutustele loodud mis tahes vastastikuste eksperdihinnangute mehhanismid, mis ei piira artiklis 90 sätestatud vastastikuse eksperdihinnangu kohaldamist;

h) käesolevas jaotises märgitud nõuete rakendamisega seotud ülesannete täitmise ja tegevuse elluviimise tulemusena kõigi osaliste saadud teabe ja andmete konfidentsiaalsus;

i) vorming ja menetlused, mida kasutavad IKT-toodete, -teenuste või -protsesside tootjad või pakkujad täiendava küberturvalisuse alase teabe esitamisel ja ajakohastamisel kooskõlas artikliga 84 ning

j) sertifitseerimistegevuse jätkumine erakorralistes kriisiolukordades, mis ei ole välditavad ja mis takistavad sertifitseerimiskava normide kohaldamist.

3. Euroopa küberturvalisuse sertifitseerimise kava sisaldab vajaduse korral ka järgmist:

a) usaldusväärsuse tase(med) ja vastavad hindamistasemed;

b) kaitseprofiilid, et täpsustada turvanõuded, mis on kohaldatavad IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste konkreetse kategooria suhtes;

c) profiilide laiendamine, et kehtestada täiendavaid turvanõudeid, sh asjakohasel juhul liidu õiguse ülevõtmiseks riiklikes õigusnormides sätestatud turvanõudeid;

d) selgitus, milline vastavushindamistegevus, sh kalibreerimine, testimine, sertifitseerimine ja inspekteerimine usaldusväärsuse taseme „kõrge“ puhul või vastavuse tõendamiseks ja vastavuseelduse tagamiseks, on lubatud väljaspool Euroopa Majanduspiirkonda (edaspidi „EMP“);

e) teave sama liiki või samasse kategooriasse kuuluvaid IKT-tooteid, -teenuseid, -protsesse, hallatud turbeteenuseid või üksuste turvaolekut hõlmavate riiklike või rahvusvaheliste küberturvalisuse sertifitseerimise kavade kohta;

f) vastavushindamisasutuste suhtes kohaldatavad lisa- või erinõuded, et tagada nende tehniline pädevus hinnata küberturvalisuse nõudeid;

g) sertifitseerimiseks vajalik teave, mille taotluse esitaja esitab vastavushindamisasutustele või mille ta teeb neile muul viisil kättesaadavaks;

h) märgid või märgistused ning tingimused kõnealuste märkide või märgistuste kasutamiseks;

i) Euroopa küberturvalisuse sertifikaatide rahvusvahelise tunnustamise tingimused kooskõlas artikliga 87.

4. Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud nõuded peavad olema kooskõlas liidu õigusaktide nõuetega.

5. Komisjonil on volitus võtta vastu rakendusakte, millega kehtestatakse ühised põhimõtted ja näidissätted lõigetes 1, 2 ja 3 sätestatud elementide kohta Euroopa küberturvalisuse sertifitseerimise kavade puhul. Kui see on asjakohane ja kättesaadav, siis võib Euroopa küberturvalisuse sertifitseerimise kava sisaldada viiteid kõnealustele põhimõtetele ja näidissätetele.

6. Käesoleva artikli lõikes 5 osutatud rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega. Euroopa küberturvalisuse sertifitseerimise kavade jaoks ühispõhimõtete ja näidissätete koostamisel või muutmisel konsulteerib komisjon ENISAga ja võtab vajaduse korral arvesse Euroopa küberturvalisuse sertifitseerimise rühma, asjaomaste sidusrühmade ja muude asjaomaste asutuste arvamusi.

Artikkel 82

Euroopa küberturvalisuse sertifitseerimise kavade usaldusväärsuse ja hindamise tasemed

1. Euroopa küberturvalisuse sertifitseerimise kavas võidakse määrata IKT-toodetele, -teenustele, -protsessidele ning hallatud turbeteenustele või üksuste turvaolekule üks või mitu järgmist usaldusväärsuse taset: baastase, märkimisväärne tase või kõrge tase. Need usaldusväärsuse tasemed on samaväärsed IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse ettenähtud kasutusega või sertifitseeritava turvaolekuga üksuste olemusega ning nende tegevuskeskkonnaga seotud riskitasemega, võttes arvesse intsidendi toimumise tõenäosust ja mõju.

2. Euroopa küberturvalisuse sertifikaadid osutavad sellise Euroopa küberturvalisuse sertifitseerimise kavas määratud usaldusväärsuse tasemele, mille alusel kõnealune sertifikaat välja anti. ELi vastavusdeklaratsioonid osutavad usaldusväärsuse baastasemele.

3. Asjakohases Euroopa küberturvalisuse sertifitseerimise kavas määratakse kindlaks igale usaldusväärsuse tasemele vastavad turvanõuded, sh vastavad turvakontrollid ning IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuse turvaoleku puhul nõutav hindamine.

4. Euroopa küberturvalisuse sertifikaadis või ELi vastavusdeklaratsioonis osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sh tehnilisele kontrollile, mille eesmärk on vähendada küberintsidentide riski või ennetada küberintsidente.

5. Euroopa küberturvalisuse sertifikaat või ELi vastavusdeklaratsioon, mis osutab usaldusväärsuse baastasemele, annab kindluse, et IKT-tooted, -teenused, -protsessid, hallatud turbeteenused või üksuste turvaolek, mille kohta kõnealune sertifikaat või ELi vastavusdeklaratsioon on välja antud, vastavad asjaomastele turvanõuetele, sh turvakontrollidele, ning et neid on hinnatud tasemel, mille eesmärk on minimeerida intsidentide ja küberrünnete teadaolevaid põhilisi riske. Hindamine hõlmab vähemalt tehnilise dokumentatsiooni läbivaatamist. Kui tehnilise dokumentatsiooni läbivaatamine ei ole asjakohane, tuleb selle asemel kasutada muud samaväärse mõjuga hindamist.

6. Euroopa küberturvalisuse sertifikaat, mis osutab märkimisväärsele usaldusväärsuse tasemele, annab kindluse, et IKT-tooted, -teenused, -protsessid, hallatud turbeteenused või üksuste turvaolek, mille kohta kõnealune sertifikaat on välja antud, vastavad asjaomastele turvanõuetele, sh turvakontrollidele, ning et neid on hinnatud tasemel, mille eesmärk on minimeerida teadaolevaid intsidentide ja küberrünnete toimumise riske ning piiratud oskuste ja vahenditega isikute poolt toimepandavate küberrünnete riske. Hindamine hõlmab vähemalt kontrolli, mis tõendab, et ei esine avalikult teadaolevaid nõrkusi, ning teste, mis tõendavad, et IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste puhul rakendatakse nõuetekohaselt vajalikke turvakontrolle. Kui selline hindamine ei ole asjakohane, tuleb selle asemel kasutada muud samaväärse mõjuga hindamist.

7. Euroopa küberturvalisuse sertifikaat, mis osutab kõrgele usaldusväärsuse tasemele, annab kindluse, et IKT-tooted, -teenused, -protsessid, hallatud turbeteenused või üksuste turvaolek, mille kohta kõnealune sertifikaat on välja antud, vastavad asjaomastele turvanõuetele, sh turvakontrollidele, ning et neid on hinnatud tasemel, mille eesmärk on minimeerida intsidentide riski ning märkimisväärsete oskuste ja

vahenditega isikute poolt toimepandavate tipptasemel küberrünnete riski. Hindamine hõlmab vähemalt järgmist:

a) kontroll, mis tõendab, et ei esine avalikult teadaolevaid nõrkuseid;

b) testid, mis tõendavad, et IKT-toodete, -teenuste ja -protsesside ning hallatud turbeteenuste või üksuste puhul rakendatakse vajalikke turvakontrolle korrektselt ja tipptasemel;

c) IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste võime hindamine panna vastu suurte oskustega ründajatele, kasutades vajaduse korral läbistustestimist.

Kui selline hindamine ei ole asjakohane, tuleb selle asemel kasutada muud samaväärse mõjuga hindamist. Kõrge usaldusväärsuse taseme puhul viiakse mis tahes vastavushindamistegevus, sh kalibreerimine, testimine, sertifitseerimine ja inspekteerimine ellu Euroopa Majanduspiirkonnas, kui Euroopa küberturvalisuse sertifitseerimise kavas ei ole ette nähtud teisiti.

8. Kui Euroopa küberturvalisuse sertifitseerimise kava on koostatud, et tõendada vastavust konkreetsele liidu õigusaktile või tagada selle nõuetele vastavuse eeldus, siis antakse Euroopa küberturvalisuse sertifikaadiga kindlus, et sertifitseeritud IKT-tooted, -teenused, -protsessid, hallatud turbeteenused või üksuste turvaolek vastab kõnealuse õigusakti asjakohastele küberturvalisuse nõuetele. Nõuetele vastavuse eelduse puhul viiakse mis tahes vastavushindamistegevus, sh kalibreerimine, testimine, sertifitseerimine ja inspekteerimine ellu Euroopa Majanduspiirkonnas, kui Euroopa küberturvalisuse sertifitseerimise kavas ei ole ette nähtud teisiti.

9. Euroopa küberturvalisuse sertifitseerimise kavas võidakse täpsustada konkreetse usaldusväärsuse taseme puhul mitu hindamistaset. Iga hindamistase vastab ühele usaldusväärsuse tasemele.

Artikkel 83
Vastavuse enesehindamine

1. Euroopa küberturvalisuse sertifitseerimise kavas võidakse lubada vastavuse enesehindamise läbiviimist IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste tootja või pakkuja või sertifitseeritava turvaolekuga üksuse ainuvastutusel. Vastavuse enesehindamine on lubatud üksnes väikese riskiga IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku suhtes, mis vastavad usaldusväärsuse baastasemele.

2. IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja või üksus, kelle turvaolekut sertifitseeritakse, võib anda välja ELi vastavusdeklaratsiooni, milles kinnitatakse, et Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud nõuete täitmist on tõendatud. ELi vastavusdeklaratsiooni väljaandmisega võtab tootja, pakkuja või üksus vastutuse IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või turvaoleku vastavuse eest kõnealuses kavas kindlaks määratud nõuetele.

3. IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja või üksus, kelle turvaolekut sertifitseeritakse, hoiab ELi vastavusdeklaratsiooni, tehnilist dokumentatsiooni ja muud asjaomast teavet, mis käsitleb IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või turvaoleku vastavust Euroopa küberturvalisuse sertifitseerimise kavale, asjaomases kavas kindlaks määratud tähtaja

jooksul kättesaadavana artikli 89 kohaselt määratud riiklikule küberturvalisuse sertifitseerimise asutusele. ELi vastavusdeklaratsiooni koopia esitatakse põhjendamatu viivituseta riiklikule küberturvalisuse sertifitseerimise asutusele ja ENISA-le.

Artikkel 84
Täiendav küberturvalisuse alane teave sertifitseeritud IKT-toodete, -teenuste ja -protsesside kohta

1. Nende IKT-toodete, -teenuste või -protsesside tootja või pakkuja, mille kohta on väljastatud ELi vastavusdeklaratsioon või Euroopa küberturvalisuse sertifikaat, teevad kasutajale kättesaadavaks järgmise täiendava küberturvalisuse teabe:

   a) asjaomase IKT-toote, -teenuse või -protsessi ettenähtud kasutusotstarve, sh tootja või pakkuja tagatud turvakeskkond;

   b) suunised ja soovitused, mis aitavad kasutajal IKT-tooteid või -teenuseid turvaliselt konfigureerida, paigaldada, kasutusele võtta ning neid käitada ja hooldada;

   c) see, millist liiki tehnilist turvatuge tootja või pakkuja pakub, ja selle toe kestuse lõppkuupäev, mille jooksul võivad kasutajad eeldada, et nõrkustega tegeletakse ja neile pakutakse turvauuendeid;

   d) kui tootja või pakkuja otsustab teha tarkvara koostenimekirja kasutajale kättesaadavaks, siis teave selle kohta, kust on võimalik seda vaadata.

2. Nende IKT-toodete, -teenuste või -protsesside tootja või pakkuja, mille kohta on väljastatud ELi vastavusdeklaratsioon või Euroopa küberturvalisuse sertifikaat, teeb üldsusele kättesaadavaks järgmise täiendava küberturvalisuse teabe:

   a) ühtne kontaktpunkt, kuhu võib saata ja kus võetakse vastu teavet nõrkuste kohta ning kust võib leida tootja nõrkuste koordineeritud avalikustamise põhimõtted;

   b) teave parandatud nõrkuste kohta, sh nõrkuste kirjeldus, teave, mille põhjal kasutaja saab kindlaks teha, milliseid digielemente sisaldavaid tooteid need mõjutasid, nõrkuste mõju, raskusaste ning selge ja juurdepääsetav teave, mis aitaks kasutajatel nõrkused kõrvaldada; igakülgselt põhjendatud juhtudel, kui tootjad leiavad, et avaldamisest tulenevad turvariskid kaaluvad üles turvalisusega seotud kasu, võivad nad parandatud nõrkust käsitleva teabe avalikustamise edasi lükata, kuni kasutajatele on antud võimalus asjaomast paika kasutada.

3. Lõigetes 1 ja 2 osutatud teave peab olema kättesaadav elektroonilisel kujul ning see peab olema kättesaadav ja seda tuleb ajakohastada kehtivuse ajal ja vähemalt viie aasta jooksul pärast vastava Euroopa küberturvalisuse sertifikaadi või ELi vastavusdeklaratsiooni kehtivuse lõppemist või kehtetuks tunnistamist.

4. Lõigetes 1 ja 2 sätestatud kohustusi ei kohaldata juhul, kui avalikustatav teave võib asjakohase IKT-toote, -teenuse või -protsessi turvalisust kahjustada.

III PEATÜKK
Euroopa küberturvalisuse sertifitseerimise raamistiku juhtimine

1. jagu
Euroopa küberturvalisuse sertifitseerimise kavade üldnormid ja haldamine

Artikkel 85
Euroopa küberturvalisuse sertifikaatide väljastamine

1. Kui IKT-tooted, -teenused, -protsessid, hallatud turbeteenused või üksuse turvaolek on sertifitseeritud Euroopa küberturvalisuse sertifitseerimise kava kohaselt, eeldatakse, et nad vastavad kõnealuse kava nõuetele.

2. Euroopa küberturvalisuse sertifikaadi annavad välja artiklis 91 osutatud vastavushindamisasutused artikli 74 kohaselt komisjoni poolt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavas sisalduvate kriteeriumide alusel.

3. Erandina lõikest 2 võib Euroopa küberturvalisuse sertifitseerimise kavas ette näha, et nimetatud kavast tuleneva Euroopa küberturvalisuse sertifikaadi võivad välja anda üksnes järgmised avaliku sektori asutused:

   a) artiklis 88 osutatud riiklik küberturvalisuse sertifitseerimise asutus, mis on akrediteeritud vastavushindamisasutusena artikli 91 lõike 1 kohaselt;

   b) artikli 91 lõike 1 kohaselt vastavushindamisasutusena akrediteeritud avaliku sektori asutus.

4. Kui artikli 74 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavaga määratakse kindlaks kõrge usaldusväärsuse tase või kui kõnealuses kavas on märgitud vastupidist, siis annab kõnealuse kava kohase Euroopa küberturvalisuse sertifikaadi välja ainult artiklis 88 osutatud riiklik küberturvalisuse sertifitseerimise asutus, mis on akrediteeritud vastavushindamisasutusena artikli 91 lõike 1 kohaselt, või

   a) vastavushindamisasutus eelneva heakskiidu mudeli alusel või

   b) vastavushindamisasutus üldise delegeerimise mudeli alusel.

5. Komisjonil on volitus võtta vastu rakendusakte, milles määratakse kindlaks käesoleva artikli lõikes 4 osutatud eelneva heakskiidu või üldise delegeerimise mudelite menetlused. Rakendusaktide ettevalmistamisel konsulteerib komisjon Euroopa küberturvalisuse sertifitseerimise rühmaga. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.

6. Füüsiline või juriidiline isik, kes esitab oma IKT-tooted, -teenused, -protsessid või hallatud turbeteenused sertifitseerimiseks või üksus, kes taotleb oma turvaoleku sertifitseerimist, peab tegema artikli 89 kohaselt määratud riiklikule küberturvalisuse sertifitseerimise asutusele, kui kõnealune asutus on Euroopa küberturvalisuse sertifikaati väljaandev asutus, või artiklis 91 osutatud vastavushindamisasutusele kättesaadavaks kogu sertifitseerimiseks vajaliku teabe.

7. Vastavushindamisasutused ja vajaduse korral riiklikud küberturvalisuse sertifitseerimise asutused teavitavad ENISAt põhjendamatu viivituseta nende otsustest, mis mõjutavad Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide seisundit kooskõlas artikliga 94.

8. Euroopa küberturvalisuse sertifikaadi saanud isik teavitab vastavushindamisasutust ja asjakohasel juhul lõikes 7 osutatud riiklikku küberturvalisuse sertifitseerimise asutust mis tahes edasistest avastatud nõrkustest või mittevastavustest sertifitseeritud IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuse turvaoleku puhul, mis

tõenäoliselt mõjutavad selle vastavust sertifikaadile. Kõnealune asutus edastab selle teabe põhjendamatu viivituseta asjaomasele riiklikule küberturvalisuse sertifitseerimise asutusele ja hindab sertifikaadi mõju kooskõlas kava tingimustega, nagu on osutatud artikli 81 lõike 2 punktis d.

9. Nende sertifitseeritud IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste puhul, mis on kas täielikult või osaliselt tehtud kindlaks oluliste varadena kooskõlas artikliga 102, ei kasuta Euroopa küberturvalisuse sertifikaadi saanud isikud, paigalda ega integreeri muul viisil sertifitseeritud IKT-toodetesse, -teenustesse, -protsessidesse või hallatud turbeteenustesse IKT-komponente või IKT-komponente sisaldavaid komponente, mis pärinevad suure riskiga tarnijatelt.

10. Euroopa küberturvalisuse sertifikaat antakse Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud tähtajaks ja selle kehtivust võib pikendada, kui asjakohased nõuded on jätkuvalt täidetud.

11. Komisjon teeb liikmesriikidega koostööd, et tagada Euroopa küberturvalisuse sertifikaatide väljastamisega seotud sätete kohaldamisel ka artikli 100 lõike 4 punkti b arvesse võtmine. Vastavushindamisasutus ja vajaduse korral riiklik küberturvalisuse sertifitseerimise asutus esitavad komisjonile taotluse korral ja põhjendamatu viivituseta kogu teabe, mis käsitleb asjaomaste Euroopa küberturvalisuse sertifikaatide või ELi vastavusdeklaratsioonide väljastamist.

Artikkel 86
Riiklikud küberturvalisuse sertifitseerimise kavad ja sertifikaadid

1. Euroopa küberturvalisuse sertifitseerimise kava reguleerimiseseme ja kohaldamisalaga hõlmatud riiklike küberturvalisuse sertifitseerimise kavade ning nendega hõlmatud IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ning üksuste turvaolekuga seotud menetluste õiguslik toime lõpeb artikli 74 lõike 9 kohaselt vastu võetud rakendusaktis kindlaks määratud kuupäeval. Euroopa küberturvalisuse sertifitseerimise kava reguleerimiseseme ja kohaldamisalaga hõlmamata riiklike küberturvalisuse sertifitseerimise kavade ning nendega hõlmatud IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ning üksuste turvaolekuga seotud menetluste õiguslik toime võib jääda kehtima.

2. Liikmesriigid ei võta kasutusele uusi riiklikke küberturvalisuse sertifitseerimise kavasid ning nendega seotud IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ning üksuste turvaolekuga seotud menetlusi, mis on juba hõlmatud Euroopa küberturvalisuse sertifitseerimise kava reguleerimiseseme ja kohaldamisalaga.

3. Riiklike küberturvalisuse sertifitseerimise kavade alusel väljastatud sertifikaadid, mis on hõlmatud Euroopa küberturvalisuse sertifitseerimise kava reguleerimiseseme ja kohaldamisalaga, jäävad kehtima kuni oma kehtivusaja lõpuni.

4. Liikmesriigid teavitavad komisjoni ja Euroopa küberturvalisuse sertifitseerimise rühma enne IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ja üksuste turvaoleku uute riiklike küberturvalisuse sertifitseerimise kavade vastuvõtmist.

5. Komisjon võib soovitada liikmesriigil kehtetuks tunnistada IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku riikliku küberturvalisuse sertifitseerimise kava, kui on juba esitatud taotlus kõnealuseid tooteid, teenuseid, protsesse või turvaolekut hõlmava Euroopa küberturvalisuse sertifitseerimise kava

koostamiseks kooskõlas artikliga 73, võttes arvesse kõnealuse kava koostamise plaani.

Artikkel 87
Euroopa küberturvalisuse sertifikaatide rahvusvaheline tunnustamine

1. IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ja üksuste turvaoleku kolmandate riikide sertifikaate võib tunnustada võrdväärsena Euroopa küberturvalisuse sertifikaatidega rakendusaktiga või liidu ja kõnealuse kolmanda riigi või rahvusvahelise organisatsiooni vahel lepingu sõlmimise teel, kui asjaomase kolmanda riigi või rahvusvahelise organisatsiooni kava nõudeid peetakse Euroopa küberturvalisuse sertifitseerimise kava nõuetega võrdväärseks. Komisjonil on õigus selliseid rakendusakte vastu võtta. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.
2. Rakendusaktid ja lepingud, millele on osutatud lõikes 1, põhinevad artikli 74 lõike 11 kohaselt sätestatud Euroopa küberturvalisuse sertifikaatide rahvusvahelise tunnustamise tingimustel.
3. Lõikes 1 osutatud kolmandate riikide sertifikaatide või rahvusvaheliste organisatsioonide sertifikaatide tunnustamise lepingud sõlmitakse ainult juhul, kui nendes tunnustatakse samuti Euroopa küberturvalisuse sertifikaate võrdväärsena kolmanda riigi sertifikaatidega.

Artikkel 88
Riiklikud küberturvalisuse sertifitseerimise asutused

1. Iga liikmesriik määrab oma territooriumil riikliku(d) küberturvalisuse sertifitseerimise asutuse(d) või vastastikusel kokkuleppel teise liikmesriigiga riikliku(d) küberturvalisuse sertifitseerimise asutuse(d), mis asub või asuvad nimetatud teises liikmesriigis ja mis vastutab või vastutavad järelevalveülesannete eest määravas liikmesriigis.
2. Iga liikmesriik teatab komisjonile määratud riiklike küberturvalisuse sertifitseerimise asutuse andmed. Kui liikmesriik määrab rohkem kui ühe asutuse, teatab ta komisjonile igale asutusele määratud ülesannetest.
3. Iga riiklik küberturvalisuse sertifitseerimise asutus peab olema oma korralduse, rahastamisotsuste, õigusliku struktuuri ja otsustusprotsessi seisukohast sõltumatu üksustest, mille üle ta järelevalvet teeb.
4. Riiklike küberturvalisuse sertifitseerimise asutuste tegevus, mis on seotud Euroopa küberturvalisuse sertifikaatide väljastamisega käesoleva määruse alusel, tuleb rangelt eristada nende järelevalvetegevusest, mis on sätestatud käesolevas artiklis ja artikli 85 lõike 4 punktides a ja b, ning neid tegevusi tuleb ellu viia üksteisest sõltumatult.
5. Liikmesriigid tagavad, et riiklikel küberturvalisuse sertifitseerimise asutustel on piisavad ressursid oma volituste rakendamiseks ning oma ülesannete tulemuslikuks ja tõhusaks täitmiseks.
6. Riiklikel küberturvalisuse sertifitseerimise asutustel on järgmised ülesanded:
   a) nad osalevad artikli 90 lõike 2 kohaselt Euroopa küberturvalisuse sertifitseerimise rühmas;

b) nad teevad Euroopa küberturvalisuse sertifitseerimise kavade üle järelevalvet ja tagavad nende nõuete täitmise kooskõlas artikli 81 lõike 2 punktiga a eesmärgiga tagada IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ja üksuste turvaoleku vastavus nende Euroopa küberturvalisuse sertifikaatide nõuetele, mis on väljastatud nende vastavatel territooriumidel, koostöös asjaomase turujärelevalve- või järelevalveasutusega, sh pädevate asutustega Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555[82] või määruse (EL) 2024/2847 alusel;

c) nad teevad nende vastaval territooriumil asutatud ning vastava Euroopa küberturvalisuse sertifitseerimise kava kohaselt vastavuse enesehindamist tegevate käesolevas määruses sätestatud IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootjate või pakkujate või sertifitseeritava turvaolekuga üksuste kohustuste täitmise üle järelevalvet ning tagavad nende kohustuste täitmise koostöös asjaomaste turujärelevalveasutustega;

d) nad aitavad aktiivselt ja toetavad riiklikke akrediteerimisasutusi või muid asjaomaseid asutusi vastavushindamisasutuste poolt käesoleva määruse kohaldamiseks läbi viidava tegevuse jälgimisel ja järelevalvel, ilma et see piiraks artikli 91 lõike 3 kohaldamist;

e) nad teevad koostööd komisjoniga, kui vastavushindamisasutuse pädevus seatakse kahtluse alla kooskõlas artikliga 94;

f) nad jälgivad ja kontrollivad artikli 85 lõikes 3 osutatud avaliku sektori asutuste tegevust;

g) kui see on kohaldatav, siis nad volitavad vastavushindamisasutusi kooskõlas artikliga 93, teevad vastavushindamisasutuste kohustuste täitmise üle järelevalvet ja tagavad nende täitmise artikli 81 lõike 3 punkti f kohaselt Euroopa küberturvalisuse sertifitseerimise kavade lisa- või erinõuete alusel ning piiravad kehtivaid lubasid, peatavad need või tunnistavad need kehtetuks, kui vastavushindamisasutused ei täida käesoleva määruse nõudeid;

h) nad käsitlevad füüsiliste või juriidiliste isikute kaebusi seoses Euroopa küberturvalisuse sertifikaatidega, mille on välja andnud riiklikud küberturvalisuse sertifitseerimise asutused, või kooskõlas artikli 85 lõikega 4 vastavushindamisasutused, või seoses artikli 83 kohaselt välja antud ELi vastavusdeklaratsioonidega, ning uurivad asjakohasel määral nende kaebuste sisu ja teavitavad kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest;

i) nad esitavad komisjonile, ENISA-le ja Euroopa küberturvalisuse sertifitseerimise rühmale igal aastal aastaaruande oma põhitegevuse kohta 31. märtsiks [jõustumise aasta + 12 kuud] ja teevad kõnealused aruanded kättesaadavaks vastastikuse eksperdihinnangu rühmale, kui riikliku küberturvalisuse sertifitseerimise asutuse suhtes kohaldatakse vastastikust eksperdihinnangut kooskõlas artikliga 89;

---

[82] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

j) nad teevad koostööd teiste riiklike küberturvalisuse sertifitseerimise asutuste, turujärelevalveasutuste või muude avaliku sektori asutustega, muu hulgas jagades teavet IKT-toodete, -teenuste ja -protsesside, hallatud turbeteenuste ja üksuste turvaoleku võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele;

k) nad jälgivad küberturvalisuse sertifitseerimise valdkonna asjakohast arengut.

7. Igal riiklikul küberturvalisuse sertifitseerimise asutusel on vähemalt järgmised volitused:

a) anda vastavushindamisasutustele, Euroopa küberturvalisuse sertifikaadi omanikele ja ELi vastavusdeklaratsiooni väljaandjatele korraldus esitada teavet, mis on vajalik tema ülesannete täitmiseks;

b) uurida auditi vormis vastavushindamisasutusi, Euroopa küberturvalisuse sertifikaadi omanikke ja ELi vastavusdeklaratsiooni väljaandjaid, et kontrollida nende poolt käesolevas jaotises sätestatud nõuete järgimist;

c) võtta asjakohaseid meetmeid vastavalt liikmesriigi õigusele tagamaks, et vastavushindamisasutused, Euroopa küberturvalisuse sertifikaadi omanikud ja ELi vastavusdeklaratsiooni väljaandjad järgivad käesoleva määruse ja Euroopa küberturvalisuse sertifitseerimise kava nõudeid;

d) saada juurdepääs kõigile vastavushindamisasutuste ja Euroopa küberturvalisuse sertifikaadi omanike ruumidele, et viia läbi uurimisi kooskõlas liidu õigusaktide või liikmesriigi menetlusõigusega;

e) tunnistada liikmesriigi õiguse kohaselt kehtetuks Euroopa küberturvalisuse sertifikaadid, mille on välja andnud riiklikud küberturvalisuse sertifitseerimise asutused või vastavushindamisasutused kooskõlas artikli 85 lõikega 4, kui need sertifikaadid ei vasta käesolevale määrusele või Euroopa küberturvalisuse sertifitseerimise kavale;

f) määrata liikmesriigi õiguse kohaselt artiklis 97 osutatud karistusi ning nõuda käesolevas määruses sätestatud kohustuste rikkumise viivitamatut lõpetamist.

8. Riiklikud küberturvalisuse sertifitseerimise asutused teevad omavahel ja komisjoniga koostööd, eelkõige vahetavad teavet, kogemusi ja häid tavasid seoses IKT-toodete, -teenuste ja -protsesside, hallatud turbeteenuste ja üksuste turvaoleku küberturvalisuse sertifitseerimisega ning küberturvalisust puudutavate tehniliste küsimustega.

9. ENISA koostab [jõustumise kuupäev + kuus kuud] käesoleva artikli lõike 6 punktis i osutatud aruande vormi koostöös komisjoni ja Euroopa küberturvalisuse sertifitseerimise rühmaga.

Artikkel 89
Vastastikune eksperdihinnang

1. Riiklike küberturvalisuse sertifitseerimise asutuste suhtes kohaldatakse vastastikust eksperdihinnangut.

2. Vastastikune eksperdihinnang viiakse läbi mõistlike ja läbipaistvate hindamiskriteeriumide ja -menetluste alusel, mis käsitlevad eelkõige struktuuridele, inimressurssidele ja menetlustele kohaldatavaid nõudeid, konfidentsiaalsust ja kaebusi.

3. Vastastikuse eksperdihinnangu puhul hinnatakse järgmist:

a) kas riikliku küberturvalisuse sertifitseerimise asutuse tegevus, mis on seotud käesolevas määruses osutatud Euroopa küberturvalisuse sertifikaatide väljaandmisega, on rangelt lahus artiklis 88 sätestatud järelevalvetegevusest ning kas nimetatud tegevusi viiakse läbi üksteisest sõltumatult, kui see on asjakohane;

b) IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ja üksuste turvaoleku Euroopa küberturvalisuse sertifikaatide nõuetele vastavuse jälgimise reeglite järelevalve ja täitmise tagamise menetlused kooskõlas artikli 88 lõike 7 punktiga a;

c) artikli 88 lõike 7 punkti b kohased IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste tootjate või pakkujate või sertifitseeritava turvaolekuga üksuste kohustuste täitmise järelevalve ja kohustuste täitmise tagamise menetlused;

d) vastavushindamisasutuste tegevuse jälgimise, selleks loa andmise ja selle üle järelevalve tegemise menetlused.

4. Vastastikuse eksperdihinnangu viivad vähemalt kord iga viie aasta tagant läbi vähemalt kaks teiste liikmesriikide küberturvalisuse sertifitseerimise asutust ja komisjon. ENISA osaleb samuti vastastikuses eksperdihinnangus vaatlejana. Vastastikuse eksperdihinnangu rühm koostab lõpparuande ja vastastikuse eksperdihinnangu kokkuvõtte.

5. ENISA toetab vastastikuse eksperdihinnangu mehhanismi ja vastastikuste eksperdihinnangute korraldamist, sh töötades välja asjakohased suunisdokumendid ja vormid koostöös komisjoni ning Euroopa küberturvalisuse sertifitseerimise rühmaga.

6. Komisjonil on õigus võtta vastu rakendusakte, millega kehtestatakse vastastikuse hindamise kava, mis hõlmab vähemalt viit aastat, sätestatakse vastastikuse hindamise rühma koosseisu kriteeriumid, vastastikuse hindamise metoodika, ajakava, sagedus ja muud vastastikuse hindamisega seotud ülesanded. Rakendusaktide ettevalmistamisel konsulteerib komisjon Euroopa küberturvalisuse sertifitseerimise rühmaga ja ENISAga. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.

7. Euroopa küberturvalisuse sertifitseerimise rühm vaatab lõpparuande, sh võimalikud suunised või soovitused ja vastastikuse eksperdihinnangu kokkuvõtte läbi ning kiidab kokkuvõtte heaks artikli 79 lõikes 2 osutatud veebisaidil avaldamiseks.

Artikkel 90
Euroopa küberturvalisuse sertifitseerimise rühm

1. Moodustatakse Euroopa küberturvalisuse sertifitseerimise rühm.

2. Euroopa küberturvalisuse sertifitseerimise rühm koosneb riiklike küberturvalisuse sertifitseerimise asutuste esindajatest või teiste asjakohaste riiklike asutuste esindajatest. Euroopa küberturvalisuse sertifitseerimise rühma liige võib esindada üksnes kahte liikmesriiki.

3. Euroopa küberturvalisuse sertifitseerimise rühmal on järgmised ülesanded:

a) nõustada ja aidata komisjoni tema töös eesmärgiga tagada käesolevas jaotises sätestatud normide järjepidev rakendamine ja kohaldamine, küberturvalisuse

sertifikaadi poliitikaküsimused ning poliitiliste lähenemisviiside koordineerimine;

b) nõustada ja abistada komisjoni Euroopa küberturvalisuse sertifitseerimise kavade taotluste koostamisel kooskõlas artikliga 73;

c) abistada ja nõustada ENISAt ja teha temaga koostööd ettevalmistava kava koostamisel kooskõlas artikliga 74 ning tehniliste kirjelduste koostamisel kooskõlas artikliga 77;

d) abistada ja nõustada ENISAt ja komisjoni ning teha nendega koostööd haldamise tegevuse puhul kooskõlas artikliga 75;

e) abistada ja nõustada komisjoni ja teha temaga koostööd kehtivate Euroopa küberturvalisuse sertifitseerimise kavade läbivaatamisel või kehtetuks tunnistamisel kooskõlas artikliga 76;

f) soovitada esitada komisjonile taotlus Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava koostamiseks kooskõlas artikli 73 lõikega 2;

g) võtta vastu komisjonile suunatud arvamusi seoses olemasolevate Euroopa küberturvalisuse sertifitseerimise kavade haldamise, läbivaatamise ja kehtetuks tunnistamisega;

h) analüüsida olulisi arenguid küberturvalisuse sertifitseerimise valdkonnas, sh riiklikul tasandil kooskõlas artikliga 86, ning vahetada teavet ja häid tavasid küberturvalisuse sertifitseerimise kavade kohta;

i) edendada koostööd riiklike küberturvalisuse sertifitseerimise asutuste vahel käesolevas jaotises sätestatud normide kohaselt suutlikkuse suurendamise ja teabevahetuse teel, eelkõige küberturvalisuse sertifitseerimist käsitlevate küsimuste puhul;

j) toetada vastastikuse eksperdihinnangu mehhanismi rakendamist kooskõlas artikliga 89 ning vastastikuse hindamise mehhanisme kooskõlas artikli 81 lõike 2 punkti g kohaselt Euroopa küberturvalisuse sertifitseerimise kavas kehtestatud normidega;

k) hõlbustada Euroopa küberturvalisuse sertifitseerimise kavade vastavusse viimist rahvusvaheliselt tunnustatud standarditega, sh olemasolevate Euroopa küberturvalisuse sertifitseerimise kavade haldamise osana, ja asjakohasel juhul esitada ENISA-le soovitusi teha koostööd asjaomaste Euroopa või rahvusvaheliste standardiorganisatsioonidega, et kõrvaldada kehtivate Euroopa rahvusvaheliselt tunnustatud standardite puudused ja lüngad.

4. Komisjon juhatab ENISA abiga Euroopa küberturvalisuse sertifitseerimise rühma ja osutab sellele sekretariaaditeenust.

5. Komisjon võib luua Euroopa küberturvalisuse sertifitseerimise rühma allrühmad mis tahes järgmisel otstarbel:

a) konkreetsete küsimuste läbivaatamiseks komisjoni antud pädevuse alusel;

b) Euroopa sertifitseerimise kavade haldamiseks ja läbivaatamiseks kooskõlas käesoleva määrusega ning komisjoni antud pädevuse alusel.

6. Allrühmad annavad aru Euroopa küberturvalisuse sertifitseerimise rühmale.

7. Komisjon ja ENISA on allrühmade kaaseesistujad ning ENISA tagab allrühmade sekretariaaditeenused.

8. Euroopa küberturvalisuse sertifitseerimise rühm ja selle allrühmad võtavad komisjoni ettepaneku alusel ja kokkuleppel komisjoniga rühma ja allrühmade liikmete lihthäälteenamusega vastu kodukorra.

2. jagu
Vastavushindamisasutused

Artikkel 91
Vastavushindamisasutuste pädevus

1. Vastavushindamisasutusi akrediteerivad määruse (EÜ) nr 765/2008 kohaselt määratud riiklikud akrediteerimisasutused. Vastavushindamisasutus akrediteeritakse üksnes siis, kui ta vastab käesoleva määruse I lisas sätestatud nõuetele.

2. Kui Euroopa küberturvalisuse sertifikaadi annab välja riiklik küberturvalisuse sertifitseerimise asutus vastavalt käesolevale määrusele, akrediteeritakse lõike 1 kohaselt riikliku küberturvalisuse sertifitseerimise asutuse sertifitseerimise organ vastavushindamisasutuseks.

3. Lõikes 1 osutatud vastavushindamisasutuste akrediteerimine kehtib maksimaalselt viis aastat ja selle kehtivust võib pikendada, kui vastavushindamisasutus vastab käesolevas artiklis sätestatud nõuetele. Riiklik akrediteerimisasutus võtab mõistliku aja jooksul kõik asjakohased meetmed, et piirata lõike 1 kohast vastavushindamisasutuse akrediteerimist, see peatada või kehtetuks tunnistada, kui akrediteerimise tingimused ei ole täidetud või ei ole enam täidetud või kui vastavushindamisasutus ei täida käesoleva määruse nõudeid.

4. Artikli 92 kohaselt IKT-tooteid hõlmava Euroopa küberturvalisuse sertifitseerimise kava akrediteerimise lisa- või erinõuete kehtestamisel proovitakse võimaluse korral tagada koostoime määruse (EL) 2024/2847 alusel teada antud asutusi käsitlevate nõuete ning akrediteerimisnõuetega juba vastu võetud küberturvalisuse sertifitseerimise kavade alusel.

5. Kui vastavushindamisasutus on akrediteeritud kooskõlas määrusega (EL) 2024/2847, võivad asjaomased asutused kasutada uuesti varasema akrediteerimise protsessi tulemusi, mis käsitlevad mis tahes kattuvaid nõudeid, tõenditena käesoleva määruse alusel läbiviidava akrediteerimisprotsessi vältel.

Artikkel 92
Vastavushindamisasutuste pädevuse täiendav ühtlustamine

1. Kui Euroopa küberturvalisuse sertifitseerimise kavas on artikli 81 lõike 3 punkti f kohaselt sätestatud lisa- või erinõuded, annavad vastavushindamisasutused artikli 88 lõike 1 kohaselt määratud riiklikule küberturvalisuse sertifitseerimise asutusele loa kõnealuse kava alusel ülesannete täitmiseks. Kõnealune luba antakse ainult juhul, kui vastavushindamisasutus on akrediteeritud ning vastab lisa- või erinõuetele, mis on sätestatud Euroopa küberturvalisuse sertifitseerimise kavas.

2. Kui vastavushindamisasutus taotleb luba käesoleva artikli alusel, esitab ta taotluse selle asutamise liikmesriigi riiklikule küberturvalisuse sertifitseerimise asutusele või riiklikule küberturvalisuse sertifitseerimise asutusele, kelle poole asjaomane liikmesriik on pöördunud vastavalt artikli 88 lõikele 1.

3. Vastavushindamisasutus võib siiski taotleda muu kui lõikes 2 osutatud riikliku küberturvalisuse sertifitseerimise asutuse luba, kui on tegemist ühega järgmistest olukordadest:

   a) kui lõikes 1 osutatud riiklik küberturvalisuse sertifitseerimise asutus ei anna lubasid sellisteks vastavushindamisteks, mille jaoks luba taotletakse;

   b) kui lõikes 1 osutatud riiklik küberturvalisuse sertifitseerimise asutus ei ole läbinud artikli 89 kohast vastastikust eksperdihinnangut nende vastavushindamiste suhtes, mille jaoks luba taotletakse.

4. Kui riiklik küberturvalisuse sertifitseerimise asutus saab taotluse vastavalt lõikele 3, teatab ta sellest selle liikmesriigi riiklikule küberturvalisuse sertifitseerimise asutusele, kus taotluse esitanud vastavushindamisasutus on asutatud. Neil juhtudel võib kõnealuse liikmesriigi riiklik küberturvalisuse sertifitseerimise asutus osaleda loa andmisel vaatlejana.

5. Riiklik küberturvalisuse sertifitseerimise asutus võib esitada teisele riiklikule küberturvalisuse sertifitseerimise asutusele taotluse viia läbi osa hindamisest. Sellisel juhul väljastab loa sertifikaadi taotluse esitanud asutus.

6. Lõikes 1 osutatud luba kehtib kuni akrediteerimise kehtivusaja lõpuni ja seda võidakse uuendada tingimusel, et vastavushindamisasutus vastab lõikes 1 sätestatud nõuetele ja selle akrediteeringut on samuti uuendatud.

7. Riiklik küberturvalisuse sertifitseerimise asutus võtab mõistliku aja jooksul kõik asjakohased meetmed, et piirata lõike 1 kohast vastavushindamisasutuse luba, see peatada või kehtetuks tunnistada, kui loa saamise tingimused ei ole täidetud või ei ole enam täidetud või kui vastavushindamisasutus ei täida käesoleva määruse nõudeid.

8. Komisjonil on õigus võtta vastu rakendusakte, et kehtestada vastavushindamisasutustele loa andmise menetlused, sh piiriülese koostöö kohta. Rakendusaktide ettevalmistamisel konsulteerib komisjon ENISA ja Euroopa küberturvalisuse sertifitseerimise rühmaga. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 93
Vastavushindamisasutustest teada andmine

1. Iga Euroopa küberturvalisuse sertifitseerimise kava puhul annavad liikmesriigi riiklikud küberturvalisuse sertifitseerimise asutused komisjonile ja muudele liikmesriikidele teada akrediteeritud ja asjakohasel juhul artikli 92 kohaselt loa saanud vastavushindamisasutustest.

2. Riiklikud küberturvalisuse sertifitseerimise asutused viivad lõikes 1 osutatud teavitamise läbi, kasutades komisjoni väljatöötatud ja hallatud elektroonilist teavitamisvahendit.

3. Komisjonil on õigus võtta vastu rakendusakte, et kehtestada käesoleva artikli lõikes 1 osutatud teavitamise asjaolud, vormingud ja kord, sh teiste liikmesriikide vastuväidete esitamise kord teavitamisprotsessi ajal, vastavushindamisasutuste kordumatu identifitseerimistunnus ning teavitamise piiramise, peatamise või kehtetuks tunnistamise asjaolud. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 94

Vastavushindamisasutuste pädevusega seotud probleemid

1. Komisjon uurib iga juhtumit, mille puhul tal on kahtlusi või talle on teatatud kahtlustest seoses vastavushindamisasutuse pädevusega täita tema suhtes kehtivaid nõudeid ja kohustusi või seoses sellega, kas vastavushindamisasutus täidab neid jätkuvalt.
2. Riiklik küberturvalisuse sertifitseerimise asutus esitab komisjonile taotluse korral kogu teabe teavitamise aluse või asjaomase vastavushindamisasutuse pädevuse säilimise kohta.
3. Komisjon tagab, et kogu tundlikku teavet, mis uurimise käigus saadi, käsitletakse konfidentsiaalsena.
4. Kui komisjon teeb kindlaks, et vastavushindamisasutus ei täida või enam ei täida temast teada andmise aluseks olevaid nõudeid, teavitab ta sellest riiklikku küberturvalisuse sertifitseerimise asutust ja nõuab temalt vajalike parandusmeetmete võtmist, sh vajaduse korral teavitamise tühistamist.
5. Liikmesriigid tagavad, et teavitatud asutuste otsuste vaidlustamiseks on olemas asjakohane menetlus.

Artikkel 95

Vastavushindamisasutusi käsitlev teave ja teabe säilitamise kohustus

1. Vastavushindamisasutused teavitavad riiklikku küberturvalisuse sertifitseerimise asutust järgmisest:
   a) kõik juhtumid, kui sertifikaat jäetakse andmata, seda kitsendatakse, see peatatakse või tunnistatakse kehtetuks;
   b) artikli 93 lõikes 1 osutatud teavitamise ulatust ja tingimusi mõjutavad asjaolud;
   c) kõik turujärelevalveasutustelt saadud teabetaotlused vastavushindamistoimingute kohta;
   d) taotluse korral vastavushindamistoimingud, mis on teavitamisega hõlmatud valdkonnas läbi viidud, ja muu tegevus, sh piiriülene tegevus ja alltöövõtt.
2. Vastavushindamisasutused esitavad samuti ENISA-le lõike 1 punktis a osutatud teabe, et lihtsustada selle ülesannete täitmist artikli 79 alusel.
3. Vastavushindamisasutused esitavad muudele vastavushindamisasutustele, mis viivad käesoleva määruse alusel läbi samalaadset vastavushindamistegevust samade IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või sertifitseeritava turvaolekuga üksuste puhul, põhjendamatu viivituseta asjakohase teabe küsimuste kohta, mis käsitlevad vastavushindamise negatiivseid ja taotluse korral positiivseid tulemusi.
4. Vastavushindamisasutused hoiavad kasutuses aruannete süsteemi, mis sisaldab kõiki dokumente ja tõendeid, mis on esitatud või saadud iga nende läbiviidud hindamise ja sertifitseerimise puhul. Aruandeid säilitatakse turvalisel ja juurdepääsetaval viisil sertifitseerimiseks vajaliku aja jooksul ning vähemalt viis aastat pärast asjaomase Euroopa küberturvalisuse sertifikaadi aegumist või kehtetuks tunnistamist.

3. jagu
Muud sätted

Artikkel 96
Õigus esitada kaebus ja õigus tõhusale õiguskaitsevahendile

1. Füüsilistel ja juriidilistel isikutel on õigus esitada kaebus Euroopa küberturvalisuse sertifikaadi väljaandjale või asjaomasele riiklikule Euroopa küberturvalisuse sertifitseerimise asutusele, kui kaebus on seotud artikli 85 lõike 4 kohaselt tegutseva vastavushindamisasutuse välja antud Euroopa küberturvalisuse sertifikaadiga.

2. Asutus, kellele kaebus esitatakse, teavitab kaebuse esitajat kaebuse menetlemise käigust ja tehtud otsusest, samuti lõigetes 3 ja 4 osutatud õigusest tõhusale õiguskaitsevahendile.

3. Olenemata halduslikest ja muudest kohtuvälistest õiguskaitsevahenditest on füüsilistel ja juriidilistel isikutel õigus tõhusale õiguskaitsevahendile seoses järgmisega:

   a) lõikes 1 osutatud asutuse otsused, kaasa arvatud seoses Euroopa küberturvalisuse sertifikaadi ebaõige väljaandmise, välja andmata jätmise ning nende füüsiliste ja juriidiliste isikute saadud Euroopa küberturvalisuse sertifikaatide tunnustamisega, kui see on kohaldatav;

   b) lõikes 1 osutatud asutusele esitatud kaebusele reageerimata jätmine.

4. Käesoleva artikli kohased menetlused algatatakse selle liikmesriigi kohtus, kus asub asutus, mille suhtes õiguskaitsevahendit taotletakse.

Artikkel 97
Karistused

Liikmesriigid kehtestavad käesoleva jaotise ja Euroopa küberturvalisuse sertifitseerimise kavade rikkumise korral kohaldatavad karistusnormid, ning võtavad kõik vajalikud meetmed nende rakendamise tagamiseks. Kehtestatud karistused peavad olema mõjusad, proportsionaalsed ja hoiatavad. Liikmesriigid teavitavad komisjoni viivitamata nimetatud normidest ja meetmetest ning kõikidest nende hilisematest muudatustest.

IV JAOTIS
IKT TARNEAHELATE TURVALISUS

I PEATÜKK
Usaldusväärse IKT tarneahela raamistik

Artikkel 98
Raamistiku kohaldamisala

1. Usaldusväärse IKT tarneahela raamistik tagab liidu tasandil turvamehhanismi, et maandada mittetehnilisi riske väga kriitilise tähtsusega ja muudes kriitilise tähtsusega sektorites, nagu on osutatud direktiivis (EL) 2022/2555. Mehhanismi alusel määratakse kindlaks olulised IKT-varad kriitilise tähtsusega IKT tarneahelates ning

kehtestatakse asjakohased ja proportsionaalsed leevendusmeetmed direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste jaoks.

2. Käesolevas jaotises sätestatud kohustused ei piira kohustusi mis on sätestatud määruse (EL) 2024/2847 artiklis 13 ning riiklikes sätetes, millega võetakse üle direktiivi (EL) 2022/2555 artikkel 21.

3. Käesolevas peatükis kehtestatud sätted ei takista liikmesriike vastu võtmast või kehtima jätmast sätteid, millega tagatakse kõrgem IKT tarneahelate küberturvalisuse tase, tingimusel et sellised sätted on kooskõlas liikmesriikide kohustustega, mis on sätestatud liidu õiguses.

Artikkel 99
Turvariski hindamine

1. Komisjon või vähemalt kolmest liikmesriigist koosnev rühm võib esitada direktiivi (EL) 2022/2555 artikli 14 kohaselt loodud koostöörühmale (edaspidi „võrgu- ja infoturbe koostöörühm“) taotluse viia läbi liidu tasandi koordineeritud turvariski hindamine kooskõlas kõnealuse direktiivi artikliga 22. Kui turvariski hindamine viiakse kõnealuse taotluse alusel läbi, siis hõlmab see eelkõige vastava IKT tarneahela oluliste IKT-varade ning samuti kõnealuseid varasid mõjutavate peamiste ohusubjektide, riskide ja nõrkuste väljapakutud kindlakstegemist. Liidu tasandi koordineeritud turvariski hindamiste käigus koostatakse riskistsenaariumid ja pakutakse välja meetmed kindlaks tehtud riskide maandamiseks.

2. Liidu tasandi koordineeritud turvariski hindamised viiakse läbi kuue kuu jooksul alates lõikes 1 osutatud taotluse esitamisest. Komisjoni taotlusel võib võrgu- ja infoturbe koostöörühm nõustuda lühema ajavahemikuga.

3. Kui komisjonil on piisav põhjus olla seisukohal, et IKT tarneahelast tuleneb liidu turvalisusele oluline küberoht ja et siseturu nõuetekohase toimimise säilitamiseks on vaja võtta meetmeid, siis teeb komisjon viivitamata järgmist:

   a) konsulteerib liikmesriikidega vajaduse asjus võtta üks või mitu artiklis 103 osutatud leevendusmeedet ning

   b) viib läbi turvariski hindamise, võttes arvesse liikmesriikidega konsulteerimist. Turvariski hindamine hõlmab oluliste IKT-varade ning samuti kõnealuseid varasid mõjutavate peamiste ohusubjektide, riskide ja nõrkuste väljapakutud kindlakstegemist. Turvariski hindamise käigus koostatakse riskistsenaariumid ja pakutakse välja meetmed kindlaks tehtud riskide maandamiseks.

Artikkel 100
Küberturvalisuse seisukohast muret tekitavate kolmandate riikide kindlaks määramine

1. Kui artiklis 99 osutatud turvariski hindamise tulemusena või muude allikate, näiteks liidu või liikmesriigi nimel tehtud avaliku pöördumise alusel näib, et kolmas riik põhjustab IKT tarneahelatele tõsise ja struktuurse mittetehnilise riski, kontrollib komisjon kõnealuse riigi põhjustatud riski, võttes arvesse järgmisi elemente:

   a) kolmandas riigi õigusaktide olemasolu, millega nõutakse nende jurisdiktsiooni kuuluvatelt üksustelt teabe esitamist tark- või riistvara nõrkuste kohta kõnealuse kolmanda riigi asutustele, enne kui on saadud teada kõnealuste nõrkuste ärakasutamisest;

b) sõltumatute allikate alusel tõendatud olemasolevad tavad kolmandas riigis, millega nõutakse kolmanda riigi jurisdiktsiooni kuuluvatelt üksustelt teabe esitamist tark- või riistvara nõrkuste kohta kõnealuse kolmanda riigi asutustele, enne kui on saadud teada kõnealuste nõrkuste ärakasutamisest;

c) tulemuslike õiguskaitsevahendite ning sõltumatute ja demokraatlike kontrollimehhanismide puudumine, mis võivad kõrvaldada kindlaks tehtud turvaprobleemid, sh punktis b osutatud kehtivate tavadega seoses;

d) põhjendatud teave kõnealuse riigi territooriumil tegutsevate ning pahatahtlikku kübertegevust või kampaaniaid ellu viivate ohusubjektidega seotud ühe või enama intsidendi kohta ning kolmanda riigi puudulik võime või valmidus teha komisjoni või liikmesriikidega koostööd kõnealuste ohusubjektide tegevusest tuleneva riski maandamiseks;

e) liidu tasandi koordineeritud turvariski hindamistest või liikmesriikide või rahvusvaheliste organisatsioonide aruannetest tulenev asjakohane teave.

2. Kui komisjon järeldab pärast lõikes 1 osutatud kontrolli, et kolmas riik põhjustab tõsise ja struktuurse mittetehnilise riski IKT tarneahelatele, siis võib ta rakendusakti abil määrata kõnealuse kolmanda riigi IKT tarneahelate jaoks küberturvalisuse seisukohast muret tekitavaks riigiks. Nimetatud rakendusakt võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.

3. Komisjon vaatab korrapäraselt läbi lõike 2 kohaselt vastu võetud rakendusaktid.

4. Suure riskiga tarnijatel ei ole õigust:

a) osaleda määruse (EL) 1025/2012 artikli 10 lõikes 1 osutatud Euroopa standardite või Euroopa standardimisdokumentide ning määruse (EL) 2024/2847 artiklis 27 osutatud ühtsete kirjelduste koostamises, nende hindamises ning nende asjus konsulteerimises või otsuste tegemises küberturvalisuse valdkonnas;

b) esitada Euroopa küberturvalisuse sertifikaadi saamise taotlust või olla selle omanik kooskõlas III jaotisega;

c) saada akrediteeritud vastavushindamisasutuseks kooskõlas III jaotisega;

d) esitada taotlust, et saada Euroopa individuaalsete küberturbeoskuste tunnistuste volitatud tõendajaks kooskõlas II jaotise 4. jaoga;

e) osaleda direktiivi 2014/24/EL ja 2014/25/EL ülevõtmise õigusaktide kohaselt korraldatud riigihankemenetlustes IKT-komponentide või IKT-komponente sisaldavate komponentide pakkumiseks, mida kasutatakse artikli 102 kohaselt kindlaks määratud olulistes IKT-varades;

f) osaleda kooskõlas määruse (EL, Euratom) 2024/2509 artikliga 136 eelarve otsese ja kaudse täitmise ning liidu sektoripõhiste normide alusel rakendatavate liidu rahastamisprogrammide ja -vahendite mis tahes tegevustes ning samuti mis tahes liidu rahastamistegevuses, mida rakendatakse eelarve jagatud täitmise alusel, IKT-komponentide või IKT-komponente sisaldavate komponentide pakkumise puhul, mida kasutatakse artikli 102 kohaselt kindlaks määratud olulistes IKT-varades.

Punktides a–f osutatud menetluste eest vastutavad asutused viivad läbi käesoleva lõike otstarbel vajalikud hindamised. Asutused võivad sel otstarbel samuti tugineda artiklis 104 osutatud loetelule.

5. Kui suure riskiga tarnija on juba saanud Euroopa küberturvalisuse sertifikaadi III jaotise kohaselt, tunnistab pädev asutus selle ilma põhjendamatu viivituseta kehtetuks.

Artikkel 101
Üldine IKT tarneahela turvamehhanism

Kui võrgu- ja infoturbe koostöörühm on teinud kooskõlas käesoleva määruse artikli 99 lõikega 1 liidu tasandi koordineeritud turvariski hindamise või pärast IKT tarneahela puhul artikli 99 lõike 3 kohaselt olulise küberohu menetluse lõpuleviimist võib komisjon võtta artiklis 102 ja artikli 103 lõigetes 1 ja 2 sätestatud meetmeid.

Artikkel 102
Oluliste IKT-varade kindlaksmääramine

1. Kui artikli 99 lõike 1 või 3 kohaselt läbiviidud riskihindamine osutab IKT tarneahela puhul märkimisväärsetele küberturvalisuse riskidele, on komisjonil õigus võtta vastu rakendusakte, milles määratakse kindlaks olulised IKT-varad, mida kasutavad toodete tootmiseks või teenuste osutamiseks direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksused. Need rakendusaktid võetakse vastu kooskõlas käesoleva määruse artikli 118 lõikes 2 osutatud kontrollimenetlusega.

2. Lõikes 1 osutatud oluliste IKT-varade kindlaks tegemisel võtab komisjon arvesse järgmisi elemente:

   a) kas kõnealustel varadel on direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuse toodetavate toodete või pakutavate teenuste toimimise jaoks olulised ja tundlikud funktsioonid;

   b) kas intsidendid, sh kui need on tekkinud kõnealuste varadega seotud ärakasutatavate nõrkuste tõttu, võivad põhjustada IKT tarneahelate olulisi häireid siseturul või viia andmete väljatoimetamiseni;

   c) kas kõnealuste varade puhul sõltutakse piiratud arvust tarnijatest;

   d) artiklis 99 osutatud riskihindamise tulemused.

Artikkel 103
IKT tarneahelaga seotud leevendusmeetmed

1. Komisjonil on õigus võtta vastu rakendusakte, mille kohaselt direktiivi (EL) 2022/2555 I ja II lisas osutatud konkreetset liiki üksused ei tohi kasutada, paigaldada ega integreerida mis tahes kujul IKT-komponente või IKT-komponente sisaldavaid komponente suure riskiga tarnijatelt, kes on määratud kindlaks kooskõlas artikliga 104, artikli 102 kohaselt kindlaks määratud oluliste IKT-varade puhul, kui see on vajalik liidus kõrgetasemelise küberturvalisuse, küberkerksuse ja usalduse tagamiseks. Kõnealustes rakendusaktides nähakse ette sobilikud üleminekuperioodid, mille vältel komisjon avaldab artiklis 104 osutatud suure riskiga tarnijate loetelud, ning täiendavad ajavahemikud asjaomaste IKT-komponentide ja IKT-komponente sisaldavate komponentide järkjärguliseks kasutusest kõrvaldamiseks. Kõnealuses rakendusaktis võidakse samuti määrata kindlaks kõnealused IKT-komponendid või IKT-komponente sisaldavad komponendid.

2. Komisjonil on õigus võtta vastu rakendusakte, mille kohaselt direktiivi (EL) 2022/2555 I ja II lisas osutatud konkreetset liiki üksuste suhtes kohaldatakse

ühte või mitut järgmist leevendusmeedet nende IKT tarneahela puhul ja eelkõige artikli 102 kohaselt kindlaks määratud nende oluliste IKT-varade puhul, et maandada artikli 99 kohaselt läbiviidud turvariski hindamistes kindlaks tehtud riske, kui see on vajalik liidus kõrgetasemelise küberturvalisuse, küberkerksuse ja usalduse tagamiseks:

a) läbipaistvusnõuete kohaldamine seoses pädevale asutusele teabe esitamisega IKT tarneahelas kooskõlas artikliga 102 kindlaks määratud oluliste IKT-varade tarnijate kohta;

b) keelud, mis on seotud andmeedastusega kolmandatesse riikidesse ja andmete kaugtöötlusega kolmandast riigist;

c) kolmanda isiku auditeeritavad tehnilised meetmed, sh:

i) seadmepõhise töötluse kasutamine;

ii) võrgusüsteemide konkreetne segmentimine;

iii) olulistele IKT-varadele mis tahes kaug- või füüsilise juurdepääsu keelamine;

iv) mitteoluliste funktsioonide keelamine;

v) operatiivvõrgu seire;

vi) tark- ja riistvara testimine;

d) tegevuskontrolliga seotud piirangud, sh organisatsiooni funktsioonide edasi andmine hallatud teenuse osutajatele;

e) üksuse ja selle tarnijate lepinguliste suhetega seotud piirangud;

f) nõuded, mille kohaselt võivad teenust käitada, hallata, hooldada või toetada asjaomase riikliku pädeva asutuse kontrollitud töötajad;

g) IKT-komponentide või IKT-komponente sisaldavate komponentide tarne mitmekesistamine.

3. Komisjon võib lõikes 2 osutatud meetmete kehtestamisel kehtestada meetmete tehnilised ja metodoloogilised nõuded.

4. Komisjon hindab enne lõigetes 1 ja 2 osutatud rakendusaktide vastuvõtmist võimalikke riske ja sõltuvusi ning eelkõige:

a) kui see on kohaldatav, siis riskitaset, mis on seotud oluliste IKT-varade suure riskiga tarnijatelt pärinevate IKT-komponentide või IKT-komponente sisaldavate komponentide mis tahes kujul kasutamise, paigaldamise või integreerimisega;

b) direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksustele kohustustest tekkida võiv majanduslik ja sotsiaalne mõju;

c) muude tarnijate kui suure riskiga tarnijate kättesaadavus;

d) üksuse IKT tarneahelat mõjutavast intsidentist põhjustatud võimalikud häired piiriüleses majandus- ja sotsiaaltegevuses.

5. Käesoleva artikli lõigetes 1 ja 2 osutatud rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega ja need vaadatakse läbi vähemalt iga 36 kuu tagant.

6. Erandolukorras, mis põhjendab sekkumist siseturu nõuetekohase toimimise säilitamiseks ja kui komisjonil on piisavalt põhjust olla seisukohal, et selliste IKT-komponentide või IKT-komponente sisaldavate komponentide kasutamine, paigaldamine või integreerimine, mis on pärit üksuselt, mis on asutatud kolmandas riigis või on selle kontrolli all, või kolmandast riigist pärit üksuste või kolmanda riigi kodaniku kontrolli all, tekitab olulise mittetehnilise küberriski vähemalt kolme liikmesriigi majandus- või sotsiaaltegevusele, konsulteerib komisjon viivitamata liikmesriikidega liidu tasandil meetmete võtmise vajaduse asjus.

7. Komisjonil on õigus võtta vastu rakendusakte eesmärgiga määrata kindlaks, et direktiivi (EL) 2022/2555 I ja II lisas osutatud konkreetset liiki üksustel keelatakse kasutada, paigaldada ja integreerida IKT-komponente või IKT-komponente sisaldavaid komponente lõikes 6 osutatud üksuselt. Selleks konsulteerib ta direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksustega, kes võivad olla keeluga hõlmatud. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega. Asjakohasel juhul hõlmavad need sobivaid ajavahemikke kõnealuste IKT-komponentide või IKT-komponente sisaldavate komponentide järkjärguliseks kasutuselt kõrvaldamiseks. Kõnealuses rakendusaktis võidakse samuti määrata kindlaks kõnealused IKT-komponendid või IKT-komponente sisaldavad komponendid, mille suhtes keeldu kohaldatakse. Keeld hõlmab samuti IKT-komponente või IKT-komponente sisaldavaid komponente kõigilt üksustelt, kes on lõikes 6 osutatud konkreetse üksuse kontrolli all.

8. Lõigetes 1, 2 ja 7 osutatud rakendusaktides võidakse samuti täpsustada, et leevendusmeetmeid kohaldatakse ainult direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste suhtes, mis on konkreetse suurusega.

9. Artikli 100 lõiget 4 kohaldatakse kolmandas riigis asutatud või kolmanda riigi, kolmanda riigi konkreetse üksuse või kolmanda riigi kodaniku kontrolli all olevate konkreetsete üksuste suhtes, kellele on osutatud lõikes 7.

10. Lõigete 1, 2 ja 7 kohaselt vastu võetud rakendusakte, mis on kohaldatavad direktiivi (EL) 2022/2555 I lisa punktis 10 osutatud liiki üksuste suhtes, kohaldatakse *mutatis mutandis* Euroopa Liidu institutsioonide, organite ja asutuste suhtes.

Artikkel 104
Suure riskiga tarnijate kindlakstegemine

1. Komisjon kehtestab rakendusaktidega loetelud suure riskiga tarnijatest, kelle suhtes kohaldatakse artikli 103 lõike 1 või 7 kohaselt vastu võetud rakendusaktides sätestatud keelde või artikli 111 lõikes 1 osutatud keeldu.

2. Sel otstarbel kaardistab komisjon IKT-komponentide ja IKT-komponente sisaldavate komponentide tarnijad, mis on asjakohased lõikes 1 osutatud keelu puhul.

   Sellest lähtuvalt viib komisjon läbi esialgse hindamise, et teha kindlaks, millised kaardistatud tarnijad võivad olla asutatud artikli 100 kohaselt kindlaks määratud kolmandas riigis või olla sellise kolmanda riigi, sellises kolmandas riigis asutatud üksuse või sellise kolmanda riigi kodaniku kontrolli all. Komisjon viib samuti läbi artikli 103 lõikes 6 osutatud üksuse kontrolli all olla võivate tarnijate esialgse kaardistamise.

3. Komisjon hindab lõike 2 teise lõigu kohaselt kindlaks määratud tarnijate asutamiskohta ning omandi ja kontrolli struktuuri.

4. Komisjonil on lõikes 3 osutatud hindamise otstarbel õigus taotleda tarnijatelt vajalikku teavet. Kui tarnija ei esita vajalikku teavet kindlaks määratud tähtaja jooksul, võib komisjon järeldada, et tarnija on asutatud artikli 100 kohaselt kindlaks määratud kolmandas riigis, sellise kolmanda riigi või sellise kolmanda riigi üksuste või sellise kolmanda riigi kodanike kontrolli all. Kui komisjon viib läbi hindamist artikli 103 lõike 7 otstarbel ja tarnija ei esita vajalikku teavet kindlaks määratud tähtpäevaks, võib komisjon järeldada, et tarnija on kõnealuse artikli kohaselt määratud üksuse kontrolli all. Artiklis 112 osutatud pädevad asutused jagavad samuti komisjoniga taotluse korral asjakohast teavet.

5. Komisjon jagab asutamise, kontrolli ja omandi hindamise esialgseid tulemusi asjaomase tarnijaga. Komisjon annab tarnijale võimaluse olla nende esialgsete tulemuste asjus ära kuulatud.

6. Komisjon võib esitada pädevale asutusele taotluse tarnija asutamise, omandi ja kontrolli esialgse hindamise läbiviimiseks, kui see on kõnealuse tarnija tegevuse omadusi arvesse võttes põhjendatud. Pädev asutus võib teha ettepaneku kõnealune esialgne hindamine läbi viia. Komisjon kontrollib kõnealuseid esialgseid järeldusi, et otsustada, kas tarnija tuleks lisada suure riskiga tarnijate loetellu.

7. Komisjon ajakohastab korrapäraselt suure riskiga tarnijate loetelu, et kõrvaldada või lisada suure riskiga tarnijaid. Loetellu lisatud suure riskiga tarnijad võivad esitada komisjonile taotluse nende asutamise, kontrolli ja omandi struktuuri uuesti hindamiseks, kui nad on esitanud tõendeid asjassepuutuvate muudatuste kohta.

8. Kui pädev asutus saab teada, sh direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuse esitatud teabe alusel, et võib olla vaja lisada tarnija suure riskiga tarnijate loetellu, teavitab ta sellest viivitamata komisjoni.

Artikkel 105

Erandi tegemine küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud või sellise kolmanda riigi üksuste kontrolli all olevatele üksustele

1. Artikli 100 kohaselt kindlaks määratud küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud või sellise kolmanda riigi üksuste kontrolli all olev üksus võib esitada komisjonile põhjendatud taotluse teha talle erand:

   a) direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste suhtes kohaldatavast keelust, mille alusel nad ei tohi mis tahes kujul kasutada, paigaldada ega integreerida kõnealuste üksuste oluliste IKT-varade puhul selle IKT-komponente või IKT-komponente sisaldavaid komponente erandina artiklist 111 või artikli 103 lõike 1 kohaselt vastu võetud rakendusaktidest;

   b) keelust osaleda direktiivi 2014/24/EL ja 2014/25/EL ülevõtmise õigusaktide kohaselt korraldatud riigihankemenetlustes IKT-komponentide või IKT-komponente sisaldavate komponentide pakkumiseks, mida kasutatakse artikli 102 kohaselt kindlaks määratud olulistes IKT-varades, erandina artikli 100 lõikest 4.

2. Lõikes 1 osutatud taotluses:

   a) määratakse kindlaks artikli 100 kohaselt kindlaks määratud küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud või sellise kolmanda riigi üksuste kontrolli all oleva üksuse huvi talle käesoleva artikli lõikes 1 osutatud erandi tegemise vastu ning

b) näidatakse selgete tõendite alusel, et võetakse kasutusele tulemuslikud leevendusmeetmed mittetehniliste riskide maandamiseks ning artikli 100 kohaselt kindlaks määratud kolmanda riigi põhjendamatu võimaliku sekkumise vältimiseks IKT-komponentide või IKT-komponente sisaldavate komponentide pakkumisel, mida kasutatakse, mis paigaldatakse või integreeritakse direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuse oluliste IKT-varade puhul.

3. Komisjonil on volitus võtta vastu rakendusakte, milles täpsustatakse lõike 2 punktis b osutatud tingimused, ning sätestada üksikasjalikud normid käesolevas artiklis osutatud menetluste kohta. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.

4. Komisjon hindab lõikes 1 osutatud taotlust õiglase ja läbipaistva protsessi alusel, võttes arvesse järgmist:

a) artikli 100 lõigetes 1 ja 2 osutatud asjaolud ja täiendavad elemendid, mis on seotud mõjuga, mida avaldab IKT tarneahelate jaoks küberturvalisuse seisukohast muret tekitav riik, kus üksus on asutatud või kust seda kontrollitakse;

b) lõike 2 punktis b osutatud leevendusmeetmete tulemuslikkus;

c) kas IKT tarneahelate jaoks küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud või selle üksuste kontrolli all olevale üksusele tehtav erand ei kahjustaks liidu huve.

5. Kui komisjon järeldab pärast lõike 3 kohast hindamist, et erandi tegemine on põhjendatud, teeb ta selleks otsuse, millest teavitab taotluse esitajat üheksa kuu jooksul alates taotluse laekumisest.

6. Lõikes 4 osutatud otsuse tegemisel võib komisjon piirata erandi tegemist konkreetse ajavahemikuga ja seada erandi tegemise eelduseks tingimused üksusele, muu hulgas:

a) lõike 2 punktis b osutatud leevendusmeetmete rakendamise ajakava;

b) korrapärased kolmanda isiku auditid eesmärgiga tagada leevendusmeetmete tulemuslik rakendamine;

c) nõuete täitmisega seotud aruandekohustus.

7. Kui komisjon järeldab pärast lõike 3 kohast hindamist, et erandi tegemine ei ole põhjendatud, teeb ta selleks otsuse, millest teavitab taotluse esitajat üheksa kuu jooksul alates taotluse laekumisest.

8. Komisjon võib enda algatusel tunnistada lõikes 4 osutatud otsuse kehtetuks või seda muuta järgmistes olukordades:

a) asjaolud, millel otsus põhineb, on oluliselt muutunud;

b) erandit taotlenud üksus ei täida oma kohustusi;

c) erand põhines taotluse esitanud üksuse esitatud mittetäielikul, valel või eksitaval teabel.

Artikkel 106
Kaitseõigus

Komisjon tagab, et enne artikli 103 lõike 7 kohaselt rakendusakti vastuvõtmist või enne otsuse tegemist, millega keeldutakse artikli 105 lõike 7 kohaselt erandi tegemisest taotluse

esitaja esitamata jäetud elementide põhjal, või enne kooskõlas artikli 105 lõikega 8 otsuse kehtetuks tunnistamist, antakse asjaomasele üksusele võimalus olla ära kuulatud, võttes teatavatel juhtudel arvesse vajadust kiirmenetluse järele.

Artikkel 107
Register

Komisjon peab artikli 105 lõikes 5 osutatud otsuste kohta avalikku registrit. Registris märgitakse nende üksuste nimed, mille suhtes on sellised otsused tehtud. Komisjon ajakohastab registrit korrapäraselt.

Artikkel 108
Konfidentsiaalsus

Teavet, mille komisjon on artiklite 105 ja 106 kohaselt saanud, kasutatakse ainult sel otstarbel, milleks see hangiti.

Artikkel 109
Tasud

1. Komisjon võtab artikli 105 lõike 1 kohaselt esitatud taotluste eest tasu.
2. Tasud esitatakse ja tasutakse eurodes.
3. Tasu vastab kuludele, mis on seotud artikli 105 lõikes 1 osutatud taotluste töötlemisega, artikli 105 lõikes 2 osutatud kriteeriumide ja teabe hindamisega ning artiklis 107 osutatud registri loomise, haldamise ja käitamisega. Kõnealused kulud hõlmavad kõiki komisjoni kulusid, mis on omistatavad kõnealuses tegevuses osalevatele töötajatele.
4. Komisjon võtab vastu rakendusaktid, millega kehtestatakse üksikasjalikud normid, mis käsitlevad tasusid ja millega määratakse kindlaks tasude summa ning nende maksmise viis. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.

II PEATÜKK
Elektroonilise side võrkude IKT tarneahelad

Artikkel 110
Elektroonilise side mobiili-, püsi- ja satelliitvõrkude olulised IKT-varad

1. Elektroonilise side mobiili-, püsi- ja satelliitvõrkude olulised IKT-varad on määratud kindlaks II lisas.
2. Suure riskiga tarnijate tarnitud IKT-komponendid või selliseid IKT-komponente sisaldavad komponendid kõrvaldatakse järkjärgult kasutuselt elektroonilise side mobiili-, püsi- ja satelliitvõrkude olulistes IKT-varades.
3. Elektroonilise side mobiilivõrkude puhul ei ületa suure riskiga tarnijate tarnitud IKT-komponentide või selliseid IKT-komponente sisaldavate komponentide järkjärgulise kasutuselt kõrvaldamise aeg 36 kuud alates artiklis 104 osutatud elektroonilise side mobiilivõrkude puhul suure riskiga tarnijate loetelu avaldamisest.

4. Komisjonil on õigus võtta kooskõlas artikli 118 lõikega 2 vastu rakendusakte, et täpsustada elektroonilise side püsi- ja satelliitvõrkude puhul suure riskiga tarnijate tarnitud IKT-komponentide või selliseid IKT-komponente sisaldavate komponentide järkjärgulise kasutuselt kõrvaldamise ajavahemik.

5. Komisjonil on kooskõlas artikliga 119 õigus võtta vastu delegeeritud õigusakte, et muuta käesoleva määruse II lisa eesmärgiga kohandada seda tehnoloogia arenguga, võttes arvesse artikli 103 lõikes 4 osutatud elemente.

Artikkel 111
Elektroonilise side mobiili-, püsi- ja satelliitvõrkude puhul kehtestatavad keelud

1. Elektroonilise side mobiili-, püsi- ja satelliitvõrkude pakkujad ei tohi II lisas osutatud oluliste IKT-varade käitamisel ühelgi kujul kasutada, paigaldada ega integreerida IKT-komponente või IKT-komponente sisaldavaid komponente, mis on saadud suure riskiga tarnijatelt.

2. Juhul kui käesoleva määruse kohaselt liikmesriigis määratud pädev asutus erineb määruse (EL) XX/XXXX [digivõrkude õigusakti ettepanek] kohaselt määratud pädevast asutusest, teavitab käesoleva määruse kohaselt määratud pädev asutus viivitamata määruse (EL) XX/XXXX [digivõrkude õigusakti ettepanek] kohast pädevat asutust artikli 114 kohaselt elektroonilise side mobiili-, püsi- ja satelliitvõrkude pakkujate suhtes kehtestatud meetmetest. Ametiasutused tagavad tiheda koostöö kõnealuste meetmete tulemusliku järelevalve ja täitmiste tagamise otstarbel.

III PEATÜKK
Pädevad asutused, järelevalve ja täitmise tagamine, jurisdiktsioon, kaitseõigus

Artikkel 112
Pädevad asutused

1. Iga liikmesriik määrab direktiivi (EL) 2022/2555 artiklis 8 osutatud pädevad asutused artiklis 114 osutatud järelevalve- ja täitemeetmete võtmise eest vastutava asutusena.

2. Pädevad asutused peavad olema struktuurselt ja funktsionaalselt täiesti sõltumatud ja vabad mis tahes otsesest või kaudsest välismõjust ning eelkõige ei või nad taotleda ega vastu võtta juhiseid üheltki avaliku sektori asutuselt ega erasektori üksuselt.

3. Liikmesriigid tagavad, et nende pädevatel asutustel on sobilikud volitused, piisavad inim- ja tehnilised ressursid ning asjakohased eksperditeadmised, et tulemuslikult rakendada artiklis 114 osutatud järelevalve- ja täitemeetmeid.

4. Iga liikmesriik teavitab komisjoni põhjendamatu viivituseta lõike 1 kohaselt määratud pädevate asutuste nimedest, nende asutuste vastavatest ülesannetest ning nende mis tahes edasistest muudatustest. Iga liikmesriik avalikustab samuti lõike 1 kohaselt määratud pädevate asutuste nimed.

Artikkel 113
Komisjoni koostöö- ja tugiteenuste võrgustik

Komisjon loob tulemusliku järelevalve tagamiseks artiklis 112 osutatud liikmesriikide pädevate asutuste ja komisoni koostöövõrgustiku, millest saab koostöö- ja teabevahetusplatvorm, eelkõige artiklis 104 osutatud asutamise, kontrolli ja omandi hindamise otstarbel. Komisjon pakub võrgustikule haldustuge.

Artikkel 114
Järelevalve- ja täitemeetmed

1. Artiklis 112 osutatud pädevatel asutustel on õigus võtta direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste suhtes järelevalve- ja täitemeetmeid. Liikmesriigid tagavad, et eespool nimetatud meetmed on tulemuslikud, proportsionaalsed ja hoiatavad, võttes arvesse iga üksikjuhtumi asjaolusid. Liikmesriigid teavitavad komisjoni sel otstarbel kehtestatud normidest ja nende edasistest muudatustest.

2. Direktiivi (EL) 2022/2555 I ja II lisas osutatud üksustega seotud järelevalveülesannete täitmisel on pädevatel asutustel õigus teha kõnealuste üksuste puhul järgmist:

   a) nõuda nende asjaomaste tarnijate ja teenuseosutajate üksikasjalikku ja ajakohast loetelu;

   b) nõuda juurdepääsu andmetele, dokumentidele ja teabele, mida on vaja käesolevale määrusele vastavuse kontrollimiseks;

   c) teha kohapealset kontrolli ja kaugjärelevalvet, sh pistelisi kontrolle, mida teevad eriväljaõppe saanud spetsialistid;

   d) esitada taotlused riist- või tarkvaratoodete koosseisu kohta, mis on paigaldatud või integreeritud mis tahes kujul võrku või süsteemi, sh komponendid ja transitiivsed sõltuvused, üldkasutatavas ja masinloetavas vormingus.

3. Direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste suhtes nõuete täitmise tagamise ülesannete täitmisel on pädevatel asutustel õigus teha järgmist:

   a) esitada hoiatusi asjaomaste üksuste poolsete käesoleva määruse rikkumiste kohta, nimetades asjakohased faktid ja õiguslikud kaalutlused;

   b) võtta vastu otsuseid, millega nõutakse, et asjaomased üksused lõpetaksid käesoleva määruse rikkumise või kõrvaldaksid leevendusmeetmete rakendamisel kindlaks tehtud puudused;

   c) anda asjaomastele üksustele korraldus lõpetada tegevus, mis rikub käesolevat määrust, ja hoiduda sellist tegevust kordamast ning

   d) kehtestada karistusi kooskõlas normidega, mis käsitlevad artiklis 115 sätestatud summat, või taotleda asjaomastelt asutustelt, kohtutelt või vahekohtutelt kõnealuste karistuste kehtestamist kooskõlas liikmesriigi õigusega.

4. Eelmises lõikes osutatud täitemeetmete võtmisel arvestavad pädevad asutused iga individuaalse juhtumi asjaolusid ning võtavad nõuetekohaselt arvesse järgmisi tegureid:

   a) rikkumise raskusaste ja rikutud sätete tähtsus;

   b) rikkumise kestus;

c) kõnealuse üksuse asjakohane käive;

d) asjaomase üksuse mis tahes asjassepuutuvad varasemad rikkumised;

e) asjakohasel juhul rikkumisest põhjustatud mis tahes varaline või mittevaraline kahju, sh rahaline või majanduslik kahju, mõju teistele üksustele ja mõjutatud kasutajate arv;

f) asjaomase üksuse tahtlus või hooletus;

g) meetmed, mida üksus on võtnud varalise või mittevaralise kahju ennetamiseks või vähendamiseks;

h) vastutavate füüsiliste või juriidiliste isikute koostöö pädevate asutustega.

Esimese lõigu punkti a kohaldamisel käsitatakse tõsise rikkumisena järgmist:

i) korduv rikkumine;

j) olulistest intsidentidest teatamata jätmine või parandusmeetmete võtmata jätmine;

k) pädevatelt asutustelt saadud siduvate juhiste järel puuduste kõrvaldamata jätmine.

5. Pädevad asutused teavitavad enne täitemeetmete võtmist asjaomaseid üksuseid oma esialgsetest järeldustest. Asjaomastele üksustele antakse mõistlik aeg esialgsete järelduste kohta märkuste esitamiseks. Pädevad asutused esitavad oma täitemeetmete üksikasjaliku põhjenduse.

6. Pädevad asutused peavad austama konfidentsiaalsuse ning ameti- ja ärisaladuse hoidmise põhimõtet.

7. Pädevad asutused teevad käesoleva jaotise alusel järelevalve ja täitmise tagamise otstarbel omavahel ja komisjoniga koostööd kooskõlas artikliga 116.

Artikkel 115
Karistused

1. Liikmesriigid kehtestavad käesoleva määruse rikkumise korral kohaldatavad karistusnormid ja võtavad kõik vajalikud meetmed nende rakendamise tagamiseks.

2. Kehtestatud karistused peavad olema mõjusad, proportsionaalsed ja hoiatavad. Liikmesriigid teavitavad komisjoni nimetatud normidest ja meetmetest ning teavitavad teda viivitamata nende hilisematest muudatustest.

3. Karistused määratakse lisaks artikli 114 lõike 3 punktides a, b ja c osutatud meetmetele.

4. Karistuse määramise ja selle suuruse üle otsustamisel võetakse iga üksikjuhtumi puhul nõuetekohaselt arvesse vähemalt artikli 114 lõike 4 esimeses lõigus sätestatud asjaolusid.

5. Artikli 103 lõike 2 punkti a rikkumiste suhtes kohaldatakse kooskõlas käesoleva artikli lõikega 3 karistusi kuni 1 % ulatuses selle ettevõtja eelmise majandusaasta kogu ülemaailmsest aastakäibest, kuhu üksus kuulub.

6. Artikli 103 lõike 2 punktide b–g rikkumiste suhtes kohaldatakse kooskõlas käesoleva artikli lõikega 3 karistusi kuni 2 % ulatuses selle ettevõtja eelmise majandusaasta kogu ülemaailmsest aastakäibest, kuhu üksus kuulub.

7. Artikli 103 lõike 1 ja artikli 111 rikkumiste suhtes kohaldatakse kooskõlas käesoleva artikli lõikega 3 karistusi kuni 7 % ulatuses selle ettevõtja eelmise majandusaasta kogu ülemaailmsest aastakäibest, kuhu üksus kuulub.

Artikkel 116
Vastastikune abi

1. Kui direktiivi (EL) 2022/2555 I või II lisas osutatud liiki üksus osutab teenuseid rohkem kui ühes liikmesriigis või osutab teenuseid ühes või enamas liikmesriigis ning selle olulised IKT-varad asuvad ühes või enamas muus liikmesriigis, siis teevad asjaomase liikmesriigi pädevad asutused üksteisega ja komisjoniga koostööd ning nad abistavad üksteist ja komisjoni, et tagada määruse tulemuslik ja tõhus kohaldamine. Sel eesmärgil kohaldatakse vähemalt järgmisi norme:

   a) liikmesriigis järelevalve- või täitemeetmeid kohaldavad pädevad asutused teavitavad teiste asjaomaste liikmesriikide pädevaid asutusi võetud järelevalve- ja täitemeetmetest ning konsulteerivad nendega;

   b) liikmesriigi pädev asutus võib teise liikmesriigi teiselt pädevalt asutuselt taotleda järelevalve- või täitemeetmete võtmist;

   c) liikmesriigi pädev asutus osutab teise liikmesriigi teise pädeva asutuse põhjendatud taotluse korral teisele pädevale asutusele enda võimaluste piires vastastikust abi, et järelevalve- või täitemeetmeid saaks rakendada tulemuslikult, tõhusalt ja järjepidevalt.

2. Lõike 1 punktis c osutatud vastastikune abi võib hõlmata teabenõudeid ja järelevalvemeetmeid, sh taotlusi teha kohapealseid kontrolle või kaugjärelevalvet või sihipäraseid turvaauditeid. Abitaotluse saanud pädev asutus ei või taotlust tagasi lükata, välja arvatud juhul, kui leitakse, et asutus ei ole pädev taotletud abi andma või et taotletav abi ei ole pädeva asutuse järelevalveülesannete suhtes proportsionaalne või kui taotlus käsitleb teavet või sisaldab tegevust, mille avalikustamine või läbiviimine oleks vastuolus asjaomase liikmesriigi riikliku julgeoleku, avaliku julgeoleku või riigikaitse oluliste huvidega. Enne sellise taotluse rahuldamata jätmist konsulteerib pädev asutus teiste asjaomaste pädevate asutustega ning ühe asjaomase liikmesriigi taotluse korral ka komisjoniga.

3. Asjakohasel juhul võivad eri liikmesriikide pädevad asutused omavahelisel kokkuleppel võtta järelevalvemeetmeid ühiselt.

4. Võttes arvesse artikli 114 lõikes 6 osutatud kohustust järgida konfidentsiaalsuse ning ameti- ja ärisaladuse põhimõtet, kasutatakse abitaotluse kontekstis vahetatud ja käesoleva artikli kohaselt esitatud mis tahes teavet ainult selle küsimuse eesmärgil, milleks seda taotleti.

Artikkel 117
Jurisdiktsioon ja territoriaalsus

1. Käesoleva määruse kohaldamisalasse kuuluvaid direktiivi (EL) 2022/2555 I ja II lisas loetletud liiki üksusi loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on nende tegevuskoht või kus nad on asutatud, välja arvatud järgmistel juhtudel:

   a) üldkasutatavate elektroonilise side võrkude pakkujaid või üldkasutatavate elektroonilise side teenuste osutajaid loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus nad oma teenuseid osutavad;

b) domeeninimede süsteemi teenuse osutajaid, tippdomeeninimede registreid, pilvandmetöötlusteenuse osutajaid, andmekeskusteenuse osutajaid, sisulevivõrgu pakkujaid, hallatud teenuse osutajaid, hallatud turbeteenuse osutajaid ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite ja sotsiaalvõrguteenuse platvormide pakkujaid loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on nende lõike 2 kohane peamine tegevuskoht liidus;

c) avaliku halduse üksusi loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus nad tegutsevad;

d) lennuettevõtjaid loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, mille lennutegevusluba väljaandev pädev asutus väljastas üksusele tegevusloa kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EÜ) nr 1008/2008[83] või, kui tegevusluba või võrdväärset luba ei ole antud kooskõlas kõnealuse määrusega, siis loetakse neid selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on nende peamine tegevuskoht liidus kooskõlas lõikega 2.

2. Käesoleva määruse kohaldamisel käsitatakse lõike 1 punktis b osutatud üksuse peamise tegevuskohana seda liidu liikmesriiki, kus küberriski juhtimise meetmeid käsitlevad otsused valdavalt tehakse. Kui sellist liikmesriiki ei ole võimalik kindlaks teha või kui selliseid otsuseid ei tehta liidus, käsitatakse peamise tegevuskohana seda liikmesriiki, kus toimub suurem osa küberturvalisuse alasest tegevusest. Kui sellist liikmesriiki ei ole võimalik kindlaks teha, käsitatakse peamise tegevuskohana seda liikmesriiki, mille territooriumil on asjaomasel üksusel liidus kõige suurema arvu töötajatega tegevuskoht.

3. Direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuse tegevuskoht ei ole liidus või ta ei ole seal asutatud, kuid ta pakub liidus oma teenuseid, määrab ta endale liidus esindaja. Esindaja peab olema asutatud ühes nendest liikmesriikidest, kus teenuseid osutatakse. Kõnealust üksust loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus esindaja on asutatud. Kui selline üksus on lõike 1 punktis a osutatud üksus, loetakse ta selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus ta oma teenuseid osutab. Kui käesoleva lõike kohast esindajat liidus määratud ei ole, võib üksuse vastu, kes rikub käesolevat määrust, võtta õiguslikke meetmeid iga liikmesriik, kus üksus teenuseid osutab.

4. Esindaja määramine lõike 1 punktis b osutatud üksuse poolt ei piira õiguslike meetmete võtmist üksuse enda vastu.

5. Liikmesriik, kes on saanud seoses lõike 1 punktis b osutatud üksusega vastastikuse abi taotluse, võib võtta kõnealuse üksuse suhtes, mis osutab selle riigi territooriumil teenuseid või millel on seal võrgu- ja infosüsteem, taotluse ulatuses asjakohaseid järelevalve- ja täitemeetmeid.

VI JAOTIS
LÕPPSÄTTED

[83] Euroopa Parlamendi ja nõukogu 24. septembri 2008. aasta määrus (EÜ) nr 1008/2008 ühenduses lennuteenuste osutamist käsitlevate ühiseeskirjade kohta (ELT L 293, 31.10.2008, lk 3–20, ELI: https://eur-lex.europa.eu/eli/reg/2008/1008/oj/est).

Artikkel 118
Komiteemenetlus

1. Komisjoni abistab komitee. Komiteel on kaks koosseisu. II ja III jaotise puhul abistab komisjoni komitee esimeses koosseisus ning IV jaotise puhul abistab komisjoni komitee teises koosseisus. Nimetatud komitee on komitee määruse (EL) nr 182/2011 tähenduses.

2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 5.

Artikkel 119
Delegeeritud volituste rakendamine

1. Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.

2. Artikli 80 lõikes 2 ja artikli 110 lõikes 5 osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile määramata ajaks alates käesoleva määruse jõustumise kuupäevast.

3. Euroopa Parlament ja nõukogu võivad artikli 80 lõikes 2 ja artikli 110 lõikes 5 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.

4. Enne delegeeritud õigusakti vastuvõtmist konsulteerib komisjon kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetega iga liikmesriigi määratud ekspertidega.

5. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle samal ajal teatavaks Euroopa Parlamendile ja nõukogule.

6. Artikli 80 lõike 2 ja artikli 110 lõike 5 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kahe kuu jooksul pärast õigusakti teatavakstegemist Euroopa Parlamendile ja nõukogule esitanud selle kohta vastuväidet või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväidet. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kahe kuu võrra.

Artikkel 120
Hindamine ja läbivaatamine

1. [PP KK AAAA] ja seejärel iga viie aasta tagant tellib komisjon hindamise, mis viiakse läbi kooskõlas komisjoni suunistega.

2. Lõikes 1 osutatud hindamine peab hõlmama järgmist:

   a) ENISA tulemused selle eesmärkide, volituste, missiooni, ülesannete, juhtimise ja asukoha puhul;

   b) käesoleva määruse II jaotise II peatüki 4. jaos sätestatud Euroopa individuaalsete küberturbeoskuste tõendamise kavade tulemuslikkus, tõhusus ja ELi lisaväärtus;

c) käesoleva määruse III jaotise sätete mõju, tulemuslikkus ja tõhusus seoses eesmärgiga tagada IKT-toodete, -teenuste ja -protsesside, hallatud turbeteenuste ja üksuste piisav küberturvalisuse tase liidus ning parandada siseturu toimimist;

d) käesoleva määruse IV jaotise sätete mõju, tulemuslikkus ja tõhusus usaldusväärse IKT tarneahela raamistiku eesmärkide seisukohast.

3. Lõike 1 punktis a osutatud hindamise eesmärk on eelkõige võtta arvesse võimalikku vajadust muuta ENISA volitusi ja selliste võimalike muudatuste finantsmõju.

4. Lõike 1 punktis a osutatud iga teise hindamise käigus hindab komisjon samuti ENISA saavutatud tulemusi, võttes arvesse tema eesmärke, volitusi, missiooni, juhtimist ja ülesandeid, muu hulgas seda, kas ENISA tegevuse jätkamine on neid eesmärke, volitusi, missiooni, juhtimist ja ülesandeid silmas pidades endiselt põhjendatud.

5. Komisjon esitab hindamistulemused Euroopa Parlamendile, nõukogule ja haldusnõukogule. Hindamise järeldused avalikustatakse.

Artikkel 121
Kehtetuks tunnistamine ja õigusjärglus

1. Euroopa Parlamendi ja nõukogu määrus (EL) nr 2019/881 tunnistatakse kehtetuks alates PP.KK.AAAA.

2. Viited määrusele (EL) 2019/881, ENISA-le ja Euroopa küberturvalisuse sertifitseerimise kavadele, nagu on määratud kindlaks kõnealuse määrusega, käsitatakse viidetena käesolevale määrusele ja neid loetakse kooskõlas käesoleva määruse III lisas esitatud vastavustabeliga.

3. Käesoleva määrusega reguleeritud ENISA on omandiõiguse, lepingute, õiguslike kohustuste, töölepingute, finantskohustuste ja vastutuse osas määrusega (EL) 2019/881 asutatud ENISA õigusjärglane. Kõik määruse (EL) 2019/881 kohaselt vastu võetud haldusnõukogu ja juhatuse otsused jäävad kehtima, tingimusel et nad on kooskõlas käesoleva määrusega.

4. Määruse (EL) 2019/881 artikli 15 lõike 1 punkti n alusel ametisse nimetatud tegevdirektor jääb ametisse ning täidab käesoleva määruse artiklis 32 osutatud tegevdirektori ülesandeid ja kohustusi oma ametiaja lõpuni. Tema lepingu muud tingimused ei muutu.

5. Ettevalmistavaid kavasid, mille koostamise taotlus on esitatud määruse (EL) 2019/881 artikli 49 alusel, käsitatakse sellisena, nagu nende taotlus oleks esitatud käesoleva määruse vastavate sätete alusel. Käesoleva määruse III jaotise sätteid kohaldatakse vastavalt kõnealuste ettevalmistavate kavade suhtes.

6. Määruse (EL) 2019/881 artikli 14 alusel komisjoni ametisse nimetatud haldusnõukogu liikmed ja nende asendusliikmed jäävad ametisse ja täidavad käesoleva määruse artiklis 27 osutatud haldusnõukogu liikmete ülesandeid oma ametiaja lõpuni. Määruse (EL) 2019/881 artikli 14 alusel liikmesriikide poolt ametisse nimetatud haldusnõukogu liikmed ja nende asendusliikmed jäävad ametisse ja täidavad käesoleva määruse artiklis 27 osutatud haldusnõukogu liikmete ülesandeid, kui nad täidavad artikli 24 lõikes 3 osutatud ülesandeid.

Artikkel 122
Jõustumine

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

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Strasbourg,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

FINANTS- JA DIGISELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

Ettepanek: Euroopa Parlamendi ja nõukogu määrus, mis käsitleb Euroopa Liidu Küberturvalisuse Ametit (ENISA), Euroopa küberturvalisuse sertifitseerimise raamistikku ja IKT tarneahela turvalisust ning millega tunnistatakse kehtetuks määrus (EL) 2019/881 (küberturvalisuse 2. määrus)

(EMPs kohaldatav tekst)

Lühipealkiri: Küberturvalisuse 2. määrus (KTM2)

ja

Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, millega muudetakse direktiivi (EL) 2022/2555 seoses lihtsustamismeetmetega ja vastavusse viimisega [küberturvalisuse 2. määruse ettepanekuga]

1.2. Asjaomased poliitikavaldkonnad

Poliitikavaldkond: 09 – Sidevõrgud, sisu ja tehnoloogia

Meede: 09.02 digitaalne ühtne turg

1.3. Eesmärgid

1.3.1. Üldeesmärgid

Sekkumise peamised eesmärgid on järgmised:

1) suurendada küberturvalisuse alast suutlikkust ja vastupanuvõimet

Aidata tugevdada liidu küberturvalisuse juhtimist ning aidata tagada, et asjaomased institutsioonid, asutused ja muud sidusrühmad on paremini ette valmistatud, et koordineeritud viisil ja tõhusalt ennetada ja avastada küberohte ja neile reageerida.

2) hoida ära siseturu killustumist

Toetades ühiste liidu küberturvalisust käsitlevate õigusaktide, näiteks sertifitseerimiskavade väljatöötamist, rakendamist ja kasutuselevõttu ning tagada ühtlustatud raamistikud, mis suurendavad usaldust ja koostalitlusvõimet kõigis liikmesriikides.

Need üldeesmärgid vastavad peamistele probleemidele, mis tehti kindlaks kavandatud algatuse mõjuhinnangus esitatud probleemimääratluses. Need kajastavad üldist poliitilist eesmärki tugevdada liidus küberturvalisuse juhtimist ning toetada turvalise, vastupidava ja konkurentsivõimelise digitaalse ühtse turu arengut.

1.3.2. Erieesmärgid

Kõrvaldada ebakõla ELi küberturvalisuse poliitikaraamistiku ja sidusrühmade vajaduste vahel

Erieesmärk nr 1: luua suutlikkus liidu küberturvalisuse poliitika tulemuslikuks rakendamiseks ja järjepidevaks operatiivkoostööks, mis võimaldab struktureeritumat liikmesriikidevahelist koostööd.

Erieesmärk nr 2: töötada välja ja võtta kasutusele vahendid ja mehhanismid, et tõhusalt toetada liikmesriike, tööstust ja muid sidusrühmi ning rahuldada nende vajadusi;

Tegeleda Euroopa küberturvalisuse sertifitseerimise raamistiku vähese kasutuselevõtu ja tulemuslikkusega.

Erieesmärk nr 3: luua eeltingimused turuvajadustest lähtuvate küberturvalisuse sertifitseerimise kavade kiiremaks väljatöötamiseks, laiendades Euroopa küberturvalisuse sertifitseerimise raamistiku kohaldamisala, tagades raamistiku tõhusa haldamise ja kiired menetlused ning suurendades raamistiku läbipaistvust.

Vähendada killustatust nõuete täitmisel ning horisontaalsete ja valdkondlike raamistike keerukust:

Erieesmärk nr 4: luua mehhanismid ja tingimused, et hõlbustada küberturvalisuse nõuete täitmist, muutes seeläbi nende rakendamise sidusamaks ja tõhusamaks.

Vähendada küberriske tarneahelates:

Erieesmärk nr 5: vähendada riske kriitilise tähtsusega IKT tarneahelates, mis saavad alguse üksustest, mis on asutatud küberturvalisuse seisukohast muret tekitavates riikides, või nende üksuste kontrolli all olevatest üksustest (suure riskiga tarnijad), ning vähendada kriitilist sõltuvust, töötades välja sidusa ja tõhusa ELi tasandi raamistiku tegelemiseks IKT tarneahelates esinevate turvariskidega.

1.3.3. Oodatavad tulemused ja mõju

Märkige, milline peaks olema ettepaneku/algatuse oodatav mõju toetusesaajatele/sihtrühmale.

Oodatavad tulemused on järgmised:

1) ENISA tegevuse reformimine;

2) Euroopa küberturvalisuse sertifitseerimise raamistiku reformimine – kohaldamisala laiendamine, uus kord ja täiustatud juhtimine;

3) liidu asjakohase küberturvalisusealase õigusraamistikuga vastavuse tagamise edasine lihtsustamine;

4) terviklik ja horisontaalne raamistik IKT tarneahelate küberohtude käsitlemiseks.

Üldine mõju

Ettepanekul on tohutu mõju liidu küberturvalisusele, kuna selles käsitletakse mitut valdkonda, nagu Euroopa Liidu Küberturvalisuse Ameti vajalik tugevdamine, tugevdatakse toetust liidu õiguse rakendamisele, kehtestatakse reformid Euroopa sertifitseerimise raamistiku sujuvaks rakendamiseks, toetatakse liidu ühist arusaamist küberohtudest ja käsitletakse küberohtude leevendamist, arvestades geopoliitilist tegelikkust. Kavandatavate sätete rakendamine tagab suure tulemuslikkuse ja sidususe ning hoiab ära liigse regulatiivse koormuse. Pakett on koostatud nii, et see oleks rakendamisprobleemide esinemise korral paindlik ning toetaks pikaajalist poliitikavaldkondade sidusust kogu digi- ja küberturvalisuse ökosüsteemis. See suurendab selgust, kõrvaldades ebatõhususe ja ühtlustades eri õigusraamistikes sätestatud kordi, samal ajal aidates kaasa kõrgtasemel küberturvalisuse saavutamisele kogu ELis. Euroopa Komisjoni ühe peamise prioriteetse eesmärgina toovad kavandatud lihtsustamispüüdlused ettevõtjatele, sh VKEdele märkimisväärset majanduslikku kasu enam kui 14,63 miljardi euro ja avaliku sektori asutustele 7,5 miljoni euro ulatuses.

Konkreetsed tulemused on järgmised:

– suurem teadlikkus ja tegevuse parem koordineerimine, mis võib tagada ettevõtjatele, avaliku sektori asutustele ja kodanikele märkimisväärse kulude kokkuhoiu intsidentide kiirema avastamise ja neile reageerimise vallas;

– ENISA kohaldamisala ja volituste täpsustamine, samal ajal tagades tema põhiülesannete vajaliku prioriseerimise;

– selle tagamine, et sidusrühmad saavad piisavat toetust poliitika rakendamiseks, operatiivtegevuseks ja üldiseks koordineerimiseks;

– liidu ühise olukorrateadlikkuse toetamine;

– tõhustatud koostöö EU-CyCLONe, CSIRTide võrgustiku, komisjoni, Europoli ja CERT-EU ning asjaomaste liidu üksustega, et töötada välja kontrollitud ja usaldusväärse küberohuteadmuse hoidlad;

– lunavararünnete leevendamiseks tehtavate jõupingutuste toetamine;

– tõhustatud koordineerimine erasektoriga küberturvalisusega seotud teemadel;

– varajase hoiatamise kaudu õigeaegse teabe levitamine olulise või ulatusliku intsidendi või piiriülese küberohu kohta direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorite puhul;

– tõhusa koostoime edendamine teiste ELi organite ja asutustega;

– oskuste sertifitseerimise hinna alandamine, muu hulgas suurendades pakkumist turul, võttes kasutusele Euroopa oskuste tõendamise kavad;

– oskuste nappuse kaotamise toetamine Euroopas individuaalsete küberturbeoskuste tunnistuste abil ning liikmesriikide ja tööstuse toetamine nende tööjõu tugevdamisel;

– Euroopa küberturvalisuse sertifitseerimise raamistiku ebaselguse ja vähese mõju käsitlemine, selle kohaldamisala laiendamine ja juhtimismudeli parandamine;

– vastuvõetud kavade maine tõstmine, kehtestades haldussüsteemi ning võttes kasutusele õigeaegse ja läbipaistva arendusprotsessi;

– tasude mehhanismi kehtestamine seoses kuludega, mis tekivad seoses Euroopa individuaalsete küberturbeoskuste tõendamise kavade väljatöötamise ja haldamisega, taotluste menetlemisega ja tõendajatele lubade andmisega ning Euroopa küberturvalisuse sertifitseerimise raamistiku raames vastu võetud kavade haldamisega, mis aitab kaasa ameti finantsstabiilsusele ja säästab ELi eelarvet;

– Euroopa sertifitseerimiskavade kooskõlastamine kehtiva õigusraamistikuga, et seeläbi paremini toetada rakendamispüüdlusi ja toetada ettevõtjate nõuete täitmisega seotud vajadusi;

– hetkel külmutatud kavade vastuvõtmise võimaldamine;

– Euroopa ettevõtete konkurentsivõime soodustamine, edendades rahvusvaheliste ja Euroopa standardite ühtlustamist;

– küberturvalisuse meetmete ja nõuete killustatuse vähendamine;

– õigusselguse tagamine ja halduskoormuse olulisel määral vähendamine, ilma et see tooks kaasa märkimisväärset õiguskindlusetust sidusrühmade seas, kes on hiljuti vastu võetud õigusraamistikega kohanemas;

– küberturvalisuse 2. direktiivi kohaste üksuste nõuetele vastavuse hõlbustamine, mis aitaks kaasa ka üldisele nõuetele vastavuse parandamisele ja sisukamate küberturvalisuse meetmete kehtestamisele, samal ajal muutes järelevalveprotsessi ametiasutuste jaoks tõhusamaks.

Muu

– VKEdele kaasneks algatusest laialdane positiivne mõju, arvestades suuremat konkurentsivõimet ELi küberturvalisuse turul ning väiksemaid kulusid ja halduskoormust:

1. *positiivne mõju VKEdele, kelle küberkerksus suureneks tänu ENISA tõhustatud rollile ja ameti koostatavatele tehnilistele suunistele;*
2. *VKEd kui volitatud tõendajad, kes annavad välja tõendeid Euroopa oskuste tõendamise kava alusel, suurendavad nähtavust, mainet ja võidavad juurde kliente. Lisaks aitavad Euroopa individuaalsete küberturbeoskuste tunnistused VKEdel leida nõuetekohaste oskustega kandidaate;*
3. *hästitoimivad Euroopa sertifitseerimiskavad võivad lihtsustada usaldusväärsete IKT-tehnoloogiate valimist VKEde puhul ning aidata suurendada nende üldist küberkerksust;*
4. *domeeninimede süsteemi teenuse osutajatena saavad VKEd kasu meetmetest, mis on seotud küberturvalisuse 2. direktiivi rakendamisega, kuna nad on domeeninimede süsteemi teenuse osutajate kohaldamisalast välja jäetud;*
5. *VKEd saaksid kasu kohaldamisala täpsustamisest, mis piiraks kohustuste kohaldamist teatavatele üksustele mõne küberturvalisuse 2. direktiivis loetletud sektori puhul;*
6. *IKT tarneahela turbemeetmete puhul saaksid VKEd üldiselt kasu usaldusväärsete tehnoloogiate kasutamisest. Tarnijatena, kes tegutsevad sektorites, mille suhtes kohaldatakse piiranguid, mõjutaksid asendamised ja tehingukulud neid oluliselt rohkem kui suuremaid ettevõtteid. VKEd kui usaldusväärsed tarnijad saavad siiski kasu uutest turuvõimalustest.*

– Ühegi eesmärgi puhul ei eeldata märkimisväärse keskkonnamõju tekkimist.

– ELi eelarve puhul võib eeldada, et tõhusus suureneb tänu paremale koostööle ja tegevuse koordineerimisele ELi institutsioonide, organite ja asutuste vahel. Pikas perspektiivis oodatakse kokkuhoidu tänu tasude mehhanismi kehtestamisele.

1.3.4. Tulemusnäitajad

Märkige, milliste näitajate abil jälgitakse edusamme ja saavutusi.

Eesmärk: luua suutlikkus küberturvalisuse alaste liidu poliitikameetmete tulemuslikuks rakendamiseks ja pidevaks operatiivkoostööks, mis võimaldab struktureeritumat koostööd liikmesriikide vahel.

– ENISA asjakohaste panuste arv ELi ja liikmesriikide poliitika ja seadusandlike algatuste rakendamisse

– Sidusrühmade positiivne tagasiside ENISA asjakohaste panuste kohta

– 25 % kasv võrreldes 2023. aasta lähtetasemega, nagu on esitatud ENISA iga-aastases tegevusaruandes (asjakohaste panuste arvu kohta) ja ENISA iga-aastases rahulolu-uuringus (positiivse tagasiside kohta)

– ELi nõrkuste andmebaasi kasutamise statistika

– Kasutajate arvu suurenemine 25 % võrreldes 2025. aastaga

Küberkerksuse määruse platvormi kättesaadavus, turvalisus ja toimimine

– Platvormi seisakute ja intsidentide arvu vähenemine 25 % võrreldes 2025. aasta statistikaga platvormi seisakute ja intsidentide kohta

Eesmärk: töötada välja ja võtta kasutusele vahendid ja mehhanismid, et tõhusalt toetada liikmesriike, tööstust ja muid sidusrühmi ning rahuldada nende vajadusi;

– ENISA toetatud sidusrühmade arv ja pakutava toetuse kvaliteet

– Sidusrühmade toetamiseks võetud meetmete arv

– Toetatud sidusrühmade arvu kasv 10 % ja toetatud sidusrühmade rahulolutaseme kasv 10 % võrreldes 2025. aastaga

Eesmärk: luua eeltingimused turuvajadustest lähtuvate küberturvalisuse sertifitseerimise kavade kiiremaks väljatöötamiseks, laiendades Euroopa küberturvalisuse sertifitseerimise raamistiku kohaldamisala, tagades raamistiku tõhusa haldamise ja kiired menetlused ning suurendades raamistiku läbipaistvust.

– Vastuvõetud kavade arv

– Kava väljatöötamiseks kuluva aja lühenemine 50 % võrreldes 2025. aastaga

– Igal aastal välja antavate kehtivate sertifikaatide arv

– 25 % kasv võrreldes 2025. aasta lähtestsenaariumiga

– Sidusrühmade positiivne tagasiside nende kaasamise kohta kava väljatöötamisse ja Euroopa küberturvalisuse sertifitseerimise raamistiku läbipaistvuse kohta

– 25 % kasv võrreldes ENISA iga-aastase rahulolu-uuringu lähtestsenaariumiga 2027. aasta võrdluses

Eesmärk: kehtestada mehhanismid ja tingimused, et hõlbustada küberturvalisuse nõuete täitmist ning muuta seeläbi nende rakendamine sidusamaks ja tõhusamaks.

– VKEde küberturvalisuse 2. direktiivi ja küberturvalisuse eeskirjade järgimise kulude protsentuaalne osakaal kõigist nõuete täitmisega seotud kuludest

– >70 % VKEdest teatab küberturvalisuse nõuete täitmisega seotud kulude vähenemisest võrreldes 2025. aastaga

– Lunavararünnete arv ja kahjusumma eurodes

– Lunavararünnete arvu vähenemine >1 % võrreldes 2027. aastaga

– Piiriüleste intsidentide protsent, mille ajal või järgselt kasutasid liikmesriikide ametiasutused vastastikuse abi mehhanisme

– Nende juhtumite, mille puhul kasutati vastastikust abi, osakaalu suurenemine >20 protsendipunkti võrreldes 2025. aastaga

Eesmärk: vähendada kriitilist sõltuvust, töötades ELi tasandil välja sidusa ja tõhusa raamistiku IKT tarneahela turvariskidega tegelemiseks.

– Võetud meetmete arv

– Võetud meetmete ja kindlaks tehtud peamiste varade arvu 25 % suurenemine võrreldes vastuvõtmise kuupäevaga + 6 kuud

– Peamiste IKT-varade suure riskiga tarnijatest sõltuvuse vähenemine 25 % võrreldes 2025. aastaga

1.4. Ettepanek/algatus käsitleb

☒ uut meedet (*IV jaotis „Tarneahel“ ja V jaotis „Lihtsustamine“*)

☐ uut meedet, mis tuleneb katseprojektist / ettevalmistavast meetmest[84]

☒ olemasoleva meetme pikendamist (*II jaotis „ENISA volitused“ ja III jaotis „Sertifitseerimine“*)

☐ ühe või mitme meetme ümbersuunamist teise või uude meetmesse või ühendamist teise või uue meetmega

1.5. Ettepaneku/algatuse põhjendused

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused, sealhulgas algatuse rakendamise üksikasjalik ajakava

2024. aasta juulis kutsus Euroopa Komisjoni president Ursula von der Leyen oma poliitilistes suunistes[85] üles ELi õigusakte lihtsustama, tugevdama ja kodifitseerima, et kõrvaldada kattuvused ja vastuolud, samal ajal säilitades kõrged standardid. Juhtivale asepresidendile Virkkunenile[86] saadetud missioonikirjas mainitakse eelkõige Euroopa küberturvalisuse sertifitseerimise kavade vastuvõtmise protsessi täiustamist ning vajadust kaitsta meie tööstust, kodanikke ja haldusasutusi sisemiste ja väliste ohtude eest. Lisaks kutsutakse Niinistö 2024. aasta aruandes[87] üles vähendama elutähtsate tehnoloogiate puhul soovimatuid tarneahelast sõltuvuse riske. ELi presidendi tellitud Draghi[88] ja Letta[89] aruannete kesksed aspektid kajastasid vajadust säilitada lihtsustamise kaudu ühtse turu konkurentsivõime ning tagada kõrgeim turvalisuse ja strateegilise autonoomia tase. Sellest tulenevalt on küberturvalisuse määruse läbivaatamine komisjoni julgeolekualase töö nurgakivi ja Euroopa küberturvalisuse regulatiivse ökosüsteemi põhjaliku läbivaatamise alus. KTM2 ettepanekuga kehtestatakse mehhanismid tarneahela küberohtude käsitlemiseks ning mehhanismid nõuete täitmise killustatuse ning horisontaalsete ja valdkondlike raamistike keerukuse vähendamiseks. Eeldatakse, et ENISA aitab kaasa ka aruandluskohustuste suuremale lihtsustamisele ühtse kontaktpunkti lõimimise kaudu.

Võttes arvesse pärast küberturvalisuse määruse vastuvõtmist 2019. aastal kehtestatud valdkondlike sätete arvukust ja kiiresti muutuvat küberohtude maastikku, tuleb ENISA volitused läbi vaadata, et sätestada sihipärasemad ja uuendatud ülesanded eesmärgiga toetada tulemuslikult ja tõhusalt liikmesriikide, ELi institutsioonide ja

84 Vastavalt finantsmääruse artikli 58 lõike 2 punktile a või b.
85 Poliitilised suunised 2024.
86 Juhtiva asepresidendi Virkkuneni missioonikiri.
87 Sauli Niinistö aruanne.
88 Draghi aruanne Euroopa konkurentsivõime tuleviku kohta.
89 Enrico Letta, „Much more than a market“ (aprill 2024).

muude sidusrühmade jõupingutusi turvalise küberruumi tagamiseks Euroopa Liidus. Euroopa küberturvalisuse sertifitseerimise raamistiku tugevdamise teel tagatakse ettepanekus, et ELil on lihtne, kaasaegne ja kohandatav sertifitseerimissüsteem, mis toetab tarneahela meetmeid ja küberkerksuse määruse kiiret rakendamist. Kokkuvõttes on volituste kavandatud ulatus piiritletud, tugevdades neid valdkondi, mille puhul amet on üles näidanud selget lisaväärtust, ning lisades uusi valdkondi, mille puhul on vaja toetust, pidades silmas uusi poliitika prioriteete ja vahendeid, ning et tugevdada Euroopa küberturvalisuse sertifitseerimise raamistikku.

Küberturvalisuse määruse läbivaatamise eesmärk on seega teha suur samm edasi ELi turvaolekus ning Euroopa Liidu üldises julgeolekus, valmisolekus ja vastupanuvõimes.

1.5.2. ELi meetme lisaväärtus (see võib tuleneda eri teguritest, nagu kooskõlastamisest saadav kasu, õiguskindlus, suurem tõhusus või vastastikune täiendavus). Käesoleva punkti kohaldamisel tähendab „ELi meetme lisaväärtus“ väärtust, mis tuleneb liidu sekkumisest ja lisandub väärtusele, mille liikmesriigid oleksid muidu üksi loonud.

2019. aastal võeti vastu küberturvalisuse määrus, mille õiguslik alus on ELi toimimise lepingu artikkel 114, millega antakse ELi seadusandjale õigus võtta vastu meetmeid, millega ühtlustatakse riigisiseseid õigusnorme, mille eesmärk on siseturu rajamine ja selle toimimine.

Küberturvalisuse määruse läbivaatamise ettepaneku eesmärk on ühtlustada küberturvalisust käsitlevaid õigusakte ELi tasandil kehtiva küberturvalisuse määruse, mis kehtib alates 2019. aastast (KTM1), läbivaatamise ja täiendamise teel. KTM1 eesmärgid, millega seoses antakse Euroopa Liidu Küberturvalisuse Ametile alalised volitused, on suunatud küberturvalisuse ühtlaselt kõrge taseme tagamisele kogu ELis ning siseturu killustumise ärahoidmisele seoses küberturvalisuse sertifitseerimise kavadega, jäävad algatatud läbivaatamise raamesse. Nagu 2017. aastal küberturvalisuse määruse ettepanekus juba nõuetekohaselt analüüsitud, ei suuda liikmesriigid ise neid eesmärke piisaval määral saavutada, vaid neid saab saavutada üksnes Euroopa Liidu tasandil kooskõlas Euroopa Liidu lepingu artikliga 5.

Küberturvalisuse määruse läbivaatamise ettepanekus keskendutakse selgelt ülesannete ühtlustamisele, prioriseerimisele ja kodifitseerimisele kõigis kübervaldkonna õigusaktides, mida on võimalik saavutada ainult ELi tasandil, ning praegu selline algatus puudub. Uue ettepanekuga tugevdatakse veelgi tarneahela turvalisust ja küberturvalisuse sektorit ELis ning suurendatakse liikmesriikide ja tööstuse valmisolekut ja vastupanuvõimet. Sõltuvus küberturvalisuse seisukohast muret tekitavates kolmandates riikides asutatud üksustest või nendes riikides asuvate üksuste kontrollitavatest üksustest (suure riskiga tarnijad) mõjutab üksusi kogu liidus, kuna olulised tarneahela küberintsidendid levivad sageli üle riigipiiride. Selle küsimuse käsitlemine üksnes liikmesriigi tasandil ei ole tõenäoliselt tulemuslik.

ENISA-le antavad uued ülesanded on keskse tähtsusega, et saavutada küberturvalisuse kõrge tase kogu ELis. Hoolimata asjaolust, et amet teeb koostööd teiste ELi julgeolekuasutustega, nagu Europol, ning küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskusega (ECCC), mis vastutab rakendamise rahastamise eest, on ameti missioon ja ülesanded ainulaadsed ning praegu ei ole ühtegi teist organit, kel oleks seda laadi kohustused. ELi küberturvalisuse ökosüsteemis töötavad kõik asjaomased üksused tihedas koostoimes ja selgete volituste piires. Seetõttu tugevdatakse KTM2 ettepanekuga üksnes neid

aspekte, millel on selge lisaväärtus, tagades, et ei esineks sisuliste ülesannete dubleerimist ega ka muude küberturvalisuse ökosüsteemi asutuste rahastamisega seotud ebaselgust.

Üksikasjad

ENISA volitusi on hilisemate õigusaktidega laiendatud, ilma et tema põhiülesandeid ja vahendeid oleks põhjalikult läbi vaadatud. See on põhjustanud kattuvusi, ebatõhusust ja liikmesriikide peamiste tugiülesannete ebapiisavat prioriseerimist.

Mitu liikmesriiki on kasutusele võtnud oma riiklikud küberturvalisuse sertifitseerimise kavad, mille kohaldamisala ja vastavushindamismenetlused on väga erinevad. See tekitab turu killustatust ja dubleerivat koormust ettevõtjatele ja VKEdele, kes soovivad saada ühekorraga sertifitseeritud ja tegutseda kogu ELis. Euroopa küberturvalisuse sertifitseerimise raamistik loodi küberturvalisuse määrusega, et vähendada turu killustatust, kuid selle rakendamine on olnud aeglane ja ebaühtlane.

Samuti on mitmes horisontaalses ja valdkondlikus õigusaktis sätestatud küberturvalisuse meetmed, millel on erinevad otstarbed ja eesmärgid, mis põhjustab ka erinevusi liikmesriikide kehtestatud vastavuskontrollis ja järelevalvealastes lähenemisviisides. Seetõttu seisavad üksused, eelkõige VKEd ja mitmes liikmesriigis tegutsevad ettevõtjad, silmitsi täiendava regulatiivse koormusega, mis mõjutab negatiivselt nende konkurentsivõimet.

Erinevad lähenemisviisid IKT tarneahela turvalisusele ja liikmesriikide võetavad erinevad meetmed toovad kaasa turu killustumise ja erinevad vastavusnõuded üksustele. Võttes eelkõige arvesse IKT tarneahelate piiriülest olemust, kahjustaks vastavusnõuete killustatus siseturul ettevõtjate õiguskindlust. Suure riskiga tarnijate piiramiseks ettenähtud erinevad riiklikud raamistikud võivad luua tõkkeid kaupade ja teenuste piiriülesele liikumisele siseturul. Kuna IKT tarneahelad võivad hõlmata kriitilise tähtsusega üksusi ja taristut, olenemata asjaomaste tarnijate asukohast, tekitavad küberturvalisuse meetmete killustatus ja lüngad neile üksustele täiendavaid turvariske.

Lisaks sisaldavad mitmeaastase finantsraamistiku programme käsitlevad ettepanekud horisontaalset sätet, millega nähakse ette liidu õiguse alusel kindlaks tehtud suure riskiga tarnijate puhul erandid, et kaitsta ELi eelarve terviklikkust ja tagada, et liidu kulutused ei ole vastuolus liidu oluliste julgeolekuhuvidega. Küberturvalisuse määruse tarneahela raamistik oleks mehhanism, mis võimaldab asjaomast kindlakstegemist IKT tarneahelate valdkonnas ja mida saab seega ellu viia üksnes ELi tasandil.

Küberründed on oma olemuselt piiriülest laadi, arvestades eelkõige ülekanduvat mõju, mis võib tuleneda algselt ühest mõjutatud sisenemispunktist. Küberturvalisusega seotud ohud ja riskid mõjutavad kogu Euroopa Liitu ning seetõttu võib ühine olukorrateadlikkuse ülevaade märkimisväärselt parandada üksuste küberturvalisuse taset Euroopa Liidus. ENISA läbivaadatud volituste raames esitatud ettepanekutes käsitletakse seda küsimust eesmärgiga suurendada märkimisväärselt ELi küberkerksust.

Kokkuvõttes on ELi sekkumine ülioluline, kuna küberohud ja nendega seotud probleemid ulatuvad üksikutest liikmesriikidest kaugemale. Killustatud riiklikud lahendused on osutunud ebapiisavaks, et saavutada usaldus ja koordineerimine kogu turul. Selleks et kõrvaldada tõkked, tagada järjekindel rakendamine ja toetada

liikmesriike üha keerukamas regulatiivses ja ohukeskkonnas on vaja läbivaadatud ELi õigusraamistikku.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

ENISA asutati 2004. aastal tähtajaliste volitustega. 2019. aastal jõustus küberturvalisuse määrus, millega anti ENISA-le alalised volitused ja eesmärk saada kübervaldkonna oskusteabe keskuseks Euroopas. Praegu on ENISA tunnustatud kaubamärk ja ELi sidusrühmade usaldusväärne partner. Ameti pädevused kujunesid järk-järgult välja 25 aasta jooksul, kajastades muutuvat küberturvalisuse ökosüsteemi.

Vastavalt küberturvalisuse määruse artiklile 67 hindab komisjon iga viie aasta järel ENISA ja selle töökorralduse mõju, tulemuslikkust ja tõhusust, võimalikku muudatuste tegemise vajadust ning selliste muudatuste finantsmõju. Hindamise käigus hinnatakse ka Euroopa sertifitseerimise raamistikuga seotud sätete mõju, tulemuslikkust ja tõhusust.

Komisjon tegi nende sätete kohaselt ameti ja Euroopa küberturvalisuse sertifitseerimise raamistiku hindamise, mis hõlmas avalikku konsultatsiooni ja sõltumatut uuringut. Kooskõlas parema õigusloome tavadega on komisjon algatanud ka avaliku konsultatsiooni konkreetselt küberturvalisuse määruse läbivaatamise kohta ning tagasisidekorje, et koguda andmeid sidusrühmadelt. Hindamisel jõuti järeldusele, et ENISA on täitnud oma volitusi, saavutades peaaegu kõik kavandatud väljundid. Ameti eesmärgid on endiselt asjakohased, kuna sidusrühmad on eriti tunnustanud keerulistel aegadel – nagu COVID-19 pandeemia ja Venemaa agressioonisõda Ukraina vastu – antud panust. Olenemata sidusrühmadelt saadud enamasti positiivsest tagasisidest ENISA panuse kohta ilmnes ka, et sidusrühmade ootuste järjepideva täitmise valdkonnas on veel palju arenguruumi.

Saadud kogemused on näidanud, et tulemuslikkuse suurendamiseks oleks ENISA-l vaja rohkem strateegilist fookust, ülesannete prioriseerimist ja suutlikkuse suurendamist, et anda õigeaegset teavet esilekerkivate ohtude kohta ja strateegilisi vahendeid nendega tegelemiseks. Lisaks, nagu on märkinud mitu sidusrühma, võiks ENISA kasutusele võtta struktureeritumad ja läbipaistvamad meetodid erasektori üksustega suhtlemiseks, pannes rõhku VKEde toetamisele. Kõigis välistes konsultatsioonides rõhutati, kui oluline on suurendada ENISA rahastamist, personalialast ja tegevussuutlikkust, et võimaldada tal vastata ELi küberturvalisuse maastiku kasvavatele nõudmistele. Uuringu järgselt nägid komisjoni talitused oma hindamisaruandes selget vajadust tulevikukindlate õigusaktide järele, mis kohanduksid keeruka ja kiiresti muutuva küberohtude maastikuga, ning vajadust vastavalt tugevdada ametit vajalike vahenditega, et tagada toetus kõrgeimal tasemel küberturvalisuse saavutamiseks Euroopas. Kogutud andmete ja küberturvalisuse määruse rakendamisel saadud kogemuste põhjal jõuti järeldusele, et koordineerimist teiste asutustega tuleks ühtlustada, samuti tuleks keskenduda ENISA pakutavale toetusele liidu õiguse rakendamisel ja taotluse korral komisjoni toetamisele küberturvalisusega seotud õigusaktide koostamisel. Ettepanekus uuritakse koostoimet komisjoni geopoliitiliste prioriteetidega, et tegeleda selliste riskidega nagu kasvav sõltuvus Euroopale küberturvalisuse seisukohast muret tekitavates riikides asutatud üksustest ja nendes riikides asuvate üksuste kontrollitavatest üksustest (suure riskiga tarnijad). Oskusteabe keskusena on ENISA praegu ka oluline teabehoidla, mis on ülioluline ühise arusaama kujundamisel ELi üksusi ähvardavatest ohtudest ja riskidest. Seepärast tugineb kavandatud raamistik KTM1

rakendamisest saadud kogemustele ja koondab teabevoogude koordineerimist, et koostada terviklik olukorrateadlikkuse ülevaade.

Euroopa küberturvalisuse sertifitseerimise raamistiku hindamisest tuleneb mitu strateegilist soovitust. Hoolimata ENISA kesksest rollist liikmesriikide ja muude sidusrühmade vahelise koostöö ja tegevuse sidususe edendamisel, on Euroopa küberturvalisuse sertifitseerimise raamistiku tõhusus ja tulemuslikkus olnud selgelt piiratud peamiselt kavade vastuvõtmise protsesside keerukuse tõttu. Need probleemid tõid esile vajaduse juhtimisstruktuurid põhjalikult läbi vaadata, et suurendada tegevusselgust ja vastutust kõikidel tasanditel, mida käsitletakse küberturvalisuse määruse läbivaatamise ettepanekus. Kehtiva Euroopa küberturvalisuse sertifitseerimise raamistiku toimimisest saadud kogemused on näidanud vajadust ajakohastada ja täpsustada sertifitseerimise raamistikku ning kehtestada sertifitseerimiskavade halduskord, et need vastaksid turuvajadustele ja ohumaastikule. Lisaks ei ole algses raamistikus ette nähtud muid kui tehnilisi riske, mida võib pidada Euroopa küberturvalisuse sertifitseerimise raamistiku 5G- ja pilvandmetöötluse kavade rakendamise seiskumise põhjuseks.

ELi küberturvalisuse ökosüsteemi keerukus on tulenevalt muutuvatest küberohtudest suurenenud. Sidusrühmade kirjalikes seisukohtades oldi tugeval üksmeelel, et halduskoormust on vaja vähendada, eelkõige VKEde puhul, ning kutsuti üles lihtsustama nõuete täitmise korda. Kuigi peamised lihtsustamispüüdlused tehakse digivaldkonna koondpaketi algatuse kaudu, kajastab ettepanek sidusrühmade vajadusi, muutes küberturvalisuse 2. direktiivi, et lihtsustada rakendamisprotsessi.

1.5.4. Kooskõla mitmeaastase finantsraamistikuga ja võimalik koostoime muude asjakohaste vahenditega

KTM2ga kehtestatakse vajalikud läbivaatamised, et anda ELile vahendid ja mehhanismid küberturvalisuse maastikule ja poliitikaeesmärkidele reageerimiseks. Kavandatava määrusega tugevdatakse ENISAt veelgi vajaliku suutlikkusega, et toetada liikmesriike liidu õiguse rakendamisel ja küberohtude vastu võitlemisel. Võttes arvesse eespool nimetatud Draghi ja Letta aruandeid, seatakse mitmeaastase finantsraamistiku 2028–2034 ettepanekus kesksele kohale konkurentsivõime, julgeolek ja strateegiline autonoomia.

Seetõttu kehtestatakse mitmeaastase finantsraamistiku 2028–2034 horisontaalse paketi ettepanekutega, eelkõige Euroopa Konkurentsivõime Fondi ja programmi „Euroopa horisont“ ettepanekutega, uued rahastamiskõlblikkuse kriteeriumid, mis rajanevad põhimõttel, et „suure riskiga tarnijad“ ei saa ELi rahalisi vahendeid taotleda. KTM2 on selle põhimõttega täielikult kooskõlas ja lisaks kujutab see endast vahendit, mis võimaldab rakendada uusi „suure riskiga tarnija“ nõudeid, kuna sellega luuakse toimimisraamistik ELi tasandil küberturvalisuse seisukohast muret tekitavate riikide kindlaksmääramiseks. Selles kontekstis on KTM2 strateegiline ettepanek, mis on kooskõlas komisjoni prioriteetidega tehnoloogilise suveräänsuse saavutamiseks ja konkurentsivõime suurendamiseks Euroopas.

Praeguse killustatuse ületamiseks ühtlustatakse veelgi ELi sertifitseerimisturgu, muutes Euroopa sertifitseerimisprotsessi tõhusamaks ja kestlikumaks.

Mitmeaastase finantsraamistiku 2028–2034 ettepanekutes on lihtsustamispüüdlused seatud prioriteediks kogu raamistiku puhul. Eelarverubriike on kärbitud seitsmelt neljale, samal ajal märkimisväärselt vähendades horisontaalsete rahastamisprogrammide arvu 52-lt 16-le, mis võimaldab paindlikkust ja

kohandatavust praeguste vajadustega. Küberturvalisuse määruse läbivaatamise mõjuhinnangus rõhutati täpselt neid eesmärke: vajadus lihtsustada küberturvalisuse nõudeid mitmes õigusraamistikus, kodifitseerida ja koondada ENISA ülesanded valdkondadesse, millel on kõige suurem mõju ELi küberturvalisuse ökosüsteemi vastupanuvõime suurendamisele. Nende järelduste põhjal suurendavad kavandatud sätted lihtsustamise kaudu konkurentsivõimet; tagavad kõrgel tasemel julgeoleku, tõhustades koordineerimist ning riskide ja nõrkuste analüüsi; toetavad suuremat ühtlustamist, kõrvaldades killustatuse, mis tuleneb paljude riiklike kavade olemasolust. Lisaks on ENISA kavandatud peamise vahendina, mis edendab digivaldkonna lihtsustamispüüdlusi, kuna see lõimib teadete ühtse kontaktpunkti, nagu on kirjeldatud digivaldkonna koondpaketi algatuses[90].

Mitmeaastase finantsraamistiku 2028–2034 paketi oluline osa on ettepanek uue Euroopa Konkurentsivõime Fondi kohta, mis koondab enam kui 16 rahastamisprogrammi, nagu programm „Digitaalne Euroopa“, programm „EL tervise heaks“, Euroopa Kaitsefond jms. Programm „Euroopa horisont“ jääb ka edaspidi eraldiseisvaks programmiks, olles tihedalt seotud Euroopa Konkurentsivõime Fondiga. See uus programmitöö raamistik nõuab tugevat koordineerimist ja rahastamist, mis vastab praegustele prioriteetidele. Sellega seoses on KTM2 kavandatud sätted aluseks koordineerimise süvendamisele ENISA ja küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse vahel, kes vastutavad programmide „Digitaalne Euroopa“ ja „Euroopa horisont“ küberturvalisusega seotud programmiosade elluviimise eest. Kavandatud sätetega tagatakse ENISA ja küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse vaheline sidusus ja rõhutatakse nende koostoimet. Sama lähenemisviisi on kasutatud koostöö puhul muude asutuste ja organitega, näiteks Europoliga.

Teine KTM2 ettepaneku ja mitmeaastase finantsraamistiku 2028–2034 kooskõlastamise aspekt on paindlikkuse põhimõte. Läbivaatamise käigus teeb komisjon ettepaneku nn tasude mehhanismi kohta, mis annab ENISA-le paindliku võimaluse rahastada osaliselt oma tegevusi, mis on eelkõige seotud küberturbeoskuste tõendamise kavade väljatöötamise ja haldamisega, tõendajatele lubade andmise ja nende töötlemisega ning Euroopa küberturvalisuse sertifitseerimise kavade haldamisega. See muudatus tagab ametile paindlikkuse ja skaleeritavuse, et vastata sidusrühmade vajadustele ja teha jätkusuutlikke kulutusi oma teenuste refinantseerimise kaudu.

1.5.5. Erinevate kasutada olevate rahastamisvõimaluste, sealhulgas vahendite ümberpaigutamise võimaluste hinnang

Alates ENISA volituste viimasest läbivaatamisest 2019. aastal on suundumused näidanud ameti eeldatava panuse hüppelist suurenemist liidu õiguse rakendamise toetamise vallas. Seetõttu taotleti iga-aastast eelarvet ja töötajate arvu suurendamist üle algselt kavandatud taseme. Kavandatud läbivaatamisega lisatakse olulisi uusi ülesandeid ja ENISA volitusi, mis kehtestati muude õigusaktidega pärast KTM1 vastuvõtmist, suurendades seeläbi ENISA suutlikkust, mis nõuab täiendavaid rahalisi vahendeid ja inimressursside suurendamist. Lähtudes eesmärgist muuta digitaalne julgeolek Euroopa konkurentsieeliseks, kutsutakse ettepanekus üles keskenduma tegelikule mõjule küberturvalisuse ökosüsteemis. See oleks võimalik üksnes

[90] Lisatakse pärast avaldamist.

märkimisväärsete investeeringutega, mis vastavad soovitavale mõjule ning eelkõige liikmesriikide ja muude sidusrühmade vajadustele. Uued ülesanded hõlmavad vajadust tehnilise ja spetsialiseerunud personali järele ning finantsinvesteeringuid (vahenditesse ja platvormidesse), mida on võimalik tagada üksnes täiendavate rahaliste eraldistega ELi eelarvest.

Selleks et suurendada paindlikkust ja tagada samal ajal ameti pikaajaline jätkusuutlik eelarve, tehakse läbivaatamise käigus ettepanek tasude mehhanismi kohta, millest osaliselt rahastatakse teenuseid, mida osutatakse küberturvalisuse sertifitseerimise raamistiku haldamiseks ning seoses Euroopa individuaalsete küberturbeoskuste tõendamise kavade väljatöötamise ja haldamisega ning tõendajatele lubade andmise ja nende töötlemisega.

Kõik küberturvalisuse määruse läbivaatamist puudutavad täiendavate ressursside kalkulatsioonid tehakse tuginedes ENISA 2025. aasta lähte-eelarvele (tegevuskulud ja täistööajale taandatud töötajad). Komisjon on põhjalikult analüüsinud ametisiseseid ümberpaigutamisvõimalusi, arvestades läbivaadatud volitustes kavandatud uusi ülesandeid. Asjaolu, et amet töötab oma maksimaalse suutlikkuse piiril, ilma et oleks võimalik vähendada tema ülesandeid, ja et haldusnõukogu on juba 2023. aastal võtnud meetmeid prioriteetide muutmiseks, toetab selgelt järeldust, et praegune struktuur ei võimalda täita uusi ülesandeid kui nii eelarvet kui ka inimressursse ei suurendata. Lisaks on paljud praegused ülesanded hõlmatud ENISA ja komisjoni vaheliste rahalist toetust käsitlevate lepingutega. Seetõttu on ettepaneku eesmärk lisada need ülesanded ENISA volituste hulka ja tagada järgnevateks aastateks stabiilne eelarve.

Ilma et see piiraks läbirääkimisi järgmise mitmeaastase finantsraamistiku üle, toimub ametile alates 2028. aastast eraldatavate assigneeringute kompenseerimine mitmeaastase finantsraamistiku 2028–2034 programmide assigneeringute ümberjaotamise teel. Kompenseeriva vähendamise vajaduse korral võib olla vajalik ametile eraldatud ressursside ning nende rahastamisvoogude ja -allikate läbivaatamine. Kavandatavas KTM2 raamistikus kehtestatud meetmed hõlmavad ka ENISA partnerpeadirektoraadile (sidevõrkude, sisu ja tehnoloogia peadirektoraat) lisaülesannete andmist. Eelkõige tuleks märkida, et IKT tarneahela raamistikku rakendatakse täielikult komisjoni tasandil, sh riskihindamisega kaasnevat turuanalüüsi ja rakendusaktide väljatöötamist. Lisaks tuleb komisjonil koostada ja vastu võtta täiendavaid rakendusakte seoses tasude mehhanismi korraga. Euroopa küberturvalisuse sertifitseerimise raamistiku täitmise tagamiseks, näidissätete väljatöötamiseks, küberturvalisuse kavade haldamiseks, kolmandate riikidega sõlmitud vastastikuse tunnustamise lepingute jaoks ning ENISA järelevalvetegevuseks on vaja täiendavat järelevalvet ja abi komisjoni tasandil.

1.6. Ettepaneku/algatuse ja selle finantsmõju kestus

☐ **Piiratud kestusega**

– ☐ hõlmab ajavahemikku [PP/KK]AAAA–[PP/KK]AAAA

– ☐ finantsmõju kulukohustuste assigneeringutele avaldub ajavahemikul AAAA–AAAA ja maksete assigneeringutele ajavahemikul AAAA–AAAA.

☒ **Piiramatu kestusega**

– Rakendamise käivitumisperiood hõlmab ajavahemikku AAAA–AAAA,

– millele järgneb täieulatuslik rakendamine.

1.7. Kavandatud eelarve täitmise viis(id)

☐ **Eelarve otsene täitmine** komisjoni poolt

– ☐ tema talituste kaudu, sealhulgas kasutades liidu delegatsioonides töötavat komisjoni personali;

– ☐ rakendusametite kaudu

☐ **Eelarve jagatud täitmine** koostöös liikmesriikidega

☒ **Eelarve kaudne täitmine**, mille puhul eelarve täitmise ülesanded on delegeeritud:

– ☐ kolmandatele riikidele või nende määratud asutustele;

– ☐ rahvusvahelistele organisatsioonidele ja nende allasutustele (nimetage);

– ☐ Euroopa Investeerimispangale ja Euroopa Investeerimisfondile;

– ☒ finantsmääruse artiklites 70 ja 71 osutatud asutustele;

– ☐ avalik-õiguslikele asutustele;

– ☐ avalikke teenuseid osutavatele eraõiguslikele asutustele, sel määral, mil neile antakse piisavad finantstagatised;

– ☐ liikmesriigi eraõigusega reguleeritud asutustele, kellele on delegeeritud avaliku ja erasektori partnerluse rakendamine ja kellele antakse piisavad finantstagatised;

– ☐ asutustele või isikutele, kellele on delegeeritud Euroopa Liidu lepingu V jaotise kohaste ühise välis- ja julgeolekupoliitika erimeetmete rakendamine ja kes on kindlaks määratud asjaomases alusaktis;

– ☐ liikmesriigis asutatud asutustele, kelle suhtes kohaldatakse liikmesriigi eraõigust või liidu õigust ja kellele võib kooskõlas valdkondlike normidega usaldada liidu rahaliste vahendite või eelarveliste tagatiste haldamise niivõrd, kuivõrd selliseid asutusi kontrollivad avalik-õiguslikud asutused või avalikke teenuseid osutavad eraõiguslikud asutused ja kontrollivad organid annavad neile solidaarvastutuse vormis piisavad finantstagatised või samaväärsed finantstagatised, mis võivad iga meetme puhul piirduda liidu toetuse maksimumsummaga.

Märkused

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse reeglid

Järelevalve ja aruandlus toimub kehtivas küberturvalisuse määruses[91] ja finantsmääruses[92] sätestatud põhimõtete kohaselt ning kooskõlas ühisavalduse ja ühise lähenemisviisiga[93].

Finantsmääruse artikli 40 kohaselt peab ENISA edastama igal aastal komisjonile, Euroopa Parlamendile ja nõukogule ühtse programmdokumendi, mis sisaldab iga-aastast ja mitmeaastast programmitööd ning vahendite kavandamist. Lisaks esitatakse komisjoni ettepanekus ENISA volituste muutmise kohta komisjoni kui haldusnõukogu liikme poolthääle nõue ENISA haldusnõukogu poolt ühtse programmdokumendi vastuvõtmisel inimressursside ja eelarvega seotud küsimustes. Komisjon esitab ka arvamuse ühtse programmdokumendi kavandi kohta enne haldusnõukogus toimuvat hääletusmenetlust, mida tuleks enne ühtse programmdokumendi vastuvõtmist arvesse võtta[94].

ENISA peab esitama haldusnõukogule iga-aastase konsolideeritud tegevusaruande. See aruanne sisaldab eelkõige teavet ühtses programmdokumendis sätestatud eesmärkide ja tulemuste saavutamise kohta. Aruanne tuleb edastada ka komisjonile, Euroopa Parlamendile ja nõukogule. ENISA tegevdirektor peaks esitama haldusnõukogule iga kahe aasta tagant ENISA tegevuse järelhindamise. Amet peaks ka koostama järelmeetmete tegevuskava, mis sisaldab järelhindamise järeldusi, ja esitama iga kahe aasta järel komisjonile aruande tehtud edusammude kohta. Haldusnõukogu peaks vastutama selliste järelduste suhtes asjakohaste järelmeetmete võtmise järelevalve eest.

Kui ameti tegevuses esineb väidetavat haldusomavoli, siis uurib seda Euroopa Ombudsman vastavalt aluslepingu artiklile 228.

Kavandatud järelevalve andmeallikad oleksid peamiselt ENISA, Euroopa küberturvalisuse sertifitseerimise rühm, võrgu- ja infoturbe koostöörühm, CSIRTide võrgustik ning liikmesriikide ametiasutused. Lisaks ENISA, Euroopa küberturvalisuse sertifitseerimise rühma, võrgu- ja infoturbe koostöörühma, CSIRTide võrgustiku ja komisjoni aruannetest (sh iga-aastastest tegevusaruannetest) saadud andmetele kasutatakse vajaduse korral spetsiaalseid andmekogumisvahendeid (näiteks küsitlused riiklikele ametiasutustele, Eurobaromeeter, sihtotstarbelised uuringud ja üleeuroopaliste õppuste aruanded).

Komisjoni ettepanekus KTM2 kohta jätkatakse ameti väljakujunenud läbivaatamistava ja hindamise kohaldamist. KTM2 ettepaneku artikli 119 kohaselt peab komisjon tellima ENISA hindamise hiljemalt [PP.KK.AAAA] ja seejärel iga viie aasta tagant. Hindamise käigus hinnatakse eelkõige ENISA volituste muutmise võimalikku vajadust ja iga sellise muutmise finantsmõju. Iga teise hindamise käigus hinnatakse ENISA saavutatud tulemusi, võttes arvesse tema eesmärke, volitusi, missiooni, juhtimist ja ülesandeid, sh seda, kas ENISA tegevuse jätkamine on

---

91 ELi küberturvalisuse määrus | EUR-Lex.

92 Liidu üldeelarve suhtes kohaldatav finantsmäärus (uuesti sõnastatud) – Euroopa Liidu Väljaannete Talitus.

93 https://europa.eu/european-union/sites/europaeu/files/docs/body/joint_statement_and_common_approach_2012_en.pdf.

94 Delegeeritud määrus – 2019/715 – ET – EUR-Lex.

asjaomaste eesmärkide, volituste, missiooni, juhtimise ja ülesannete seisukohast endiselt põhjendatud.

Hindamise käigus hinnatakse ka määruse III jaotise sätete mõju, tulemuslikkust ja tõhusust seoses Euroopa küberturvalisuse sertifitseerimise raamistiku eesmärkidega, et tagada liidus IKT-toodete, -teenuste ja -protsesside, hallatud turbeteenuste ja -üksuste küberturvalisuse piisav tase ning parandada siseturu toimimist.

Hindamise käigus hinnatakse ka määruse IV jaotise sätete mõju, tulemuslikkust ja tõhusust seoses IKT tarneahela turberaamistiku eesmärkidega.

Komisjon esitab Euroopa Parlamendile ja nõukogule aruande kõikide järelduste kohta ning haldusnõukogule määruse II jaotise hindamistulemuste kohta. Hindamise tulemused avalikustatakse.

2.2. Haldus- ja kontrollisüsteem(id)

2.2.1. Eelarve täitmise viisi(de), rahastuse rakendamise mehhanismi(de), maksete tegemise korra ja kavandatava kontrollistrateegia selgitus

Arvestades, et ettepanek mõjutab ELi iga-aastast toetust ENISA-le, täidetakse ELi eelarvet eelarve kaudse täitmise kaudu.

Usaldusväärse finantsjuhtimise põhimõtte kohaselt täidetakse ENISA eelarvet kooskõlas tulemusliku ja tõhusa sisekontrolliga. Seetõttu on ENISA kohustatud rakendama asjakohast kontrollistrateegiat, mida koordineerivad kontrolliahelas osalevad asjaomased osalejad.

Järelkontrollide puhul kohaldatakse ENISA kui detsentraliseeritud asutuse suhtes eelkõige järgmist:

– komisjoni siseauditi talituse korraldatav siseaudit;

– Euroopa Kontrollikoja aastaaruanded, milles esitatakse kinnitav avaldus raamatupidamise aastaaruande usaldatavuse ning selle aluseks olevate tehingute seaduslikkuse ja korrektsuse kohta;

– iga-aastane eelarve täitmisele heakskiidu andmine Euroopa Parlamendi poolt;

– võimalikud OLAFi juurdlused, mille eesmärk on eelkõige tagada, et asutustele eraldatud vahendeid kasutatakse nõuetekohaselt;

– ENISA partnerpeadirektoraadina rakendab sidevõrkude, sisu ja tehnoloogia peadirektoraat oma detsentraliseeritud asutuste kontrollistrateegiat, et tagada usaldusväärne aruandlus oma iga-aastase tegevusaruande raames. Kuigi detsentraliseeritud asutused vastutavad täielikult oma eelarve täitmise eest, vastutab sidevõrkude, sisu ja tehnoloogia peadirektoraat eelarvepädevate institutsioonide kehtestatud iga-aastaste osamaksete korrapärase maksmise eest;

– lisaks on Euroopa Ombudsman ENISA-le täiendavaks kontrolli- ja aruandlustasandiks.

Ameti hindamise ja KTM2 ettepaneku kohta tehtud mõjuhinnangu põhjal leiti, et äärmiselt oluline on tagada piisavad rahalised vahendid, et ENISA saaks täita talle uute volitustega antud ülesandeid. Ameti läbivaadatud volituste oluline uuendus on tasude mehhanismi kehtestamine, mis on ette nähtud Euroopa küberturvalisuse sertifitseerimise raamistiku raames vastu võetud Euroopa küberturvalisuse

sertifitseerimise kavade halduskulude rahastamiseks. Läbivaadatud Euroopa küberturvalisuse sertifitseerimise raamistikus võetakse halduskord ametlikult kasutusele. Haldustegevust juhib ENISA ja seda rahastatakse osaliselt tasudest, arvestades selle skaleeritavat olemust (rohkemate kavade puhul on haldamiseks vaja lisatöötajaid). Ametil on ka suutlikkus pakkuda testimisvahendeid, et toetada vastavushindamismenetluste rakendamist nii Euroopa küberturvalisuse sertifitseerimise raamistiku kui ka muude asjakohaste ELi kübervaldkonna õigusaktide alusel. Tasude kehtestamise kord sätestatakse rakendusaktis, mille võtab vastu komisjon. Lisaks nähakse läbivaatamisega ette Euroopa individuaalsete oskuste tõendamise kavade väljatöötamine ja haldamine ning otsuste tegemine selle kohta, kas lubada tõendajatel anda välja Euroopa individuaalsete küberturbeoskuste tõendeid.

2.2.2. Teave kindlakstehtud riskide ja nende vähendamiseks kasutusele võetud sisekontrollisüsteemi(de) kohta

KTM2 ettepaneku kui sellise eesmärk on leevendada ENISA volituste ja Euroopa küberturvalisuse sertifitseerimise raamistiku, sh IKT tarneahela turberaamistiku ja lihtsustamissätete raames kindlaks tehtud riske. Täpsemalt, ENISA on Euroopa Liidu amet, mis on juba olemas, ning läbivaatamise käigus on tema volitusi veelgi piiritletud, tugevdades neid valdkondi, mille puhul amet on näidanud üles selget lisaväärtust, ning lisades uusi valdkondi, millele on vaja toetust, pidades silmas uusi poliitika prioriteete ja vahendeid, nagu aruandluse ühtse kontaktpunkti lõimimise kaudu saavutatav lihtsustamine; Euroopa ühise olukorrateadlikkuse ülevaate ja operatiivkoostöö toetamine, tugevdatud ja ühtlustatud Euroopa küberturvalisuse sertifitseerimise raamistik.

Teine kindlakstehtud risk, mida ettepanekus käsitletakse, on komisjoni ja ameti poolt viimastel aastatel sõlmitud rahalist toetust käsitlevate lepingute arv. Praegusest geopoliitilisest olukorrast ja kiiresti muutuvast küberohtude maastikust tingituna on komisjon alates 2019. aastast sõlminud ametiga rahalist toetust käsitlevaid lepinguid kokku enam kui 75 miljoni euro väärtuses. Arvestades, et ENISA-le asjaomaste lepingutega antud ülesanded kuuluvad nüüd tema alaliste ülesannete hulka, kujutab nende lepingute alusel toimiv ebastabiilne eelarvevoog endast ohtu ENISA tegevustulemuste pikaajalisele saavutamisele.

Seetõttu on käesoleva ettepaneku eesmärk muu hulgas tugevdada ameti ressursisuutlikkust, uuesti määrata kindlaks tema ülesanded ja suurendada seeläbi tema tulemuslikkust. Eelkõige toetab tasude kogumise võimalus pikas perspektiivis ameti kestlikku raharinglust Euroopa küberturvalisuse sertifitseerimise raamistiku alusel vastu võetavate Euroopa sertifitseerimise kavade haldamise, vahendite katsetamise ning Euroopa individuaalsete küberturbeoskuste tõendamise kavade väljatöötamise, haldamise ja rakendamisega seotud kulude refinantseerimise teel. Pikas perspektiivis saavutatakse sellega aastas hinnanguliselt 18,5 miljoni euro suurune kokkuhoid ELi eelarves. Komisjon määrab tasude kehtestamise korra ja nende koosseisu kindlaks rakendusaktide vastuvõtmise teel.

Ameti tegevusülesannete suurenemine ei kujuta endast tegelikku riski. Need ülesanded täiendaksid liikmesriikide tegevust ja toetaksid neid vajaduse korral. Samuti piirduvad need analoogselt küberturvalisuse määrusega (EL) 2019/881[95]

[95] https://eur-lex.europa.eu/eli/reg/2019/881/oj/est.

eelnevalt kindlaks määratud teenustega. Ettepaneku uued elemendid/ülesanded loovad lisaväärtust Euroopa sidusrühmadele, kes saaksid kasu ENISAst kui teabekeskusest, kes aitab kaasa teabe jagamisele ja edastab oma osalistele hoiatusteateid.

Lisaks on ameti kavandatav mudel kooskõlas komisjoni ühise lähenemisviisiga detsentraliseeritud asutustele, millega tagatakse piisav kontroll ENISA eesmärkide saavutamiseks tehtava töö üle. Kavandatud muudatuste tegevus- ja finantsriskid näivad olevat piiratud, kuna sätted on koostatud praeguste riskide maandamiseks. Siiski võib pikas perspektiivis oodata teatavaid negatiivseid aspekte seoses järgmisega:

– liikmesriikide suurenevate tegevusvajaduste ning pidevalt muutuvate küberriskide ja -ohtude tõttu on tegevusressursid küberturvalisuse valdkonnas piiratud;

– eelarve kiire suurendamine, eeldades selle kiiret täitmist;

– tegevusvajaduste rahuldamiseks piisavate rahaliste vahendite ja inimressursside puudumine.

2.2.3. *Kontrollimeetmete hinnanguline kulutõhusus (kontrollikulude suhe hallatavate vahendite väärtusse), selle põhjendus ja oodatav veariski tase (maksete tegemise ja sulgemise ajal)*

Sidevõrkude, sisu ja tehnoloogia peadirektoraadi kulud seoses volitatud üksuste, sh ENISA seire ja järelevalvega on ligikaudu 5,25 miljonit eurot, nagu on märgitud 2024. aasta tegevusaruandes[96]. See summa sisaldab peamiselt personalikulusid ja moodustab 0,50 % nendele üksustele 2024. aastal tehtud tegevuskulude maksetest. Kontrollikulude üldmäär tõusis veidi 2023. aasta 0,46 %-lt 2024. aastal 0,50 %-le, kuid on varasemate aastatega võrreldes suhteliselt stabiilne.

Täpsemalt moodustasid ENISA kontrollikulud 2024. aastal 0,32 miljonit eurot ehk 0,70 % kontrollikuludest, võrreldes 0,69 %-ga 2023. aastal ja 1,22 %-ga 2022. aastal. Analüüs näitab, et suuremad kontrollikulud on peamiselt seotud komisjoni ja ameti vaheliste rahalist toetust käsitlevate lepingute väljatöötamise ja järelevalvega (peamiselt personalikulud), mis uute volituste puhul eeldatavasti märkimisväärselt vähenevad, mistõttu saavutatakse eeldatavalt suurem tulemuslikkus. Võrreldes muude volitatud üksustega on ENISAga sidevõrkude, sisu ja tehnoloogia peadirektoraadile kaasnevad üldkulud keskmisel tasemel (11 muu üksuse seas).

KTM2 ettepanekus nähakse ette sidevõrkude, sisu ja tehnoloogia peadirektoraadi töötajate arvu suurendamine 50 täistööajale taandatud töötaja võrra, millest üks täiendav töötaja määratakse konkreetselt täitma ülesandeid, mis tulenevad sellest, et sidevõrkude, sisu ja tehnoloogia peadirektoraat on ameti partnerpeadirektoraat. See isik toetab komisjoni arvamuse koostamist ENISA ühtse programmdokumendi kohta ja jälgib selle rakendamist; toetab ameti eelarve koostamise kontrollimist ja selle täitmise jälgimist. Abistab ametit tema tegevuse edendamisel kooskõlas liidu poliitikaga, sh osaledes asjakohastel koosolekutel. Meedet õigustavad sidevõrkude, sisu ja tehnoloogia peadirektoraadiga seotud suurenenud järelevalveülesanded, mis muu hulgas hõlmavad komisjoni poolthääle nõuet eelarve ja personaliga seotud küsimustes. Tuleb märkida, et sätete rakendamine seoses strateegilisi küberohtusid

[96] CNECT_AAR_2024_final.

kujutavate riikide kindlaksmääramisega (konkreetsete peamiste varade kõrge riskiga tarnijate puhul) on täielikult komisjoni juhitav protsess. Eespool nimetatuga seotud riskihindamiseks on hinnanguliselt vaja 25 täistööajale taandatud töötajat. Meetme vajalikkus tuleneb töö mahust, mida poliitikaraamistiku rakendamine nõuab, täpsemalt ELi koordineeritud riskihindamiste toetamine; iga IKT-toote/teenuse majandusanalüüs; vastavate rakendusaktide väljatöötamine ja raamistiku rakendamise jälgimine; omandiõiguse ja kontrolliga seotud hindamine. Komisjoni kontrollikulusid tarneahela raamistiku rakendamisel mõjutab eeldatavasti eriti see, kui palju teeb komisjon omandi ja kontrolli hindamisi. Samas aitavad nende hindamiste tulemused liikmesriikidel küberturvalisuse 2. direktiivi kohaldamisalasse kuuluvate üksuste suhtes raamistikuga kehtestatud leevendusmeetmete rakendamise ja kohustuste täitmise üle järelevalve tegemisel oluliselt kokku hoida. Liikmesriigid saavad kasutada omandi ja kontrolli hindamiste tulemusi, selle asemel et kulutada vahendeid samade hindamisvajaduste rahuldamiseks. Euroopa küberturvalisuse sertifitseerimise raamistiku tugevdamine, sellega seotud tegevuste standardimine ja rakendamine, küberturvalisuse 2. direktiivi rakendamine (sh vastavad rakendusvajadused, tasusid käsitlevad rakendusaktid ning sertifitseerimiskavade ja oskuste tõendamise kavade haldamise toetamine) vajab hinnanguliselt 19 täistööajale taandatud töötajat, samas kui operatiivkoostöö ja olukorrateadlikkuse poliitika jaoks on vaja täiendavalt viit täistööajale taandatud töötajat. Punktis 3.2.4 on esitatud ülesannete täielik kirjeldus.

ENISA jõudis oma 2023. aasta konsolideeritud tegevusaruandes[97] oma sisekontrollisüsteemide hindamise suhtes positiivsele järeldusele ja esitas heakskiitva kinnitava avalduse. Oma aastaaruandes ELi asutuste eelarveaasta 2023 kohta esitas kontrollikoda raamatupidamise aastaaruande kohta märkusteta auditiarvamuse ja märkustega arvamuse raamatupidamise aastaaruande aluseks olevate maksete seaduslikkuse ja korrektsuse kohta (millele on viidatud ka punktis 2.2.2). Sidevõrkude, sisu ja tehnoloogia peadirektoraat on aruande teadmiseks võtnud, kuid jõudnud järeldusele, et see ei mõjuta tema järelevalve tõhusust. ENISA annab korrapäraselt aru ka meetmete kohta, mida on võetud vigadega seotud leidude kordumise ärahoidmiseks, ning praegu ei viita miski sellele, et veamäär lähiaastatel halveneks või ületaks 2 %.

Lisaks on ENISA finantseeskirjade[98] artikli 80 lõikes 2 sätestatud võimalus, et ametil on ühine siseauditi üksus mõne teise samas poliitikavaldkonnas tegutseva liidu asutusega, kui üksnes ühe liidu asutuse tarbeks ette nähtud siseauditi üksuse loomine ei oleks kulutõhusus.

Kokkuvõttes võib öelda, et võttes arvesse ameti kavandatavat suurendamist enam kui 100 % võrreldes kontrollikulude suhteliselt väikese suurenemisega, näitab analüüs rahuldavat kulutasuvuse määra. Kõiki kättesaadavaid andmeid arvesse võttes ei viita miski sellele, et eeldatav veamäär võiks olla suurem kui 2 %.

2.3. Pettuste ja õigusnormide rikkumise ärahoidmise meetmed

Euroopa Liidu Küberturvalisuse Amet rakendab pettuste ja õigusnormide rikkumiste ärahoidmiseks kõrgeimaid standardeid.

Ameti personal kontrollib enne makse tegemist kõiki teenuste ja uuringute eest maksmisele kuuluvaid summasid, võttes arvesse kõiki lepingulisi kohustusi,

97 enisa.europa.eu/sites/default/files/2024-11/2023 Consolidated Annual Activity Report_1.pdf.

98 MB Decision 2019_8 Financial rules_adopted.pdf.

majanduslikke põhimõtteid ning head finantstegevus- ja juhtimistava. Pettusevastased sätted (järelevalve, aruandlusnõuded jms) lisatakse kõikidesse ameti ja mis tahes makse saajate vahelistesse kokkulepetesse ning lepingutesse.

Pettuste, korruptsiooni ja muude õigusvastaste tegude vastu võitlemiseks kohaldatakse piiranguteta Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) nr 883/2013 sätteid.

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

- Olemasolevad eelarveread

Järjestage mitmeaastase finantsraamistiku rubriigiti ja iga rubriigi sees eelarveridade kaupa

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Kulu liik	Rahaline osalus			
	Nr	Liigendatud/liigendamata[99]	EFTA riigid[100]	Kandidaatriigid ja potentsiaalsed kandidaadid[101]	Muud kolmandad riigid	Muu sihtotstarbeline tulu
	[XX.YY.YY.YY]	Liigendamata	JAH	EI	EI	JAH/EI
	[XX.YY.YY.YY]	Liigendatud/liigendamata	JAH/EI	JAH/EI	JAH/EI	JAH/EI
	[XX.YY.YY.YY]	Liigendatud/liigendamata	JAH/EI	JAH/EI	JAH/EI	JAH/EI

- Uued eelarveread, mille loomist taotletakse

Järjestage mitmeaastase finantsraamistiku rubriigiti ja iga rubriigi sees eelarveridade kaupa

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Kulu liik	Rahaline osalus			
	Nr	Liigendatud/liigendamata	EFTA riigid	Kandidaatriigid ja potentsiaalsed kandidaadid	Muud kolmandad riigid	Muu sihtotstarbeline tulu

99 Liigendatud = liigendatud assigneeringud / liigendamata = liigendamata assigneeringud.
100 EFTA: Euroopa Vabakaubanduse Assotsiatsioon.
101 Kandidaatriigid ja vajaduse korral Lääne-Balkani potentsiaalsed kandidaadid.

	[XX.YY.YY.YY]	Liigendatud/liigendamata	JAH/EI	JAH/EI	JAH/EI	JAH/EI
	[XX.YY.YY.YY]	Liigendatud/liigendamata	JAH/EI	JAH/EI	JAH/EI	JAH/EI
	[XX.YY.YY.YY]	Liigendatud/liigendamata	JAH/EI	JAH/EI	JAH/EI	JAH/EI

3.2. Ettepaneku hinnanguline finantsmõju assigneeringutele

3.2.1. Hinnanguline mõju tegevusassigneeringutele – ülevaade

– ☐ Ettepanek/algatus ei nõua tegevusassigneeringute kasutamist

– ☒ Ettepanek/algatus nõuab tegevusassigneeringute kasutamist, mis toimub järgmiselt:

3.2.1.1. Heakskiidetud eelarvest saadavad assigneeringud

miljonites eurodes (kolm kohta pärast koma)

Asutus: ENISA	Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**	**Mitmeaastane finantsraamistik 2028–2034 KOKKU**
Eelarverida <…….> / ELi eelarvest ametile antav täiendav toetus	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006

Ametile ette nähtud assigneeringute / ELi eelarve toetuse kompenseerimiseks vähendatakse programmi <….> rahastamispaketti / eelarverida: <…….> / aasta(te)l: <…….> .

			Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**	**Mitmeaastane finantsraamistik 2028–2034 KOKKU**
Tegevusassigneeringud KOKKU	Kulukohustused	(4)	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006
	Maksed	(5)	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006
Eriprogrammide vahenditest rahastatavad haldusassigneeringud KOKKU		(6)	1,365	1,365	1,470	1,785	2,100	2,415	2,625	**13,125**

Mitmeaastase finantsraamistiku	Kulukohustused	= 4 + 6	22,265	21,959	26,808	28,586	28,901	28,716	28,926	186,161
RUBRIIGI 2 assigneeringud KOKKU	Maksed	= 5 + 6	22,265	20,890	24,851	26,254	26,254	25,754	25,754	186,161

DG: CNECT	Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**	**Mitmeaastane finantsraamistik 2028–2034 KOKKU**
• Personalikulud	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**
• Muud halduskulud	0	0	0	0	0	0	0	**0**

DG CNECT **KOKKU**	Assigneeringud	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**

Mitmeaastase finantsraamistiku RUBRIIGI 4 assigneeringud KOKKU	(Kulukohustuste kogusumma = maksete kogusumma)	**2,328**	**2,328**	**3,104**	**3,492**	**3,880**	**4,268**	**4,850**	**24,25**

miljonites eurodes (kolm kohta pärast koma)

		Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**	**Mitmeaastane finantsraamistik 2028–2034 KOKKU**
Mitmeaastase	Kulukohustused	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38

finantsraamistiku										
RUBRIIKIDE 1–4 assigneeringud KOKKU	Maksed	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38	

3.2.2. Hinnanguline tegevusassigneeringutest rahastatav väljund (ei täideta detsentraliseeritud asutuste puhul)

kulukohustuste assigneeringud miljonites eurodes (kolm kohta pärast koma)

Märkige eesmärgid ja väljundid ⇩			Aasta **2028**		Aasta **2029**		Aasta **2030**		Aasta **2031**		Lisage vajalik arv aastaid, et näidata finantsmõju kestust (vt punkt 1.6)						**KOKKU**	
	VÄLJUNDID																	
	Väljundi liik[102]	Keskmine kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Väljundite arv kokku	Kulud kokku
ERIEESMÄRK nr 1[103] …																		
- Väljund																		
- Väljund																		
- Väljund																		
Erieesmärk nr 1 kokku																		
ERIEESMÄRK nr 2 ...																		
- Väljund																		
Erieesmärk nr 2 kokku																		

102 Väljunditena käsitatakse tarnitud tooteid ja osutatud teenuseid (rahastatud üliõpilasvahetuste arv, ehitatud teede pikkus kilomeetrites jms).

103 Vastavalt punktile 1.3.2 „Erieesmärgid“.

KOKKU																

3.2.3. Hinnanguline mõju haldusassigneeringutele – ülevaade

– ☐ Ettepanek/algatus ei nõua haldusassigneeringute kasutamist

– ☒ Ettepanek/algatus nõuab haldusassigneeringute kasutamist, mis toimub järgmiselt:

3.2.3.1. Heakskiidetud eelarvest saadavad assigneeringud

(täiendav)

HEAKSKIIDETUD EELARVE	Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**	**2028–2034 KOKKU**
RUBRIIK 4								
Personalikulud	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Muud halduskulud	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
RUBRIIK 4 kokku	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
RUBRIIGIST 4 välja jäävad kulud								
Personalikulud	1,365	1,365	1,470	1,785	2,100	2,415	2,625	**13,125**
Muud halduskulud	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
RUBRIIGIST 4 välja jäävad kulud kokku	**1,365**	**1,365**	**1,470**	**1,785**	**2,100**	**2,415**	**2,625**	**13,125**
KOKKU	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**

3.2.4. Hinnanguline personalivajadus (täiendav)

– ☐ Ettepanek/algatus ei nõua personali kasutamist

– ☒ Ettepanek/algatus nõuab personali kasutamist, mis toimub järgmiselt:

3.2.4.1. Rahastatakse heakskiidetud eelarvest

Hinnanguline väärtus täistööaja ekvivalendina[104]

HEAKSKIIDETUD EELARVE	Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**
• Ametikohtade loeteluga ette nähtud ametikohad (ametnikud ja ajutised töötajad)							
20 01 02 01 (komisjoni peakorteris ja esindustes)	12	12	16	18	20	22	25
20 01 02 03 (ELi delegatsioonides)	0	0	0	0	0	0	0
(kaudne teadustegevus)	0	0	0	0	0	0	0
(otsene teadustegevus)	0	0	0	0	0	0	0
Muud eelarveread (märkige)	0	0	0	0	0	0	0
• Koosseisuväline personal (täistööaja ekvivalendina)							
20 02 01 (üldvahenditest rahastatavad lepingulised töötajad ja riikide lähetatud eksperdid)	0	0	0	0	0	0	0

104 Palun täpsustage allpool esitatud tabelis, kui palju täistööaja ekvivalente on juba määratud meetme haldamiseks ja/või kui palju saab neid teie peadirektoraadis ümber paigutada ja millised on teie netovajadused.

20 02 03 (lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid ja noored eksperdid ELi delegatsioonides)		0	0	0	0	0	0	0
Haldustoetuse eelarverida	- peakorteris	0	0	0	0	0	0	0
[XX.01.YY.YY]	- ELi delegatsioonides	0	0	0	0	0	0	0
(lepingulised töötajad ja riikide lähetatud eksperdid kaudse teadustegevuse valdkonnas)		0	0	0	0	0	0	0
(lepingulised töötajad ja riikide lähetatud eksperdid otsese teadustegevuse valdkonnas)		0	0	0	0	0	0	0
Muud eelarveread (märkige) - Rubriik 4		0	0	0	0	0	0	0
Muud eelarveread (märkige) - Rubriigist 4 välja jäävad kulud		13	13	14	17	20	23	25
KOKKU		**25**	**25**	**30**	**35**	**40**	**45**	**50**

Ettepaneku rakendamiseks vajatav personal (täistööaja ekvivalendina)

	Kaetakse komisjoni talituste olemasolevast personalist	**Erakorraline lisapersonal**		
		Rahastatakse rubriigist 7 või teadusuuringute eelarveridadelt	**Rahastatakse BA ridadelt**	**Rahastatakse tasudest**
Ametikohtade loeteluga ette nähtud ametikohad		25		
Koosseisuväline personal (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud)			25	

Hinnanguline mõju kuludele ja personalile 2028. aastal ja pärast seda on esialgne ega mõjuta järgmist mitmeaastast finantsraamistikku. Liidu rahaliste kohustuste rahastamisallikas ja ulatus 2027. aasta järgsel perioodil sõltub endiselt mitmeaastase finantsraamistiku 2028–2034 üle peetavate institutsioonidevaheliste läbirääkimiste tulemustest ning iga-aastasest eelarvemenetlusest ja juhtimismehhanismist.

Komisjoni valdkondliku peadirektoraadi täidetavate ülesannete kirjeldus

Ametnikud ja ajutised töötajad	**ENISA koordineerimine (1)**: Komisjoni esindamine ameti haldusnõukogus. Komisjoni arvamuse koostamine ENISA ühtse programmdokumendi kohta ja selle rakendamise jälgimine. Ameti eelarve koostamise kontrollimine ja selle täitmise jälgimine. Ameti abistamine tema tegevuse edendamisel kooskõlas liidu poliitikaga, sh osaledes asjakohastel koosolekutel. **Oskuste tõendamise kavad / oskuste akadeemia (2)**: Sidevõrkude, sisu ja tehnoloogia peadirektoraat vajab lisatöötajaid, et koostada rakendusaktid, millega kehtestatakse tasud, mida ENISA võtab taotlejatelt, et saada volitatud tõendajaks. Nimetatud rakendusaktide arv on vähemalt 12, üks iga Euroopa küberturbeoskuste raamistiku profiili kohta. **Tarneahel** (25) Liidu koordineeritud riskihindamiste ettevalmistamise toetamine. Majandusanalüüsi tegemine iga asjaomase IKT-toote ja -teenuse kohta. Asjaomaste rakendusaktide koostamine, milles käsitletakse peamiste varade kindlakstegemist, kavandatud leevendusmeetmeid ja selliste riikide kindlaksmääramist, kes kujutavad endast konkreetsete peamiste varade puhul strateegilist küberohtu, suure riskiga tarnijate kindlakstegemist, eranditaotluste kontrollimist ja komisjoni otsuste väljatöötamist. Vastuvõetud meetmete rakendamise ja järelevalve toetamine. **Euroopa küberturvalisuse sertifitseerimise raamistik, standardimine ja sellega seotud tegevuste rakendamine, küberturvalisuse 2. direktiivi rakendamine (17)**: Küberturvalisuse määruse täitmise tagamine, eelkõige vastavushindamisasutuste juhtimine (kohustusega toimetulek) Sidusrühmade kaasamine (ja assamblee) Vastastikune tunnustamine kolmandate riikidega Rakendusakti standardne väljatöötamine (üksikasjalikud taotlused, mille puhul kasutatakse konsulteerimist ja näidissätete väljatöötamist) Kava haldamine, õiguslik läbivaatamine, komiteemenetlus Koostöö võrgu- ja infoturbe koostöörühmaga ja üksuse kava haldamine Küberturvalisuse 2. direktiivi kohased rakendusaktid Vastavushindamisasutuste vastavusse viimine küberturvalisuse määrusega, vastavuse eeldamine ning standardimine Turujärelevalve ja riikliku küberturvalisuse sertifitseerimise asutuse vaheline koostöö Küberkerksuse määruse ja sertifitseerimise kavade tehniline ühtlustamine **Tegevuse koordineerimine ja olukorrateadlikkus (5)**: Valdkondlik ja ohusubjekte puudutav oskusteave, et suurendada ELi tasandi olukorrateadlikkust elutähtsat taristut ähvardavatest ohtudest, sh kujunemisjärgus tehnoloogiaga kaasnevatest ohtudest. Koordineerimine ENISA ning muude ELi üksuste ja võrgustikega, et tagada valmisolek olulisteks ja ulatuslikeks küberintsidentideks.
Koosseisuvälised töötajad	Vt eespool.

ENISA täidetavate lisaülesannete kirjeldus

Ametnikud ja ajutised töötajad	ELi küberreservi haldamine (riikide juhid ja rakendamise toetamine, samas kui reservi tegelikud tegevuskulud kaetakse kübersolidaarsuse määruse kohaselt) (10) Küberkerksuse määruse kohane ühtse teatamisplatvormi haldamine (käitamine) (9) Ühtse teatamisplatvormiga seotud turvanõrkusteenused (4) Ühtse teatamisplatvormi laiendamine ühtsele kontaktpunktile (arendamine ja käitamine) (8) Tehniliste suuniste, tooteturbealase oskusteabe ja turuanalüüsi väljatöötamine küberkerksuse määruse rakendamise toetamiseks (7) Standardimine küberkerksuse määruse rakendamise toetamiseks / sertifitseerimine / küberturvalisuse 2. direktiiv (4) Küberkerksuse määruse kohaste turujärelevalvetoimingute toetamine (4) Toodete vastavustestimise ja turvalisuse hindamise toetamine (4) Liikmesriikide toetamine vastastikuse abi andmisel (3) Nõrkushalduse teenuste osutamine, Euroopa nõrkuste andmebaasi haldamine ning nõustamis- ja täiustamisülesannete täitmine (nõrkuste koordineeritud avalikustamine) (15) Operatiivkoostöö ja olukorrateadlikkus – leevendus- ja tugiplatvormid, nagu näiteks CNW/CyCLONe; hoiatusteadetega seotud ülesannete toetamine; tõhustatud koordineerimise toetamine muude asjaomaste üksustega, et töötada välja kontrollitud ja usaldusväärse küberohuteadmuse hoidlad (KTM2 artikli 11 lõike 1 punkt a) (5) Kriitilise tähtsusega sektorite vastupanuvõime toetamine (sh tervishoiu küberturvalisuse tegevuskava rakendamine) (4) Oskuste tõendamise kava väljatöötamine (2) Oskuste tõendamise kava haldamine ja järelevalve (6) Haldustöötaja (tasude/personali/IT arvestaja) (8) Sertifitseerimiskavade haldamine (11) Horisontaalsed ülesanded – sidusrühmade suurem kaasamine, tehniliste kirjelduste koostamine ja osalemine kavasid toetavas standardimistegevuses (1)
Koosseisuvälised töötajad	Vt eespool. Kaks kohustuslikku riikide lähetatud eksperti igast liikmesriigist, et toetada ameti tegevust, tegutsedes riiklike kontaktametnikena, keskendudes operatiivkoostööle ja nõrkuste koordineeritud avalikustamisele. (13) Ülejäänud 27 riikide lähetatud eksperti töötavad kavandatavalt tasuta ja seega ei mõjuta need eelarvet.

ENISA perioodi 2028–2034 täiendavad tegevuskulud aastas

Kulu	Eelarve	Periood	Selgitus
Küberturbeoskuste veebisait	750 000 eurot	50 % 2029. aastal 50 % 2030. aastal	Menetluste läbipaistvuse tagamiseks nõutakse ettepanekus, et

			ENISA haldaks veebisaiti, mis sisaldab Euroopa küberturvalisuse sertifitseerimise raamistiku profiile, oskuste tõendamise kavasid, teavet iga kava tasude kohta, soovituslikke tasusid iga tõendamise eest ja volitatud tõendajate loetelu.
Nõrkuste koordineeritud avalikustamine	1 miljon eurot	Alates 2028. aastast	Meie elutähtsas taristus kasutatavate toodete ja teenuste turvalisus sõltub suurel määral avastatud nõrkuste ja nende leevendamise võimaluste kohta õigeaegse teabe jagamisest.
Küberohuteadmus	3 miljonit eurot	Alates 2028. aastast	ENISA ja komisjoni koostöös valmiva olukorrateadlikkuse ülevaate väljatöötamiseks.
Ühtne kontaktpunkt	8 miljonit eurot	6 miljonit eurot 2028. aastal 500 000 eurot 2029. aastal 500 000 eurot 2030. aastal 500 000 eurot 2031. aastal 500 000 eurot 2032. aastal	Komisjoni digivaldkonna koondpaketi ettepaneku elluviimiseks, et lihtsustada küberintsidentidest ja andmetega seotud rikkumistest teatamise kohustuste täitmist, töötades selleks välja ühtse kontaktpunkti ja hallates seda.

Küberkerksuse määruse kohase ühtse teatamisplatvormi haldamine ja muu	3 miljonit eurot	Alates 2028. aastast	Kaasseadusandjate kehtestatud ühtne teatamisplatvorm on kõigi aegade suurim ENISA tegevuse ajal välja töötatud IT-süsteem, mis on küberkerksuse määruse oluline tugisammas. Seda rahastatakse praegu rahalist toetust käsitleva lepingu alusel, kuid selle igapäevane haldamine nõuab nii täistööajale taandatud töötajaid (vt eespool) kui ka tegevuskulusid. ENISA-l on keskne roll liidu tooteturvalisuse raamistiku – küberkerksuse määruse – edu tagamisel.
ENISA turvaline side ja küberturvalisuse küpsus	2 miljonit eurot +	1,1 miljoni euro suurune investeering 2028. aastal (CyCLONe / CSIRTide platvormid ning sektoripõhised kogukonnad) 1 miljon eurot haldusaasta kohta alates 2029. aastast 1,5 miljonit eurot küberküpsuse tagamiseks	Ameti küberturvalisuse ja sidevahendite tagamine.

Küberturvalisuse sertifitseerimise haldamine	1 400 000 miljonit eurot	600 000 eurot 2028. aastal 1 000 000 eurot 2029. aastal 1 200 000 eurot 2030. aastal 1 400 00 eurot 2031. aastal 1 400 000 eurot 2032. aastal 1 400 000 eurot 2033. aastal 1 400 000 eurot 2034. aastal	Kaetakse tasudega (täielikult alates 2032. aastast)
Küberturbeoskuste tõendamise kavad	212 920 eurot	Alates 2030. aastast kaetakse 50 % ELi eelarvest	Täielikult kaetakse tasudega alates 2033. aastast

3.2.5. Hinnanguline mõju digitehnoloogiaga seotud investeeringutele – ülevaade

Kohustuslik: järgmises tabelis tuleks esitada parim hinnang ettepanekust/algatusest tulenevate digitehnoloogiaga seotud investeeringute kohta.

Erandkorras, kui see on vajalik ettepaneku/algatuse rakendamiseks, tuleks rubriigi 4 assigneeringud esitada selleks ettenähtud eelarvereal.

Rubriikide 1–3 assigneeringuid tuleks kajastada „tegevusvaldkonna IT-kuludena, mis on eraldatud rakenduskavadele“. Nende kulud kuuluvad tegevuseelarvesse, mida kasutatakse otseselt algatuse rakendamisega seotud IT-platvormide/vahendite taaskasutamiseks/ostmiseks/arendamiseks ja nendega seotud investeeringuteks (nt litsentsid, uuringud, andmete säilitamine jne). Selles tabelis esitatud teave peaks olema kooskõlas 4. jaos „Digimõõde“ esitatud üksikasjadega.

Digi- ja IT-assigneeringud KOKKU	Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**	**Mitmeaastane finantsraamistik 2028–2034 KOKKU**
RUBRIIK 4								
Institutsiooni tasandi IT-kulud	0	0	0	0	0	0	0	**0**
RUBRIIK 4 kokku	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

RUBRIIGIST 4 välja jäävad kulud								
Poliitikavaldkondade IT-kulud rakenduskavadele	0	0	0	0	0	0	0	**0**
RUBRIIGIST 4 välja jäävad kulud kokku	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
KOKKU	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

3.2.6. Kooskõla kehtiva mitmeaastase finantsraamistikuga

Ettepanek/algatus:

– ☒ on täielikult rahastatav mitmeaastase finantsraamistiku asjaomase rubriigi sisese vahendite ümberpaigutamise kaudu

Ilma et see piiraks läbirääkimisi järgmise mitmeaastase finantsraamistiku üle, toimub ametile alates 2028. aastast eraldatavate assigneeringute kompenseerimine mitmeaastase finantsraamistiku 2028–2034 programmide assigneeringute ümberjaotamise teel. Kompenseeriva vähendamise vajaduse korral võib olla vajalik ametile eraldatud ressursside ning nende rahastamisvoogude ja -allikate läbivaatamine.

– ☐ tingib mitmeaastase finantsraamistiku asjaomase rubriigi mittesihtotstarbelise varu ja/või mitmeaastase finantsraamistiku määruses sätestatud erivahendite kasutuselevõtu

– ☐ nõuab mitmeaastase finantsraamistiku muutmist

3.2.7. Kolmandate isikute rahaline osalus

Ettepanek/algatus:

– ☒ ei näe ette kolmandate isikute poolset kaasrahastamist

– ☐ näeb ette kolmandate isikute poolse kaasrahastuse, mille hinnanguline summa on järgmine:

assigneeringud miljonites eurodes (kolm kohta pärast koma)

	Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Kokku
Nimetage kaasrahastav asutus					
Kaasrahastatavad assigneeringud KOKKU					

3.2.8 Detsentraliseeritud asutuse hinnanguline personali- ja assigneeringute vajadus

Täiendav personalivajadus (täistööajale taandatud töötajate arv)

Asutus: ENISA	Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**

Ajutised teenistujad (AD palgaastmed)	5	11	17	19	19	19	19
Ajutised teenistujad (AST palgaastmed)	4	7	11	12	12	12	12
Ajutised teenistujad (AD + AST) kokku	***9***	***18***	***28***	***31***	***31***	***31***	***31***
Lepingulised töötajad	22	44	66	74	74	74	74
Riikide lähetatud eksperdid	4	8	11	13	13	13	13
Lepingulised töötajad ja riikide lähetatud eksperdid kokku	26	52	77	87	87	87	87
Töötajad KOKKU	35	70	105	118	118	118	118

ELi eelarvest ette nähtud toetusest kaetavad assigneeringud miljonites eurodes (kolm kohta pärast koma)

Asutus: ENISA	Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**	**2028–2034 KOKKU**
Jaotis 1. Personalikulud	4,488	8,466	12,507	13,648	10,584	10,012	9,537	**87,766**
Jaotis 2. Taristu- ja tegevuskulud								
Jaotis 3. Tegevuskulud	16,413	11,588	11,528	11,788	11,613	11,613	11,113	**85,240**
ELi eelarvest kaetavad assigneeringud KOKKU	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**

Kui see on asjakohane, tasudest kaetavad assigneeringud miljonites eurodes (kolm kohta pärast koma)

Asutus: ENISA	Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**	**2028–2034 KOKKU**
Jaotis 1. Personalikulud		0,510	1,043	1,539	4,604	5,176	5,650	**18,522**
Jaotis 2. Taristu- ja tegevuskulud								**0,000**
Jaotis 3. Tegevuskulud								**0,000**
Tasudest kaetavad assigneeringud KOKKU	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**

Detsentraliseeritud asutuse personali- ja assigneeringute (miljonites eurodes) vajadus ettepaneku/algatuse rakendamiseks – ülevaade

Asutus: ENISA	Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**	**2028–2034 KOKKU**
Ajutised töötajad (AD + AST)	9	18	28	31	31	31	31	*31*
Lepingulised töötajad	22	44	66	74	74	74	74	74
Riikide lähetatud eksperdid	4	8	11	13	13	13	13	13
Töötajad kokku	35	70	105	118	118	118	118	**118**
ELi eelarvest kaetavad assigneeringud	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**
Tasudest kaetavad assigneeringud (kui see on asjakohane)	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**
Kaasrahastatavad assigneeringud (kui see on asjakohane)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Assigneeringud KOKKU	**20,901**	**20,564**	**25,078**	**26,976**	**26,801**	**26,801**	**26,801**	**173,922**

3.3. Hinnanguline mõju tuludele

– ☒ Ettepanekul/algatusel puudub finantsmõju tuludele

– ☐ Ettepanekul/algatusel on järgmine finantsmõju:

  – ☐ omavahenditele

  – ☐ muudele tuludele

  – ☐ märkige, kas see on kulude eelarveridasid mõjutav sihtotstarbeline tulu

miljonites eurodes (kolm kohta pärast koma)

Tulude eelarverida	Jooksval eelarveaastal kättesaadavad assigneeringud	Ettepaneku/algatuse mõju[105]						
		Aasta **2028**	Aasta **2029**	Aasta **2030**	Aasta **2031**	Aasta **2032**	Aasta **2033**	Aasta **2034**
Artikkel ….								

[105] Traditsiooniliste omavahendite (tollimaksud ja suhkrumaksud) korral tuleb märkida netosummad, st brutosumma pärast 20 % sissenõudmiskulude mahaarvamist.

Sihtotstarbeliste tulude puhul märkige, milliseid kulude eelarveridasid ettepanek mõjutab.

Muud märkused (nt tuludele avaldatava mõju arvutamise meetod/valem või muu teave).

Tasude mehhanism on seotud ENISA kolme tegevusvaldkonnaga.

– Euroopa individuaalsete küberturbeoskuste tõendamise kavade raames tõendite väljastajate volitamisega seotud tasud.

Selle meetmega seotud tasud määratakse kindlaks rakendusaktiga pärast läbivaadatud küberturvalisuse määruse vastuvõtmist. Vajalike investeeringute ja kulude hindamiseks tehti arvutused siiski ühes ELi liikmesriigis kasutusel oleva mudeli alusel[106]. Mudel sisaldab ühekordset makset ja aastatasu.

Püsikulud: 8 540 eurot

Aastatasu: 800 eurot

Tasud on ette nähtud selle konkreetse meetme kulude refinantseerimiseks. Viie aasta kulud on hinnanguliselt 1 064 600 eurot. Sellega hõlmatud meetme konkreetsed kulud on seotud kavade väljatöötamise ja haldamisega, sh sellise ajutise töörühma liikmete kuludega, kes toetaks ENISAt kavade väljatöötamisel (kulude hüvitamine ja raportööride tasud), lähetustega kohapealsete tõendajate auditeerimiseks ja hindajate koolitamisega, et tagada kavade ühetaoline rakendamine:

A) ajutise töörühma kulud 800 000 eurot;

B) kahe hindaja koolitus liikmesriigi kohta kuni 129 600 eurot;

C) ühe üksuse auditeerimine liikmesriigi kohta kuni 135 000 eurot.

(A + B + C) / 5 = 212 920 eurot kulusid aastas

Ettepanekuga nähti esimeseks kolmeks aastaks ette üleminekuperiood ja alginvesteering. Üleminekuperioodil kaetakse kulud ELi eelarvest ning 4. ja 5. aastal kaetakse kulud 50 % ulatuses, 6. ja 7. aastal kohaldatakse tasusid täies ulatuses.

Aasta	Tasud
2028	0
2029	0
2030	0
2031	106 460 (tulud)
2032	106 460 (tulud)
2033	212 920 (tulud)
2034	212 920 (tulud)

106 Decision RR-02: Price list of SNAS services: https://www.snas.sk/storage/app/uploads/public/677/e79/e4c/677e79e4cac62903312474.pdf,

– Tasud, mis on seotud Euroopa küberturvalisuse sertifitseerimise raamistiku raames vastu võetud küberturvalisuse sertifitseerimise kava halduskulude katmisega.

Selle meetmega seotud tasud määratakse kindlaks rakendusaktiga pärast läbivaadatud küberturvalisuse määruse vastuvõtmist. Kava hinnangulised halduskulud põhinevad turuanalüüsil, mis on esitatud küberturvalisuse määruse läbivaatamise ettepaneku mõjuhinnangus. Meetmega viie aasta jooksul kaasnevad arvutuslikud kogukulud: tegevuskulud 5 600 000 eurot ja täistööajale taandatud töötajate kulud 7 100 000 eurot.

Haldustegevuse iga-aastane kulu on arvutatud praeguse kogemuse põhjal järgmiselt: 200 000 eurot kava iga haldusaasta kohta[107] ja kaks täistööajale taandatud töötajat, kes tegelevad haldamisega (iga-aastane kulu 125 887 eurot täistööajale taandatud töötaja kohta), võttes arvesse asjaomase kava kavandatavat vastuvõtmisaastat. Eeldatakse, et asjaomastest tasudest saadav tulu suureneb iga uue kava vastuvõtmisel ja selliste kavade järkjärgulisel kasutuselevõtul. Seni on Euroopa küberturvalisuse sertifitseerimise raamistiku raames vastu võetud üks kava (Euroopa ühiskriteeriumidel põhinev küberturvalisuse sertifitseerimise kava, EUCC) ja selle kava haldamisest saadavat esimest tulu on oodata 2029. aastal. Kulud kaetakse eeldatavasti 2032. aastaks.

Hinnangulised tulud on arvutatud, lähtudes iga võimaliku kava puhul konkreetsetest eeldustest järgmiste aspektide kohta: eeldatav kasutuselevõtt (väljaantavate sertifikaatide arv), iga sertifikaadi kehtivusaeg ja tegevate vastavushindamisasutuste arv. Tulevase turvaoleku kava kasutuselevõtust saadakse eeldatavasti märkimisväärset tulu.

Aasta Tulud (ELi eelarvest kaetavate/makstavate kulude protsent)

2028 0

2029 250 000 (11 % / – 1 350 000 eurot) – üks kava (EUCC)

2030 783 000 (29 % / – 2 000 000 eurot) – kolm kava (EUCC, ID-kukkur, liikuv kosmoseside)

2031 783 000 (25 % / – 1 930 000 eurot) – kolm kava (EUCC, ID-kukkur, liikuv kosmoseside)

2032 3 850 000 (122 % / – 2 400 000 eurot) – viis kava (EUCC, ID-kukkur, liikuv kosmoseside, EUCS, 5G)

2033 4 000 000 (126 % / + 685 000 eurot) – kuus kava (EUCC, ID-kukkur, liikuv kosmoseside, EUCS, 5G, turvaolek)

2034 4 500 000 (141 % / + 825 000 eurot) – seitse kava

Vastavushindamismenetlusi toetavate katsevahenditega seotud tasud

[107] Täpsemalt on halduskulude puhul võetud arvesse kahte ekspertidega kohtumist aastas (100 000 eurot), kavaga seotud dokumentide väljatöötamist ja läbivaatamist toetavate töövõtjate kulusid, sertifitseerimise kavade kasutuselevõttu, vastastikust hindamist ja vastavushindamise rakendamist (4 x 15 000 = 60 000 eurot). Kulud hõlmavad ka Euroopa ühendamise rahastu platvormi ja ENISA sertifitseerimise veebisaidiga seotud tegevust (40 000 eurot).

Selle meetmega seotud tasud määratakse kindlaks rakendusaktiga pärast läbivaadatud küberturvalisuse määruse vastuvõtmist. Hinnanguliste kulude ja eeldatavate tulude näitamiseks tehti aga arvutused ENISA esitatud hinnanguliste väärtuste põhjal, mis on lisatud küberturvalisuse määruse läbivaatamise ettepaneku mõjuhinnangusse. Katse- ja hindamistegevuse toetamisega seotud kulud on hinnanguliselt järgmised:

täistööajale taandatud töötajad: 4 aastas

tegevuskulud: 800 000 eurot aastas

kogukulu: 6 500 000 eurot (5 aastat); aastas: 1 300 000 eurot.

Eeldatakse, et ENISA puhul tehakse esimesel aastal ühekordsed investeeringud, millele järgnevad halduskulud. Need kulud kaetaks järk-järgult tasudest kogutavast tulust.

Aasta	Tulu
2028	0
2029	260 000
2030	260 000
2031	650 000
2032	650 000
2033	975 000
2034	975 000

4. DIGIMÕÕDE

4.1. Diginõuded

Diginõuete ja sellega seotud kategooriate (andmed, protsesside digiteerimine ja automatiseerimine, digilahendused ja/või digitaalsed avalikud teenused) üldine kirjeldus

Viide nõudele	**Nõude kirjeldus**	**Nõudest mõjutatud või sellega seotud osaleja**	**Üldised protsessid**	**Kategooriad**
Artikli 5 lõike 1 punkt a Liidu õiguse rakendamise toetamine	a) aitab liikmesriikidel järjekindlalt rakendada küberturvalisusega seotud liidu poliitikameetmeid ja õigust, sh **väljastades tehnilisi suuniseid ja aruandeid, andes nõu ja jagades parimaid tavasid ning soodustades parimate tavade vahetamist pädevate asutuste vahel seoses sellega**;	– ENISA – Liikmesriigid	– Andmete töötlemine, et anda välja tehnilisi suuniseid, koostada aruandeid, anda nõu ja jagada parimaid tavasid ning hõlbustada parimate tavade vahetamist pädevate asutuste vahel – Parimate tavade vahetamise hõlbustamine	Andmetöötlus Andmevoog
Artikli 5 lõike 1 punkt b Liidu õiguse rakendamise toetamine	b) toetab **teabe jagamist sektorite piires ja vahel, eelkõige direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorite puhul** ning määruse (EL) 2024/2847 kohaldamisalasse kuuluvate digielemente sisaldavate toodete puhul, **jagades parimaid tavasid ja tagades suuniseid kättesaadavate vahendite ja menetluste kohta**;	– ENISA – Direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorid – Määrusest (EL) 2024/2847 mõjutatud sidusrühmad	Parimate tavade ja suuniste jagamine olemasolevate teabejagamist käsitlevate vahendite ja menetluste kohta	Andmetöötlus Andmevoog

Artikli 5 lõike 1 punkt c Liidu õiguse rakendamise toetamine	c) aitab komisjoni taotluse korral liikmesriike, andes toetust, nt **tehnilisi suuniseid muu hulgas küberriski juhtimise meetmete kohta, vahendeid küberturvalisuse küpsustaseme hindamiseks ning küberintsidentidele reageerimise käsiraamatuid**, mis on kohandatud direktiivi (EL) 2022/2555 I ja II lisas loetletud sektoritele, et edendada küberturvalisuse küpsustaseme parandamist ning küberturvalisuse valdkonnas liidu õiguse järgimist;	– Euroopa Komisjon – ENISA – Direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorid	Tehniliste suuniste jagamine	Andmetöötlus Andmevoog
Artikli 5 lõike 1 punkt e	e) aitab liikmesriikidel ja asjaomastel liidu üksustel **välja töötada ja edendada küberturvalisuse alaseid poliitikameetmeid**, mis on seotud interneti avaliku tuuma üldise kättesaadavuse ja terviklikkuse säilitamisega;	ENISA Liikmesriigid ELi üksused	Abi küberturvalisuse poliitika väljatöötamisel ja edendamisel	Andmetöötlus Andmevoog
Artikli 5 lõike 1 punkt f Liidu õiguse rakendamise toetamine	f) annab kooskõlas määrusega (EL) 2024/2847 **tehnilisi nõuandeid ja toetust** kõnealuse määruse rakendamise ja täitmise tagamisega seotud küsimustes	– ENISA – Määrusest (EL) 2024/2847 mõjutatud sidusrühmad	Tehnilise nõu ja toe pakkumiseks on vaja töödelda ja jagada teavet regulatiivsete nõuete, rakendusprobleemide ja nõuetele vastavuse suuniste kohta.	Andmetöötlus Andmevoog
Artikli 5 lõike 1 punkt h	h) annab Euroopa Andmekaitsenõukogu taotlusel nõuandeid liidu poliitikameetmete ja õiguse konkreetsete küberturvalisuse aspektide rakendamise kohta andmekaitse ja privaatsuse valdkonnas.	ENISA EAKN	Taotluse korral nõustamine	Andmetöötlus Andmevoog

Artikli 5 lõige 2 Panus liidu tasandi küberohtude hindamisse	ENISA panustab koordineeritud liidu tasandi küberriski hindamistesse, sh kui neid viiakse ellu kooskõlas direktiivi (EL) 2022/2555 artikliga 22.	ENISA Liikmesriigid Üldsus	Panustamine koordineeritud riskihindamisse, mis nõuab andmetöötlust ja andmevoogu	Andmetöötlus Andmevoog
Artikli 5 lõige 3 ENISA annab välja suunised.	ENISA **väljastab suunised** teabe jagamiseks kasutatavate võrgu- ja infosüsteemide koostalitlusvõime kohta, sh määruse (EL) 2025/38 artikli 6 lõikes 3 osutatud piiriüleste küberkeskustega.	ENISA Liikmesriigid	ENISA annab välja suunised.	Andmetöötlus Andmevoog
Artikli 5 lõige 5 Toetus komisjonile	ENISA pakub **komisjoni taotlusel eksperditeadmisi, tehnilist nõu, teavet ja analüüsitulemusi või teeb ettevalmistavat tööd** konkreetsetes küberturvalisuse küsimustes, et komisjon saaks neist lähtuda poliitikakujundamisel ja liidu õigusaktide rakendamise järelevalves.	Euroopa Komisjon ENISA	Teabe ettevalmistamine ja komisjonile saatmine	Andmetöötlus Andmevoog

Artikkel 6 Suutlikkuse suurendamine	ENISA abistab, pakkudes teadmisi ja oskusteavet, parimaid tavasid jne.	ENISA Liikmesriigid ELi üksused Avaliku ja erasektori sidusrühmad Turujärelevalveasutused Euroopa küberturvalisuse sertifitseerimise rühma liikmed ECCC	Teadmiste ja oskusteabe pakkumine	Andmetöötlus Andmevoog
Artikkel 7 Teadlikkuse suurendamine ja talendireserv	ENISA abistab liikmesriike, kui nad suurendavad teadlikkust liidu poliitikameetmetest ja õigusest küberturvalisuse valdkonnas ning edendavad nende märgatavust, **töötades välja rakendatavaid vahendeid ja suuniseid**. ENISA toetab algatusi, mille eesmärk on suurendada Euroopa küberturvalisuse alast talendireservi, eelkõige koordineerides konkursse.	ENISA Liikmesriigid	Toimivate vahendite ja suuniste väljatöötamine	Andmetöötlus
Artikli 8 lõige 1 Turuteadmised ja -analüüsid	ENISA **viib läbi** peamiste turusuundumuste **analüüse** küberturvalisuse turu nõudluse ja pakkumise poolel **ning levitab nende tulemusi**, eelkõige valdkondades, mille puhul on kasutusele võetud või kavas Euroopa küberturvalisuse sertifitseerimise kavad, direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorites ning määrusega (EL) 2024/2847, sh selle määruse III ja IV lisaga hõlmatud tootekategooriate puhul.	ENISA Direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorid Määrusega (EL) 2024/2847 hõlmatud tootekategooriad	Analüüsi tegemine ja levitamine	Andmetöötlus Andmevoog

Artikli 8 lõige 2 Turuteadmised ja -analüüsid	ENISA **viib läbi** tehnoloogiliste küberturvalisuse suundumuste analüüse **ja levitab nende tulemusi**, eelkõige direktiivi (EL) 2022/2555 kohaldamisalasse kuuluvate tegevuste ja üksuste ning määruse (EL) 2024/2847 kohaldamisalasse kuuluvate digielementidega toodete puhul.	ENISA Üldsus, sidusrühmad direktiivi (EL) 2022/2555 ja määruse (EL) 2024/2847 tähenduses	Analüüsi tegemine ja levitamine	Andmetöötlus Andmevoog
Artikli 8 lõige 3 Turualased teadmised ja ökosüsteemide toetamine	ENISA kogub teadmisi ning **levitab tehnilisi nõuandeid ja analüüse** tehnika tasemel küberturvalisuse vahendite, raamistike standardite ja parimate tavade kohta.	ENISA Üldsus	**Levitab tehnilisi nõuandeid ja analüüse** tehnika tasemel küberturvalisuse vahendite, raamistike standardite ja parimate tavade kohta.	Andmetöötlus Andmevoog
Artikkel 9 Rahvusvaheline koostöö	ENISA annab oma panuse, analüüsides rahvusvaheliste õppuste tulemusi ja andes nende kohta aru haldusnõukogule, hõlbustades parimate tavade vahetamist ning andes komisjonile eksperditeadmisi ja nõu.	Rahvusvaheline publik ENISA ENISA haldusnõukogu Euroopa Komisjon	Analüüsimine ja aruandlus; nõustamine jne.	Andmetöötlus Andmevoog
Artikli 10 lõiked 2 ja 3 Operatiivkoostöö	2. ENISA on direktiivi (EL) 2022/2555 artikli 15 lõike 1 kohaselt loodud riiklike CSIRTide võrgustiku liige ning **tagab** CSIRTide võrgustiku **sekretariaaditeenused** kooskõlas direktiivi (EL) 2022/2555 artikli 15	ENISA CSIRTid (direktiivi (EL) 2022/2555 artikli 15 lõige 1) EU-CyCLONe (direktiivi	Teabevahetuse hõlbustamine, täites võrgustike sekretariaadi ülesandeid	Andmevoog Digilahendus Digitaalne avalik teenus

	lõikega 2. 3. ENISA **tagab** Euroopa küberkriisiga tegelevate kontaktasutuste võrgustiku (edaspidi „EU-CyCLONe“) **sekretariaaditeenused** kooskõlas direktiivi (EL) 2022/2555 artikli 16 lõike 2 teise lõiguga.	(EL) 2022/2555 artikli 16 lõige 2)		
Artikli 11 lõike 1 punkt b Olukorrateadlikkus Artikkel 12 Varajased hoiatused	**varajased hoiatusteated** vastavalt artiklile 12	Euroopa Komisjon ENISA Europol EU-CyCLONe CSIRTide võrgustik CERT-EU Direktiivi (EL) 2022/2555 I ja II lisas loetletud üksused	Varajaste hoiatuste väljastamine	Andmetöötlus Andmevoog Digitaalne avalik teenus
Artikli 10 lõike 4 punkt b Operatiivkoostöö	b) ühe või mitme liikmesriigi taotluse korral **nõuannete andmist konkreetse võimaliku või toimuva intsidendi või võimaliku või avalduva küberohu kohta ning nende hindamist**, sh pakkudes oskusteadmisi ja **edendades kõnealuste intsidentide tehnilist käsitlemist**, ning **toetades asjakohase teabe ja tehniliste lahenduste vabatahtlikku jagamist liikmesriikide vahel**;	ENISA Liikmesriigid	Anda nõu ja hinnanguid seoses konkreetse võimaliku või käimasoleva intsidendi või küberohuga; Selliste intsidentide tehnilise käsitlemise hõlbustamine; Asjakohase teabe ja tehniliste lahenduste vabatahtliku jagamise toetamine liikmesriikide vahel	Andmetöötlus Andmevoog Digitaalsed avalikud teenused

Artikli 10 lõike 4 punkt c Operatiivkoostöö	c) nõrkuste, ohtude ja intsidentide analüüsimist;	ENISA Liikmesriigid	Andmete kogumine avalikest allikatest ja andmevahetus liikmesriikidega	Andmetöötlus Andmevoog
Artikli 10 lõike 4 punkt d Operatiivkoostöö	d) **ühe või mitme liikmesriigi taotluse korral** direktiivi (EL) 2022/2555 tähenduses oluliste intsidentide tehnilise järeluurimise **toetamist**;	ENISA Liikmesriigid	Intsidentidega seotud tehnilistele järelepärimistele reageerimise analüüs ja tugi	Andmetöötlus Andmevoog
Artikli 10 lõike 4 punkt e Operatiivkoostöö	e) ulatuslike küberintsidentide ja kriiside koordineeritud haldamise toetamist operatiivtasandil, eelkõige **aidates EU-CyCLONe-t poliitilise tasandi jaoks aruannete koostamisel ning edendades õigeaegset teabe jagamist CSIRTide võrgustiku ja EU-CyCLONe vahel**.	ENISA EU-CyCLONe CSIRTide võrgustik	Andmete analüüsimine, et toetada aruannete koostamist; võrkudevahelise õigeaegse teabevahetuse hõlbustamine	Andmetöötlus Andmevoog Digitaalne avalik teenus
Artikli 10 lõige 5 Operatiivkoostöö	ENISA toetab **liikmesriigi** või liidu üksuse **taotlusel** koostöös CERT-EUga järjepidevat avalikku suhtlust intsidendi või küberohu asjus.	ENISA Liikmesriigid	Taotluse vastuvõtmine ja vajaduse korral suhtlemine	Andmevoog

Artikli 10 lõige 6 Operatiivkoostöö	ENISA **toetab** liikmesriikide ja CERT-EU kaudu liidu üksuste koostööd **turvaliste sidevahendite kasutuselevõtu valdkonnas**. ENISA kasutab CSIRTide võrgustiku ja EU-CyCLONe turvalisi sidevahendeid, mida pakuvad juriidilised isikud, mis ei ole asutatud kolmandates riikides või ei ole kolmandate riikide või nende kodanike kontrolli all.	ENISA Euroopa Komisjon Liikmesriigid ELi üksused CSIRTide võrgustik EU-CyCLONe	Toetada turvaliste sidevahendite kasutuselevõttu ja kasutada selliseid vahendeid CSIRTide võrgustikus ja EU-CyCLONe-s.	Digilahendus Digitaalne avalik teenus
Artikli 11 lõike 1 punkt a Küberturvalisuse alane ühine olukorrateadlikkus	a) **töötab** koostöös EU-CyCLONe, CSIRTide võrgustiku, komisjoni, CERT-EU, Europoli ja muude asjaomaste liidu üksustega **välja** kontrollitud ja usaldusväärse küberohuteadmuse **hoidlad**, mis sisaldavad teavet intsidentide suundumuste, taktika, meetodite ja menetluste kohta;	Euroopa Komisjon ENISA EU-CyCLONe CSIRTide võrgustik Europol ELi üksused CERT-EU	Hoidlaid välja töötama	Digitaalne voog Digilahendus Digitaalne avalik teenus
Artikli 11 lõike 1 punktid c–g Küberturvalisuse alane ühine olukorrateadlikkus	esitab aegsasti sihtotstarbelised analüüsid (mõned taotluse korral); pakub analüüse ja tehnilist nõu; koostab koostöös teiste üksustega tehnilise olukorra aruande; suundumuste jälgimine ja jagamine	ENISA Liikmesriigid Euroopa Komisjon ELi üksused EU-CyCLONe CSIRTide võrgustik	Andmete analüüs, teabe jagamine ja aruannete esitamine (mõned taotluse korral)	Andmetöötlus Andmevoog

Artikli 11 lõike 2 punkt a Küberturvalisuse alane ühine olukorrateadlikkus	ENISA **teeb** küberohtude, intsidentide, suundumuste, kujunemisjärgus tehnoloogia ja nende mõju **analüüse**, sh korrapäraseid **analüüse** direktiivi (EL) 2022/2555 I ja II lisas loetletud sektorite ning määrusega (EL) 2024/2847 hõlmatud asjaomaste tootekategooriate kohta;	ENISA Üldsus	Analüüsida andmeid, et anda küberturvalisust mõjutavat teavet; korrapärane aruandlus	Andmetöötlus Andmevoog
Artikli 11 lõike 2 punkt b Küberturvalisuse alane ühine olukorrateadlikkus	ENISA **väljastab koostöös komisjoni ja vajaduse korral CSIRTide võrgustikuga nõuanded, suunised ja parimad tavad** võrgu- ja infosüsteemide turvalisuse kohta, eelkõige direktiivi (EL) 2022/2555 I ja II lisas loetletud sektoreid toetava taristu turvalisuse kohta;	Euroopa Komisjon CERT-EU CSIRTide võrgustik Üldsus	Nõuannete, suuniste ja parimate tavade väljaandmine	Andmetöötlus Andmevoog
Artikli 11 lõike 2 punkt c Küberturvalisuse alane ühine olukorrateadlikkus	ENISA koostab **pikaajalisi strateegilisi analüüse küberohtude** ja intsidentide kohta, et **teha kindlaks** uued suundumused ja aidata ennetada intsidente.	ENISA Üldsus	Andmete analüüs ja tekkivate ohtude kindlakstegemine	Andmetöötlus
Artikli 11 lõige 3 Küberturvalisuse alane ühine olukorrateadlikkus	ENISA võib **avalikustada** lõikes 2 osutatud **analüüse**, nõuandeid, suuniseid, parimaid tavasid ja aruandeid kokkuleppel nendesse panustanud üksustega, millele on osutatud lõikes 2.	ENISA Üldsus	Teabe avalikustamine	Andmevoog Digitaalne avalik teenus

Artikli 13 lõige 2 Tugi intsidentidele reageerimisel	2. ENISA **vaatab** komisjoni või EU-CyCLONe taotlusel, CSIRTide võrgustiku toetusel ja asjaomaste liikmesriikide heakskiidul **läbi olulised küberintsidendid** või ulatuslikud küberintsidendid ning hindab neid kooskõlas määruse (EL) 2025/38 artikliga 21.	Euroopa Komisjon ENISA EU-CyCLONe CSIRTide võrgustik Liikmesriigid	Oluliste küberintsidentide läbivaatamine ja hindamine	Andmetöötlus
Artikli 14 lõige 2 Küberturvalisuse õppused liidu tasandil	2. ENISA **haldab** lõikes 1 osutatud õppustest omandatud kogemuste **andmehoidlat** ning annab liikmesriikidele ja vajaduse korral liidu üksustele soovitusi saadud õppetundide tulemusliku ja tõhusa rakendamise kohta.	ENISA Liikmesriigid ELi üksused	Hoidla haldamine	Andmetöötlus Digilahendus Digitaalne avalik teenus
Artikkel 14 Küberturvalisuse õppused liidu tasandil	Olles saanud EU-CyCLONe, komisjoni, liikmesriikide või CERT-EU taotluse, korraldab ENISA küberturvalisuse õppusi või aitab kaasa nende korraldamisele. ENISA toetab komisjoni liidu tasandi küberturvalisuse õppuste iga-aastase jooksva programmi koostamisel.	ENISA Komisjon Liikmesriigid ELi üksused CERT-EU	Õppuste korraldamise või toetamise taotluste vastuvõtmine	Andmevoog Andmetöötlus

Artikkel 15 Töövahendeid ja platvorme käsitlev säte	1. **ENISA loob ja tagab operatiivsed tehnilised vahendid, sh** liidu tasandil küberturvalisusega seotud **platvormid**, eelkõige määruse (EL) 2024/2847 artikli 16 lõike 1 kohaselt loodud ühtse intsidentidest teatamise platvormi [ja direktiivi (EL) 2022/2555 artikli 23a kohaselt loodud ühtse kontaktpunkti] ning testimisvahendid, et toetada vastavushindamismenetluste rakendamist kooskõlas asjakohaste liidu õigusaktidega, **käitab neid, hoiab neid kasutuses ja ajakohastab neid vajaduse korral**. 2. Kui see on lõike 1 otstarbel asjakohane, siis **teeb ENISA koostööd ja vahetab teavet** CSIRTide võrgustikuga ning, kui see on kohaldatav, turujärelevalveasutustega.	ENISA CSIRTide võrgustik Üldsus Turujärelevalveasutused	ENISA võtab kasutusele, pakub, käitab, hooldab ja vajaduse korral ajakohastab operatiivseid tehnilisi vahendeid, näiteks platvorme.	Digilahendus Digitaalne avalik teenus Andmevoog
Artikli 16 lõige 2 Nõrkusehalduse teenused	a) pidades direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasi; b) pakkudes **sidusrühmadele** nõrkusehalduse teenuseid, tuginedes Euroopa nõrkuste andmebaasile ja kasutades ENISA-le kättesaadavat asjakohast teavet; c) kui see on asjakohane, siis tehes struktureeritud koostööd Euroopa nõrkuste andmebaasile sarnaseid programme, registreid või andmebaase pakkuvate **organisatsioonidega**; d) toetades aktiivselt **CSIRTe**, mis on määratud koordineerijateks kooskõlas direktiivi (EL) 2022/2555 artikli 12 lõikega 1, selliste nõrkuste koordineeritud avalikustamise haldamisel, millel võib olla märkimisväärne mõju rohkem kui ühe liikmesriigi üksustele;	ENISA Riiklikud CSIRTid CSIRTide võrgustik Riikide pädevad asutused Valdkond Teadusringkonnad Üldsus Programme, registreid või andmebaase pakkuvad rahvusvahelised osalejad	Nõrkusehalduse teenuste osutamine; alustada vajaduse korral struktureeritud koostööd; koostöö sidusrühmadega	Digilahendus Digitaalne avalik teenus Andmevoog

	e) töötades välja ja hoides kasutuses metoodikaid ning juhtimismehhanisme nõrkuste kindlaksmääramiseks ja koordineeritud avalikustamiseks **koostöös riiklike pädevate asutuste, CSIRTide, tööstuse ja teaduskogukonnaga**.			
Artikkel 17 Küberturvalisuse sertifitseerimine Artikkel 18 Standardimine, tehnilised kirjeldused ja suunised	Artikli 17 lõige 1 a) **Euroopa küberturvalisuse sertifitseerimise ettevalmistavate kavade (edaspidi „ettevalmistavad kavad“)** koostamine IKT-toodetele, -teenustele, -protsessidele, hallatud turbeteenustele ja üksuste turvaolekule ning, tehniliste kirjelduste koostamine kooskõlas artikliga 74; b) **vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade haldamine** kooskõlas artikliga 75, sh võttes arvesse vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade võimalikku läbivaatamist kooskõlas artikliga 76; c) vastuvõetud kavade kasutuselevõtu edendamine ning sihtotstarbelise veebisaidi haldamine, millel esitatakse teavet Euroopa küberturvalisuse sertifitseerimise kavade, Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide kohta kooskõlas artikliga 79 ning tutvustatakse neid; Artikli 17 lõige 2 e) näidissätete **koostamine**, millele osutatakse IKT-toodete, -teenuste, -protsesside, hallatud	ENISA Üldsus	Andmete analüüsimine ning andmevoogude vahetamine komisjoni ja muude sidusrühmadega; ettevalmistava sertifitseerimiskava koostamine; ENISA veebisaidi haldamine	Andmetöötlus Andmevood Digitaalne avalik teenus

	turbeteenuste ja üksuste turvaoleku Euroopa küberturvalisuse sertifitseerimise kavades („ettevalmistavad kavad“) kooskõlas artikli 81 lõikega 5. Artikkel 18 1. ENISA koostab tehnilised kirjeldused ja suunised, et toetada liidu õigusaktide rakendamist küberturvalisuse valdkonnas. 2. ENISA teeb liidu tasandil ning kooskõlas artikliga 9 rahvusvahelisel tasandil **standardite koostamise tegevuse järelevalvet ning osaleb selles ja juhib seda**. 3. ENISA toetab krüptoalgoritmide väljatöötamist ja hindamist. Kui krüptoalgoritm on saanud positiivse hinnangu, teeb ENISA kooskõlas määrusega (EL) nr 1025/2012 koostööd Euroopa standardiorganisatsioonidega, et toetada selle standardimist. 4. ENISA **pakub** komisjonile ja Euroopa küberturvalisuse sertifitseerimise rühmale **tehnilisi eksperditeadmisi** asjakohaste standardite või tehniliste kirjelduste kohta, et toetada küberturvalisusega seotud liidu poliitikat, eelkõige määrust (EL) 2024/2847, sh küberturvalisuse valdkonna liidu ühtlustamisõigusaktide ja Euroopa küberturvalisuse sertifitseerimise kavade jaoks vastavalt artikli 81 lõike 1 punktile d. 5. ENISA abistab komisjoni harmoneeritud standardite projektide hindamisel, et toetada liidu ühtlustamisõigusaktide rakendamist küberturvalisuse valdkonnas.			

Artikkel 19 – Euroopa küberturbeoskuste raamistik	ENISA **töötab välja ja teeb üldsusele kättesaadavaks Euroopa küberturbeoskuste raamistiku**. ENISA **konsulteerib komisjoniga** enne Euroopa küberturbeoskuste raamistiku üldsusele kättesaadavaks tegemist või ajakohastamist kooskõlas lõikega 4. Euroopa küberturbeoskuste raamistiku kasutamine on **avaliku ja erasektori üksustele vabatahtlik**. ENISA võib **konsulteerida** Euroopa küberturbeoskuste raamistiku väljatöötamise ja kasutuselevõtu asjus **sidusrühmadega**.	ENISA Komisjon Üldsus Liikmesriigid ELi üksused Avaliku ja erasektori sidusrühmad	Euroopa küberturbeoskuste raamistiku haldamine; konsulteerimine sidusrühmadega; Euroopa küberturbeoskuste raamistiku kasutuselevõtmine	Andmetöötlus Andmevoog Digilahendus
Artiklid 20–23 – Euroopa individuaalsete küberturbeoskuste tõendamise kavad	ENISA **töötab välja, võtab vastu ja haldab Euroopa individuaalsete küberturbeoskuste tõendamise kavasid**. Euroopa individuaalsete küberturbeoskuste tõendamise kavade kasutamine on **riiklikele avaliku sektori asutustele ja erasektori üksustele vabatahtlik**, kui liikmesriigi õiguses ei ole määratud teisiti. ENISA **konsulteerib** enne uue Euroopa individuaalsete küberturbeoskuste tõendamise kava algatamist **komisjoniga**. ENISA võtab sellise kava vastu ainult juhul, kui **komisjon on esitanud selle kohta** positiivse **arvamuse**. ENISA võib Euroopa individuaalsete küberturbeoskuste tõendamise kavade koostamisel **konsulteerida asjaomaste sidusrühmadega**. ENISA tagab Euroopa individuaalsete küberturbeoskuste tõendamise kavade koostamise vältel **tiheda koostöö liikmesriikidega**. Volitatud tõendajad **hindavad, kas üksikisikud**	ENISA Komisjon Üldsus Liikmesriigid ELi üksused Avaliku ja erasektori sidusrühmad (aitavad kaasa tõendamissüsteemi väljatöötamisele; taotlejad ja Euroopa individuaalsete küberturbeoskuste tunnistuste pakkujad, sh hindajad)	Kavade väljatöötamine ja haldamine; konsultatsioonid sidusrühmadega; taotluste menetlemine; otsuste tegemine; veebisaidi haldamine	Andmetöötlus Andmevoog Digilahendus Digitaalne avalik teenus

	vastavad Euroopa individuaalsete küberturbeoskuste tõendamise kava **nõuetele** ning, kui need nõuded on täidetud, siis väljastavad Euroopa individuaalsete küberturbeoskuste tõendi. ENISA **annab hindajatele suuniseid ja korraldab nende kohustusliku koolitamise** Euroopa individuaalsete küberturbeoskuste tõendamise kavas sisalduvate nõuete ja hindamismeetodite kohta, nagu on osutatud artikli 20 lõike 3 punktis b. Üksused, kes soovivad saada volitatud tõendajaks või oma volitust uuendada **(edaspidi „taotluse esitajad“) esitavad** ENISA-le **taotluse**. Volitatud tõendajad tagavad, et Euroopa individuaalsete küberturbeoskuste elektrooniline tõend väljastatakse **üksikisiku taotlusel** elektroonilise tõendina sellises vormingus, mille saab salvestada määruses (EL) nr 910/2014 sätestatud Euroopa digiidentiteedikukrusse. Taotluse esitajad ja volitatud tõendajad lubavad **ENISA-l teha hindamisi** esialgse taotlusprotsessi või loa säilitamise või uuendamise raames ning jagavad kogu asjakohast teavet, et tagada lõigetes 3 ja 4 sätestatud nõuete või lõikes 5 sätestatud kohustuste täitmine või jätkuv täitmine kooskõlas artikli 22 lõikega 2. Volitatud tõendajad **teavitavad ENISAt** viivitamata, kui mõni lõikes 3 loetletud nõuetest ei ole enam täidetud või kui tekib kahtlus, et kõnealused nõuded ei ole täidetud, sh hindajate			

	sõltumatuse puhul. Taotluse esitajad **maksavad** oma taotluse läbivaatamise eest **ENISA-le tasu**. Volitatud tõendajad **maksavad** oma volituse säilitamise eest **ENISA-le tasu**. **ENISA hindab**, kas taotluse esitaja või volitatud tõendaja täidab või täidab jätkuvalt artikli 21 lõigetes 3 ja 4 sätestatud nõudeid ning artikli 21 lõikes 5 sätestatud kohustusi. Pärast taotluse läbivaatamist artikli 21 lõigetes 3 ja 4 sätestatud nõuete alusel **võib ENISA teha otsuse**. **ENISA võib selliseid otsuseid muuta,** need peatada või tühistada. **ENISA haldab ja ajakohastab korrapäraselt sihtotstarbelist veebisaiti**, millel on esitatud avalik teave järgmise kohta: a) Euroopa küberturbeoskuste raamistik, sh selle ajakohastamise struktuur ja ajakava; b) Euroopa individuaalsete küberturbeoskuste tõendamise kavad, nende kulg ja nende väljatöötamise ajakava; c) iga käesoleva määruse artikli 47 kohaselt vastu võetud Euroopa individuaalsete			

	küberturbeoskuste tõendamise kavaga seotud tasud; d) Euroopa individuaalsete küberturbeoskuste tõendi hinnanguline maksumus kooskõlas artikli 20 lõikega 4; e) volitatud tõendajate loetelu.			
Artikkel 25 Haldusnõukogu koosseis	ENISA haldusnõukogu **liikmete ametisse nimetamine**.	ENISA Euroopa Komisjon Liikmesriigid	Liikmete ametisse nimetamine	Andmevoog Andmetöötlus
Artikli 28 lõige 1 Haldusnõukogu ülesanded Artikkel 30 Juhatus	b. võtab vastu artiklis 44 osutatud ENISA ühtse programmdokumendi kavandi, enne kui see **esitatakse arvamuse saamiseks komisjonile**; f) hindab ENISA tegevuse konsolideeritud aastaaruannet, sh raamatupidamisarvestus ja kirjeldus, kuidas ENISA on saavutanud oma tulemusnäitajad, ja võtab selle vastu; **esitab nii aastaaruande kui ka selle hindamise** järgmise aasta 1. juuliks Euroopa Parlamendile, nõukogule, komisjonile ja Euroopa Kontrollikojale; teeb aastaaruande üldsusele kättesaadavaks; i) tagab, et sise- või välisauditi aruannetest ja hindamistest ning Euroopa Pettustevastase Ameti (edaspidi „OLAF“) ja Euroopa	ENISA Euroopa Komisjon Euroopa Parlament ELi nõukogu Kontrollikoda Liikmesriigid Üldsus	Ühtse programmdokumendi esitamine komisjonile arvamuse saamiseks; Hindab ENISA tegevuse konsolideeritud aastaaruannet, sh raamatupidamisarvestus ja kirjeldus, kuidas ENISA on saavutanud oma tulemusnäitajad, ja võtab selle vastu, esitab nii aastaaruande kui ka hindamise; Tulemuste järelkontroll	Andmevoog Andmetöötlus

	Prokuratuuri (edaspidi „EPPO“) uurimistest tulenevate **järelduste** ja soovituste **puhul võetakse** piisavaid **järelmeetmeid**;			
Artikli 31 lõige 8 Ametisse nimetamine, ametist vabastamine ja ametiaja pikendamine	**Haldusnõukogu teavitab Euroopa Parlamenti** kavatsusest pikendada tegevdirektori ametiaega kooskõlas lõikega 6. Kolme kuu jooksul enne ametiaja pikendamist esineb tegevdirektor Euroopa Parlamendi pädeva komisjoni kutsel selle ees ja vastab parlamendiliikmete küsimustele.	ENISA ENISA haldusnõukogu Euroopa Parlament	Haldusnõukogu teavitab Euroopa Parlamenti.	Andmevoog
Artikli 32 lõige 3 Tegevdirektori ülesanded ja kohustused Artikli 32 lõige 5	3. **Tegevdirektor annab Euroopa Parlamendile** oma ülesannete täitmisest **aru**, kui temalt seda palutakse. Nõukogu võib tegevdirektorilt tema ülesannete täitmise kohta aru pärida. Eelarvekavade strateegiate ja strateegiliste dokumentide ettevalmistamine.	ENISA tegevdirektor Euroopa Parlament	Tulemuslikkust käsitlev aruandlus	Andmevoog Andmetöötlus
Artikli 35 lõiked 5 ja 6 ENISA nõuanderühm	5. ENISA nõuanderühm **nõustab ENISAt** tema ülesannete täitmisel, välja arvatud seoses käesoleva määruse III, IV ja V jaotise kohaldamisega. Eelkõige annab ENISA nõuanderühm tegevdirektorile nõu ENISA iga-aastase tööprogrammi ettepaneku koostamise kohta ning teabevahetuse tagamise kohta asjaomaste sidusrühmadega iga-aastase tööprogrammiga seotud küsimustes. 6. ENISA nõuanderühm **teavitab** korrapäraselt **haldusnõukogu** oma tegevusest.	ENISA ENISA nõuanderühma liikmed ENISA haldusnõukogu ENISA tegevdirektor	Nõustab ja teavitab oma tegevusest	Andmetöötlus Andmevoog

Artiklid 36–43 Apellatsiooninõukogu	ENISA **asutab** haldusnõukogu otsusega **apellatsiooninõukogu**. Apellatsiooninõukogu koosneb esimehest ja kolmest liikmest. Igal apellatsiooninõukogu liikmel on asendusliige. Asendusliige esindab täisliiget tema puudumise korral. Haldusnõukogu **nimetab esimehe, ülejäänud liikmed ja nende asendusliikmed komisjoni esitatud kvalifitseeritud kandidaatide nimekirjast**. Kvalifitseeritud kandidaatide nimekiri kehtib neli aastat. Haldusnõukogu võib komisjoni ettepaneku alusel pikendada nimekirja kehtivust täiendavate nelja-aastaste ajavahemike kaupa. Kui apellatsiooninõukogu peab menetletava kaebuse puhul seda vajalikuks, võib ta **haldusnõukogu** taotluse korral **nimetada** asjaomase juhtumi menetlemiseks lõikes 3 osutatud nimekirjast **veel kaks liiget ja nende asendusliikmed**. Apellatsiooninõukogu võtab vastu ja **avalikustab oma kodukorra**. Kui apellatsiooninõukogu liige leiab ühel lõikes 1 loetletud põhjusel või mis tahes muul põhjusel, et ta ei peaks osalema kaebuse menetlemises, **teatab ta sellest apellatsiooninõukogule**. Apellatsiooninõukogu **teeb otsuse** lõigetes 2 ja 3 loetletud juhtudel võetavate **meetmete kohta** ilma asjaomase liikme osavõtuta. Asjaomane liige asendatakse selle otsuse tegemiseks apellatsiooninõukogus tema asendajaga. Lõike 1 kohaselt esitatud kaebus kuulub kooskõlas artikliga 41 esialgsele	ENISA ENISA haldusnõukogu Komisjon Apellatsiooninõukogu KTM2 ettepaneku artikli 36 tähenduses Taotlejad (juriidilised isikud, kes soovivad saada volitatud tõendamisteenuse osutajaks, säilitada või uuendada oma tegevusluba)	Apellatsioonidel põhinevate otsuste tegemine Apellatsioonkaebuste menetlemine Töökorra ettevalmistamine ja avaldamine Teabevood	Andmetöötlus Andmevoog Digitaalne avalik teenus

	läbivaatamisele, enne kui see esitatakse apellatsiooninõukogule läbivaatamiseks. Taotluse esitajad artikli 21 lõike 3 tähenduses **võivad esitada kaebuse** järgmise kohta: artikli 22 lõike 3 kohaselt neile adresseeritud **ENISA otsus**; ENISA suutmatus tegutseda ENISA-le esitatud nende taotluse suhtes artikli 22 lõikes 4 sätestatud kohaldatava tähtaja jooksul. Lõike 1 punktis a osutatud juhul esitatakse kaebus koos selle põhjendustega **kirjalikult** kooskõlas artikli 36 lõikes 5 osutatud kodukorraga kahe kuu jooksul alates otsuses asjaomasele taotluse esitajale teatavaks tegemisest või selle puudumise korral päevast, kui taotluse esitaja sai otsusest teada. Lõike 1 punktis b osutatud juhul esitatakse **kaebus ENISA-le kirjalikult** kooskõlas artikli 36 lõikes 5 osutatud kodukorraga kahe kuu jooksul alates artikli 22 lõikes 4 sätestatud tähtaja möödumise kuupäevast. Kui ENISA leiab, et kaebus on vastuvõetav ja põhjendatud, **parandab ta artikli 40 lõikes 1 viidatud otsust või tegevusetust**. Kui ENISA ei paranda otsust ühe kuu jooksul alates kaebuse laekumisest, **otsustab** ta viivitamata, **kas peatada otsuse kohaldamine, ning edastab kaebuse edasiseks lahendamiseks apellatsiooninõukogule**. **Apellatsiooninõukogu otsustab** kolme kuu jooksul pärast kaebuse esitamist, kas rahuldada kaebus või lükata see tagasi. Kaebuse läbivaatamisel tegutseb apellatsiooninõukogu selle kodukorras sätestatud tähtaegade piires. Ta			

	kutsub nii sageli kui vajalik **kaebemenetluse osalisi esitama kindlaksmääratud aja jooksul märkusi enda saadetud teadete või teiste kaebemenetluse osaliste avalduste kohta**. Apellatsioonimenetluse osalistel on õigus anda **suulisi seletusi**. Kui apellatsiooninõukogu leiab, et kaebus on põhjendatud, **saadab ta juhtumi tagasi ENISA-le**. ENISA **teeb** kooskõlas apellatsiooninõukogu järeldustega **oma lõpliku otsuse ja põhjendab seda**. ENISA **teavitab** asjakohaselt kaebemenetluse **osalisi**. Artikli 22 lõike 3 kohaselt vastu võetud ENISA otsuste tühistamist või artikli 22 lõike 4 kohaselt kohaldatavate tähtaegade jooksul tegevuse puudumist käsitlevad hagid **võib esitada Euroopa Liidu Kohtusse** pärast artiklites 39–42 sätestatud ENISA apellatsioonimenetluse lõppu või kui artikli 41 lõike 2 kohaselt ei ole tegutsetud kohaldatava tähtaja piires. ENISA **võtab kõik vajalikud meetmed** Euroopa Liidu Kohtu otsuse **täitmiseks**.			
Artikkel 44 Ühtne programmdokument	2. Tegevdirektor koostab igal aastal lõikes 1 osutatud ühtse programmdokumendi kavandi ning sellele vastava finants- ja inimressursside kavandamise kooskõlas komisjoni delegeeritud määruse (EL) nr 2019/715 artikliga 32, võttes arvesse komisjoni kehtestatud suuniseid. 3. Haldusnõukogu võtab lõikes 1 osutatud ühtse programmdokumendi vastu iga aasta 30. novembriks, võttes arvesse delegeeritud määruse (EL) 2019/715 artikli 32 lõikes 7 osutatud komisjoni arvamust. Kui	ENISA tegevdirektor ENISA haldusnõukogu Euroopa Komisjon Euroopa Parlament Nõukogu	Igal aastal ühtse programmdokumendi koostamine, vastuvõtmine ja edastamine	Andmevoog

	haldusnõukogu otsustab komisjoni arvamuse mis tahes aspekti mitte arvesse võtta, peab ta seda otsust põhjalikult põhjendama. Haldusnõukogu saadab ühtse programmdokumendi Euroopa Parlamendile, nõukogule ja komisjonile hiljemalt järgmise aasta 31. jaanuariks ja edastab neile ka kõik selle hilisemad ajakohastatud versioonid.			
Artikkel 45 ENISA eelarve koostamine	4. **Komisjon edastab eelarvestuse projekti eelarvepädevatele institutsioonidele** koos liidu üldeelarve projektiga. Eelarvestuse projekt tehakse kättesaadavaks ka ENISA-le.	ENISA Euroopa Komisjon	Teabe jagamine	Andmevoog
Artikkel 47 Tasud	Artikli 22 lõikes 1 osutatud iga Euroopa individuaalsete oskuste tõendamise kava tegevuse puhul **nõutakse** artikli 21 lõike 3 tähenduses taotluse esitajatelt või volitatud tõendajatelt **järgmisi tasusid**, et katta ENISA tehtud toimingute täielikud kulud: a. lubade andmine pärast artikli 21 lõigetes 3 ja 4 sätestatud nõuete läbivaatamist, sh hindamine; b. lubade iga-aastane säilitamine; c. Euroopa individuaalsete küberturbeoskuste tõendajate volituste uuendamine, sh hindamine. Sertifitseerimise puhul **nõutakse vastavushindamisasutustelt** Euroopa küberturvalisuse sertifikaatide väljastamise aluseks olevate Euroopa küberturvalisuse sertifitseerimise kavade haldamise eest **järgmisi**	Komisjon ENISA Tõendamisteenuse osutajad Vastavushindamisasutused	Teabe töötlemine; tasude maksmine; aruandlus tasude kohta	Andmetöötlus Andmevoog

	tasusid: Euroopa küberturvalisuse sertifitseerimise kavas osalemise iga-aastane tasu; tasu Euroopa küberturvalisuse sertifitseerimise kavade alusel Euroopa küberturvalisuse sertifikaatide väljastamise eest. Punktis b osutatud tasusid nõutakse, kui vastavushindamisasutus esitab Euroopa küberturvalisuse sertifikaadid ENISA-le tema veebisaidil avaldamiseks kooskõlas artikliga 79. **Komisjon võtab** vastu rakendusaktid, millega kehtestatakse üksikasjalikud eeskirjad ENISA kogutavate tasude kohta. ENISA esitab **aruande nõutavate tasude ja neist ENISA eelarvele tekkiva mõju kohta** osana raamatupidamisarvestuse esitamise menetlusest.			
Artikkel 48 Artikkel 49 Mõju eelarvele	Artikkel 48 3. Tegevdirektor **saadab eelarvepädevatele institutsioonidele** igal aastal **kogu** asjaomase **teabe** kõigi hindamismenetluste tulemuste kohta. Artikkel 49 1. ENISA peaarvepidaja **saadab eelarveaasta** (aasta N) **esialgse raamatupidamise aastaaruande** komisjoni peaarvepidajale ja kontrollikojale järgmise eelarveaasta (aasta N + 1) 1. märtsiks. 2. ENISA peaarvepidaja esitab **konsolideerimise otstarbel vajaliku raamatupidamisteabe** aasta N + 1 1. märtsiks nõutaval viisil ja nõutavas vormingus **komisjoni peaarvepidajale**. 3. **ENISA saadab aasta N**	ENISA ENISA haldusnõukogu Euroopa Komisjon Nõukogu Euroopa Parlament	ENISA eelarvet käsitleva teabe töötlemine ja jagamine.	Andmetöötlus Andmevoog

	eelarvehalduse ja finantsjuhtimise aruande Euroopa Parlamendile, nõukogule ja kontrollikojale 31. märtsiks aastal N + 1. 4. **Kui on laekunud kontrollikoja märkused aasta N ENISA esialgsete raamatupidamise aastaaruannete kohta**, siis koostab ENISA peaarvepidaja ENISA lõpliku raamatupidamise aastaaruande. 5. **Haldusnõukogu esitab** ENISA lõpliku raamatupidamise aasta N aruande kohta **arvamuse**. **Ameti peaarvepidaja koostab ENISA lõpliku raamatupidamisaruande omal vastutusel. Tegevdirektor esitab selle haldusnõukogule arvamuse saamiseks.**			
Artikkel 52 Huvide deklaratsioon	Lepinguosalised **esitavad kohustuste deklaratsiooni ja deklaratsiooni** selle kohta, et neil puudub või on olemas otsene või kaudne huvi, mida võib pidada nende sõltumatust kahjustavaks.	ENISA juhtkond (tegevdirektor, tegevdirektori asetäitja); Haldusnõukogu, Riikide lähetatud eksperdid	Huvide deklaratsiooni andmete töötlemine ja jagamine	Andmetöötlus Andmevoog
Artikkel 58 Kontaktametnikud	1. **Iga liikmesriik määrab vähemalt kaks kontaktametnikku** [oma riiklikust küberturvalisuse asutusest] liikmesriigi ENISAsse lähetatud ekspertidena, kes töötavad selle tegevuskohas või kohalikus büroos kooskõlas artikli 59 lõikega 2. Komisjon võib samuti määrata kontaktametniku.	ENISA Liikmesriigid	Kontaktametnike määramine ja teabe jagamine	Andmetöötlus Andmevoog

	2. Nende liikmesriigi määratud kontaktametnikel on õigus **küsida ja saada oma liikmesriigist käesoleva** määrusega ette nähtud **kogu asjakohast teavet** täielikus kooskõlas oma liikmesriigi õiguse või tavadega, eelkõige andmekaitse ja konfidentsiaalsuse puhul.			
Artikkel 67 Salastatud teabe käitlemine	Pärast **komisjoniga konsulteerimist** võtab ENISA vastu julgeolekunormid, mille abil kohaldatakse julgeolekupõhimõtteid, mis sisalduvad komisjoni julgeolekunormides, mis käsitlevad salastamata tundliku teabe ja ELi salastatud teabe kaitset, nagu on sätestatud otsustes (EL, Euratom) 2015/443 ja 2015/444. ENISA julgeolekunormid hõlmavad kõnealuse **teabe vahetust, töötlemist ja säilitamist käsitlevaid sätteid**.	ENISA Haldusnõukogu Komisjon	Salastatud teavet käitlema	Andmetöötlus Andmevoog
Artiklid 68, 69 ja 70 Koostöö liidu üksuste ja riikide ametiasutustega Koostöö sidusrühmadega Koostöö kolmandate riikidega	ENISA teeb küberturvalisuse küsimustes koostööd ja vahetab teavet asjaomaste liidu üksuste, turujärelevalve- ja järelevalveasutustega; asjaomaste sidusrühmade; kolmandate riikide pädevate asutuste või rahvusvaheliste organisatsioonidega	ENISA Europol ECCC Euroopa Andmekaitsenõukogu Üldsus Nõukogu	Teabe jagamine	Andmevoog

Artikkel 72 – Üldsuse teavitamine ja konsulteerimine Euroopa küberturvalisuse sertifitseerimise kavade teemal	2. Komisjon haldab ja ajakohastab korrapäraselt sihtotstarbelist veebisaiti, millel esitatakse teavet järgmiste aspektide kohta: a) Euroopa küberturvalisuse sertifitseerimise kavad, mille loomise taotlus on esitatud; b) strateegilised prioriteedid IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ning liidu õigusaktides sätestatud turvanõuete ühtlustamiseks, sh võimalikud valdkonnad, mille tarbeks võidakse taotleda Euroopa küberturvalisuse sertifitseerimise kava. 3. Komisjon teeb käesoleva artikli lõikes 2 osutatud veebisaidil üldsusele kättesaadavaks teabe taotluse kohta, mille ta on esitanud ENISA-le artiklis 73 osutatud ettevalmistava kava koostamiseks, ja oma otsuse kohta kiita ENISA edastatud ettevalmistav kava heaks, lükata see tagasi või lõpetada selle kohaldamine kooskõlas artikli 74 lõikega 7.	Euroopa Komisjon Üldsus ENISA	Teabeveebisaidi haldamine Sellega volitatakse komisjoni esitama teavet avalikult kättesaadaval veebisaidil ja tegelema pidevalt sellega seotud andmehaldusega.	Digitaalne avalik teenus Digilahendus
Artikkel 72 – Üldsuse teavitamine ja konsulteerimine Euroopa küberturvalisuse sertifitseerimise kavade teemal	Selle aja jooksul, mil ENISA koostab artikli 74 kohast ettevalmistavat kava, **võivad Euroopa Parlament ja nõukogu taotleda komisjonilt** kui Euroopa küberturvalisuse sertifitseerimise rühma juhatajalt ja ENISA-lt asjakohase teabe esitamist ettevalmistava kava projekti kohta. **ENISA võib Euroopa Parlamendi või nõukogu taotlusel ja kokkuleppel komisjoniga** ning ilma et see piiraks artikli 54 kohaldamist, **teha Euroopa Parlamendile ja nõukogule kättesaadavaks ettevalmistava kava projekti asjakohased osad** nõutava konfidentsiaalsusega kooskõlas oleval ja asjakohasel juhul piiratud viisil.	ENISA ELi nõukogu Euroopa Parlament	ENISA koostatud ettevalmistava kava projekti kohta teabe taotlemine ja saatmine	Andmevood

	Euroopa Parlament ja nõukogu võivad kutsuda komisjoni ja ENISAt arutama IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku Euroopa küberturvalisuse sertifitseerimise kavade rakendamisega seotud küsimusi.			
Artikkel 73 Euroopa küberturvalisuse sertifitseerimise kava taotlemine Artikkel 74 Euroopa küberturvalisuse sertifitseerimise kavade koostamine ja vastuvõtmine **(hõlmatud artikliga 17)**	**Artikkel 73** **1. Komisjon võib taotleda ENISA-lt** IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku **Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava koostamist**. Nõuetekohaselt põhjendatud juhtudel võib Euroopa küberturvalisuse sertifitseerimise rühm soovitada komisjonil esitada lõikes 1 osutatud taotluse. 4. Lõikes 1 osutatud taotluse koostamisel konsulteerib **komisjon** nõuetekohaselt ENISA ja Euroopa küberturvalisuse sertifitseerimise rühmaga ning võtab arvesse kõigi **asjaomaste sidusrühmade** ja liidu üksuste seisukohti, sh (kui see on kohaldatav) neid, mis on asjakohased liidu õigusaktide alusel, mille vastavuseelduse Euroopa küberturvalisuse sertifitseerimise kava tagab. Artikkel 74 3. ENISA teeb ettevalmistava kava koostamisel **tihedat koostööd Euroopa küberturvalisuse sertifitseerimise rühmaga**. **Euroopa küberturvalisuse sertifitseerimise rühm pakub ENISA-le abi** ja eksperdinõu seoses	Euroopa Komisjon ENISA ECCG Ekspertidest sidusrühmad	Taotlus- ja sertifitseerimissüsteemi ettevalmistamine ning sellega seotud konsulteerimine sidusrühmadega	Andmetöötlus Andmevood Digitaalne avalik teenus (hõlmatud artikliga 17)

	ettevalmistava kava ning vajaduse korral sellele lisatavate tehniliste kirjelduste koostamisega. **ENISA palub Euroopa küberturvalisuse sertifitseerimise rühma liikmetel esitada ettevalmistava kava kohta kirjaliku arvamuse.** 4. **ENISA konsulteerib aegsasti sidusrühmadega** ametliku, avatud, läbipaistva ja kaasava konsulteerimisprotsessi raames. **ENISA teeb samuti koostööd asjaomaste avaliku sektori asutustega liikmesriikides, et saada neilt eksperdinõuandeid** ettevalmistava kava ja vajaduse korral sellele lisatavate tehniliste kirjelduste koostamise kohta. 6. **ENISA edastab ettevalmistava kava** komisjonile hiljemalt 60 päeva jooksul alates lõikes 5 osutatud taotluse esitamise kuupäevast. 7. Kui komisjon saab ettevalmistava **kava** kätte, siis **ta hindab**, kas kava vastab artikli 73 kohaselt esitatud taotlusele. 8. Kui komisjon saadab ettevalmistava kava kooskõlas lõike 7 punktiga b ENISA-le muutmiseks tagasi, siis kohaldatakse vastavalt lõikeid 4, 5 ja 7.			
Artikkel 75 Euroopa küberturvalisuse sertifitseerimise kava haldamine	2. ENISA tagab koostöös komisjoniga ning Euroopa küberturvalisuse sertifitseerimise rühma ja selle vastava haldamise alamrühma toetusel Euroopa küberturvalisuse sertifitseerimise kavade haldamise, võttes muu hulgas arvesse kõnealuste kavade võimalikku läbivaatamist komisjoni poolt. ENISA teeb haldamisega seoses koostööd ja vahetab teavet asjaomaste liidu üksuste ja rühmadega.	Euroopa Komisjon ENISA ECCG Vastavushindamisasutused	ENISA tagab hoolduse. See hõlmab korrapäraseid hübriid- või veebikoosolekuid, teabe kogumist, analüüsimist ja jagamist (seoses Euroopa küberturvalisuse sertifitseerimise kavaga).	Andmetöötlus Andmevoog

	5. Euroopa küberturvalisuse sertifitseerimise rühm võib esitada Euroopa küberturvalisuse sertifitseerimise kavade haldamise kohta arvamuse.			
Artikkel 76 Euroopa küberturvalisuse sertifitseerimise kava hindamine, läbivaatamine ja kehtetuks tunnistamine	1. ENISA hindab vähemalt iga nelja aasta tagant pärast Euroopa küberturvalisuse sertifitseerimise kava kohaldamist kõnealuse kava mõju ja tulemuslikkust koostöös Euroopa küberturvalisuse sertifitseerimise rühma asjaomase haldamise allrühmaga ning võttes arvesse sidusrühmadelt saadud tagasisidet. ENISA viib hindamise läbi, tehes vajaliku turuanalüüsi kooskõlas artikli 8 lõikega 1. 3. Komisjon konsulteerib Euroopa küberturvalisuse sertifitseerimise kavade läbivaatamisel või kehtetuks tunnistamisel ENISA, Euroopa küberturvalisuse sertifitseerimise rühma ja selle asjaomase haldamise allrühmaga ning võtab arvesse asjaomaste sidusrühmade ja muude liidu üksuste seisukohti. 4. Euroopa küberturvalisuse sertifitseerimise rühm võib esitada Euroopa küberturvalisuse sertifitseerimise kava läbivaatamise või kehtetuks tunnistamise kohta arvamuse. Komisjon võtab seda Euroopa küberturvalisuse sertifitseerimise kava läbivaatamisel või kehtetuks tunnistamisel nõuetekohaselt arvesse.	Euroopa Komisjon ENISA ECCG	Komisjon vaatab kavad läbi asjaomaste sidusrühmadega konsulteerides.	Andmetöötlus Andmevoog

Artikkel 77 Euroopa küberturvalisuse sertifitseerimise kavades esitatud tehnilised kirjeldused	3. Kui Euroopa küberturvalisuse sertifitseerimise kavas osutatakse tehnilistele kirjeldustele, nagu on märgitud artikli 74 lõikes 10, siis tehakse need kättesaadavaks artiklis 79 osutatud veebisaidil. 4. Nõuetekohaselt põhjendatud juhtudel, eelkõige kui tehnilised kirjeldused sisaldavad teavet, mis võib kahjustada sertifitseeritud IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku turvalisust, jaotatakse need ainult sidusrühmadele, kelle suhtes kava nõudeid kohaldatakse. Kõnealustele kavadele ei osutata Euroopa küberturvalisuse sertifitseerimise kavas, nagu on märgitud artikli 74 lõikes 10.	ENISA Liikmesriigid Vastavushindamisasutused	Teabe kättesaadavaks tegemine ENISA sertifitseerimise veebisaidil	Andmevoog Digitaalne avalik teenus
Artikkel 79 Euroopa küberturvalisuse sertifitseerimise kavade veebisait	1. ENISA korraldab tegevuse, et edendada vastu võetud Euroopa küberturvalisuse sertifitseerimise kavade kasutuselevõttu, muu hulgas hallates käesoleva artikli lõikes 2 osutatud veebisaiti. 2. ENISA haldab ja ajakohastab korrapäraselt sihtotstarbelist veebisaiti, millel on esitatud avalik teave järgmise kohta: a) Euroopa küberturvalisuse sertifitseerimise kavad; b) iga Euroopa küberturvalisuse sertifitseerimise kava haldamisega seotud tasud; c) asjakohased ENISA tehnilised kirjeldused; d) Euroopa küberturvalisuse sertifikaadid ja ELi vastavusdeklaratsioonid, sh teave selliste sertifikaatide ja deklaratsioonide kohta, mis enam ei kehti, mis on peatatud, kehtetuks tunnistatud või aegunud;	ENISA Liikmesriigid Vastavushindamisasutused	Teabeveebisaidi haldamine volitab ENISAt koguma, töötlema ja haldama põhjalikke sertifitseerimisteabe andmebaase, mis nõuab pidevat andmehaldustegevust.	Digitaalne avalik teenus Digilahendus Andmetöötlus Andmevoog

	e) asjakohane täiendav küberturvalisuse teave, mis on esitatud kooskõlas artikli 84 lõikega 2; f) vastastikuste eksperdihinnangute kokkuvõtted kooskõlas artikli 89 lõikega 7; g) Euroopa küberturvalisuse sertifitseerimise kavas märgitud tehnilised kirjeldused kooskõlas artikli 74 lõikega 10. 3. Kui see on asjakohane, **märgitakse lõikes 2 osutatud veebisaidil ära ka** riiklikud küberturvalisuse sertifitseerimise kavad, mis on asendatud Euroopa küberturvalisuse sertifitseerimise kavaga.			
Artikkel 81 Euroopa küberturvalisuse sertifitseerimise kava elemendid	5. Komisjonil on volitus võtta vastu rakendusakte, millega kehtestatakse ühised põhimõtted ja näidissätted lõigetes 1, 2 ja 3 sätestatud elementide kohta Euroopa küberturvalisuse sertifitseerimise kavade puhul. Kui see on asjakohane ja kättesaadav, siis võib Euroopa küberturvalisuse sertifitseerimise kava sisaldada viiteid kõnealustele põhimõtetele ja näidissätetele. Käesoleva artikli lõikes 5 osutatud rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega. **Euroopa küberturvalisuse sertifitseerimise kavade jaoks ühispõhimõtete ja näidissätete koostamisel või muutmisel konsulteerib komisjon ENISAga ja võtab vajaduse korral arvesse Euroopa küberturvalisuse sertifitseerimise rühma, asjaomaste sidusrühmade ja muude asjaomaste asutuste**	ENISA Üldsus Liikmesriikide ametiasutused	Konsulteerimine asjaomaste sidusrühmadega, kes vajavad andmevooge ja -töötlust	Andmevoog Andmetöötlus

	arvamusi.			
Artikkel 83 Vastavuse enesehindamine	3. IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja või üksus, kelle turvaolekut sertifitseeritakse, hoiab ELi vastavusdeklaratsiooni, tehnilist dokumentatsiooni ja muud asjaomast teavet, mis käsitleb IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või turvaoleku vastavust Euroopa küberturvalisuse sertifitseerimise kavale, asjaomases kavas kindlaks määratud tähtaja jooksul kättesaadavana artikli 89 kohaselt määratud riiklikule küberturvalisuse sertifitseerimise asutusele. **ELi vastavusdeklaratsiooni koopia esitatakse põhjendamatu viivituseta riiklikule küberturvalisuse sertifitseerimise asutusele ja ENISA-le.**	ENISA Üldsus Liikmesriikide ametiasutused	Kättesaadav teave; andmete jagamine Jagatud andmeid peavad töötlema ENISA ja liikmesriikide ametiasutused	Andmevoog Andmetöötlus
Artikkel 84 Täiendav küberturvalisuse alane teave sertifitseeritud IKT-toodete, -teenuste ja -protsesside kohta	1. Nende IKT-toodete, -teenuste või -protsesside tootja või pakkuja, mille kohta on väljastatud ELi vastavusdeklaratsioon või Euroopa küberturvalisuse sertifikaat, **teeb üldsusele kättesaadavaks järgmise täiendava küberturvalisuse teabe**.	IKT-toodete, -teenuste või -protsesside tootja või pakkuja Üldsus Vastavushindamisasutused	Teabe üldsusele elektroonilisel kujul kättesaadavaks tegemine.	Andmevoog
Artikkel 85 Euroopa küberturvalisuse sertifikaatide väljastamine	2. Euroopa küberturvalisuse sertifikaadi annavad välja artiklis 91 osutatud vastavushindamisasutused artikli 74 kohaselt komisjoni poolt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavas sisalduvate kriteeriumide alusel. 6. Füüsiline või juriidiline isik, kes esitab oma IKT-tooted, -teenused, -protsessid või hallatud turbeteenused sertifitseerimiseks või üksus, kes	ENISA Üldsus Liikmesriikide ametiasutused Vastavushindamisasutused	Sertifitseerimisprotsessidega seotud teabe jagamine	Andmevoog Andmetöötlus

	taotleb oma turvaoleku sertifitseerimist, **peab tegema** artikli 89 kohaselt määratud **riiklikule küberturvalisuse sertifitseerimise asutusele**, kui kõnealune asutus on Euroopa küberturvalisuse sertifikaati väljaandev asutus, või artiklis 91 osutatud vastavushindamisasutusele **kättesaadavaks kogu sertifitseerimiseks vajaliku teabe**. 7. Vastavushindamisasutused ja vajaduse korral riiklikud küberturvalisuse sertifitseerimise **asutused teavitavad ENISAt** põhjendamatu viivituseta nende otsustest, mis mõjutavad Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide seisundit kooskõlas artikliga 94. 8. **Euroopa küberturvalisuse sertifikaadi saanud isik teavitab vastavushindamisasutust** ja asjakohasel juhul lõikes 7 osutatud riiklikku küberturvalisuse sertifitseerimise asutust mis tahes edasistest avastatud nõrkustest või mittevastavustest sertifitseeritud IKT-toote, -teenuse, -protsessi, hallatud turbeteenuse või üksuse turvaoleku puhul, mis tõenäoliselt mõjutavad selle vastavust sertifikaadile. **Kõnealune asutus edastab põhjendamatu viivituseta selle teabe** asjaomasele riiklikule küberturvalisuse sertifitseerimise asutusele ja hindab sertifikaadi mõju kooskõlas kava tingimustega, nagu on osutatud artikli 81 punktis f.			
Artikkel 86 Riiklikud küberturvalisuse sertifitseerimise kavad	4. **Liikmesriigid teavitavad komisjoni ja Euroopa küberturvalisuse sertifitseerimise rühma enne** IKT-toodete, -teenuste, -	ENISA Liikmesriigid Euroopa Komisjon	Teabevahetus	Andmevoog

	protsesside, hallatud turbeteenuste ja üksuste turvaoleku **uute riiklike küberturvalisuse sertifitseerimise kavade vastuvõtmist**.			
Artikkel 88 Riiklikud küberturvalisuse sertifitseerimise asutused	2. Iga liikmesriik **teatab komisjonile määratud riiklike küberturvalisuse sertifitseerimise asutuste andmed**. Kui liikmesriik määrab rohkem kui ühe asutuse, teatab ta komisjonile igale asutusele määratud ülesannetest. 6. Riiklikel küberturvalisuse sertifitseerimise asutustel on järgmised ülesanded: c) **nad teevad** nende vastaval territooriumil asutatud ning vastava Euroopa küberturvalisuse sertifitseerimise kava kohaselt vastavuse enesehindamist tegevate käesolevas määruses sätestatud IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootjate või pakkujate või sertifitseeritava turvaolekuga üksuste **kohustuste täitmise üle järelevalvet ning tagavad nende kohustuste täitmise koostöös asjaomaste turujärelevalveasutustega**; d) **nad aitavad aktiivselt ja toetavad riiklikke akrediteerimisasutusi või muid asjaomaseid asutusi** vastavushindamisasutuste poolt käesoleva määruse kohaldamiseks läbi viidava tegevuse **jälgimisel ja järelevalvel**, ilma et see piiraks artikli 91 lõike 3 kohaldamist; e) nad teevad koostööd Euroopa Komisjoniga, kui vastavushindamisasutuse pädevus seatakse kahtluse alla kooskõlas artikliga 94; f) nad **jälgivad ja kontrollivad** artikli 85	ENISA Liikmesriikide ametiasutused Euroopa Komisjon Üldsus Vastavushindamisasutused	Liikmesriik teavitab komisjoni määratud riiklikest küberturvalisuse sertifitseerimise asutustest Liikmesriikide ametiasutused täidavad mitmesuguseid seire-, järelevalve- ja koostööülesandeid, mis nõuavad andmevooge ja kuupäevatöötlust.	Andmevoog Andmetöötlus

	lõikes 3 osutatud avaliku sektori asutuste **tegevust**; g) kui see on kohaldatav, siis nad volitavad vastavushindamisasutusi kooskõlas artikliga 93, teevad vastavushindamisasutuste kohustuste täitmise järelevalvet ja tagavad nende täitmise artikli 81 lõike 3 punkti f kohaselt Euroopa küberturvalisuse sertifitseerimise kavade lisa- või erinõuete alusel ning piiravad kehtivaid lubasid, peatavad või tunnistavad need kehtetuks, kui vastavushindamisasutused ei täida käesoleva määruse nõudeid; h) **nad käsitlevad** füüsiliste või juriidiliste isikute **kaebusi** seoses Euroopa küberturvalisuse sertifikaatidega, mille on välja andnud riiklikud küberturvalisuse sertifitseerimise asutused, või kooskõlas artikli 85 lõikega 4 vastavushindamisasutused, või seoses artikli 83 kohaselt välja antud ELi vastavusdeklaratsioonidega, ning uurivad asjakohasel määral nende kaebuste sisu ja teavitavad kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest; i) nad esitavad komisjonile, ENISA-le ja Euroopa küberturvalisuse sertifitseerimise rühmale igal aastal aastaaruande oma põhitegevuse kohta 31. märtsiks [jõustumise aasta + 12 kuud] ja teevad kõnealused aruanded kättesaadavaks vastastikuse eksperdihinnangu rühmale, kui riiklikud küberturvalisuse sertifitseerimise asutuse suhtes kohaldatakse vastastikust eksperdihinnangut kooskõlas artikliga 89;			

	j) **nad teevad koostööd teiste riiklike küberturvalisuse sertifitseerimise asutuste**, turujärelevalveasutuste või muude avaliku sektori asutustega, muu hulgas jagades teavet IKT-toodete, -teenuste ja -protsesside, hallatud turbeteenuste ja üksuste turvaoleku võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele; k) **nad jälgivad küberturvalisuse sertifitseerimise valdkonna asjakohast arengut**. 8. Riiklikud küberturvalisuse sertifitseerimise asutused teevad omavahel ja komisjoniga koostööd, eelkõige **vahetavad teavet, kogemusi ja häid tavasid** seoses IKT-toodete, -teenuste ja -protsesside, hallatud turbeteenuste ja üksuste turvaoleku küberturvalisuse sertifitseerimisega ning küberturvalisust puudutavate tehniliste küsimustega. 9. ENISA koostab tähtpäevaks [jõustumise kuupäev + kuus kuud] käesoleva artikli lõike 6 punktis i osutatud aruande vormi koostöös komisjoni ja Euroopa küberturvalisuse sertifitseerimise rühmaga.			
Artikkel 89 Vastastikune eksperdihinnang	5. **ENISA toetab** vastastikuse eksperdihinnangu mehhanismi ja vastastikuste eksperdihinnangute korraldamist, sh **töötades välja asjakohased suunisdokumendid ja vormid** koostöös komisjoni ning Euroopa küberturvalisuse sertifitseerimise rühmaga. 7. Euroopa küberturvalisuse sertifitseerimise	EL ENISA ECCG	Andmete internetis kättesaadavaks tegemine	Andmevoog Andmetöötlus

	rühm vaatab **lõpparuande, sh võimalikud** suunised või soovitused ja vastastikuse eksperdihinnangu kokkuvõtte läbi ning kiidab kokkuvõtte heaks artikli 79 lõikes 2 osutatud veebisaidil avaldamiseks.			
Artikkel 90 Euroopa küberturvalisuse sertifitseerimise rühm (ECCG)	3. Euroopa küberturvalisuse sertifitseerimise rühmal on järgmised ülesanded: [viide teistele artiklitele] h) analüüsida olulisi arenguid küberturvalisuse sertifitseerimise valdkonnas, sh riiklikul tasandil kooskõlas artikliga 86, ning vahetada teavet ja häid tavasid küberturvalisuse sertifitseerimise kavade kohta; i) edendada koostööd riiklike küberturvalisuse sertifitseerimise asutuste vahel käesolevas jaotises sätestatud normide kohaselt suutlikkuse suurendamise ja teabevahetuse teel, eelkõige küberturvalisuse sertifitseerimist käsitlevate küsimuste puhul; [viide teistele artiklitele] k) hõlbustada Euroopa küberturvalisuse sertifitseerimise kavade vastavusse viimist rahvusvaheliselt tunnustatud standarditega, sh olemasolevate Euroopa küberturvalisuse sertifitseerimise kavade haldamise osana, ja asjakohasel juhul esitada ENISA-le soovitusi teha koostööd asjaomaste Euroopa või rahvusvaheliste standardiorganisatsioonidega, et kõrvaldada kehtivate Euroopa rahvusvaheliselt tunnustatud standardite puudused ja lüngad.	Liikmesriigid ENISA Euroopa Komisjon	Analüüs, teabe jagamine ja koostöö liikmesriikide ametiasutuste ja rahvusvaheliste organisatsioonide vahel seoses Euroopa küberturvalisuse sertifitseerimisega	Andmetöötlus Andmevoog

Artikkel 92 Vastavushindamisasutuste pädevuse täiendav ühtlustamine	4. Kui riiklik küberturvalisuse sertifitseerimise asutus saab taotluse vastavalt lõikele 3, **teatab ta sellest selle liikmesriigi riiklikule küberturvalisuse sertifitseerimise asutusele, kus taotluse esitanud vastavushindamisasutus on asutatud**. Neil juhtudel võib kõnealuse liikmesriigi riiklik küberturvalisuse sertifitseerimise asutus osaleda loa andmisel vaatlejana.	Liikmesriikide ametiasutused Vastavushindamisasutused	Teabe jagamine ja säilitamine	Andmevoog Andmetöötlus
Artikkel 93 Vastavushindamisasutustest teada andmine	1. Iga Euroopa küberturvalisuse sertifitseerimise kava puhul **annavad liikmesriigi riiklikud küberturvalisuse sertifitseerimise asutused komisjonile ja muudele liikmesriikidele teada** akrediteeritud ja asjakohasel juhul artikli 92 kohaselt loa saanud vastavushindamisasutustest. 2. **Riiklikud küberturvalisuse sertifitseerimise asutused viivad lõikes 1 osutatud teavitamise läbi**, kasutades komisjoni väljatöötatud ja hallatud elektroonilist teavitamisvahendit.	ENISA Liikmesriigid Euroopa Komisjon Vastavushindamisasutused	Akrediteeritud ja volitatud vastavushindamisasutustest teavitamine	Andmevood Andmetöötlus
Artikkel 94 Vastavushindamisasutuste pädevusega seotud probleemid	1. 1. **Komisjon uurib** iga juhtumit, mille puhul tal on kahtlusi või talle on teatatud kahtlustest seoses vastavushindamisasutuse pädevusega täita tema suhtes kehtivaid nõudeid ja kohustusi või seoses sellega, kas vastavushindamisasutus täidab neid jätkuvalt. 2. **Riiklik küberturvalisuse sertifitseerimise asutus esitab komisjonile** taotluse korral kogu teabe teavitamise aluse või asjaomase vastavushindamisasutuse pädevuse säilimise kohta.	Komisjon Liikmesriigid ENISA	Vastavushindamisasutuste pädevusega seotud probleemid	Andmevoog Andmete töötlemine Digitaalne avalik teenus

	3. **Komisjon tagab, et kogu tundlikku teavet, mis uurimise käigus saadi, käsitletakse konfidentsiaalsena.** 4. Kui komisjon teeb kindlaks, et teada vastavushindamisasutus ei täida või enam ei täida temast teada andmise aluseks olevaid nõudeid, **teavitab ta sellest riiklikku küberturvalisuse sertifitseerimise asutust** ja nõuab temalt vajalike parandusmeetmete võtmist, sh vajaduse korral teada andmise tühistamist.			
Artikkel 95 Vastavushindamisasutusi käsitlev teave ja teabe säilitamise kohustus	1. Vastavushindamisasutused **teavitavad riiklikku küberturvalisuse sertifitseerimise asutust** järgmisest: a) kõik juhtumid, kui sertifikaat jäetakse andmata, seda kitsendatakse, see peatatakse või tunnistatakse kehtetuks; b) artikli 93 lõikes 1 osutatud teavitamise ulatust ja tingimusi mõjutavad asjaolud; c) kõik turujärelevalveasutustelt saadud teabetaotlused vastavushindamistoimingute kohta; d) taotluse korral vastavushindamistoimingud, mis on teavitamisega hõlmatud valdkonnas läbi viidud, ja muu tegevus, sh piiriülene tegevus ja alltöövõtt. 2. **Vastavushindamisasutused esitavad samuti ENISA-le** lõike 1 punktis a osutatud **teabe**, et lihtsustada selle ülesannete täitmist artikli 79 alusel. 3. **Vastavushindamisasutused esitavad muudele vastavushindamisasutustele**, mis	Liikmesriikide ametiasutused Vastavushindamisasutused	Teabevahetus vastavushindamisasutuste vahel	Andmevoog Andmetöötlus

	viivad käesoleva määruse alusel läbi samalaadset vastavushindamistegevust samade IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või sertifitseeritava turvaolekuga üksuste puhul, põhjendamatu viivituseta **asjakohase teabe** küsimuste kohta, mis käsitlevad vastavushindamise negatiivseid ja taotluse korral positiivseid tulemusi. 4. **Vastavushindamisasutused hoiavad kasutuses aruannete süsteemi**, mis sisaldab kõiki dokumente ja tõendeid, mis on esitatud või saadud iga nende läbiviidud hindamise ja sertifitseerimise puhul. Aruandeid säilitatakse turvalisel ja juurdepääsetaval viisil sertifitseerimiseks vajaliku aja jooksul ning vähemalt viis aastat pärast asjaomase Euroopa küberturvalisuse sertifikaadi aegumist või kehtetuks tunnistamist.			
Artikkel 96 Õigus esitada kaebus ja õigus tõhusale õiguskaitsevahendile	2. Asutus, kellele kaebus esitatakse, **teavitab kaebuse esitajat kaebuse menetlemise käigust** ja tehtud otsusest, samuti lõigetes 3 ja 4 osutatud õigusest tõhusale õiguskaitsevahendile. 4. Käesoleva artikli kohased menetlused algatatakse selle liikmesriigi kohtus, kus asub asutus, mille suhtes õiguskaitsevahendit taotletakse.	Liikmesriikide ametiasutused Euroopa Komisjon Üldsus Sertifikaadi omanikud	Kaebustega seotud teabe liikumine ametiasutuste ja üldsuse vahel Menetlus liikmesriigi kohtutes	Andmevoog
Artikkel 97 Karistused	**Liikmesriigid teavitavad komisjoni viivitamata** nimetatud normidest ja meetmetest	Liikmesriikide ametiasutused Euroopa Komisjon	Teabevoog, mis on seotud liikmesriikide poolt komisjonile	Andmevoog

	ning kõikidest nende hilisematest muudatustest.		karistustest teatamisega.	
Artikkel 99 Turvariski hindamine	Komisjon või vähemalt kolm liikmesriiki võivad paluda võrgu- ja infoturbe koostöörühmal teha kuue kuu jooksul koordineeritud riskihindamise. Komisjon võib taotleda lühemaid tähtaegu. Riskihinnangutes töötatakse välja riskistsenaariumid ja eeldatakse andmete analüüsi. Koordineeritud turvariski hindamise ettevalmistamine Juhtudel, mis õigustavad viivitamatut sekkumist, konsulteerib komisjon viivitamata liikmesriikidega ja viib läbi riskihindamise. Otsused riskihindamise läbiviimiseks (andmetöötlus/analüüs).	Euroopa Komisjon ELi liikmesriigid Võrgu- ja infoturbe koostöörühm ENISA	Teabe taotlemine ja saamine; andmete analüüs koordineeritud riskihindamise eesmärgil Konsulteerimine liikmesriikidega ja riskihindamise läbiviimine	Andmetöötlus Andmevoog
Artikli 100 lõiked 1 ja 2 – Küberturvalisuse seisukohast muret tekitavate kolmandate riikide kindlaks määramine	1. Kui artiklis 99 osutatud turvariski hindamise tulemusena või muude allikate, näiteks liidu või liikmesriigi nimel tehtud avaliku pöördumise alusel näib, et kolmas riik põhjustab IKT tarneahelatele märkimisväärse ja struktuurse mittetehnilise riski, siis kontrollib komisjon kõnealuse riigi põhjustatud ohtu, võttes arvesse järgmisi elemente, mille tulemuseks on andmete töötlemine, analüüs. 2. Kui komisjon järeldab pärast lõikes 1 osutatud kontrolli, et kolmas riik põhjustab	ELi liikmesriigid Euroopa Komisjon	Teabe vastuvõtmine, analüüsimine, teabevahetus.	Andmevood Andmetöötlus

	tõsise ja struktuurse mittetehnilise riski IKT tarneahelatele, siis võib ta otsustada rakendusakti abil määrata kõnealuse kolmanda riigi kindlaks IKT tarneahelate jaoks küberturvalisuse seisukohast muret tekitava riigina, mille tulemuseks andmete on andmete töötlemise analüüs ja andmevood.			
Artikkel 101 Üldine IKT tarneahela mehhanism Artikkel 102 Oluliste IKT-varade kindlaksmääramine ja Artikkel 103 IKT tarneahelaga seotud leevendusmeetmed	1. Kui võrgu- ja infoturbe koostöörühm on teinud kooskõlas käesoleva määruse artikli 99 lõigetega 1 ja 2 liidu tasandi koordineeritud turvariski hindamise või pärast artikli 99 lõike 3 kohaselt olulise küberohu menetluse lõpuleviimist võib komisjon võtta artiklis 102 ja artiklis 103 sätestatud meetmeid. Komisjonil on õigus võtta vastu rakendusakte, milles määratakse kindlaks peamised IKT-varad ja leevendusmeetmed, sh IKT tarneahelate piirangud ja keelud (üksikasjalikult kirjeldatud allpool punktis 4.5). Selle protsessi ettevalmistamisel võtab komisjon arvesse ja kaalub mitmeid aspekte, mis viitavad **andmetöötlusele/analüüsile ja mõnel juhul andmevoole**: Artikli 102 punktid a–f	Euroopa Komisjon Võrgu- ja infoturbe koostöörühm Asjaomased sidusrühmad	Andmete analüüs/andmetöötlus; konsulteerimine asjaomaste sidusrühmadega	Andmetöötlus Andmevoog

	Artikli 103 lõike 4 punktid a–d Artikli 103 lõige 6			
Artikkel 104 Suure riskiga tarnijate kindlakstegemine	Komisjon määrab rakendusaktide alusel kindlaks suure riskiga tarnijate loetelud, kelle suhtes kohaldatakse keelde, mis on sätestatud artikli 103 lõike 1 kohaselt vastu võetud rakendusaktides, või artikli 111 lõikes 1 osutatud keeldu. Komisjon kaardistab tarnijad, kes pakuvad IKT-komponente ja komponente, mis sisaldavad IKT-komponente, ning teeb esialgse hindamise selle kohta, millised tarnijad võivad olla asutatud artikli 100 kohaselt määratud kolmandates riikides või keda võidakse kontrollida nendest kolmandatest riikidest. Komisjon hindab asutamiskohta ning omandi- ja kontrollistruktuuri. Komisjonil on õigus nõuda tarnijatelt vajalikku teavet ning jagada asjaomasele tarnijale esialgseid järeldusi kindlaksmääramise, omandiõiguse ja kontrolli hindamise kohta ning anda neile võimalus esitada oma seisukohad.	Euroopa Komisjon Pädevad asutused Tarnijad	Andmete analüüs/andmetöötlus; konsulteerimine pädevate asutustega, konsulteerimine tarnijatega	Andmetöötlus Andmevoog

	Komisjon võib esitada pädevale asutusele taotluse tarnija asutamise, omandi ja kontrolli esialgse hindamise läbiviimiseks, kui see on kõnealuse tarnija tegevuse omadusi arvesse võttes põhjendatud. Pädev asutus võib teha ettepaneku kõnealune esialgne hindamine läbi viia. Komisjon kontrollib kõnealuseid esialgseid järeldusi, et otsustada, kas tarnija tuleks lisada suure riskiga tarnijate loetellu. Komisjon ajakohastab korrapäraselt suure riskiga tarnijate loetelu, et kõrvaldada sellest või lisada sinna suure riskiga tarnijaid. Loetellu lisatud suure riskiga tarnijad võivad esitada komisjonile taotluse nende asutamise, kontrolli ja omandi struktuuri uuesti hindamiseks, kui nad on esitanud tõendeid asjasse puutuvate muudatuste kohta.			
Artikkel 105 Küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud või sellise kolmanda riigi üksuste kontrolli all olevate üksuste väljaarvamine Artikkel 108 Konfidentsiaalsus	1) Kindlaksmääratud kolmandas riigis asutatud või sellest kontrollitav üksus, kes tekitab küberturvalisusega seotud probleeme, **võib esitada komisjonile põhjendatud taotluse**. 3) Komisjon hindab ja võtab vastu otsuse, võttes arvesse mitut andmeanalüüsini **viivat aspekti**. (Artikli 105 lõiked 3 ja 4) Teavet, mille komisjon on saanud,	Euroopa Komisjon Küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud või sellise kolmanda riigi üksuste kontrolli all olevad üksused	Komisjon saab taotluse; andmete analüüsimine.	Andmevoog Andmetöötlus

	kasutatakse ainult omandatu otstarbel.			
Artikkel 107 Register	Komisjon peab artiklis 105 osutatud otsuste kohta avalikku registrit. Registris märgitakse nende üksuste nimed, mille suhtes on kõnealused otsused tehtud.	Euroopa Komisjon Küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud või sellise kolmanda riigi kontrolli all olevad üksused	Komisjon peab üldsusele kättesaadavat registrit.	Digilahendus
Artikkel 111 Elektroonilise side mobiili-, püsi- ja satelliitvõrkude puhul kehtestatavad keelud	Käesoleva määruse alusel määratud pädev asutus **teavitab** viivitamata määruse (EL) XX/XXXX [DNA ettepanek] kohast pädevat asutust meetmetest, mis on kehtestatud elektroonilise side mobiili-, püsi- ja satelliitvõrkude pakkujatele.	Pädev asutus määruse (EL) XX/XXXX [DNA ettepanek] artikli 9 või 20 tähenduses Elektroonilise side mobiili-, püsi- ja satelliitvõrkude pakkujad	Lubadega seotud teabe liikumine pädevalt asutuselt üksustele.	Andmevoog
Artikli 112 lõiked 1 ja 4 Pädevad asutused	1) **Iga liikmesriik määrab** ühe või mitu pädevat asutust, kes vastutavad artiklis 114 osutatud järelevalve- ja täitmise tagamise ülesannete täitmise eest. 4) Iga liikmesriik teavitab komisjoni põhjendamatu viivituseta lõike 1 kohaselt määratud pädevate asutuste nimedest, nende	ELi liikmesriigid Euroopa Komisjon Üldsus	Liikmesriigid, kes määravad pädevad asutused ja teavitavad komisjoni.	Andmevoog

	asutuste vastavatest ülesannetest ning nende mis tahes edasistest muudatustest. Iga liikmesriik avalikustab samuti lõike 1 kohaselt määratud pädevate asutuste nimed.			
Artikkel 113 Komisjoni koostöö- ja tugiteenuste võrgustik	1. Komisjon loob liikmesriikide pädevate asutuste ja komisjoni koostöövõrgustiku, mis toimib koostöö- ja teabevahetusplatvormina. Komisjon pakub võrgustikule haldustuge. 2. Selleks et toetada liikmesriike nende järelevalveülesannete täitmisel, hindab komisjon, kas tarnijad, keda konkreetsed keelud võivad mõjutada, asuvad artikli 100 kohaselt määratud kolmandates riikides või on nende kontrolli all. Selleks jagab pädev asutus komisjoniga asjakohast teavet. 3. Hindamise eesmärgil on komisjonil õigus nõuda vajalikku teavet tarnijatelt, keda võivad mõjutada konkreetsed keelud, mis on kehtestatud või mida kontrollitakse artikli 100 kohaselt määratud kolmandates riikides. 4. Kui hindamine on lõpule viidud, jagab komisjon tulemusi pädevate asutustega lõike 1 kohaselt loodud võrgustikus. Pädevad asutused teavitavad direktiivi	Komisjon Pädevad asutused Direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksused	Komisjon hindab tarnijaid ja jagab teavet pädevate asutustega, kes jagavad teavet direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksustega Komisjon nõuab tarnijatelt teavet Komisjoni teavitavad pädevad asutused	Andmete töötlemine Andmevood

	(EL) 2022/2555 I ja II lisas osutatud liiki asjaomaseid üksusi õigeaegselt järeldustest. 5. Kui pädev asutus saab teada, et tarnija, keda konkreetsed keelud võivad mõjutada, asub küberturvalisusega seotud probleeme tekitavas kolmandas riigis või on selle kolmanda riigi kontrolli all ning seda ei ole hinnatud, teavitab ta sellest põhjendamatu viivituseta komisjoni.			
Artikkel 114 Järelevalve- ja täitemeetmed	Nõuded liikmesriikidele, kes tagavad teabevahetuse direktiivi (EL) 2022/2555 I ja II lisas osutatud üksustega. Pädevad asutused teavitavad asjaomaseid üksuseid nende esialgsetest järeldustest enne täitemeetmete võtmist. Pädevad asutused teevad omavahel ja komisjoniga koostööd.	ELi liikmesriigid Euroopa Komisjon Üksused direktiivi (EL) 2022/2555 I ja II lisa tähenduses	Nõuded, millega tagatakse teabe liikumine;	Andmevoog Andmetöötlus
Artikkel 115 Karistused	Liikmesriigid teavitavad komisjoni nimetatud normidest ja meetmetest ning teavitavad teda viivitamata nende hilisematest muudatustest.	Euroopa Komisjon ELi liikmesriigid	Liikmesriigid teavitavad komisjoni	Andmevoog

Artikkel 116 Vastastikune abi	Kui direktiivi (EL) 2022/2555 I või II lisas osutatud liiki üksus osutab teenuseid rohkem kui ühes liikmesriigis või osutab teenuseid ühes või enamas liikmesriigis ning selle olulised varad asuvad ühes või enamas muus liikmesriigis, **siis teevad asjaomase liikmesriigi pädevad asutused üksteisega ja komisjoniga koostööd ning nad abistavad üksteist vajadust mööda**. Lõike 1 punktis c osutatud vastastikune abi võib hõlmata teabenõudeid ja järelevalvemeetmeid, sh taotlusi teha kohapealseid kontrolle või kaugjärelevalvet või sihipäraseid turvaauditeid. Abitaotluse saanud pädev asutus ei või taotlust tagasi lükata, välja arvatud juhul, kui leitakse, et asutus ei ole pädev taotletud abi andma või et taotletav abi ei ole pädeva asutuse järelevalveülesannete suhtes proportsionaalne või kui taotlus käsitleb teavet või sisaldab tegevust, mille avalikustamine või läbiviimine oleks vastuolus asjaomase liikmesriigi riikliku julgeoleku, avaliku julgeoleku või riigikaitse oluliste huvidega. Enne sellise taotluse rahuldamata jätmist konsulteerib pädev asutus teiste asjaomaste pädevate asutustega ning ühe asjaomase liikmesriigi taotluse korral ka komisjoniga. Asjakohasel juhul võivad eri liikmesriikide	ELi liikmesriigid	Vastastikune abi järelevalvetegevuses.	Andmevoog Andmetöötlus

	pädevad asutused omavahelisel kokkuleppel võtta järelevalvemeetmeid ühiselt.			
Direktiivi artikli 1 punkt 8 Lunavararünnetest teatamine (Küberturvalisuse 2. direktiivi artikkel 27.13)	artiklisse 23 lisatakse lõiked 12 ja 13: „13. Liikmesriigid tagavad, et lunavararünde põhjustatud olulise intsidendi korral teavitavad asjaomased üksused CSIRTi või, kui see on kohaldatav, pädeva asutuse taotlusel CSIRTi või, kui see on kohaldatav, pädeva asutuse pakutava sidekanali kaudu järgmist: kui üksus on saanud lunarahanõude ja kui see on asjakohane, siis kes seda tegi; kui lunaraha maksti ja kui maksti, siis millises maksevahendis ja millisele saajale või saajale, sh krüptovarale ja krüptovarateenuse osutajale, kui see on asjakohane.“	ELi liikmesriigid Elutähtsad ja olulised üksused	Aruandlus	Andmevoog
Direktiivi artikli 1 punkt 10 Üksuste ja registri loetelu (Küberturvalisuse 2. direktiivi artikli 27 lõige 1)	**ENISA loob elutähtsate ja oluliste üksuste ning domeeninimede registreerimise teenuseid osutavate üksuste registri ja haldab seda, tuginedes ühtsetelt kontaktpunktidelt lõike 2 kohaselt saadud teabele.**	ENISA ELi liikmesriigid (küberturvalisuse 2. direktiivi kohased elutähtsad ja olulised üksused, domeeninimede registreerimise teenuseid osutavad üksused)	ENISA loob registri ja haldab seda.	Digilahendus Digitaalne avalik teenus

Direktiivi artikli 1 punkt 11 Üksuste ja registri loetelu (Küberturvalisuse 2. direktiivi artikli 27 lõige 4)	**„4. Artikli 3 lõikes 4 osutatud teabe saamisel edastab asjaomase liikmesriigi ühtne kontaktpunkt selle põhjendamatu viivituseta ENISA-le.“**	ENISA ELi liikmesriigid	ENISAga teavet jagavad liikmesriigid	Andmevoog
Direktiivi artikli 1 punkt 12 Vastastikune abi (Küberturvalisuse 2. direktiivi artikli 37a lõiked 1, 2 ja 3)	**1. ENISA abistab** liikmesriike vastastikuse abi osutamisel artikli 37 tähenduses ning **aitab hõlbustada selliseid koostööprotsesse** elutähtsate ja oluliste üksuste jaoks (...). 2. **ENISA teeb põhjaliku analüüsi (...) ENISA töötab koostöös** komisjoni ja koostöörühmaga välja metoodika. Aruannet ajakohastatakse igal aastal. (3.) ENISA soovitab vajaduse korral järgmist: töötada välja suunised; abistavad (...)	ENISA ELi liikmesriigid Olulised ja elutähtsad üksused küberturvalisuse 2. direktiivi tähenduses Euroopa Komisjon	ENISA abistab liikmesriike ja aitab hõlbustada koostööprotsessi. Analüüside, suuniste, metoodika ja aruannete koostamine.	Andmetöötlus Andmevoog
Direktiivi artikli 1 punkt 12 Vastastikune abi (Küberturvalisuse 2. direktiivi artikli 37a lõige 4)	4. Käesoleva artikli lõike 4 punkti e kohaldamisel **esitavad asjaomaste liikmesriikide pädevad asutused ENISA-le (...), kui need on kättesaadavad, järgmise teabe**: 5. Kui liikmesriik saab artikli 37 lõike 1 esimese lõigu punktis c osutatud vastastikust abi, **teavitab ühtne kontaktpunkt ENISAt** vastastikuse abi osutamisest.	ENISA ELi liikmesriigid	Teabevahetus	Andmevoog
Artikkel 119 Delegeeritud volituste rakendamine	3. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, **teeb ta selle samal ajal teatavaks** Euroopa Parlamendile ja nõukogule. vana	Euroopa Komisjon Euroopa Parlament Nõukogu	Euroopa Parlamendile ja nõukogule saadetud teave	Andmevoog
Artikkel 120 Hindamine ja läbivaatamine	1. Hiljemalt [PP.KK.AAAA] ja seejärel iga viie aasta tagant tellib komisjon kooskõlas komisjoni suunistega hinnangu ENISA tegevuse kohta seoses tema eesmärkide, volituste,	ENISA Euroopa Komisjon Üldsus	Andmete kogumine ja analüüs; teabe üldsusele kättesaadavaks tegemine	Andmetöötlus Andmevoog

	missiooni, ülesannete, juhtimise ja asukohaga. 5. Komisjon esitab hindamistulemused Euroopa Parlamendile, nõukogule ja haldusnõukogule. Hindamise järeldused avalikustatakse.			

4.2. Andmed

Kohaldamisalasse kuuluvate andmete ja seonduvate standardite / tehniliste kirjelduste üldine kirjeldus

Andmete liik	**Viide (viited) nõudele**	**Standard ja/või tehniline kirjeldus (kui see on asjakohane)**
Andmed, mis on seotud küberkerksuse ja ühiskonna seisukohast oluliste analüüside/aruannetega	**Artikli 5 lõike 1 punktid a, b, c, e, f ja h** **Artikli 5 lõiked 2, 3 ja 4** **Artikkel 6** **Artikkel 7** **Artikkel 8** **Artikkel 9** **Artikkel 10** **Artikli 11 lõike 2 punktid b ja c** **Artikli 12 lõige 4** **Artikkel 15** **Direktiivi artikli 1 punkt 7**	Artikli 11 lõike 1 punktides a–e ja lõikes 2 loetletud toimingute tegemisel kasutab ENISA oma analüüse ning vajaduse korral oma ülesannete täitmisel saadud teavet, sh järgmist: a) avalikult kättesaadavates allikates esitatud teave, sh IKT-toodete või -teenuste avalikult teadaolevad nõrkused, mis on kättesaadavad direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasis; b) teave, mida jagavad liikmesriigid, liidu üksused, CERT-EU, erasektori või valitsusvälised partnerid ning kolmandad riigid ja rahvusvahelised organisatsioonid, arvestades võimalikke levitamispiiranguid, mis tulenevad selle teabe edasist levitamist käsitlevast nähtavast tähistusest. ENISA annab välja suunised teabevahetuseks kasutatavate võrgu- ja infosüsteemide koostalitlusvõime kohta, sh seoses määruse

		(EL) 2025/38 artikli 6 lõikes 3 osutatud piiriüleste küberkeskustega.
Operatiivkoostöö ja olukorrateadlikkuse seisukohast olulised andmed	**Artikli 10 lõike 4 punktid a–g** **Artikli 10 lõige 6** **Artikli 11 lõike 1 punktid a–g** **Artikli 11 lõike 2 punktid a, b ja c** **Artikli 11 lõige 3** **Artikli 11 lõige 4** **Artikli 13 lõige 2** **Artikkel 15** **Artikli 16 lõike 2 punkt e**	**Konfidentsiaalsuse ja tundliku teabe käsitlemise standardid** Artikli 11 lõike 1 punktides a–e ja lõikes 2 loetletud toimingute tegemisel kasutab ENISA oma analüüse ning vajaduse korral oma ülesannete täitmisel saadud teavet, sh järgmist: a) avalikult kättesaadavates allikates esitatud teave, sh IKT-toodete või -teenuste avalikult teadaolevad nõrkused, mis on kättesaadavad direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasis; b) teave, mida jagavad liikmesriigid, liidu üksused, CERT-EU, erasektori või valitsusvälised partnerid ning kolmandad riigid ja rahvusvahelised organisatsioonid, arvestades võimalikke levitamispiiranguid, mis tulenevad selle teabe edasist levitamist käsitlevast nähtavast tähistusest.
Euroopa individuaalsete küberturbeoskuste tõendamise kavade ja tõendajatele lubade andmise seisukohast olulised andmed **Euroopa küberturvalisuse sertifitseerimise kavade eesmärkide, otstarbe ja sisu seisukohast olulised andmed**	**Artikkel 17** **Artikkel 18** **Artiklid 19–23** **Artiklid 72, 73, 74, 75, 76, 77, 79, 81, 83 ja 84**	Euroopa individuaalsete küberturbeoskuste tõendamise kava sisaldab järgmist (...): eeskirjad volitatud tõendajate poolt andmete säilitamise kohta. Volitatud tõendajad tagavad, et isiku taotlusel antakse Euroopa individuaalsete küberturbeoskuste tõendamise raames välja elektrooniline tunnistus, mida saab salvestada määruses (EL) nr 910/2014 sätestatud Euroopa digiidentiteedikukrutesse. Komisjon ja ENISA peaksid Euroopa küberturvalisuse sertifitseerimise kava koostamisel andmete osas järgima liidu õigusaktide asjakohaseid sätteid.
Euroopa küberturvalisuse sertifitseerimise raamistiku juhtimisega seotud andmed	**Artiklid 85, 86, 88, 89, 90, 92, 93, 94, 95, 96 ja 97**	ENISA, vastavushindamisasutused ja riiklikud küberturvalisuse sertifitseerimise asutused peaksid tagama andmete konfidentsiaalsuse ja järgima asjaomase kava sätteid, milles

		osutatakse rahvusvahelistele standarditele, milles on nõuded kindlaks määratud.
ENISA toimimise jaoks olulised andmed (eelarve, ühtne programmdokument, sisestrateegiad)	**Artikkel 25** **Artikli 28 lõige 1** **Artikkel 30** **Artikli 31 lõige 8** **Artikli 32 lõiked 3 ja 5** **Artikli 35 lõiked 5 ja 6** **Artiklid 36–43** **Artikkel 44** **Artikkel 45** **Artikli 47 lõige 10** **Artiklid 48–49** **Artiklid 52 ja 58**	**Finantsmääruse vormid ja suunised; sisesuunised**
Isikuandmed	**Artikkel 22** **II jaotise III peatüki 6. jagu, apellatsiooninõukogu** **Artikkel 66** **Artikli 80 lõike 1 punktid c ja x** **Artikli 81 lõige 2** **Artikli 88 lõike 6 punkt h** **Artikkel 95** **Artikkel 96**	**Määrus (EL) 2018/1725** **Määrus (EL) 2016/679**

Koordineeritud riskihindamise, riskistsenaariumide väljatöötamise ja oluliste IKT-varade kindlaksmääramise käigus kogutud ja analüüsitud andmed	**Artikkel 98** **Artikkel 99** **Artikkel 102** **Artikkel 103** **Artikkel 105**	Ilma et see piiraks määruse (EL) 2024/2847 artikli 13 ja direktiivi (EL) 2022/2555 artikli 21 kohaldamist.
Kolmandaid riike / kolmandate riikide üksusi käsitlevad andmed	**Artikli 100 lõiked 1, 3 ja 4** **Artikkel 104** **Artikkel 105** **Artikkel 107** **Artikkel 113**	Ei kohaldata
Riiklikke ametiasutusi käsitlevad andmed	**Artikkel 112** **Artikkel 114** **Artikkel 116**	Ei kohaldata
Riskihindamise seisukohast olulised andmed	**Artikli 5 lõige 2**	**Konfidentsiaalsuse ja tundliku teabe käsitlemise standardid**
Liikmesriikide vastastikune abi	**Määruse artikli 5 lõike 1 punkt g ja direktiivi artikli 1 punkt 12**	/

Kooskõla Euroopa andmestrateegiaga

Selgitage, kuidas nõue (nõuded) on kooskõlas Euroopa andmestrateegiaga

KTM2 ettepaneku nõuded on Euroopa andmestrateegiaga kooskõlas, ilma et neil oleks sellele teadaolevalt konkreetset mõju.

Kooskõla ühekordsuse põhimõttega

Selgitage, kuidas on kaalutud ühekordsuse põhimõtet, kuidas on uuritud olemasolevate andmete taaskasutamise võimalust

Üks ettepaneku eesmärke on maksimeerida komisjoni lihtsustamispüüdlusi ning vähendada liikmesriikide ja sidusrühmade halduskoormust. Viimastel aastatel on ENISAst kujunenud teabekeskus, kus hoitakse eri allikatest pärit teavet. Selles mõttes on paljud ENISA ülesanded seotud teabe taaskasutamise ja ringlussevõtuga mitmesuguste analüüside tarbeks. Näiteks: teatud juhtudel direktiivi (EL) 2022/2555 artiklite 23 ja 30 kohaselt teatatud teabe taaskasutamine; teave, millest on teatatud, mida on jagatud või analüüsitud vastavalt määruse (EL) 2024/2847 artikli 14 lõigetele 1–3, artiklile 15 ning artikli 17 lõigetele 1 ja 3. Tarneahela raamistiku sätted eeldavad, et selle rakendamist toetavad direktiivi (EL) 2022/2555 artikli 22 alusel saadavad andmed, mis viitab teabe taaskasutamisele ja koordineerimisele.

Selgitage, kuidas on uued loodud andmed leitavad, juurdepääsetavad, koostalitlusvõimelised ja taaskasutatavad ning vastavad kvaliteetsetele standarditele

Seadusandlikus ettepanekus on sõnaselgelt märgitud, millal tuleks andmed üldsusele kättesaadavaks teha. Ettepanekus kaalutakse rangete turvalisuse ja konfidentsiaalsuse aspektidega sätteid ning seetõttu ei ole kõik küberturvalisuse määruse läbivaatamise käigus loodud andmed mõeldud avalikuks kasutamiseks. Vajalike sätete puhul on tagatud kooskõla Euroopa digiidentiteedikukruga. ENISA ülesanne on pakkuda varajase hoiatamise teenust masinloetavas vormingus.

Andmevood

Kohaldamisalasse kuuluvate andmete ja seonduvate standardite / tehniliste kirjelduste üldine kirjeldus

Andmete liik	Selgitage andmevoogu	Viited
ENISA koostab aruandeid ja analüüse, tehnilisi suuniseid ja parimaid tavasid.	Need andmevood on suunatud ENISA sidusrühmadele, toetades ELi poliitika ja õiguse rakendamist. Asjaomaste andmevoogude raames kogub ENISA teavet, enamasti avalike allikate kaudu, koostab analüüse ja jagab tulemusi sidusrühmadega. ENISA täidab teatavaid ülesandeid ka komisjoni taotluse korral.	Artikli 5 lõike 1 punktid a, b, c, e, f ja h Artikli 5 lõige 2, artikli 5 lõige 3, artikli 5 lõige 5 Artikkel 6 Artikkel 7 Artikkel 8 Artikkel 9 Artikkel 10 Artikli 11 lõige 2 Artikli 11 lõige 4 Artikkel 14
ELi küberturvalisuse ökosüsteemi raames komisjoni, ENISA, liikmesriikide ja muude asjaomaste osalejate vahel edastatavad operatiivkoostööd puudutavad andmevood.	Seda liiki andmevood luuakse operatiivkoostöö ja olukorrateadlikkuse eesmärgil. Teabevahetus toimub mõlemas suunas, nii sisse- kui ka väljapoole. Toimub operatiivandmete vahetamine.	Artikli 10 lõike 4 punktid a–g Artikli 11 lõike 1 punktid b–g Artikli 11 lõike 2 punktid a ja b Artikli 11 lõige 3 Artikkel 15 Artikli 16 lõike 2 punkt e
Andmevood, mis on loodud Euroopa küberturbeoskuste raamistiku ja Euroopa individuaalsete küberturbeoskuste tõendamise kavade ning nende rakendamise toetamiseks	Need andmevood toetavad teabevahetust järgmistes valdkondades: – Euroopa küberturbeoskuste raamistiku haldamine ja kasutuselevõtt ning ENISA ja selle ajutise töörühma liikmete vahelised ning ENISA ja komisjoni vahelised andmevood; – Euroopa individuaalsete küberturbeoskuste tõendamise kavade väljatöötamine ja haldamine ning ENISA ja selle ajutise töörühma liikmete vahelised ning ENISA, komisjoni ja liikmesriikide vahelised andmevood; – Euroopa individuaalsete küberturbeoskuste	Artiklid 19–23 Artiklid 36–43

	tõendamise kavade rakendamine ning taotlejate ja ENISA vahelised andmevood; – apellatsiooninõukogu, ENISA, komisjoni ja taotlejate vahelised andmevood.	
Euroopa küberturvalisuse sertifitseerimise kavade eesmärkide, otstarbe ja sisu seisukohast olulised andmed	Seda liiki andmevood on olulised Euroopa küberturvalisuse sertifitseerimise kavade kavandamiseks, taotlemiseks, arendamiseks, vastuvõtmiseks ja haldamiseks (sh võimalikuks läbivaatamiseks). Need on eelkõige seotud sidusrühmade, ENISA ja liikmesriikide ametiasutuste kaasamise ja spetsialistide nõuannete tagamisega Euroopa küberturvalisuse sertifitseerimise rühma kaudu menetluse eri etappides. Lisaks on täiendavad andmevood seotud üldsusele asjakohase teabe esitamisega komisjoni ja ENISA spetsiaalsete veebisaitide kaudu. Peale selle nähakse raamistikuga ette täiendava küberturvalisuse alase teabe avalik kättesaadavus selliste IKT-toodete, -teenuste või -protsesside tootjate või pakkujate poolt, mille kohta on nende endi vahenditega välja antud ELi vastavusdeklaratsioon või Euroopa küberturvalisuse sertifikaat.	Artikkel 18 Artikkel 19 Artiklid 72, 73, 74, 75, 76, 77, 79, 81, 83 ja 84
Euroopa küberturvalisuse sertifitseerimise raamistiku juhtimisega seotud andmed	Need andmevood toetavad teabevahetust järgmistes valdkondades: – Euroopa küberturvalisuse sertifitseerimise kavade koordineerimine ja haldamine; – vastavushindamisasutuste akrediteerimine ja neile volituste andmine ning nende edasine teavitamine asjaomase platvormi ja sellega seotud menetluste kaudu; – edasikaebemenetlused, nagu kaebuse esitamise õigus, õiguskaitsevahendid ning edasikaebe- ja muutmismenetlused.	Artiklid 85, 86, 88, 89, 90, 92, 93, 94, 95 ja 96

Ameti haldustegevusega seotud andmevood	ENISA, haldusnõukogu, liikmesriikide ja komisjoni vahelised vood. Teave puudutab ameti haldustegevust, mõlemal suunal. Mõnel juhul edastatakse teavet ka Euroopa Parlamendile (asjaomane andmevoog on esitatud allpool).	Artikkel 25 Artikli 28 lõige 1 Artikkel 30 Artikli 31 lõige 8 Artikli 32 lõiked 3 ja 5 Artikli 35 lõiked 5 ja 6 Artiklid 36–43 Artikkel 44 Artikkel 45
Euroopa Parlamendile edastatavad andmed	Euroopa Parlamendile suunatud andmevood, mis on seotud ENISA tegevuse ja ülesannete täitmisega; eelarve haldamise ja finantsjuhtimise, koostööga kolmandate riikide ja rahvusvaheliste organisatsioonidega, tegevdirektori kandidaadi kuulamisega; Euroopa küberturvalisuse sertifitseerimist puudutavate küsimustega.	Artikli 28 lõike 1 punkt f, artikli 31 lõige 8, artikli 32 lõige 3, artikli 44 lõige 3, artikli 49 lõige 6, artikli 49 lõige 9, artikli 70 lõige 5, artikli 72 lõiked 4 ja 5, artikli 119 lõige 3 „Delegeeritud volituste rakendamine“, artikkel 120 „Hindamine ja läbivaatamine“
Euroopa Liidu Nõukogule edastatavad andmed	Euroopa Parlamendile suunatud andmevood, mis on seotud ENISA tegevuse ja ülesannete täitmisega; eelarve haldamise ja finantsjuhtimisega, koostööga kolmandate riikide ja rahvusvaheliste organisatsioonidega, tegevdirektori kandidaadi kuulamisega; Euroopa küberturvalisuse sertifitseerimise raamistiku kohaselt väljatöötatavate ettevalmistavate kavadega.	Artikli 28 lõike 1 punkt f, artikli 31 lõige 8, artikli 32 lõige 3, artikli 32 lõige 7, artikli 49 lõiked 6 ja 9, artikli 70 lõige 5, artikli 72 lõiked 4 ja 5, artikli 119 lõige 3 „Delegeeritud volituste rakendamine“, artikkel 120 „Hindamine ja läbivaatamine“
Kaebuste esitamisega seotud andmevood	Füüsiliste või juriidiliste isikute kaebuste menetlemiseks seoses Euroopa küberturvalisuse sertifikaatidega, mille on välja andnud riiklikud küberturvalisuse sertifitseerimise asutused, või Euroopa küberturvalisuse sertifikaatidega, mille on välja andnud vastavushindamisasutused	Artikli 55 lõige 3, artikli 88 lõike 7 punkt f, artikkel 96

	kooskõlas artikli 84 lõikega 4, või seoses ELi vastavusdeklaratsioonidega. Füüsilistel ja juriidilistel isikutel on õigus esitada kaebus Euroopa küberturvalisuse sertifikaadi väljastajale, või kui kaebus on seotud vastavushindamisasutuse väljastatud Euroopa küberturvalisuse sertifikaadiga.	
Lunavararünnetega seotud andmevood	Teatavast teabest teatamine lunavararünnete korral	Direktiivi artikli 1 punkt 8

Andmete liik	**Viide (viited) nõudele (nõuetele)**	**Osalejad, kes andmed esitavad**	**Osalejad, kes andmed saavad**	**Andmevahetuse ajend**	**Sagedus (kui see on asjakohane)**
Komisjoni ja liikmesriikide vahelised andmevood seoses liidu tasandil turvariski koordineeritud hindamise tegemisega	Artikkel 99 Turvariski hindamine	Komisjon ja liikmesriigid	Liikmesriigid (võrgu- ja infoturbe koostöörühm)	Artikkel 99 Turvariski hindamine	Ei kohaldata
Komisjoni ja nõukogu vahelised andmevood seoses küberturvalisuse seisukohast muret tekitavate kolmandate riikide kindlaksmääramisega	Artikkel 100 Küberturvalisuse seisukohast muret tekitavate kolmandate riikide kindlaks määramine	Euroopa Komisjon	Nõukogu	Artikkel 100 Kolmandast riigist lähtuva ohu kontrollimine komisjoni poolt	

Andmete liik	**Viide (viited) nõudele (nõuetele)**	**Osalejad, kes andmed esitavad**	**Osalejad, kes andmed saavad**	**Andmevahetuse ajend**	**Sagedus (kui see on asjakohane)**
Komisjoni ja liikmesriikide vahelised andmevood seoses erakorraliste asjaoludega rakendatavate leevendusmeetmetega	Artikli 103 lõige 6 IKT tarneahelaga seotud leevendusmeetmed	Euroopa Komisjon	Liikmesriigid	Erakorralised asjaolud	Ei kohaldata
Komisjoni ja tarnijate ning komisjoni ja pädevate asutuste vahelised andmevood seoses tarnijate asutamise, omandiõiguse ja kontrolli hindamisega	Artikkel 104 lõiked 4, 5 ja 6 Suure riskiga tarnijate kindlakstegemine	Tarnijad Euroopa Komisjon Pädevad asutused	Pädevad asutused Tarnijad Euroopa Komisjon	Rakendusaktid, mis on vastu võetud kooskõlas artikli 103 lõikega 1 ja seoses artikli 111 lõikes 1 sätestatud keeluga	Ei kohaldata
Komisjoni ja liikmesriikide vaheline andmevoog seoses usaldusväärse IKT tarneahela turberaamistiku rakendamise järelevalvevolitustega	Artikli 112 lõiked 1 ja 4 Pädevad asutused Artikkel 114 Järelevalve- ja täitemeetmed	Liikmesriigid	Euroopa Komisjon	Artikli 112 lõiked 1 ja 4 Pädevad asutused Artikkel 114 Järelevalve- ja täitemeetmed (Komisjon avaldab koostöös liikmesriikidega suure riskiga tarnijatega seotud üksuste loetelu.)	Ei kohaldata

Andmete liik	**Viide (viited) nõudele (nõuetele)**	**Osalejad, kes andmed esitavad**	**Osalejad, kes andmed saavad**	**Andmevahetuse ajend**	**Sagedus (kui see on asjakohane)**
Komisjoni ja kolmandate isikute vaheline andmevoog seoses erandite tegemisega	Artikkel 105 Küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud üksustele või selles riigis asuvate üksuste kontrollitavatele üksustele erandi tegemine	Kolmandad isikud (küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud üksused või nendes riikides asuvate üksuste kontrollitavad üksused (artikli 100 tähenduses, eranditaotluse esitamisel)) Euroopa Komisjon (otsuste tegemisel)	Komisjon (eranditaotluse saamisel) Kolmandad isikud (küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud üksused või nendes riikides asuvate üksuste kontrollitavad üksused (artikli 100 tähenduses, komisjoni otsuse saamisel))	Artikli 100 „Küberturvalisuse seisukohast muret tekitavate kolmandate riikide kindlaks määramine“ kohane otsus	Ei kohaldata
Liikmesriikide ja kolmandate isikute vaheline andmevoog seoses elektroonilise side võrkudes kehtivate keeldudega	Artikkel 111 Elektroonilise side mobiili-, püsi- ja satelliitvõrkude puhul	Liikmesriigid (pädevad asutused)	Kolmandad isikud (elektroonilise side mobiili-, püsi- ja	Käesoleva määruse alusel määratud pädev asutus teavitab viivitamata määruse (EL)	Ei kohaldata

Andmete liik	Viide (viited) nõudele (nõuetele)	Osalejad, kes andmed esitavad	Osalejad, kes andmed saavad	Andmevahetuse ajend	Sagedus (kui see on asjakohane)
	kehtestatavad keelud		satelliitvõrkude pakkujad)	XX/XXXX [DNA ettepanek] kohast pädevat asutust meetmetest, mis on kehtestatud elektroonilise side mobiili-, püsi- ja satelliitvõrkude pakkujate suhtes.	
Komisjoni ja liikmesriikide vaheline andmevoog seoses koostöö- ja tugiteenuste võrgustikuga	Artikkel 113 Komisjoni koostöö- ja tugiteenuste võrgustik	Euroopa Komisjon Liikmesriigid (pädevad asutused)	Euroopa Komisjon Liikmesriigid (pädevad asutused)	Küberturvalisuse seisukohast muret tekitavate kolmandate riikide kindlaks määramine	
Liikmesriikide ja kolmandate isikute vaheline andmevoog seoses järelevalve- ja täitemeetmetega	Artikkel 114 Järelevalve- ja täitemeetmed	Kolmandad isikud (direktiivi (EL) 2022/2555 I ja II lisas osutatud laadi üksused)	Liikmesriigid (pädevad asutused)	IV jaotises ettenähtud meetmete rakendamine	
Liikmesriikidevaheline andmevoog seoses vastastikuse abiga	Artikkel 116 Vastastikune abi	Liikmesriigid	Liikmesriigid	Kui direktiivi (EL) 2022/2555 I või II lisas osutatud üksus osutab	Ei kohaldata

Andmete liik	Viide (viited) nõudele (nõuetele)	Osalejad, kes andmed esitavad	Osalejad, kes andmed saavad	Andmevahetuse ajend	Sagedus (kui see on asjakohane)
				teenuseid rohkem kui ühes liikmesriigis või osutab teenuseid ühes või mitmes liikmesriigis ja tema peamised IKT-varad asuvad ühes või mitmes teises liikmesriigis, teevad asjaomaste liikmesriikide pädevad asutused omavahel koostööd ja vajaduse korral abistavad üksteist.	

4.3. Digilahendused

Digilahenduste üldine kirjeldus

Iga digilahenduse puhul selgitus selle kohta, kuidas digilahendus vastab kohaldatavale digipoliitikale ja õigusaktidele

Digilahendus	Viide (viited) nõudele (nõuetele)	Peamised volitatud funktsioonid	Vastutav asutus	Kuidas on arvesse võetud juurdepääsetavust?	Kuidas on arvesse võetud korduvkasutatavust?	Tehisintellektitehnoloogia kasutamine (kui see on asjakohane)
ENISA on **CSIRTide**						

võrgustiku ja EU-CyCLONe sekretariaat ning võtab CSIRTide võrgustikus ja EU-CyCLONe-s kasutusele **turvalised sidevahendid**, mida pakuvad juriidilised isikud, mis ei ole asutatud kolmandates riikides ja mida ei ole asutanud kolmandate riikide kodanikud ning mis ei ole nende kontrolli all.	Artikli 10 lõiked 2, 3 ja 5	Ei ole avalik teave	ENISA	Ei ole avalik teave	Ei ole avalik teave	Ei ole avalik teave
Koostöös EU-CyCLONe, CSIRTide võrgustiku, komisjoni, Europoli ja CERT-EU ning asjaomaste liidu üksustega töötatakse välja **kontrollitud ja usaldusväärse küberohuteadmuse** (sh intsidentide, taktika, meetodite ja menetluste suundumused) **hoidlad**.	Artikli 11 lõike 1 punkt a	Kontrollitud ja usaldusväärne küberohuteadmus, sh intsidentide, taktika, meetodite ja menetluste suundumused	ENISA EU-CyCLONe, CSIRTide võrgustik, komisjon, Europol ja CERT-EU ning asjaomased liidu üksused	Ei kohaldata	Ei kohaldata	Ei kohaldata
ENISA **peab saadud kogemuste andmebaasi**.	Artikli 14 lõige 2	ENISA peab õppuste käigus saadud kogemuste andmebaasi ning soovitab liikmesriikidele ja vajaduse korral liidu üksustele, kuidas saadud	ENISA	Ei kohaldata	Ei kohaldata	Ei kohaldata

		kogemusi saaks tulemuslikult ja tõhusalt rakendada.				
ENISA võtab kasutusele, pakub, käitab, haldab ja vajaduse korral ajakohastab tehnilisi operatiivvahendeid, näiteks liidu tasandi küberturvalisuse **platvorme**, eelkõige määruse (EL) 2024/2847 artikli 16 lõike 1 kohaselt loodud ühtset teatamisplatvormi [ja direktiivi (EL) 2022/2555 artikli 23a kohaselt loodud intsidentidest teatamise ühtset kontaktpunkti], või testimisvahendeid, et toetada vastavushindamismenetluste rakendamist kooskõlas asjakohaste liidu õigusaktidega.	Artikkel 15	Ühtne teatamisplatvorm Määruse (EL) 2024/2847 artikli 16 lõige 1 [ühtne kontaktpunkt direktiivi (EL) 2022/2555 artikkel 23a]	ENISA	Ei kohaldata	Ei kohaldata	Ei kohaldata
Direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasi haldamine ja **nõrkushalduse teenuste osutamine**	Artikli 16 lõige 2	Direktiivi (EL) 2022/2555 artikli 12 lõige 2 Andmebaasi haldamine ja nõrkushalduse teenuste osutamine	ENISA	Ei kohaldata	Ei kohaldata	Ei kohaldata
ENISA haldab ja ajakohastab korrapäraselt		Spetsiaalse veebisaidi –	ENISA	Ei kohaldata	Ei kohaldata	Ei kohaldata

spetsiaalset veebisaiti, mis pakub avalikku teavet.	Artiklid 19–23	mis pakub avalikku teavet Euroopa küberturbeoskuste raamistiku kohta, sh raamistiku ja selle ajakohastamise ajakava kohta – haldamine ja korrapärane ajakohastamine; Euroopa individuaalsete küberturbeoskuste tõendamise kavad, nende kulg ja nende väljatöötamise ajakava; iga Euroopa individuaalsete küberturbeoskuste tõendamise kavaga seotud tasud; Euroopa individuaalsete küberturbeoskuste tõendamise soovituslik maksumus; volitatud tõendajate loetelu.				
Komisjon haldab ja ajakohastab korrapäraselt spetsiaalset avalikku veebisaiti	Artikkel 72	Järgmine teave: a) Euroopa küberturvalisuse sertifitseerimise kavad, mille väljatöötamist taotletakse; b) strateegilised	Euroopa Komisjon	Suuniste järgimine	Suuniste järgimine	Ei kohaldata

		prioriteedid IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ning liidu õigusaktides sätestatud turvanõuete ühtlustamiseks, sh võimalikud valdkonnad, mille tarbeks võidakse taotleda Euroopa küberturvalisuse sertifitseerimise kava.				
ENISA haldab spetsiaalset sertifitseerimise veebisaiti	Artikkel 79	Teabe jagamine järgmise kohta: a) Euroopa küberturvalisuse sertifitseerimise kavad; b) iga Euroopa küberturvalisuse sertifitseerimise kava haldamisega seotud tasud; c) asjakohased ENISA tehnilised kirjeldused; d) Euroopa küberturvalisuse sertifikaadid ja ELi vastavusdeklaratsioonid, sh teave selliste sertifikaatide ja	ENISA	Suuniste järgimine	Suuniste järgimine	Ei kohaldata

		deklaratsioonide kohta, mis enam ei kehti või mis on peatatud, kehtetuks tunnistatud või aegunud; e) artikli 84 lõike 2 kohaselt esitatud asjakohane täiendav küberturvalisuse alane teave; f) vastastikuste eksperdihinnangute kokkuvõtted kooskõlas artikli 89 lõikega 7; g) Euroopa küberturvalisuse sertifitseerimise kavas märgitud tehnilised kirjeldused kooskõlas artikli 74 lõikega 10.				
Register (erandite kohta, mida kohaldatakse üksuste suhtes, mis on asutatud küberturvalisuse seisukohast muret tekitavates kolmandates riikides või mis on nendes riikides asuvate üksuste kontrollitavad üksused)	Artikkel 107 Register	Komisjon peab artikli 105 lõikes 4 osutatud otsuste kohta avalikku registrit. Registris märgitakse nende üksuste nimed, mille suhtes on kõnealused otsused tehtud. Komisjon	Euroopa Komisjon	„Komisjon peab avalikku registrit.“	Ei kohaldata	Ei kohaldata

		ajakohastab seda korrapäraselt.				
Platvorm (komisjoni ja pädevate asutuste vaheliseks koostööks ja teabevahetuseks)	Artikkel 113	Komisjon loob liikmesriikide pädevate asutuste ja komisjoni koostöövõrgustiku, mis toimib koostöö- ja teabevahetusplatvormina. Komisjon pakub võrgustikule haldustuge.	Euroopa Komisjon	Ei ole avalik, üksnes pädevatele asutustele.	Ei kohaldata	Ei kohaldata
ENISA loob elutähtsate ja oluliste üksuste ja domeeninimede registreerimise teenuseid osutavate üksuste **registri ning haldab seda**.	Direktiivi artikli 1 punkt 11	Elutähtsate ja oluliste üksuste ning domeeninimede registreerimise teenuseid osutavate üksuste register	ENISA	Ei kohaldata	Ühtsetelt kontaktpunktidelt lõike 2 kohaselt saadud teabe põhjal (küberturvalisuse 2. direktiivi artikkel 27).	Ei kohaldata

Eespool esitatud tabelis sisalduvad digilahendused

Digi- ja/või valdkondlik poliitika (kui see on asjakohane)	Selgitus selle kohta, kuidas see on kooskõlas
Tehisintellektimäärus	Ei kohaldata
ELi küberturvalisuse raamistik	Ei kohaldata
eIDAS	Ei kohaldata
Ühtne digivärav ja siseturu infosüsteem	Ei kohaldata
Muu	Ei kohaldata

Üldine kirjeldus digitaalsete avalike teenuste kohta, mida nõuded mõjutavad

Digitaalne avalik teenus või digitaalsete avalike teenuste kategooria	Kirjeldus	Viide (viited) nõudele (nõuetele)	Koostalitleva Euroopa lahendus(ed) (EI KOHALDATA)	Muu(d) koostalitluslahendus(ed)
ENISA kui võrgustike sekretariaat ja turvaliste sidevahendite kasutuselevõtt	ENISA tagab CSIRTide võrgustiku sekretariaadi teenused vastavalt direktiivi (EL) 2022/2555 artikli 15 lõikele 2. ENISA tagab EU-CyCLONe-le sekretariaadi teenused vastavalt direktiivi (EL) 2022/2555 artikli 16 lõikele 2 [ja intsidentidest teatamise ühtse kontaktpunkti, mis on loodud vastavalt direktiivi (EL) 2022/2555 artiklile 23a] ning testimisvahendid, et toetada	Artikkel 11	//	Ei kohaldata

	vastavushindamismenetluste rakendamist kooskõlas asjakohaste liidu õigusaktidega. ENISA võtab CSIRTide võrgustikus ja EU-CyCLONe-s kasutusele turvalised sidevahendid, mida pakuvad juriidilised isikud, mis ei ole asutatud kolmandates riikides ja mida ei ole asutanud kolmandate riikide kodanikud ning mis ei ole nende kontrolli all.			
Varajased hoiatused	Varajaste hoiatuste väljastamine	Artikkel 11 Artikkel 12		
Konkreetse võimaliku või käimasoleva intsidendi või küberohuga seoses pakutav tugi	Ühe või mitme liikmesriigi taotlusel konsulteerimine ja hindamiste tegemine seoses konkreetse võimaliku või käimasoleva intsidendi või küberohuga, sh oskusteabe pakkumine ja intsidentide tehnilise käsitlemise hõlbustamine ning asjakohase teabe ja tehniliste lahenduste vabatahtliku jagamise toetamine liikmesriikide vahel.	Artikkel 10		
Ulatuslike küberintsidentide ja -kriiside koordineeritud ohjamise toetamine operatiivtasandil	Ulatuslike küberintsidentide ja -kriiside koordineeritud ohjamise toetamisele kaasaaitamine operatiivtasandil, eelkõige aidates EU-CyCLONe-l koostada aruandeid poliitika tasandil, hõlbustades õigeaegset teabevahetust CSIRTide võrgustiku ja EU-CyCLONe vahel.	Artikkel 10		
Kontrollitud ja usaldusväärse küberohuteadmuse hoidlad	Koostöös EU-CyCLONe, CSIRTide võrgustiku, komisjoni, Europoli ja CERT-EU ning asjaomaste liidu üksustega kontrollitud ja usaldusväärse küberohuteadmuse (sh intsidentide,	Artikkel 11		

	taktika, meetodite ja menetluste suundumused) hoidlate väljatöötamine.			
Saadud kogemuste andmebaas	ENISA peab asjaomastest õppustest saadud kogemuste andmebaasi ning annab liikmesriikidele ja vajaduse korral liidu üksustele soovitusi, kuidas saadud kogemusi saaks tulemuslikult ja tõhusalt rakendada.	Artikkel 14		
ENISA võtab kasutusele, pakub, käitab, haldab ja vajaduse korral ajakohastab tehnilisi operatiivvahendeid, näiteks platvorme.	ENISA võtab kasutusele, pakub, käitab, haldab ja vajaduse korral ajakohastab tehnilisi operatiivvahendeid, näiteks liidu tasandi küberturvalisuse platvorme, eelkõige määruse (EL) 2024/2847 artikli 16 lõike 1 kohaselt loodud ühtset teatamisplatvormi [ja direktiivi (EL) 2022/2555 artikli 23a kohaselt loodud intsidentidest teatamise ühtset kontaktpunkti], ning testimisvahendeid, et toetada vastavushindamismenetluste rakendamist kooskõlas asjakohaste liidu õigusaktidega.	Artikkel 15		
Direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasi haldamine	Direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasi haldamine. Sidusrühmadele nõrkusehalduse teenuste osutamine, tuginedes Euroopa nõrkuste andmebaasile ja kasutades ENISA-le kättesaadavat asjakohast teavet. Struktureeritud koostöö organisatsioonidega, kes pakuvad Euroopa nõrkuste andmebaasiga sarnaseid programme, registreid või andmebaase. Direktiivi (EL) 2022/2555 artikli 12	Artikkel 16		

	lõike 1 kohaselt koordinaatoriteks määratud CSIRTe aktiivne toetamine seoses selliste nõrkuste koordineeritud avalikustamise haldamisega, millel võib olla märkimisväärne mõju rohkem kui ühe liikmesriigi üksustele. Koostöös riiklike pädevate asutuste, CSIRTide, tööstuse ja teadusringkondadega nõrkuste tuvastamise ja koordineeritud avalikustamise metoodika ja juhtimismehhanismide väljatöötamine ning nende haldamine.			
Euroopa küberturvalisuse sertifitseerimise ettevalmistavate kavade väljatöötamine	Üksuste IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ning turvaoleku Euroopa küberturvalisuse sertifitseerimise ettevalmistavate kavade väljatöötamine ja nendega seotud tehnilised kirjeldused kooskõlas artikliga 74. Vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade haldamine kooskõlas artikliga 75, sh võttes arvesse vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade võimalikku läbivaatamist kooskõlas artikliga 76.	Artikkel 17		
ENISA töötab välja Euroopa individuaalsete küberturbeoskuste tõendamise kavad ja tegeleb nende haldamisega	ENISA töötab välja Euroopa individuaalsete küberturbeoskuste tõendamise kavad ja tegeleb nende haldamisega. ENISA teeb põhjendatud otsuse, millega antakse taotlejale luba välja anda individuaalseid Euroopa tunnistusi kavade täitmiseks ja	Artiklid 20–22		

	haldamiseks või otsuse, millega ei anta taotlejale luba või millega lõpetatakse taotluse menetlemine taotleja esitatud ebapiisava teabe või lisateabe taotlusele vastamata jätmise tõttu.			
ENISA haldab ja ajakohastab korrapäraselt spetsiaalset veebisaiti	ENISA haldab ja ajakohastab korrapäraselt sihtotstarbelist veebisaiti, millel on esitatud avalik teave järgmise kohta: a) Euroopa küberturbeoskuste raamistik, sh selle ajakohastamise struktuur ja ajakava; b) Euroopa individuaalsete küberturbeoskuste tõendamise kavad, nende kulg ja nende väljatöötamise ajakava; c) iga käesoleva määruse artikli 47 kohaselt vastu võetud Euroopa individuaalsete küberturbeoskuste tõendamise kavaga seotud tasud; d) Euroopa individuaalsete küberturbeoskuste tõendi hinnanguline maksumus kooskõlas artikli 20 lõikega 4; e) volitatud tõendajate loetelu.	Artikkel 23		
Komisjon haldab ja ajakohastab korrapäraselt spetsiaalset avalikku veebisaiti	Komisjon haldab ja ajakohastab korrapäraselt sihtotstarbelist veebisaiti, millel esitatakse teavet järgmiste aspektide kohta: a) Euroopa küberturvalisuse sertifitseerimise kavad, mille väljatöötamist taotletakse; b) strateegilised prioriteedid IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ning liidu	Artikkel 72		

	õigusaktides sätestatud turvanõuete ühtlustamiseks, sh võimalikud valdkonnad, mille tarbeks võidakse taotleda Euroopa küberturvalisuse sertifitseerimise kava.			
ENISA haldab spetsiaalset sertifitseerimise veebisaiti	ENISA haldab ja ajakohastab korrapäraselt sihtotstarbelist veebisaiti, millel on esitatud avalik teave järgmise kohta: a) Euroopa küberturvalisuse sertifitseerimise kavad; b) iga Euroopa küberturvalisuse sertifitseerimise kava haldamisega seotud tasud; c) asjakohased ENISA tehnilised kirjeldused; d) Euroopa küberturvalisuse sertifikaadid ja ELi vastavusdeklaratsioonid, sh teave selliste sertifikaatide ja deklaratsioonide kohta, mis enam ei kehti või mis on peatatud, kehtetuks tunnistatud või aegunud; e) artikli 84 lõike 2 kohaselt esitatud asjakohane täiendav küberturvalisuse alane teave; f) vastastikuste eksperdihinnangute kokkuvõtted kooskõlas artikli 89 lõikega 7; g) Euroopa küberturvalisuse sertifitseerimise kavas märgitud tehnilised kirjeldused kooskõlas artikli 74 lõikega 10.	Artikkel 79		
Uurimised	Komisjon uurib iga juhtumit, mille puhul tal on kahtlusi või talle on teatatud kahtlustest seoses	Artikkel 94		

	vastavushindamisasutuse pädevusega täita tema suhtes kehtivaid nõudeid ja kohustusi või seoses sellega, kas vastavushindamisasutus täidab neid jätkuvalt. Komisjon tagab, et kogu tundlikku teavet, mis uurimise käigus saadi, käsitletakse konfidentsiaalsena.			
ENISA loob elutähtsate ja oluliste üksuste ning domeeninimede registreerimise teenuseid osutavate üksuste registri ja haldab seda	Elutähtsate ja oluliste üksuste ning domeeninimede registreerimise teenuseid osutavate üksuste register. Taotluse korral võimaldab ENISA pädevatele asutustele juurdepääsu domeeninimede süsteemi teenuse osutajaid, tippdomeeninimede registreid, domeeninimede registreerimise teenuseid osutavaid üksusi, pilvandmetöötlusteenuse osutajaid, andmekeskusteenuse osutajaid, sisulevivõrgu pakkujaid, hallatud teenuse osutajaid, turbetarnijaid ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite ja sotsiaalvõrguteenuse platvormide pakkujaid käsitlevale teabele, mida säilitatakse asjaomases registris, samal ajal tagades vajaduse korral teabe konfidentsiaalsuse kaitse.	Direktiivi artikli 1 punkt 11		

4.4. Koostalitlusvõime hindamine

Nõude (nõuete) mõju piiriülesele koostalitlusvõimele digitaalsete avalike teenuste kaupa

Andmebaasid / platvormid / varajased hoiatused / sekretariaat / operatiivkoostöö / nõrkuste koordineeritud avalikustamise andmebaas

Hindamine	Meetmed	Võimalikud allesjäänud tõkked
Hinnake kooskõla kehtivate digi- ja valdkondlike poliitikameetmetega Loetlege kohaldatavad kindlakstehtud digi- ja valdkondlikud poliitikameetmed	*Küberturvalisus*	*Teadaolevad tõkked puuduvad*
Hinnake korralduslikke meetmeid digitaalsete avalike teenuste sujuvaks osutamiseks Loetlege kavandatud juhtimismeetmed	*ENISA haldusnõukogu* *CSIRTide võrgustik* *EU-CyCLONe* *Võrgu- ja infoturbe koostöörühm* *Kõik need on foorumid, kus saab küsimusi tõstatada.*	*Ei kohaldata*
Hinnake meetmeid, mis on võetud andmete ühise mõistmise tagamiseks Loetlege sellised meetmed	*Ei kohaldata*	*Ei kohaldata*
Hinnake ühiselt kokku lepitud avalike tehniliste kirjelduste ja standardite kasutamist Loetlege sellised meetmed	*Ei kohaldata*	*Ei kohaldata*

Euroopa individuaalsete küberturbeoskuste tõendamise kavad

Hindamine	Meetmed	Võimalikud allesjäänud tõkked
Hinnake kooskõla kehtivate digi- ja valdkondlike poliitikameetmetega Loetlege kohaldatavad kindlakstehtud digi- ja valdkondlikud poliitikameetmed	*Ettepanek põhineb teatisel COM(2023)207 final (küberturbeoskuste akadeemia) – ENISA töötab Euroopa küberturbeoskuste tõendamise kava koostamise uurimiseks välja katseprojekti.* *Selleks kasutatakse määrust (EL) 2024/1183 (Euroopa digiidentiteedikukkur), kehtestades, et ENISA ja volitatud tõendajad tagavad, et*	*Teadaolevad tõkked puuduvad*

	Euroopa individuaalsete küberturbeoskuste tõendamise raames välja antud elektroonilised tõendid edastatakse Euroopa digiidentiteedikukrutele. *Küberturvalisus* *Isikuandmete kaitse üldmäärus (andmete säilitamine tõendajate poolt)*	
Hinnake korralduslikke meetmeid digitaalsete avalike teenuste sujuvaks osutamiseks **Loetlege kavandatud juhtimismeetmed**	*Sidusrühmadega konsulteerimine Euroopa individuaalsete küberturbeoskuste tõendamise kava koostamisel.* *Tegevuste eraldamine ENISAs, et tagada selle sõltumatu toimimine.* *Apellatsiooninõukogu*	*Euroopa individuaalsete küberturbeoskuste tõendamise kavade kasutamine ja tunnustamine jääb avaliku ja erasektori üksuste jaoks vabatahtlikuks.*
Hinnake meetmeid, mis on võetud andmete ühise mõistmise tagamiseks **Loetlege sellised meetmed**	*Selliste kavade väljatöötamine, milles täpsustatakse muu hulgas tõendite sisu ja vormi käsitlevad eeskirjad* *Volitatud tõendajad tagavad, et isiku taotlusel antakse Euroopa individuaalsete küberturbeoskuste tõendamise raames välja elektrooniline tunnistus, mida saab salvestada Euroopa digiidentiteedikukrutesse, et ENISA saaks anda hindajatele suuniseid ja korraldada kohustuslikku koolitust seoses Euroopa individuaalsete küberturbeoskuste tõendamise kavas sisalduvate nõuete ja hindamismeetoditega.* *Avaliku teabe jagamine veebisaidil* *Tasusid käsitlevad rakendusaktid*	*Olenemata sellest, et kavad peavad olema piisavalt üksikasjalikud, et tagada ühine arusaamine ja lihtsustada rakendamist, ning kuigi ENISA annab hindajatele suuniseid ja korraldab nende kohustuslikku koolitust, et tagada kavade ühetaoline rakendamine, võivad esile kerkida ettenägematud asjaolud, mille puhul volitatud tõendajad peavad suhtlema ENISA, teiste tõendajate või hindajatega.*
Hinnake ühiselt kokku lepitud avalike tehniliste kirjelduste ja standardite kasutamist	*Euroopa individuaalsete küberturbeoskuste tõendamise kavad töötatakse välja asjaomaste*	*Ei kohaldata*

Loetlege sellised meetmed	*sidusrühmade toel.*	

Euroopa küberturvalisuse sertifitseerimise ettevalmistavate kavade väljatöötamine / numbrite määramine vastavushindamisasutustele

Hindamine	**Meetmed**	**Võimalikud allesjäänud tõkked**
Hinnake kooskõla kehtivate digi- ja valdkondlike poliitikameetmetega **Loetlege kohaldatavad kindlakstehtud digi- ja valdkondlikud poliitikameetmed**	*Ettepaneku eesmärk on viia juhtimine kooskõlla uue õigusraamistikuga, eelkõige määruse (EÜ) nr 765/2008[26] puhul.* *Ettepaneku eesmärk on hõlbustada asjakohaste küberturvalisuse alaste valdkondlike õigusaktide järgimist spetsiaalsete Euroopa küberturvalisuse sertifitseerimise kavade väljatöötamise kaudu.*	*Teadaolevad tõkked puuduvad*
Hinnake korralduslikke meetmeid digitaalsete avalike teenuste sujuvaks osutamiseks **Loetlege kavandatud juhtimismeetmed**	*Euroopa küberturvalisuse sertifitseerimise rühm;* *ENISA;* *ajutised töörühmad;* *Euroopa küberturvalisuse sertifitseerimise assamblee;* *konsulteerimine sidusrühmadega Euroopa küberturvalisuse sertifitseerimise kavade taotlemisel, väljatöötamisel ja vastuvõtmisel;* *komiteemenetlused Euroopa küberturvalisuse sertifitseerimise kavadega seotud kavandatavate rakendusaktide jaoks.*	*Euroopa küberturvalisuse sertifitseerimise kasutamine on vabatahtlik, kui Euroopa õigusaktides ei ole sätestatud teisiti.*
Hinnake meetmeid, mis on võetud andmete ühise mõistmise tagamiseks **Loetlege sellised meetmed**	*Punktis 4.5 loetletud rakendusaktid.*	*Euroopa küberturvalisuse sertifitseerimise kasutamine on vabatahtlik, kui Euroopa õigusaktides ei ole sätestatud teisiti.*
Hinnake ühiselt kokku lepitud avalike tehniliste kirjelduste ja standardite kasutamist	*Punktis 4.5 loetletud rakendusaktid.* *Euroopa küberturvalisuse sertifitseerimise kava täpsustatud nõuded peavad olema kooskõlas*	*Ei kohaldata*

Loetlege sellised meetmed	*liidu õigusaktide nõuetega.* *Euroopa küberturvalisuse sertifitseerimise kavade puhul kasutatakse hindamisel kohaldatud rahvusvahelisi, Euroopa või riiklikke standardeid ja viidatakse neile, või kui sellised standardid ei ole kättesaadavad või asjakohased, siis ENISA koostatud tehnilisi kirjeldusi.*	

Avalikud veebisaidid

Hindamine	Meetmed	Võimalikud allesjäänud tõkked
Hinnake kooskõla kehtivate digi- ja valdkondlike poliitikameetmetega **Loetlege kohaldatavad kindlakstehtud digi- ja valdkondlikud poliitikameetmed**	*ELi ligipääsetavuse akt ja veebi juurdepääsetavuse direktiiv* *Küberturvalisus*	*Teadaolevad tõkked puuduvad*
Hinnake korralduslikke meetmeid digitaalsete avalike teenuste sujuvaks osutamiseks **Loetlege kavandatud juhtimismeetmed**	*Ei kohaldata*	*Ei kohaldata*
Hinnake meetmeid, mis on võetud andmete ühise mõistmise tagamiseks **Loetlege sellised meetmed**		*Ei kohaldata*
Hinnake ühiselt kokku lepitud avalike tehniliste kirjelduste ja standardite kasutamist **Loetlege sellised meetmed**		*Ei kohaldata*

4.5. Digimõõtme rakendamist toetavad meetmed

Digitaalset rakendamist toetavate meetmete üldine kirjeldus

Meetme kirjeldus	**Viide (viited) nõudele (nõuetele)**	**Komisjoni roll** (kui see on asjakohane)	**Kaasatavad osalejad** (kui see on asjakohane)	**Eeldatav ajakava** (kui see on asjakohane)
Komisjonil on ENISA koostatud ettevalmistava kava alusel, mille komisjon on heaks kiitnud, volitus võtta vastu rakendusakte, millega sätestatakse IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste või üksuste turvaoleku Euroopa küberturvalisuse sertifitseerimise kava, mis vastab artiklites 80 ja 81 sätestatud nõuetele. Nimetatud rakendusakt võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.	Artikli 75 lõige 9	Komisjonil on õigus võtta vastu rakendusakte		Ei kohaldata
Komisjonil on õigus võtta kooskõlas artikliga 119 vastu delegeeritud õigusakte, et muuta käesoleva artikli lõiget 1, lisades või muutes turvalisusega seotud eesmärke, tagamaks, et need kajastavad uusimaid tehnoloogia arenguid ja uusi seonduvaid ohte, ning võtta vastu uusi liidu õigusakte, milles sätestatakse eeldus, et Euroopa küberturvalisuse sertifitseerimise kaudu on tagatud vastavus kõnealustes õigusaktides sätestatud asjakohastele küberturvalisuse nõuetele.	Artikli 80 lõige 2	Komisjonil on õigus võtta vastu delegeeritud õigusakte		Ei kohaldata
Komisjonil on volitus võtta vastu rakendusakte, millega kehtestatakse ühised	Artikli 81 lõige 5	Komisjonil on õigus võtta vastu	ENISA ECCG	Ei kohaldata

põhimõtted ja näidissätted lõigetes 1, 2 ja 3 sätestatud elementide kohta Euroopa küberturvalisuse sertifitseerimise kavade puhul. Kui see on asjakohane ja kättesaadav, siis võib Euroopa küberturvalisuse sertifitseerimise kava sisaldada viiteid kõnealustele põhimõtetele ja näidissätetele. Esimeses lõigus osutatud rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega. Euroopa küberturvalisuse sertifitseerimise kavade jaoks ühispõhimõtete ja näidissätete koostamisel või muutmisel konsulteerib komisjon ENISAga ja võtab vajaduse korral arvesse Euroopa küberturvalisuse sertifitseerimise rühma, asjaomaste sidusrühmade ja muude asjaomaste asutuste arvamusi.		rakendusakte		
Komisjonil on volitus võtta vastu rakendusakte, milles määratakse kindlaks käesoleva artikli lõikes 4 osutatud eelneva heakskiidu või üldise delegeerimise mudelite menetlused. Rakendusaktide ettevalmistamisel konsulteerib komisjon Euroopa küberturvalisuse sertifitseerimise rühmaga. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.	Artikli 85 lõige 5	Komisjonil on õigus võtta vastu rakendusakte	ECCG	Ei kohaldata

IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ja üksuste turvaoleku kolmandate riikide sertifikaate võib tunnustada võrdväärsena Euroopa küberturvalisuse sertifikaatidega rakendusaktiga või liidu ja kõnealuse kolmanda riigi või rahvusvahelise organisatsiooni vahel lepingu sõlmimise teel, kui asjaomase kolmanda riigi või rahvusvahelise organisatsiooni kava nõudeid peetakse Euroopa küberturvalisuse sertifitseerimise kava nõuetega võrdväärseks. Komisjonil on õigus selliseid rakendusakte vastu võtta. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.	Artikli 87 lõige 1	Komisjonil on õigus võtta vastu rakendusakte		Ei kohaldata
Komisjonil on õigus võtta vastu rakendusakte, millega kehtestatakse vastastikuse hindamise kava, mis hõlmab vähemalt viit aastat, sätestatakse vastastikuse hindamise rühma koosseisu kriteeriumid, vastastikuse hindamise metoodika, ajakava, sagedus ja muud vastastikuse hindamisega seotud ülesanded. Rakendusaktide ettevalmistamisel konsulteerib komisjon Euroopa küberturvalisuse sertifitseerimise rühmaga ja ENISAga. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2	Artikli 89 lõige 6	Komisjonil on õigus võtta vastu rakendusakte		Ei kohaldata

osutatud kontrollimenetlusega.				
Komisjonil on õigus võtta vastu rakendusakte, et kehtestada vastavushindamisasutustele loa andmise menetlused, sh piiriülese koostöö kohta. Rakendusaktide väljatöötamise käigus konsulteerib komisjon ENISA ja Euroopa küberturvalisuse sertifitseerimise rühmaga. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.	Artikli 92 lõige 8	Komisjonil on õigus võtta vastu rakendusakte	ENISA ECCG	Ei kohaldata
Komisjonil on õigus võtta vastu rakendusakte, et kehtestada käesoleva artikli lõikes 1 osutatud teavitamise asjaolud, vormingud ja kord, sh teiste liikmesriikide vastuväidete esitamise kord teavitamisprotsessi ajal, vastavushindamisasutuste kordumatu identifitseerimistunnus ning teavitamise piiramise, peatamise või kehtetuks tunnistamise asjaolud. Need rakendusaktid võetakse vastu kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega.	Artikli 93 lõige 3	Komisjonil on õigus võtta vastu rakendusakte		Ei kohaldata
Komisjon võib võtta kooskõlas artikliga 100 vastu rakendusakte kolmanda riigi kindlaksmääramiseks, kes põhjustab IKT tarneahelates küberturvalisuse probleeme.	Artikli 100 lõige 2 Küberturvalisuse seisukohast muret tekitavate kolmandate riikide kindlaks määramine	Rakendusaktide vastuvõtmine		Ei kohaldata Ajakava puudub, kuid rakendusaktid tuleks korrapäraselt läbi vaadata

Komisjon võib võtta vastu rakendusakte, et näha ette üks või mitu artikli 103 lõikes 2 osutatud leevendusmeedet.	Artikli 103 lõige 2 IKT tarneahelaga seotud leevendusmeetmed	Rakendusaktide vastuvõtmine	Ei kohaldata	Ei kohaldata Ajakava puudub, kuid läbivaatamine toimub iga 36 kuu järel (kooskõlas artikli 118 lõikes 2 osutatud kontrollimenetlusega)
Komisjon võib võtta kooskõlas artikliga 102 vastu rakendusakte, et teha kindlaks peamised IKT-varad, mida kasutatakse toodete tootmiseks või teenuste osutamiseks direktiivi (EL) 2022/2555 I ja II lisas osutatud liiki üksuste poolt.	Artikli 102 lõige 1 Oluliste IKT-varade kindlaksmääramine	Rakendusaktide vastuvõtmine	Ei kohaldata	Ei kohaldata
Komisjon võib võtta vastu rakendusakte, millega keelatakse artikli 100 lõike 2 kohaselt kindlaks määratud suure riskiga tarnijate IKT-komponentide või komponentide, mis sisaldavad nende tarnijate IKT-komponente, artikli 102 kohaselt kindlaks määratud peamistes IKT-varades mis tahes kujul kasutamine, nendesse paigaldamine või integreerimine.	Artikli 103 lõige 1 IKT tarneahelaga seotud leevendusmeetmed	Rakendusaktide vastuvõtmine	Ei kohaldata	Ei kohaldata
Komisjon võib võtta vastu rakendusakte, millega kehtestatakse, et direktiivi (EL) 2022/2555 I ja II lisas osutatud teatud liiki üksustel on keelatud kasutada, paigaldada või integreerida konkreetse üksuse IKT-komponente või komponente,	Artikli 103 lõige 7	Rakendusaktide vastuvõtmine	Konsulteerimine liikmesriikide ja asjaomaste üksustega	Ei kohaldata

mis sisaldavad konkreetse üksuse IKT-komponente.				
Komisjon kehtestab rakendusaktidega loetelud suure riskiga tarnijatest, kelle suhtes kohaldatakse artikli 103 lõike 1 kohaselt vastu võetud rakendusaktides sätestatud keelde või artikli 111 lõikes 1 osutatud keeldu.	Artikli 104 lõige 1	Rakendusaktide vastuvõtmine	Ei kohaldata	Ei kohaldata
Komisjon võib võtta vastu rakendusakte, et veelgi täpsustada artikli 105 lõike 2 punktis b osutatud tingimusi ja kehtestada üksikasjalikud eeskirjad artiklis 105 osutatud korra kohta.	Artikkel 105 Erandi tegemine küberturvalisuse seisukohast muret tekitavas kolmandas riigis asutatud või sellise kolmanda riigi üksuste kontrolli all olevatele üksustele	Rakendusaktide vastuvõtmine	Ei kohaldata	Ei kohaldata
Komisjon võib võtta vastu rakendusakte, millega kehtestatakse tasudega seotud üksikasjalikud eeskirjad, täpsustades tasude summad ja nende maksmise viisi.	Artikkel 109 Tasud	Rakendusaktide vastuvõtmine	Ei kohaldata	Ei kohaldata
Komisjon võtab vastu rakendusakte, et määrata seoses elektroonilise side püsi- ja satelliitvõrkudega kindlaks ajakava suure riskiga tarnijate pakutavate IKT-komponentide või komponentide, mis sisaldavad nende tarnijate IKT-komponente, järkjärguliseks kasutuselt kõrvaldamiseks.	Artikli 110 lõige 4 Elektroonilise side mobiili-, püsi- ja satelliitvõrkude olulised IKT-varad	Rakendusaktide vastuvõtmine	Ei kohaldata	Ei kohaldata
Komisjon võib kooskõlas artikliga 119 võtta vastu delegeeritud õigusakte II lisa muutmiseks, et kohandada seda	Artikli 110 lõige 5	Delegeeritud õigusaktide vastuvõtmine	Ei kohaldata	Ei kohaldata

tehnoloogia arengutega, võttes arvesse artikli 103 lõikes 3 osutatud elemente.				
7. Artikli 21 lõiget 5 muudetakse järgmiselt: a) teine lõik asendatakse järgmisega: „Komisjon võib võtta vastu rakendusakte, milles sätestatakse lõikes 2 osutatud meetmete tehnilised ja metoodilised nõuded ning vajaduse korral valdkondlikud nõuded seoses muude kui käesoleva lõike esimeses lõigus osutatud elutähtsate ja oluliste üksustega. Siseturu toimimise parandamiseks hindab komisjon korrapäraselt, kas käesolevas lõigus osutatud rakendusaktid võetakse vastu konkreetsete sektorite või üksuste liikide kohta. Nende hindamiste tulemuste põhjal võib komisjon teha ettepanekuid nimetatud rakendusaktide vastuvõtmiseks kindlaksmääratud sektorite või üksuste liikide kohta. Selliste hindamiste väljatöötamisel keskendub komisjon eelkõige sektorite või üksuste liikide piiriülesele olemusele ning viib läbi avatud, läbipaistva ja kaasava konsultatsiooniprotsessi asjaomaste sidusrühmade ja liikmesriikidega.“ b) neljanda lõigu järele lisatakse järgmine lõik: „Kui komisjon võtab vastu käesoleva lõike esimeses ja teises lõigus osutatud	Direktiivi artikli 1 punkt 7 Maksimaalne ühtlustamine	Komisjon võib võtta vastu rakendusakte		Ei kohaldata

rakendusaktid, ei kehtesta liikmesriigid nende rakendusaktide kohaldamisalasse kuuluvatele üksustele direktiivi (EL) 2022/2555 artikli 21 lõikes 2 osutatud meetmetega seotud täiendavaid tehnilisi ega metoodilisi nõudeid.“				