Euroopa Liidu
Nõukogu

Brüssel, 29. mai 2018
(OR. en)

9350/18

**Institutsioonidevaheline dokument:
2017/0225 (COD)**

**CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463**

MÄRKUS

Saatja:	Eesistujariik
Saaja:	Nõukogu
Eelmise dok nr:	8834/18
Komisjoni dok nr:	12183/17
Teema:	Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, mis käsitleb ENISAt ehk ELi küberturvalisuse ametit, millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 ja mis käsitleb info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist („küberturvalisust käsitlev õigusakt“) – Üldine lähenemisviis

I. SISSEJUHATUS

1. 13. septembril 2017 võttis komisjon digitaalse ühtse turu strateegia kontekstis vastu ning edastas nõukogule ja Euroopa Parlamendile eespool mainitud ettepaneku[1], mille õiguslikuks aluseks on ELi toimimise lepingu artikkel 114. Nn küberturvalisuse paketi osana püüdleb see ettepanek küberturvalisuse, kübervastupidavusvõime ja usalduse kõrge taseme poole liidus, eesmärgiga tagada siseturu nõuetekohane toimimine.

2. Kavandatud määruses sätestatakse ENISA ehk Euroopa Liidu Küberturvalisuse Ameti eesmärgid, ülesanded ja organisatsioonilised aspektid ning luuakse Euroopa küberturvalisuse sertifitseerimise kavade kehtestamise raamistik, et kindlustada liidus IKT toodete ja teenuste küberturvalisuse piisav tase. Komisjoni ettepanekule on lisatud mõjuhinnang, milles analüüsitakse kaheksast konkreetsest poliitikavariandist koosnevat paketti, mis hõlmab ENISA ja IKT küberturvalisuse sertifitseerimise läbivaatamist.

3. Kavandatud määrus sisaldab kahte olulist suunda:

   - alaline mandaat ametile koos piiritletud kohaldamisalaga, pidades silmas uutest poliitilistest prioriteetidest ja instrumentidest tulenevaid vajadusi ning ameti uued ülesanded ja funktsioonid, et toetada tulemuslikult ja tõhusalt liikmesriikide, ELi institutsioonide ja muude sidusrühmade jõupingutusi turvalise küberruumi tagamiseks;

   - Euroopa küberturvalisuse sertifitseerimise raamistik IKT toodetele ja teenustele ning Euroopa küberturvalisuse sertifitseerimise kavasid reguleerivad normid, mis võimaldavad kavade alusel väljastatud sertifikaatide kehtivust ja tunnustamist kõikides liikmesriikides ning vähendavad praegust turu killustatust.

[1] Dok 12183/17; dok 12183/1/17 REV 1; dok 12183/2/17 REV 2.

4. 2017. aasta oktoobris kutsus Euroopa Ülemkogu[2] komisjoni üles lähenema küberturvalisuse ettepanekute väljatöötamisele terviklikult ning esitama need õigel ajal ja vaatama need viivitamata läbi, võttes aluseks nõukogu kehtestatava tegevuskava.

5. 12. detsembril 2017 võttis üldasjade nõukogu vastu tegevuskava[3] nõukogu järelduste[4] rakendamiseks, milles käsitletakse Euroopa Parlamendile ja nõukogule esitatud ühisteatist[5] „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“. Tegevuskava kajastas nõukogu ambitsiooni saavutada ettepaneku suhtes üldine lähenemisviis 2018. aasta juuniks.

6. Euroopa Parlamendis nimetati raportööriks Angelika NIEBLER (ITRE, EPP). Hääletamine tööstuse, teadusuuringute ja energeetikakomisjoni raporti üle on kavandatud 19. juunile 2018.

7. Euroopa Majandus- ja Sotsiaalkomitee võttis oma arvamuse vastu 14. veebruaril 2018.

II. TÖÖ NÕUKOGUS

8. Komisjon esitas käesoleva ettepaneku ja selle mõjuhinnangu horisontaalsele küberküsimuste töörühmale (edaspidi „töörühm“) 26. septembril 2017. Sellele järgnes mõjuhinnangu analüüs töörühmas 20. oktoobril 2017. Järgnenud aruteludel keskenduti ameti tegevussuutlikkusele ja pädevate riiklike asutustega toimuva suhtluse ulatusele, samuti mõjule, mida sertifitseerimise raamistik avaldab turule ja ettevõtete konkurentsivõimele. Üldiselt pälvisid nii mõjuhinnang kui ka ettepanek delegatsioonide heakskiidu.

---

2 EUCO 14/17, punkt 11.
3 Dok 15748/17.
4 Dok 14435/17.
5 Dok 12211/17.

9. Töörühma arutelud ettepaneku enda üle algasid 2017. aasta novembris Eesti eesistumise ajal ning jätkusid Bulgaaria eesistumise ajal. Ettepanekuga seoses peeti 12 koosolekut, mille tulemuseks oli ettepaneku kaheksa järjestikkust muudetud versiooni, eesmärgiga leppida kokku üldises lähenemisviisis eelseisval, 8. juunil 2018 toimuval transpordi, telekommunikatsiooni ja energeetika nõukogu (telekommunikatsioon) istungil.

10. 14.–15. mail 2018 töörühmas peetud arutelude tulemus, nagu ka eesistujariigi muudetud kompromisstekst on esitatud käesoleva märkuse lisas. Põhjendusi on kohandatud, et neis kajastuksid regulatiivosas tehtud muudatused. Kõik muudatused võrreldes komisjoni ettepanekuga on märgitud **paksus kirjas** või nurksulgudega [...]. Muudatused võrreldes töörühma viimase dokumendiga (8834/18) on märgitud **paksus allajoonitud kirjas** ja väljajätmised on märgitud nurksulgudega **[...]**.

III. KOKKUVÕTE

11. Lisas esitatud eesistujariigi kompromisstekst kajastab eesistujariigi ja liikmesriikide jõupingutusi, et saavutada tekstis asjakohane tasakaal.

12. Alaliste esindajate komitee saavutas oma 25. mai 2018. aasta koosolekul kokkuleppe eesistujariigi kompromissteksti suhtes lisas esitatud kujul, mille puhul on muudetud artikli 19 lõiget 5 ja artikli 48 lõiget 5.

13. Sellest tulenevalt palutakse nõukogul võtta üldine lähenemisviis vastu oma 8. juuni 2018. aasta istungil ning volitada eesistujariiki alustama Euroopa Parlamendi ja Euroopa Komisjoni esindajatega läbirääkimisi käesoleva ettepaneku üle.

LISA

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

mis käsitleb ENISAt ehk [...] *Euroopa Liidu Küberturvalisuse Ametit*, millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 ja mis käsitleb info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist („küberturvalisust käsitlev õigusakt“)

(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[6],

võttes arvesse Regioonide Komitee arvamust[7],

toimides seadusandliku tavamenetluse kohaselt

[6] ELT C , , lk .
[7] ELT C , , lk .

ning arvestades järgmist:

(1) Võrgu- ja infosüsteemidel ning telekommunikatsioonivõrkudel ja -teenustel on ühiskonnas elutähtis roll ning neist on saanud majanduskasvu tugisammas. Info- ja kommunikatsioonitehnoloogia on aluseks keerukatele süsteemidele, millele toetub ühiskondlik tegevus, mis tagavad majanduse toimimise võtmetähtsusega sektorites nagu tervishoid, energeetika, rahandus ja transport ning mis toetavad ennekõike siseturu toimimist.

(2) Võrgu- ja infosüsteemide kasutamine kogu liidu kodanike, ettevõtjate ja valitsusasutuste seas on nüüd valdav. Digiteeritus ja ühenduvus on muutumas üha suurema hulga toodete ja teenuste põhitunnusteks ning asjade interneti kasutuselevõtuga võib eeldada, et järgmise kümne aasta jooksul võetakse kogu ELis kasutusele miljoneid kui mitte miljardeid ühendatud digitaalseid seadmeid. Kuigi internetti ühendatud seadmete arv kasvab, ei ole turvalisus ja vastupidavus neisse piisavalt sisse projekteeritud ning see toob kaasa ebapiisava küberturvalisuse. Sellises olukorras tähendab sertifitseerimise piiratud kasutamine, et organisatsioonidest ja eraisikutest kasutajatel ei ole IKT toodete ja teenuste küberturvalisuse omaduste kohta piisavalt teavet ning see vähendab usaldust digilahenduste vastu.

(3) Ulatuslikum digiteerimine ja ühenduvus toovad kaasa suuremad küberturvalisuse riskid, mille tõttu on kogu ühiskond küberohtude poolt lihtsamini haavatav ning üksikisikute, sh haavatavate isikute (nt laste) vastu suunatud ohud tulevad selgemalt esile. Et seda ühiskonna vastu suunatud riski leevendada, tuleb võtta kõik vajalikud meetmed, et parandada ELis küberturvalisust ning pakkuda küberohtude eest paremat kaitset võrgu- ja infosüsteemidele, telekommunikatsioonivõrkudele, digitaalsetele toodetele, teenustele ja seadmetele, mida kasutavad kodanikud, valitsused ja ettevõtjad alates VKEdest kuni elutähtsate taristute operaatoriteni.

(4) Küberründeid tuleb ette üha sagedamini ning küberohtude poolt lihtsamini haavatavat ühendatud majandust ja ühiskonda tuleb jõulisemalt kaitsta. Kuigi küberründed on sageli piiriülesed, on küberturvalisusega tegelevate ametiasutuste reageeringud ja õiguskaitseasutuste pädevus valdavalt riigipõhised. Mastaapsed küberintsidendid võivad katkestada elutähtsate teenuste pakkumise kogu ELis. See tähendab, et ELi tasandil on vaja tõhusat reageerimist ja kriisihaldust, mis tugineks sellekohastele põhimõtetele ning Euroopa solidaarsuse ja vastastikuse abi mitmekülgsetele vahenditele. Seepärast on usaldusväärsetel liidu andmetel põhinev liidu küberturvalisuse ja vastupidavuse olukorra regulaarne hindamine ning nii liidu kui ka maailma tasandi edasiste arengusuundade, väljakutsete ja ohtude süstemaatiline hindamine tähtis nii poliitikakujundajate ja tööstuse kui ka kasutajate jaoks.

(5) Arvestades, et liitu ähvardavad küberturvalisuse probleemid kasvavad, on vaja igakülgset meetmete kogumit, mis toetuks liidu varasemale tegevusele ja edendaks üksteist vastastikku tugevdavaid eesmärke. Siia hulka kuulub vajadus veelgi suurendada liikmesriikide ja ettevõtjate suutlikkust ja valmisolekut ning parandada koostööd ja koordineerimist liikmesriikide ja ELi institutsioonide, asutuste ja organite vahel. Küberohud ei hooli riigipiiridest ja seepärast tuleb suurendada liidu tasandi suutlikkust, et see täiendaks liikmesriikide meetmeid eeskätt mastaapsete piiriüleste küberintsidentide ja -kriiside korral. Rohkem tuleb ära teha ka selleks, et suurendada kodanike ja ettevõtjate teadlikkust küberturvalisuse küsimustest. Ühtlasi tuleks veelgi suurendada usaldust digitaalse ühtse turu vastu ning pakkuda selleks läbipaistvat teavet IKT toodete ja teenuste turvalisuse tasemete kohta. Sellele saab kaasa aidata kogu ELi hõlmava sertifitseerimisega, mis tagab ühised küberturvalisuse nõuded ja hindamiskriteeriumid liikmesriikide turgudel ja sektorites.

(6) Euroopa Parlament ja nõukogu võtsid 2004. aastal vastu määruse (EÜ) nr 460/2004,[8] millega loodi ENISA, et aidata kaasa kõrgetasemelise võrgu- ja infoturbe tagamise eesmärkidele liidus ning arendada võrgu- ja infoturbekultuuri kodanike, tarbijate, ettevõtete ja ametiasutuste heaks. 2008. aastal võtsid Euroopa Parlament ja nõukogu vastu määruse (EÜ) nr 1007/2008,[9] millega pikendati ameti mandaati 2012. aasta märtsini. Määrusega (EÜ) nr 580/2011[10] pikendati ameti mandaati 13. septembrini 2013. 2013. aastal võtsid Euroopa Parlament ja nõukogu vastu määruse (EL) nr 526/2013, mis käsitleb ENISAt ja millega tunnistatakse kehtetuks määrus (EÜ) nr 460/2004[11]; selle määrusega pikendati ameti mandaati kuni 2020. aasta juunikuuni.

---

8 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).

9 Euroopa Parlamendi ja nõukogu 24. septembri 2008. aasta määrus (EÜ) nr 1007/2008, millega muudetakse määrust (EÜ) nr 460/2004 (millega luuakse Euroopa Võrgu- ja Infoturbeamet) seoses selle kestusega (ELT L 293, 31.10.2008, lk 1).

10 Euroopa Parlamendi ja nõukogu 8. juuni 2011. aasta määrus (EL) nr 580/2011, millega muudetakse määrust (EÜ) nr 460/2004 (millega luuakse Euroopa Võrgu- ja Infoturbeamet) seoses selle tegevusaja kestusega (ELT L 165, 24.6.2011, lk 3).

11 Euroopa Parlamendi ja nõukogu 21. mai 2013. aasta määrus (EL) nr 526/2013, mis käsitleb Euroopa Liidu Võrgu- ja Infoturbeametit (ENISA) ning millega tunnistatakse kehtetuks määrus (EÜ) nr 460/2004 (ELT L 165, 18.6.2013, lk 41).

(7) Euroopa Liit on juba astunud olulisi samme, et tagada küberturvalisus ja suurendada usaldust digitehnoloogia vastu. 2013. aastal võeti vastu ELi küberjulgeoleku strateegia, millest juhinduda liidu poliitilises reageerimises küberturvalisuse ohtudele ja riskidele. Et eurooplasi veebis paremini kaitsta, võttis liit 2016. aastal vastu küberturvalisuse valdkonna esimese õigusakti – direktiivi (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (edaspidi „võrgu- ja infoturbe direktiiv“). Võrgu- ja infoturbe direktiiviga pandi paika riikide suutlikkust puudutavad nõuded küberturvalisuse valdkonnas, kehtestati liikmesriikide vahelise strateegilise ja operatiivkoostöö edendamise esimesed mehhanismid ning juurutati turbemeetmete ja intsidentidest teatamise kohustused majanduse ja ühiskonna jaoks eluliselt tähtsates sektorites, nagu energeetika, transport, veevarustus, pangandus, finantsturutaristud, tervishoid, digitaristu, aga ka oluliste digitaalsete teenuste osutajate puhul (otsingumootorid, pilvandmetöötlusteenused ja internetipõhised kauplemiskohad). ENISA-le anti selle direktiivi rakendamise toetamisel põhiroll. Võitlus küberkuritegevusega on olulisel kohal ka Euroopa julgeoleku tegevuskavas, kus see aitab kaasa küberturvalisuse kõrge taseme saavutamise üldeesmärgile.

(8) Tuleb tõdeda, et 2013. aasta küberjulgeoleku strateegia vastuvõtmisest ja ameti mandaadi viimasest läbivaatamisest möödunud aja jooksul on üldine poliitiline kontekst oluliselt muutunud, seda ka seoses ebakindlama ja vähem turvalise üldise õhustikuga maailmas. Sellist olukorda arvestades on vaja liidu uue küberturvalisuse poliitika raames läbi vaadata ENISA mandaat, et määrata kindlaks ameti roll muutunud küberturvalisuse tingimustes ning tagada, et see annab tulemusliku panuse sellesse, kuidas liit reageerib põhjalikult muutunud ohtude maastikul esile kerkivatele küberturvalisuse probleemidele, millega toimetulemiseks ei ole praegune mandaat ameti hinnangul piisav.

(9) Käesoleva määrusega loodav amet peaks olema määrusega (EL) nr 526/2013 asutatud ENISA õigusjärglane. Amet peaks täitma talle käesoleva määruse ja küberturvalisuse valdkonna liidu õigusaktidega pandud ülesandeid, pakkudes muu hulgas oskusteavet ja nõuandeid ning tegutsedes liidu selle valdkonna teabe- ja teadmuskeskusena. Amet peaks edendama parimate tavade vahetamist liikmesriikide ja eraõiguslike sidusrühmade vahel, tehes selleks Euroopa Komisjonile ja liikmesriikidele poliitikameetmete alaseid ettepanekuid, tegutsedes küberturvalisuse küsimustes liidu valdkondliku poliitika algatuste kontaktüksusena ning soodustades nii liikmesriikide omavahelist kui ka liikmesriikide ja Euroopa Liidu institutsioonide, asutuste ja organite vahelist operatiivkoostööd.

(10) Liikmesriikide esindajad otsustasid Euroopa Ülemkogu 13. detsembri 2003. aasta kohtumisel vastuvõetud otsuses 2004/97/EÜ, Euratom, et ENISA asukohaks saab Kreeka valitsuse määratud linn Kreekas. Ameti asukohaliikmesriik peaks tagama ameti tõrgeteta ja tõhusaks tegevuseks parimad võimalikud tingimused. Ameti ülesannete nõuetekohaseks ja tulemuslikuks täitmiseks, personali värbamiseks ja töölhoidmiseks ning võrgustikuga seotud tegevuse tulemuslikkuse tõhustamiseks peab amet asuma sobivas asukohas, mis muu hulgas pakub asjakohaseid transpordiühendusi ning rajatisi töötajate abikaasade ja laste jaoks. Vajalik kord tuleks sätestada ameti ja asukohaliikmesriigi vahelises kokkuleppes, mis sõlmitakse pärast ameti haldusnõukogu heakskiitu.

(11) Arvestades liidu ees seisvate küberturvalisusega seotud probleemide kasvu, tuleks suurendada ametile eraldatavaid finants- ja inimressursse, et need vastaksid ameti tõhustatud rollile ja ülesannetele ning ameti tähtsale positsioonile Euroopa digitaalse ökosüsteemi kaitsmisel.

(12) Amet peaks välja kujundama oskusteabe kõrge taseme ja seda hoidma ning tegutsema kontaktüksusena, mis tekitab ühtsel turul usaldust ja kindlustunnet tänu oma sõltumatusele, antud nõu ja levitatava teabe kvaliteedile, menetluste ja töömeetodite läbipaistvusele ning oma ülesannete hoolikale täitmisele. Täites oma ülesandeid täielikus koostöös liidu institutsioonide, [...] asutuste **ja organitega**, aga ka liikmesriikidega, peaks amet **toetama** riikide jõupingutusi **ja andma proaktiivse panuse** [...] liidu tegevusse. Lisaks peaks amet arendama edasi erasektorilt saadud sisendit, lähtudes erasektori ja muude asjaomaste sidusrühmadega tehtavast koostööst. Ameti ülesannete kogumiga tuleks paika panna, kuidas amet peab oma eesmärgid saavutama, tagades talle samas tööks vajaliku paindlikkuse.

(13) Amet peaks abistama komisjoni nõuannete, arvamuste ja analüüsidega kõigis liidu küsimustes, mis on seotud küberturvalisuse valdkonna **ja selle sektoripõhiste aspektide alase** poliitika ja õigusaktide väljatöötamisega, ajakohastamisega ja läbivaatamisega**, et suurendada küberturvalisuse mõõdet sisaldavate ELi poliitikate ja õigusaktide olulisust ja võimaldada nende järjepidevat rakendamist riiklikul tasandil** [...]. Amet peaks tegutsema nõuandva ja oskusteavet pakkuva kontaktüksusena selliste liidu sektorispetsiifilise poliitika ja õigusalaste algatuste jaoks, mis puudutavad küberturvalisust.

(14) Ameti põhiülesanne on toetada asjakohase õigusraamistiku järjepidevat rakendamist, eelkõige võrgu- ja infoturbe direktiivi tulemuslikku rakendamist, mis on kübervastupidavusvõime suurendamise jaoks eluliselt tähtis. Arvestades seda, kui kiiresti küberturvalisuse ohud muutuvad, on selge, et liikmesriike tuleb toetada igakülgsema ja eri valdkondi hõlmava poliitilise lähenemisega kübervastupidavusvõime loomisele.

(15) Amet peaks abistama liikmesriike ja liidu institutsioone, [...] asutusi **ja organeid** nende jõupingutustes, et luua ja suurendada suutlikkust ja valmisolekut ennetada ja avastada küber[...]**ohte** ja -intsidente ning neile reageerida, ning seoses võrgu- ja infosüsteemide turvalisusega. Eeskätt peaks amet toetama riiklike küberturbe intsidentide lahendamise üksuste (CSIRTide) arendamist ja tõhustamist, et neil oleks kogu liidus ühtemoodi kõrge küpsuse aste. **ENISA poolt ellu viidud tegevused, mis on seotud liikmesriikide tegevussuutlikkusega, peaksid üksnes täiendama liikmesriikide endi poolt võrgu- ja infoturbe direktiivist tulenevate kohustuste täitmiseks võetud meetmeid ega tohiks neid meetmeid asendada** [...].

(15a) Samuti peaks amet abistama liidu ja, taotluse korral, liikmesriikide võrgu- ja infosüsteemide turvalisuse strateegiate väljatöötamist ja uuendamist, eelkõige küberturvalisuse osas, ning edendama nende levitamist ja jälgima nende rakendamist. Lisaks peaks amet pakkuma koolitusi ja koolitusmaterjali avalikele asutustele ning koolitama vajaduse korral koolitajaid, et aidata liikmesriikidel kujundada välja nende endi koolitussuutlikkus.

(16) Amet peaks abistama võrgu- ja infoturbe direktiiviga loodud koostöörühma selle ülesannete täitmisel, eeskätt pakkuma oskusteavet ja nõu ning hõlbustama parimate tavade vahetamist peamiselt seoses oluliste teenuste operaatorite identifitseerimisega liikmesriikide poolt, sealhulgas selles osas, mis puudutab riskide ja intsidentidega seotud piiriüleseid sõltuvusseoseid.

(17) Selleks et ergutada avaliku ja erasektori koostööd ning erasektorisisest koostööd, [...] **peaks amet** toetama **teabe jagamist sektorite sees ja vahel, eeskätt direktiivi (EL) 2016/1148 II lisas loetletud valdkondades, pakkudes parimaid tavasid ja juhiseid kättesaadavate töövahendite ja menetluste kohta ning selle kohta, kuidas lahendada teabe jagamisega seotud regulatiivsed küsimused, näiteks hõlbustades** [...] valdkondlike teabe jagamise ja analüüsimise keskuste (ISACide) loomist [...].

(18) Amet peaks koondama ja analüüsima riikide **vabatahtlikult jagatud** CSIRTide ja CERT-EU aruandeid, **et abistada liikmesriike** teabevahetuse jaoks ühiste [...] **menetluste**, keele ja terminoloogia koostamisel. Võrgu- ja infoturbe direktiiviga loodud CSIRTide võrgustikuga loodi alus vabatahtlikuks tehnilise teabe vahetamiseks operatiivtasandil [...] CSIRTide võrgustiku **sees** – selle raames peaks amet kaasama ka erasektori.

(19) Amet peaks andma oma panuse sellesse, kuidas ELi tasandil reageeritakse mastaapsetele piiriülestele küberturvalisuse intsidentidele ja kriisidele. Seda funktsiooni tuleks **täita kooskõlas tema mandaadiga, mis on antud vastavalt käesolevale määrusele, ja lähenemisviisiga, mille suhtes on liikmesriigid leppinud kokku ulatuslike küberturvalisuse intsidentide ja kriiside korral koordineeritud reageerimist käsitleva komisjoni soovituse kontekstis**. **See võiks** hõlmata asjaomase teabe kogumist ning vahendajarolli CSIRTide võrgustiku ja tehnilise kogukonna, aga ka kriisi haldamise eest vastutavate otsusetegijate vahel. Lisaks võiks amet toetada intsidendikäsitlust tehnilise külje pealt, hõlbustades vajalike lahenduste tehnilist vahetamist liikmesriikide vahel ja pakkudes sisendit avaliku teabevahetuse jaoks. Amet peaks seda protsessi toetama sellise koostöö aspektide testimisega [...] **korrapäraste** küberturvalisuse õppuste käigus.

(20) [...] **Toetades** operatiiv**koostööd**, peaks amet kasutama CERT-EU kaudu kättesaadavaid **tehnilisi ja operatiivseid** oskusteadmisi struktureeritud koostöö kaudu [...]. [...] Vajaduse korral tuleks kahe organisatsiooni vahel kehtestada erikord, et määrata kindlaks sellise koostöö praktiline kulg **ja vältida tegevuse dubleerimist**.

(21) Amet peaks kooskõlas oma [...] ülesannetega **toetada operatiivkoostööd CSIRTide võrgustikus** olema suuteline pakkuma toetust liikmesriikidele **nende taotluse korral**, näiteks jagama nõu, **kuidas parandada intsidentide vältimise, nende avastamise ja neile reageerimise suutlikkust, hõlbustades [...] märkimisväärse või olulise mõjuga intsidentide** tehnilist **lahendamist [...]** või tagades ohtude ja intsidentide analüüsimise. **Märkimisväärse või olulise mõjuga intsidentide tehnilise lahendamise hõlbustamine peaks eelkõige hõlmama seda, et ENISA toetab tehniliste lahenduste vabatahtlikku jagamist liikmesriikide vahel või loob kombineeritud tehnilist teavet, nt liikmesriikide poolt vabatahtlikult jagatud tehnilised lahendused.** Komisjoni soovituses koordineeritud reageerimiseks ulatuslike küberturvalisuse intsidentide ja kriiside korral on öeldud, et liikmesriigid peaksid tegema heas usus koostööd ja jagama ilma põhjendamatute viivitusteta nii omavahel kui ka ENISAga teavet mastaapsete küberturvalisuse intsidentide ja kriiside kohta. Sellisest teabest oleks ENISA-l [...] **operatiivkoostöö toetamisel** täiendavat abi.

(22) Amet peaks liidu olukorrateadlikkust toetava tehnilise tasandi korrapärase koostöö raames korrapäraselt **ja tihedas koostöös liikmesriikidega** koostama intsidentide ja ohtude kohta ELi küberturvalisuse tehnilist olukorda käsitlevaid aruandeid, mis põhinevad avalikult kättesaadaval teabel, tema enda analüüsidel ja aruannetel, mida jagavad temaga liikmesriikide CSIRTid [...] või võrgu- ja infosüsteemide direktiivi kohased ühtsed kontaktpunktid **(mõlemad vabatahtlikkuse alusel)**, Europoli juures tegutsev küberkuritegevuse vastase võitluse Euroopa keskus (EC3), CERT-EU ja kui asjakohane, siis Euroopa Liidu luureandmete analüüsi keskus (INTCEN) Euroopa välisteenistuse juures. Aruanne tuleks teha kättesaadavaks nõukogu asjakohastele organitele, komisjonile, liidu välisasjade ja julgeolekupoliitika kõrgele esindajale ja CSIRTide võrgustikule.

(23) Märkimisväärse mõjuga intsidendi puhul [...] peaks **ameti toetus asjaomaste** liikmesriikide taotluse korral tehtavale tehnilisele järel**uurimisele** [...] keskenduma edasiste intsidentide ärahoidmisele [...]. **Asjaomased liikmesriigid peaksid pakkuma vajalikku teavet, et võimaldada ametil tõhusalt toetada tehnilist uurimist.**

(24) [...]

(25) Liikmesriigid võivad paluda, et intsidendist mõjutatud ettevõtjad teeksid koostööd ning pakuksid ametile vajalikku teavet ja abi, ilma et see piiraks nende õigust kaitsta tundlikku äriteavet.

(26) Et küberturvalisuse valdkonna probleemidest paremini aru saada ning liikmesriikidele ja liidu institutsioonidele pikaajalist strateegilist nõu anda, peab amet analüüsima praeguseid ja kujunemisjärgus riske. Sel eesmärgil peaks amet koostöös liikmesriikidega ja vajaduse korral ka statistikaasutuste ja muude asutustega koguma asjakohast, **avalikult kättesaadavat või vabatahtlikult jagatud** teavet ning analüüsima kujunemisjärgus tehnoloogiaid ja andma teemakohaseid hinnanguid võrgu- ja infoturbe, eeskätt küberturvalisuse tehnoloogiliste uuenduste eeldatavale ühiskondlikule, õiguslikule, majanduslikule ja regulatiivsele mõjule. Peale selle peaks amet toetama ohtude ja intsidentide analüüsimise kaudu liikmesriike ja liidu institutsioone, asutusi ja organeid esilekerkivate suundumuste kindlakstegemisel ja küberturvalisuse [...] **intsidentide** vältimisel.

(27) Amet peaks liidu vastupidavuse suurendamiseks arendama [...] **küber**turvalisuse alaseid teadmisi seoses nende infrastruktuuridega, **mis toetavad eeskätt võrgu- ja infosüsteemide direktiivi II lisas loetletud valdkondi ja mida kasutavad kõnealuse direktiivi III lisas loetletud digitaalsete teenuste osutajad,** pakkudes nõuandeid, juhiseid ja parimaid tavasid. Et tagada hõlpsam juurdepääs paremini struktureeritud teabele küberturvalisuse riskide ja võimalike lahenduste kohta, peaks amet arendama välja liidu teabekeskuse ja hoidma seda käigus. Teabekeskus oleks universaalne portaal, mis jagaks üldsusele küberturvalisuse kohta teavet, mis on saadud ELi ja riikide institutsioonidelt, asutustelt ja organitelt.

(28) Amet peaks aitama suurendada üldsuse teadlikkust küberturvalisusega seotud riskidest ja jagama kodanikele ja organisatsioonidele mõeldud juhiseid individuaalsete kasutajate heade tavade kohta. Amet peaks aitama kaasa ka parimate tavade ja lahenduste propageerimisele üksikisikute ja organisatsioonide tasandil; selleks tuleks koguda ja analüüsida avalikult kättesaadavat teavet oluliste intsidentide kohta ning koostada aruanded, et pakkuda ettevõtjatele ja kodanikele juhiseid ning parandada valmisoleku ja vastupidavuse üldist taset. Amet peaks korraldama koostöös liikmesriikidega ja liidu institutsioonide, [...] asutuste **ja organitega** korrapäraseid lõppkasutajatele suunatud üldsuse harimise ja teavituskampaaniaid, mille eesmärk on propageerida üksikisikute ohutumat veebikäitumist ja suurendada teadlikkust küberkeskkonnas varitseda võivatest ohtudest, sealhulgas sellistest küberkuritegudest nagu andmepüügi rünnakud, robotvõrgud, finants- ja pangapettused, ning tutvustada autentimise ja andmekaitse alaseid elementaarseid nõuandeid. Ametil peaks olema keskne roll selles, et lõppkasutajad saaksid kiiremini teadlikuks seadmete turvalisusest.

(29) Küberturvalisuse sektoris tegutsevate ettevõtjate, aga ka küberturvalisuse lahenduste kasutajate toetuseks peaks amet rajama nn turuseirekeskuse ja seda käigus hoidma, analüüsides korrapäraselt nii küberturvalisuse turu nõudluse kui ka pakkumise poole peamisi suundumusi ja neid tutvustades.

(30) Tagamaks et amet saavutab oma eesmärgid täies ulatuses, peaks ta suhtlema asjaomaste institutsioonide, asutuste ja organitega, kelle hulgas on CERT-EU, Europoli juures tegutsev küberkuritegevuse vastase võitluse Euroopa keskus (EC3), Euroopa Kaitseagentuur (EDA), Vabadusel, Turvalisusel ja Õigusel Rajaneva Ala Suuremahuliste IT-süsteemide Operatiivjuhtimise Euroopa Amet (eu-LISA), Euroopa Lennundusohutusamet (EASA), **Euroopa Globaalse Satelliitnavigatsioonisüsteemi Agentuur (GNSSi Agentuur)** ja mistahes muud ELi ametid, kes tegelevad küberturvalisusega. Peale selle peaks ta suhtlema veel andmekaitsega tegelevate ametiasutustega, et vahetada oskusteavet ja parimaid tavasid ning anda nõu küberturvalisuse aspektide kohta, mis võiksid mõjutada nende tööd. Riikide ja liidu õiguskaitseasutuste ja andmekaitseasutuste esindajad peaksid olema esindatud ameti alalises sidusrühmas. Õiguskaitseasutustega koostöö tegemisel võrgu- ja infoturbe küsimustes, mis võivad nende tööd mõjutada, peaks amet arvestama olemasolevate teabekanalite ja rajatud võrgustikega.

(31) Amet, **täites** CSIRTide võrgustiku [...] sekretariaadi **rolli**, peaks toetama liikmesriikide CSIRTe ja CERT-EUd operatiivkoostöös, mis lisandub CSIRTide võrgustiku kõigile asjaomastele ülesannetele, mis on kindlaks määratud võrgu- ja infoturbe direktiivis. Veelgi enam, amet peaks edendama ja toetama ka asjaomaste CSIRTide koostööd, kui toimuvad intsidendid, ründed või häired CSIRTide hallatavates või kaitstavates võrkudes või taristutes, mis hõlmavad või võivad hõlmata vähemalt kahte CSIRTi, võttes sealjuures nõuetekohaselt arvesse CSIRTide võrgustiku standardset töökorda.

(32) Selleks et suurendada liidu valmisolekut reageerida küberturvalisuse intsidentidele, peaks amet korraldama [...] **korrapäraselt** liidu tasandil küberturvalisuse õppusi ning toetama liikmesriike ja ELi institutsioone, asutusi ja organeid nende taotluse korral õppuste korraldamisel.

(33) Lisaks peaks amet arendama ja säilitama oma oskusteavet küberturvalisuse sertifitseerimise kohta, et toetada liidu poliitikat selles valdkonnas. Amet peaks edendama küberturvalisuse sertifitseerimise kasutuselevõttu liidus muu hulgas sellega, et aitab kehtestada liidu tasandil küberturvalisuse sertifitseerimise raamistiku ja seda hallata, et suurendada IKT toodete ja teenuste küberturvalisuse alase usaldusväärsuse läbipaistvust ning tugevdada seeläbi usaldust digitaalse siseturu vastu.

(34) Tõhusad küberturvalisuse alased poliitikameetmed peaksid tuginema hästi väljatöötatud riskihindamismeetoditele, seda nii avalikus kui ka erasektoris. Riskihindamismeetodeid kasutatakse erinevatel tasanditel ning puudub nende tõhusa kohaldamise üldine tava. Riskide hindamise ja koostalitlusvõimeliste riskihalduse lahenduste parimate tavade propageerimine ja arendamine avaliku ja erasektori organisatsioonides tõstab küberturvalisuse taset liidus. Selleks peaks amet toetama sidusrühmade koostööd liidu tasandil, hõlbustades nende jõupingutusi seoses elektrooniliste toodete, süsteemide, võrkude ja teenuste – mis koos tarkvaraga moodustavad võrgu- ja infosüsteemid – riskihalduse ja mõõdetava turvalisuse Euroopa ja rahvusvaheliste standardite väljatöötamise ja kasutuselevõtmisega.

(35) Amet peaks innustama liikmesriike ja teenusepakkujaid tõstma oma üldisi turbestandardeid, et kõik internetikasutajad saaksid võtta vajalikud meetmed oma isikliku küberturvalisuse tagamiseks. Eelkõige peaksid tootjad ja teenuseosutajad võtma tagasi või taaskasutusse tooted ja teenused, mis ei vasta küberturvalisuse standarditele. Koostöös pädevate asutustega võib ENISA jagada teavet siseturul pakutavate toodete ja teenuste küberturvalisuse taseme kohta ning avaldada teenusepakkujatele ja tootjatele suunatud hoiatusi, milles nõutakse nende toodete ja teenuste turvalisuse, sealhulgas küberturvalisuse parandamist.

(36) Amet peaks täies ulatuses võtma arvesse tehtavaid uuringuid, arendustegevust ja tehnoloogilisi hindamisi, eelkõige neid, mida teostatakse erinevates Euroopa Liidu teadusalgatustes, et nõustada liidu institutsioone, [...] asutusi **ja organeid** ning kui see on asjakohane, liikmesriike nende taotlusel seoses vajadusega teadusuuringute järele [...] küberturvalisuse valdkonnas. **Amet peaks teadustöö vajaduste ja prioriteetide kindlakstegemiseks konsulteerima ka asjaomaste kasutajarühmadega.**

(37) Küberturvalisusega seotud [...] **ohud** on ülemaailmsed. Vaja on teha tihedamat rahvusvahelist koostööd, et parandada **küber**turbe standardeid (sealhulgas määratleda ühised käitumisnormid) ja teabe jagamist, millega edendatakse nii kiiremat rahvusvahelist koostööd reageerimise valdkonnas kui ka ühtset ülemaailmset lähenemisviisi võrgu- ja infoturbele. Selleks peaks amet toetama liidu tihedamat kaasamist ning koostööd kolmandate riikide ja rahvusvaheliste organisatsioonidega, pakkudes vajaduse korral asjaomastele liidu institutsioonidele, [...] asutustele **ja organitele** vajalikku oskusteavet ja analüüsi.

(38) Amet peaks suutma reageerida liikmesriikide ja ELi institutsioonide, asutuste ja organite *ad hoc* nõuande- ja abitaotlustele, mis kuuluvad ameti eesmärkide hulka.

(39) Ameti juhtimisel on oluline rakendada teatavaid põhimõtteid, et järgida ühisavaldust ja ühist lähenemisviisi, mille institutsioonidevaheline ELi detsentraliseeritud ametite töörühm 2012. aasta juulis kokku leppis ning mille eesmärk on ühtlustada ametite tegevust ja parandada nende toimimist. Ühisavaldus ja ühine lähenemisviis peaksid vajaduse korral samuti kajastuma ameti tööprogrammides, ameti hindamistes ning ameti aruandlus- ja haldustavades.

(40) Liikmesriikide ja komisjoni esindajatest koosnev haldusnõukogu peaks määrama kindlaks ameti tegevuse üldsuuna ning tagama, et amet täidab oma ülesandeid vastavalt käesolevale määrusele. Haldusnõukogule tuleks anda õigus koostada ameti eelarve ja kontrollida selle täitmist, võtta vastu kohased finantseeskirjad, kehtestada ameti otsuste tegemiseks läbipaistev kord, võtta vastu ameti ühtne programmdokument, võtta vastu ameti töökord, nimetada ametisse tegevdirektor ning otsustada tegevdirektori ametiaja pikendamise ja tema ametiaja lõpetamise üle.

(41) Ameti nõuetekohaseks ja tulemuslikuks toimimiseks peaksid komisjon ja liikmesriigid tagama, et haldusnõukogu liikmeteks nimetatavatel isikutel on vajalikud erialateadmised ja kogemused. Komisjon ja liikmesriigid peaksid püüdma piirata oma esindajate vahetumist haldusnõukogus, et tagada selle töö järjepidevus.

(42) Ameti sujuvaks toimimiseks on tarvis, et tegevdirektor nimetataks ametisse silmas pidades tema teeneid, dokumenteeritud haldamis- ja juhtimisoskust ning küberturvalisuse alaseid teadmisi ja kogemusi ning et tegevdirektori ülesandeid täidetaks täiesti sõltumatult. Tegevdirektor peaks pärast komisjoniga konsulteerimist koostama ettepaneku ameti tööprogrammi kohta ning võtma kõik vajalikud meetmed ameti tööprogrammi nõuetekohase täitmise tagamiseks. Tegevdirektor peaks koostama igal aastal haldusnõukogule esitatava aruande**, sealhulgas ameti iga-aastase tööprogrammi rakendamise kohta**, koostama ameti tulude ja kulude kalkulatsiooni eelnõu ning vastutama eelarve täitmise eest. Lisaks peaks tegevdirektoril olema võimalus luua ajutisi töörühmi selleks, et käsitleda eelkõige teaduslikke, tehnilisi, juriidilisi või sotsiaal-majanduslikke küsimusi. Tegevdirektor peaks tagama, et ajutistesse töörühmadesse valitakse liikmed kõige põhjalikumate erialateadmiste põhjal, võttes nõuetekohaselt arvesse, et seal oleksid (lähtuvalt sellest, kuidas see on konkreetset küsimust arvestades asjakohane) tasakaalustatult esindatud liikmesriikide riiklikud haldusorganid, liidu institutsioonid ja erasektor, sealhulgas majandusringkonnad, kasutajad ning võrgu- ja infoturbe alal pädevad teaduseksperdid.

(43) Juhatus peaks aitama kaasa haldusnõukogu tõhusale toimimisele. Osana haldusnõukogu otsustega seotud ettevalmistustööst peaks juhatus põhjalikult analüüsima asjakohast teavet ja olemasolevaid võimalusi ning pakkuma nõuandeid ja lahendusi haldusnõukogu asjakohaste otsuste ettevalmistamiseks.

(44) Ametil peaks olema nõuandva organina alaline sidusrühm, mis tagaks regulaarse dialoogi erasektori, tarbijate organisatsioonide ja teiste asjaomaste sidusrühmadega. Tegevdirektori ettepanekul haldusnõukogu asutatud alaline sidusrühm peaks keskenduma sidusrühmade jaoks olulistele küsimustele ja juhtima neile ameti tähelepanu. Alalise sidusrühma koosseis ja ülesanded (eelkõige tuleb rühmaga konsulteerida tööprogrammi projekti üle) peaksid tagama sidusrühmade piisava esindatuse ameti töös.

(45) Amet peaks vastu võtma huvide konfliktide ennetamise ja lahendamise eeskirjad. Amet peaks kohaldama ka asjaomaseid liidu sätteid, mis käsitlevad üldsuse juurdepääsu dokumentidele, nagu on sätestatud Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 1049/2001[12]. Isikuandmeid tuleks töödelda vastavalt Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrusele (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta[13]. Amet peaks teabe, eelkõige tundliku salastamata teabe ja ELi salastatud teabe käitlemisel järgima liidu institutsioonide kohta kehtivaid sätteid ja liikmesriikide õigusakte.

---

[12] 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).

[13] EÜT L 8, 12.1.2001, lk 1.

(46) Et tagada ameti täielik autonoomia ja sõltumatus ning võimaldada tal täita uusi ja lisaülesandeid, sealhulgas kiireloomulisi erakorralisi ülesandeid, tuleks ametile eraldada piisav ja autonoomne eelarve, mille peamine tulu tuleb liidu osamaksest ja ameti töös osalevate kolmandate riikide sissemaksetest. Enamik ameti töötajaid peaks olema otseselt tegev ameti mandaadi rakendamises. Asukohaliikmesriigil või mis tahes muul liikmesriigil peaks olema lubatud teha ameti tuludesse vabatahtlikult sissemakseid. Liidu eelarvemenetluse kohaldamist tuleks jätkata mis tahes subsiidiumide suhtes, mida makstakse Euroopa Liidu üldeelarvest. Lisaks sellele peaks ameti raamatupidamisarvestust läbipaistvuse ja vastutuse tagamiseks auditeerima kontrollikoda.

(47) [...]

(48) Küberturvalisuse sertifitseerimisel on tähtis ülesanne IKT toodete ja teenuste turvalisuse ja nende vastu usalduse suurendamises. Digitaalne ühtne turg ning eelkõige andmepõhine majandus ja asjade internet saavad olla edukad vaid juhul, kui avalikkusel on kindlustunne, et sellised tooted ja teenused pakuvad teatavat küberturvalisuse taset. Internetiühendusega ja automatiseeritud autod, elektroonilised meditsiiniseadmed, tööstuslikud automatiseeritud juhtimissüsteemid või arukad võrgud on vaid mõned näited sektoritest, kus sertifitseerimist juba ulatuslikult kasutatakse või tõenäoliselt hakatakse lähitulevikus kasutama. Võrgu- ja infoturbe direktiiviga reguleeritud sektorid on ka sektorid, kus küberturvalisuse sertifitseerimine on äärmiselt oluline.

(49) 2016. aasta teatises „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine“ tõi komisjon välja vajaduse kvaliteetsete, taskukohaste ja koostalitlusvõimeliste küberturvalisuse toodete ja -lahenduste järele. IKT toodete ja teenuste pakkumine ühtsel turul on endiselt geograafiliselt väga killustatud. Selle põhjuseks on asjaolu, et küberturvalisuse tööstus on Euroopas peamiselt arenenud riikliku, täpsemalt valitsuse nõudluse najal. Lisaks kuulub kübeturvalisuse ühtse turu kitsaskohtade hulka koostalitusvõimeliste lahenduste (tehniliste standardite), tavade ja kogu ELi hõlmavate sertifitseerimismehhanismide puudumine. Ühest küljest teeb see riiklikul, Euroopa ja üleilmsel tasandil konkureerimise Euroopa ettevõtjate jaoks keerukaks. Teisest küljest tähendab see üksikisikute ja ettevõtjate jaoks võimaliku ja kasutatava küberturvalisuse tehnoloogia kättesaadavust väiksemas valikus. Euroopa digitaalse ühtse turu strateegia rakendamise vahekokkuvõttes rõhutas komisjon vajadust turvaliste võrgustatud toodete ja süsteemide järele ning märkis, et Euroopa IKT turvalisuse raamistiku loomine, millega kehtestatakse õigusnormid selle kohta, kuidas korraldada IKT turvalisuse sertifitseerimist liidus, võib aidata säilitada usaldust interneti vastu ja vähendada küberturvalisuse turu praegust killustatust.

(50) Praegu kasutatakse IKT **protsesside,** toodete ja teenuste küberturvalisuse sertifitseerimist ainult piiratud ulatuses. Kui sertifitseerimine on olemas, siis peamiselt liikmesriigi tasandil või tööstusest lähtuvate kavade raames. Sellistes tingimustes ei tunnusta teised liikmesriigid üldiselt ühe riigi küberturvalisuse asutuse poolt välja antud sertifikaati. Seega võib juhtuda, et ettevõtted peavad sertifitseerima oma tooted ja teenused mitmes liikmesriigis, kus nad tegutsevad, näiteks et osaleda riiklikes hankemenetlustes. Lisaks sellele paistab, et kuigi on tekkimas uusi kavasid, ei ole ühtset ja terviklikku lähenemisviisi küberturvalisuse horisontaalsetele küsimustele, näiteks asjade interneti valdkonnas. Olemasolevatel kavadel on märkimisväärseid puudujääke ning erinevusi tootehõlmavuses, usaldusväärsuse tasemetes, sisulistes kriteeriumides ja tegelikus kasutamises.

(51) Minevikus on tehtud pingutusi, et saavutada Euroopas sertifikaatide vastastikune tunnustamine. See on olnud aga vaid osaliselt edukas. Kõige olulisem näide siinkohal on kõrgemate ametnike infosüsteemide turvalisuse rühma (SOG-IS) vastastikuse tunnustamise kokkulepe. Kuigi see on kõige tähtsam koostöö ja vastastikuse tunnustamise mudel turvalisuse sertifitseerimise valdkonnas, [...] hõlmab SOG-IS vaid osa liidu liikmesriike. See on piiranud SOG-IS vastastikuse tunnustamise kokkuleppe tulemuslikkust siseturu seisukohast.

(52) Eelnevat arvestades on vaja luua Euroopa küberturvalisuse sertifitseerimise raamistik, milles kehtestatakse välja töötatavate Euroopa küberturvalisuse sertifitseerimise kavade peamised horisontaalsed nõuded ning mis võimaldab tunnustada ja kasutada ELi IKT toodete ja teenuste **vastavusdeklaratsioone** kõigis liikmesriikides. Euroopa raamistikul peaks olema kaks eesmärki: ühest küljest peaks see aitama suurendada usaldust nende kavade kohaselt sertifitseeritud IKT toodete ja teenuste vastu. Teisest küljest peaks see vältima üksteisele vastukäivate või kattuvate riiklike küberturvalisuse sertifikaatide paljusust ja seeläbi vähendama digitaalsel ühtsel turul tegutsevate ettevõtjate kulusid. Kavad peaksid olema mittediskrimineerivad ning põhinema rahvusvahelistel ja/või [...] **Euroopa** standarditel, välja arvatud juhul, kui need standardid on ebatõhusad või ebasobivad ELi õiguspäraste eesmärkide saavutamiseks selles valdkonnas.

(53) Komisjonile tuleks anda volitused võtta vastu Euroopa küberturvalisuse sertifitseerimise kavad konkreetsete IKT **protsesside,** toodete ja teenuste rühmade kohta. Neid kavu peaksid rakendama ja nende üle järelevalvet teostama riiklikud **küberturvalisuse** sertifitseerimise [...] asutused ning nende kavade kohaselt välja antud sertifikaadid peaksid kehtima ja olema tunnustatud kogu liidus. Tööstuse või muude eraorganisatsioonide rakendatavad sertifitseerimiskavad peaksid jääma väljapoole määruse kohaldamisala. Siiski võivad selliseid kavu haldavad asutused teha komisjonile ettepaneku kaaluda nende heakskiitmist Euroopa kavana.

(54) Käesoleva määruse sätted ei tohiks mõjutada liidu õigusakte, milles on sätestatud konkreetsed eeskirjad IKT toodete ja teenuste sertifitseerimise kohta. Isikuandmete kaitse üldmäärus sisaldab sätteid selliste sertifitseerimismehhanismide ning andmekaitsepitserite ja -märgiste kasutuselevõtuks, mille abil saab tõendada, et vastutavate töötlejate ja volitatud töötlejate isikuandmete töötlemise toimingud vastavad kõnealusele määrusele. Sellised sertifitseerimismehhanismid ning andmekaitsepitserid ja -märgised peaksid võimaldama andmesubjektidel kiiresti hinnata asjakohaste toodete ja teenuste andmekaitse taset. Käesolev määrus ei piira andmetöötlustoimingute sertifitseerimist isikuandmete kaitse üldmääruse kohaselt, sealhulgas juhul, kui sellised toimingud sisalduvad toodetes või teenustes.

(55) Euroopa küberturvalisuse sertifitseerimise kavade eesmärk on kinnitada, et sellise kava kohaselt sertifitseeritud IKT **protsessid,** tooted ja teenused vastavad kirjeldatud nõuetele [...] **eesmärgiga** [...] **kaitsta** salvestatud, edastatud või töödeldud andmete või nende toodete, protsesside, teenuste ja süsteemide asjaomaste funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust **kogu olelusringi kestel** käesoleva määruse tähenduses. Käesolevas määruses ei ole võimalik üksikasjalikult kirjeldada kõigi IKT **protsesside,** toodete ja teenuste suhtes kohaldatavaid küberturvalisuse nõudeid. IKT **protsessid,** tooted ja teenused ning nendega seotud küberturvalisuse vajadused on nii mitmekesised, et on väga raske esitada üldiseid küberturvalisuse nõudeid, mis kehtiksid kõikjal. Seetõttu on vaja sertifitseerimise eesmärgil võtta kasutusele lai ja üldine küberturvalisuse mõiste, mida täiendab rida konkreetseid küberturvalisuse eesmärke, mida tuleb Euroopa küberturvalisuse sertifitseerimise kavade koostamisel arvesse võtta. Nende eesmärkide saavutamise meetodid konkreetsete IKT **protsesside,** toodete ja teenuste puhul tuleks täpsustada üksikasjalikult igas individuaalses sertifitseerimiskavas, mille komisjon vastu võtab, näiteks viidates standarditele või tehnilistele kirjeldustele**, kui asjakohased standardid puuduvad**.

(55a) Euroopa küberturvalisuse sertifitseerimise kavas kasutatavad tehnilised kirjeldused tuleks määrata kindlaks määruse (EL) nr 1025/2012 II lisas sätestatud põhimõtteid järgides. Mõned kõrvalekalded nendest põhimõtetest võivad siiski olla vajalikud nõuetekohaselt põhjendatud juhtudel, kui nimetatud tehnilisi kirjeldusi kasutatakse Euroopa küberturvalisuse sertifitseerimise kavas, mis osutab kõrgele usaldusväärsuse tasemele. Selliste kõrvalekallete põhjused tuleb teha avalikult kättesaadavaks.

(55b) Sertifitseeritud vastavuse hindamine on protsess, mille käigus hinnatakse, kas IKT protsessi, toote või teenusega seotud erinõuded on täidetud. Seda protsessi teostab sõltumatu kolmas isik, kes ei ole toote tootja või teenuseosutaja. Sertifikaadi väljastamise protsess järgneb IKT protsessi, toote või teenuse eduka hindamise protsessile. Seda tuleks käsitleda kinnitusena, et asjaomane hindamine on nõuetekohaselt läbi viidud. Sõltuvalt usaldusväärsuse tasemest tuleks Euroopa küberturvalisuse kavas ette näha, kas sertifikaadi väljastab era- või avalik-õiguslik asutus. Vastavushindamine ja sertifitseerimine iseenesest ei taga, et sertifitseeritud IKT tooted ja teenused on küberturvalised. Pigem on see menetlus ja tehniline metoodika tõendamaks, et IKT tooteid ja teenuseid on kontrollitud ja et need vastavad teatavatele küberturvalisuse nõuetele, mis on sätestatud mujal, näiteks tehnilistes standardites.

(55c) Sertifikaadi kasutajate poolne sertifitseerimise asjakohase taseme ja seotud turvanõuete valik peaks põhinema IKT protsessi, toote või teenuse kasutamise riskianalüüsil. Usaldusväärsuse tase peab seega vastama IKT protsessi, toote või teenuse ettenähtud kasutamisega seotud riskitasemele.

(55d) Euroopa küberturvalisuse sertifitseerimise kavas võidakse ette näha vastavushindamise läbiviimine IKT toodete tootjate või IKT teenuste osutajate ainuvastutusel (vastavuse enesehindamine). Sellistel juhtudel piisab sellest, kui tootja või teenuseosutaja teeb ise kõik kontrollid, et tagada IKT protsessi, toodete või teenuste vastavus sertifitseerimise kavale. Sellist liiki vastavuse hindamist võiks pidada asjakohaseks vähekeerukate (nt lihtsa konstruktsiooni ja tootmismehhanismiga) IKT toodete ja teenuste puhul, mis kujutavad endast väikest riski avalikule huvile. Lisaks saavad vastavuse enesehindamise subjektiks olla üksnes usaldusväärsuse baastasemega IKT tooted ja teenused.

(55e) Euroopa küberturvalisuse sertifitseerimise kavas võib ette näha nii IKT toodete ja teenuste sertifitseerimise kui ka vastavuse enesehindamise. Sellisel juhul tuleks kavas ette näha selged ja arusaadavad vahendid tarbijatele või teistele kasutajatele, et eristada tooteid ja teenuseid, mida hinnatakse tootja või teenuseosutaja vastutusel, ning tooteid ja teenuseid, mille on sertifitseerinud kolmas isik.

(55f) IKT toodete tootja või teenuste osutaja, kes teostab vastavuse enesehindamise, peaks vastavushindamismenetluse raames koostama ja allkirjastama ELi vastavusdeklaratsiooni. ELi vastavusdeklaratsioon on dokument, millega kinnitatakse, et teatav IKT toode või teenus vastab kavas esitatud nõuetele. ELi vastavusdeklaratsiooni koostamisel ja allkirjastamisel võtab tootja või teenuseosutaja vastutuse IKT toote või teenuse vastavuse eest kavas esitatud seadusest tulenevatele nõuetele. ELi vastavusdeklaratsiooni koopia esitatakse riiklikule küberturvalisuse sertifitseerimise asutusele ja ENISA-le.

(55g) IKT toodete tootja või teenuste osutaja hoiab ELi vastavusdeklaratsiooni ja asjaomast tehnilist dokumentatsiooni, mis puudutab kogu teavet IKT toodete või teenuste vastavuse kohta kavale, konkreetses Euroopa küberturvalisuse sertifitseerimise kavas määratletud perioodi jooksul pädeva riikliku küberturvalisuse sertifitseerimise asutuse jaoks kättesaadavana. Tehnilistes dokumentides tuleks määrata kindlaks kohaldatavad nõuded ja käsitleda hindamiseks vajalikul määral IKT toote või teenuse projekteerimist, tootmist ja toimimist. Tehniline dokumentatsioon peaks olema koostatud nii, et see võimaldaks hinnata IKT toote või teenuse vastavust asjaomastele nõuetele.

(55h) Liikmesriikidel ja huvitatud sidusrühmade organisatsioonidel peaks olema õigus teha Euroopa küberturvalisuse sertifitseerimise rühmale ettepanek koostada ettevalmistav kava. Huvitatud sidusrühmade organisatsioonid on tööstuse või tarbijate esindajate organisatsioonid, sealhulgas VKEde organisatsioonide esindajad, kes tunnevad õiguspärast huvi konkreetse Euroopa küberturvalisuse sertifitseerimise kava väljatöötamise vastu. Selliseid ettepanekuid tuleks analüüsida, võttes arvesse Euroopa küberturvalisuse sertifitseerimise rühma poolt väljatöötatud kriteeriume, tuginedes läbipaistvuse, avatuse, erapooletuse, konsensuse, tõhususe, asjakohasuse ja sidususe põhimõtete alusel koostatud suunistele.

(56) Komisjonile **ja rühmale** tuleks anda volitused paluda ENISA-l koostada **põhjendamatu viivituseta** ettevalmistav sertifitseerimiskava konkreetsete IKT **protsesside,** toodete ja teenuste jaoks. Seejärel tuleks anda komisjonile volitused võtta ENISA esitatud ettevalmistava kava põhjal rakendusaktidega vastu Euroopa küberturvalisuse sertifitseerimise kava. Võttes arvesse käesolevas määruses määratletud üldeesmärki ja turvalisusega seotud eesmärke, tuleks komisjoni poolt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavades täpsustada konkreetse kava sisu, ulatuse ja toimimise minimaalsed üksikasjad. Need peaksid hõlmama muu hulgas küberturvalisuse sertifitseerimise ulatust ja sisu, sealhulgas hõlmatud IKT **protsesside,** toodete ja teenuste kategooriad, küberturvalisuse nõuete üksikasjalik kirjeldus, näiteks viide standarditele või tehnilistele kirjeldustele, konkreetsed hindamiskriteeriumid ja -meetodid ning kavandatud usaldusväärsuse tase: baastase, märkimisväärne ja/või kõrge tase **ning vajaduse korral hindamise tase**.

(56a) Euroopa sertifitseerimise kava usaldusväärsus loob kindlustunde, et IKT protsess, toode või teenus vastab konkreetse Euroopa küberturvalisuse sertifitseerimise kava turvanõuetele. Sertifitseeritud IKT protsesside, toodete ja teenuste raamistiku järjepidevuse tagamiseks võiks Euroopa küberturvalisuse sertifitseerimise kavas täpsustada nimetatud kava alusel väljastatud Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide usaldusväärsuse tasemed. Iga sertifikaat võiks osutada ühele usaldusväärsuse tasemele: baastase, märkimisväärne või kõrge tase, samas kui ELi vastavusdeklaratsioon võiks osutada üksnes usaldusväärsuse baastasemele. Usaldusväärsuse tase annab ettekujutuse hindamiseks vajalikust jõupingutusest [...] ning seda iseloomustatakse, osutades sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilistele kontrollidele, mille eesmärk on vähendada või vältida küberturvalisuse intsidente. Iga usaldusväärsuse tase peaks olema järjepidev eri valdkondade lõikes, kus sertifitseerimist kohaldatakse.

(56b) Euroopa küberturvalisuse sertifitseerimise kavas võib täpsustada mitu hindamise taset, sõltuvalt kasutatud hindamismetoodika rangusest ja ulatuslikkusest, mis peaks vastama ühele usaldusväärsuse tasemele ja olema seotud usaldusväärsuse komponentide asjakohase kombinatsiooniga. Kõigi usaldusväärsuse tasemete puhul peaks IKT toode või teenus sisaldama mitmeid turvalisi funktsioone, nagu on määratletud kavas, mis võivad hõlmata järgmist: turvaline tehasekonfiguratsioon (*secure out-of-the-box configuration*), märgiga kood (*signed code*), turvaline uuendus (*secure update)* ja vallutuse leevendus (*exploit mitigations*) ning täielik pinu/kuhja mälu kaitse (*full stack/heap memory protections*). Neid funktsioone oleks tulnud arendada ja hallata, kasutades turvalisusele suunatud arendamisalaseid lähenemisviise ja seotud vahendeid, et tagada nende tõhusate mehhanismide (nii tarkvara kui ka riistvara) usaldusväärne inkorporeerimine. Usaldusväärsuse baastaseme puhul tuleks hindamisel juhinduda vähemalt järgmistest usaldusväärsuse komponentidest: hindamine peaks hõlmama vähemalt IKT toote või teenuse tehnilise dokumentatsiooni läbivaatamist vastavushindamisasutuse poolt. Kui sertifitseerimine hõlmab IKT protsesse, peaks tehnilist läbivaatamist kohaldama ka protsesside suhtes, mida on kasutatud IKT toote või teenuse projekteerimiseks, arendamiseks ja säilitamiseks. Juhul kui Euroopa küberturvalisuse sertifitseerimise kavas nähakse ette vastavuse enesehindamine, peaks piisama sellest, kui tootja või teenuseosutaja on viinud läbi enesehindamise IKT protsesside, toodete või teenuste vastavuse kohta sertifitseerimise kavale. Märkimisväärse usaldusväärsuse taseme puhul tuleks hindamisel lisaks usaldusväärsuse baastasemele juhinduda vähemalt IKT toote või teenuse turvafunktsioonide vastavuse kontrollimisest selle toote või teenuse tehnilisele dokumentatsioonile. Kõrge usaldusväärsuse taseme puhul tuleks hindamisel lisaks märkimisväärsele usaldusväärsuse tasemele juhinduda vähemalt tõhususe kontrollist, mille käigus hinnatakse IKT toote või teenuse turvafunktsioonide võimet panna vastu neile, kes panevad märkimisväärsete oskuste ja vahendite abil toime läbimõeldud küberrünnakuid.

(56c) Ettevalmistava kava koostamisel peaks ENISA konsulteerima kõigi asjaomaste sidusrühmadega nagu Euroopa standardiorganisatsioonid, asjakohased riiklikud asutused, vastastikuse tunnustamise kokkulepete alusel moodustatud organisatsioonid nagu SOG-IS, VKEd, tarbijaorganisatsioonid ning keskkondlikud ja ühiskondlikud sidusrühmad.

(56d) ENISA peaks haldama veebisaiti, mis tutvustab Euroopa küberturvalisuse sertifitseerimise kavasid ja pakub nende kohta teavet, mis muu hulgas hõlmab taotlusi Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava koostamiseks ning ENISA poolt ettevalmistavas etapis teostatud konsulteerimise käigus saadud tagasisidet. Selline veebisait peaks samuti pakkuma teavet käesoleva määruse kohaselt välja antud sertifikaatide ja ELi vastavusdeklaratsioonide kohta.

(57) Euroopa küberturvalisuse sertifitseerimise **ja ELi vastavusdeklaratsiooni** kasutamine peaks jääma vabatahtlikuks, kui liidu õigusaktides **või liidu õiguse kohaselt vastu võetud** siseriiklikes õigusaktides pole sätestatud teisiti. **Ühtlustatud õigusaktide puudumise korral võivad liikmesriigid võtta vastu riiklikke tehnilisi norme vastavalt direktiivile (EL) 2015/1535, nähes ette kohustusliku sertifitseerimise Euroopa küberturvalisuse sertifitseerimise kava raames. Liikmesriigid võiksid Euroopa küberturvalisuse sertifitseerimist kasutada samuti riigihangete ja direktiivi 2014/214/EL kontekstis. [...]**

(57a) Käesoleva määruse eesmärkide saavutamiseks ja siseturu killustumise vältimiseks tuleks siiski lõpetada riiklike küberturvalisuse sertifitseerimise kavade või menetluste kohaldamine Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT toodete ja teenuste suhtes alates kuupäevast, mille komisjon on rakendusaktiga kehtestanud. Lisaks ei peaks liikmesriigid kehtestama uusi riiklikke küberturvalisuse sertifitseerimise kavasid IKT toodetele ja teenustele, mis on juba kaetud kehtiva Euroopa küberturvalisuse sertifitseerimise kavaga. Liikmesriike ei tohiks aga takistada võtmast vastu või säilitamast riiklikke sertifitseerimise kavasid riikliku julgeolekuga seotud eesmärkidel.

(58) Kui Euroopa küberturvalisuse sertifitseerimise kava on vastu võetud, peaksid IKT toodete tootjad või IKT teenuste osutajad saama esitada enda valitud vastavushindamisasutusele taotluse oma toodete või teenuste sertifitseerimiseks. Kui vastavushindamisasutused vastavad käesolevas määruses sätestatud teatavatele konkreetsetele nõuetele, peaks akrediteerimisasutus need akrediteerima. Akrediteeringu saab anda maksimaalselt viieks aastaks ja selle kehtivust võib pikendada samadel tingimustel senikaua, kuni vastavushindamisasutus vastab nõuetele. Akrediteerimisasutus peaks vastavushindamisasutuse akrediteeringut **piirama, selle peatama või** tühistama, kui akrediteeringu andmise tingimused ei ole täidetud või ei ole enam täidetud või asutuse poolt võetavad meetmed rikuvad käesolevat määrust.

(59) [...] Liikmesriigid [...] **peaksid** määrama ühe **või mitu** küberturvalisuse sertifitseerimise [...] asutust, kes jälgiksid **käesolevast määrusest tulenevate kohustuste täitmist**. **Kui liikmesriik peab seda asjakohaseks, võidakse ülesanded anda juba olemasolevatele asutustele. Samuti peaks liikmesriikidel olema võimalik vastastikusel kokkuleppel teise liikmesriigiga otsustada määrata selle teostamiseks kõnealuses teises liikmesriigis asuv järelevalveasutus või mitu järelevalveasutust. Asutus peaks ennekõike jälgima ja jõustama tema riigi territooriumil asuvate IKT toodete tootjate ja IKT teenuste osutajate kohustusi seoses ELi vastavusdeklaratsiooniga, abistama riiklikke akrediteerimisasutusi vastavushindamisasutuste tegevuse seire ja järelevalve osas, pakkudes neile oskusteavet ja asjakohast teavet, volitama vastavushindamisasutusi täitma oma ülesandeid, kui nad vastavad kavas sätestatud täiendavatele nõutele ja seiravad asjakohaseid arenguid küberturvalisuse sertifitseerimise valdkonnas [...].** Riiklikud **küberturvalisuse** sertifitseerimise [...] asutused peavad käsitlema füüsiliste või juriidiliste isikute esitatud kaebusi seoses **nende või vastavushindamisasutuste poolt väljastatud kõrge usaldusväärsuse tasemega sertifikaatidega**, [...] uurima asjakohasel määral kaebuse sisu ja teavitama kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest. Lisaks peavad nad tegema koostööd teiste riiklike **küberturvalisuse** sertifitseerimise [...] asutuste või muude avaliku sektori asutustega, sealhulgas jagades teavet IKT toodete ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete küberturvalisuse sertifitseerimise kavade nõuetele.

(60) Et tagada Euroopa küberturvalisuse sertifitseerimise raamistiku järjekindel rakendamine, tuleks luua Euroopa küberturvalisuse sertifitseerimise rühm (edaspidi „rühm“), mis koosneb riiklike **küberturvalisuse** sertifitseerimise [...] asutuste **või muude asjakohaste riiklike asutuste esindajatest**. Rühma peamised ülesanded peaksid olema nõustada ja abistada komisjoni töös, mille eesmärk on tagada Euroopa küberturvalisuse sertifitseerimise raamistiku järjepidev rakendamine ja kohaldamine; aidata ametit ja teha temaga tihedat koostööd ettevalmistavate küberturvalisuse sertifitseerimise kavade koostamisel; soovitada, et komisjon paluks ametil koostada ettevalmistav Euroopa küberturvalisuse sertifitseerimise kava ning võtta vastu **ametile** adresseeritud arvamusi **ettevalmistavate kavade kohta** ja komisjonile adresseeritud arvamusi seoses olemasolevate Euroopa küberturvalisuse sertifitseerimise kavade alalhoidmise ja läbivaatamisega.

(60a) Rühm peaks soodustama heade tavade ja oskusteabe vahetamist riiklike küberturvalisuse sertifitseerimise asutuste vahel, kes vastutavad vastavushindamisasutustele lubade andmise ja sertifikaatide väljastamise eest. Rühm peaks toetama vastastikuse hindamise mehhanismi väljatöötamist ettevalmistava kava koostamise ja selle rakendamise kontekstis kõrge usaldusväärsuse tasemega Euroopa küberturvalisuse sertifikaate väljastavate asutuste jaoks. Sellise vastastikuse hindamise käigus tuleks eeskätt hinnata, kas asjaomastel asutustel on piisavalt oskusteavet ja kas nad täidavad ülesandeid harmoneeritud viisil. Vastastikuse hindamise tulemused tuleks teha avalikult kättesaadavaks. Need asutused võivad võtta asjakohaseid meetmeid, et kohandada oma tavasid ja oskusteavet.

(61) Et suurendada teadlikkust ja hõlbustada tulevaste Euroopa küberturvalisuse kavade aktsepteerimist, võib Euroopa Komisjon välja anda üldiseid või sektoripõhiseid küberturvalisuse suuniseid, näiteks küberturvalisuse heade tavade või vastutustundliku küberruumis käitumise kohta, tuues välja sertifitseeritud IKT toodete ja teenuste kasutamise positiivse mõju.

(61a) Et veelgi enam soodustada kaubavahetust ja tunnistades, et IKT tarneahelad on ülemaailmsed, võib liit sõlmida ELi toimimise lepingu artikli 218 kohaselt vastastikuse tunnustamise lepinguid Euroopa küberturvalisuse sertifitseerimise raamistiku alusel kehtestatud kavade raames väljastatud sertifikaatide kohta. Võttes arvesse ENISA-lt ja Euroopa küberturvalisuse sertifitseerimise rühmalt saadud nõu, võib komisjon soovitada alustada vastavaid läbirääkimisi. Igas kavas tuleks näha ette kolmandate riikidega toimuva vastastikuse tunnustamise konkreetsed tingimused.

(62) [...]

(63) [...]

(64) Et tagada ühetaolised tingimused käesoleva määruse rakendamiseks, tuleks komisjonile anda käesolevas määruses sätestatud rakendusvolitused. Neid volitusi tuleks teostada kooskõlas määrusega (EL) nr 182/2011.

(65) Kontrollimenetlust tuleks kasutada selliste rakendusaktide vastuvõtmiseks, milles käsitletakse IKT toodete ja teenuste suhtes kohaldatavaid Euroopa küberturvalisuse sertifitseerimise kavasid; ameti korraldatavate [...] **uurimiste** üksikasju; ning asjaolusid, vorminguid ja korda, mille kohaselt riiklikud **küberturvalisuse** sertifitseerimise [...] asutused teavitavad komisjoni akrediteeritud vastavushindamisasutustest.

(66) Ameti tööd tuleks hinnata sõltumatult. Hindamisel tuleks pidada silmas ameti eesmärkide saavutamist, selle töövõtteid ning ülesannete asjakohasust. Selle hindamise käigus tuleks vaadelda ka Euroopa küberturvalisuse sertifitseerimise raamistiku mõju, tulemuslikkust ja tõhusust.

(67) Määrus (EL) nr 526/2013 tuleks kehtetuks tunnistada.

(68) Kuna käesoleva määruse eesmärke ei suuda liikmesriigid piisavalt saavutada ning seetõttu on neid parem saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Nimetatud artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus kaugemale sellest, mis on vajalik nimetatud eesmärgi saavutamiseks,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I JAOTIS
ÜLDSÄTTED

Artikkel 1

Reguleerimisese ja kohaldamisala

1. Et tagada siseturu nõuetekohane toimimine ja püüelda samas küberturvalisuse, kübervastupidavusvõime ja usalduse kõrge taseme poole liidus, tehakse käesoleva määrusega järgmist:

a) sätestatakse ENISA ehk [...] **Euroopa Liidu Küberturvalisuse** Ameti (edaspidi „amet“) eesmärgid, ülesanded ja organisatsioonilised aspektid ning

b) sätestatakse Euroopa küberturvalisuse sertifitseerimise kavade kehtestamise raamistik, et kindlustada liidus IKT **protsesside,** toodete ja teenuste küberturvalisuse piisav tase. Sellise raamistiku kohaldamine ei piira konkreetseid sätteid, mis puudutavad muudes liidu õigusaktides kirjeldatud vabatahtlikku või kohustuslikku sertifitseerimist.

2. **Käesolev määrus ei piira liikmesriikide küberturvalisuse alast pädevust ning samuti ei piira see mingil juhul tegevusi, mis on seotud avaliku julgeoleku, riigikaitse, riikliku julgeoleku ja riigi tegevusega kriminaalõiguse valdkonnas.**

Artikkel 2

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

(1) „küberturvalisus“ – hõlmab kõiki tegevusi, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja mõjutatud isikuid küberohtude eest;

(2) „võrgu- ja infosüsteem“ – direktiivi (EL) 2016/1148 artikli 4 punktis 1 määratletud süsteem;

(3) „riiklik võrgu- ja infosüsteemide turvalisuse strateegia“ – direktiivi (EL) 2016/1148 artikli 4 punktis 3 määratletud raamistik;

(4) „oluliste teenuste operaator“ – direktiivi (EL) nr 2016/1148 artikli 4 punktis 4 määratletud avaliku või erasektori üksus;

(5) „digitaalse teenuse osutaja“ – direktiivi (EL) 2016/1148 artikli 4 punktis 6 määratletud juriidiline isik, kes pakub digitaalset teenust;

(6) „intsident“ – direktiivi (EL) 2016/1148 artikli 4 punktis 7 määratletud sündmus;

(7) „intsidendi käsitlemine“ – direktiivi (EL) 2016/1148 artikli 4 punktis 8 määratletud protseduur;

(8) „küberoht“ – mistahes võimalik asjaolu või sündmus, mis võib **kahjustada või häirida** võrgu- ja infosüsteeme, nende kasutajaid ja mõjutatud isikuid **või neile muul viisil** halba mõju avaldada;

(9) „Euroopa küberturvalisuse sertifitseerimise kava“ – ELi tasandil määratletud normide, tehniliste nõuete, standardite ja menetluste põhjalik kogum, mida kasutatakse selle konkreetse kava kohaldamisalasse kuuluvate info- ja kommunikatsioonitehnoloogia (IKT) **protsesside,** toodete ja teenuste sertifitseerimiseks **või nende vastavuse hindamiseks**;

(9a) „riiklik küberturvalisuse sertifitseerimise kava“ – riikliku avaliku asutuse poolt välja töötatud ja vastu võetud normide, tehniliste nõuete, standardite ja menetluste põhjalik kogum, mida kasutatakse selle konkreetse kava kohaldamisalasse kuuluvate info- ja kommunikatsioonitehnoloogia (IKT) protsesside, toodete ja teenuste sertifitseerimiseks või nende vastavuse hindamiseks;

(10) „Euroopa küberturvalisuse sertifikaat“ – dokument, [...] mis tõendab, et **hinnatud on** asjaomase IKT **protsessi,** toote või teenuse **vastavust** Euroopa küberturvalisuse sertifitseerimise kavas sätestatud konkreetsetele **turva**nõuetele;

(11) „IKT toode [...]“ – võrgu- ja infosüsteemide mistahes element või elementide rühm;

(11a) „IKT teenus“ – teenus, mis koosneb täielikult või enamasti võrgu- ja infosüsteemide kaudu teabe edastamisest, säilitamisest, väljavõtmisest või töötlemisest;

(11b) „IKT protsess“ – tegevused, mille käigus kavandatakse ja töötatakse välja IKT toode või teenus, seda tarnitakse ja hallatakse;

(12) „akrediteerimine“ – akrediteerimine, nagu on kindlaks määratud määruse (EÜ) nr 765/2008 artikli 2 punktis 10;

(13) „riiklik akrediteerimisasutus“ – riiklik akrediteerimisasutus, nagu on kindlaks määratud määruse (EÜ) nr 765/2008 artikli 2 punktis 11;

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

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

(16) „standard“ – määruse (EL) nr 1025/2012 artikli 2 punktis 1 määratletud standard**;**

(16a) „tehniline kirjeldus“ – dokument, milles nähakse ette IKT protsessile, tootele või teenusele esitatavad tehnilised nõuded;

(16b) „usaldusväärsuse tase“ – loob kindlustunde, et IKT protsess, toode või teenus vastab konkreetse Euroopa küberturvalisuse sertifitseerimise kava turvanõuetele ning näitab, millisel tasemel on seda hinnatud; usaldusväärsuse tase ei mõõda IKT protsessi, toote või teenuse enda turvalisust.

II JAOTIS

ENISA ehk [...] *Euroopa Liidu Küberturvalisuse Amet*

I PEATÜKK

MANDAAT JA EESMÄRGID *[...]*

Artikkel 3

Mandaat

1. Amet hakkab tegelema ülesannetega, mis talle käesoleva määrusega pannakse, et panustada kõrgetasemelisse küberturvalisusse **kogu** liidus**, eelkõige toetades liikmesriike ja liidu institutsioone, asutusi ja organeid küberturvalisuse parandamisel**. **Amet tegutseb küberturvalisuse vallas liidu institutsioonidele, asutustele ja organitele nõuandva ja oskusteavet pakkuva kontaktüksusena.**

2. Amet teostab ülesandeid, mis talle antakse liidu õigusaktidega, milles sätestatakse meetmed liikmesriikide küberturvalisusega seotud õigus- ja haldusnormide lähendamiseks.

2a. Oma ülesannete täitmisel tegutseb amet sõltumatult ja võtab täiel määral arvesse liikmesriikide asjaomaste asutuste riiklikku oskusteavet, vältides samas tegevuse dubleerimist.

3. [...]

Artikkel 4

Eesmärgid

1. Ametist saab küberturvalisuse alaste teadmiste keskus tänu oma sõltumatusele, antava nõu ja abi ning levitatava teabe teaduslikule ja tehnilisele kvaliteedile, töökorra ja töömeetodite läbipaistvusele ning oma ülesannete hoolikale täitmisele.

2. Amet aitab liidu institutsioonidel, asutustel ja organitel ning liikmesriikidel töötada välja **liidu** küberturvalisuse alaseid poliitikameetmeid**, sealhulgas küberturvalisuse valdkondlikke poliitikameetmeid,** ja neid rakendada.

3. Amet toetab suutlikkuse ja valmisoleku arendamist kogu liidus sellega, et aitab liidu **institutsioonidel, asutustel ja organitel, nagu ka** liikmesriikidel ning avaliku ja erasektori sidusrühmadel suurendada võrgu- ja infosüsteemide kaitset, arendada **ja parandada kübervastupanuvõimet ja reageerimissuutlikkust ning arendada** küberturvalisuse valdkonna oskusi ja pädevusi [...].

4. Amet edendab liidu tasandil küberturvalisusega seotud küsimuste alast koostööd ja koordineerimist liikmesriikide, liidu institutsioonide, asutuste ja organite ning asjaomaste **era- ja avaliku sektori** [...] sidusrühmade seas, kaasa arvatud erasektoris.

5. Amet **aitab suurendada** [...] liidu tasandil küberturvalisuse alast suutlikkust, et [...] **abistada** liikmesriike küberohtude ennetamisel ja neile reageerimisel, seda eeskätt piiriüleste intsidentide puhul.

6. Amet propageerib sertifitseerimist**, et aidata vältida sertifitseerimiskavade killustatust ELis**. **Eelkõige** [...] aitab **amet** kaasa küberturvalisuse sertifitseerimise raamistiku loomisele ja haldamisele liidu tasandil vastavalt käesoleva määruse III jaotisele, et suurendada IKT toodete ja teenuste küberturvalisuse alase usaldusväärsuse läbipaistvust ning tugevdada seeläbi usaldust digitaalse siseturu vastu.

7. Amet edendab kodanike ja ettevõtjate heal tasemel teadlikkust küberturvalisusega seotud küsimustest.

IA PEATÜKK
ÜLESANDED

Artikkel 5

Liidu poliitikameetmete ja õiguse [...] arendamine ja rakendamine

Amet aitab liidu poliitikameetmete ja õiguse arendamisele ja rakendamisele kaasa järgmiselt.

1. Abistab ja annab nõu, eeskätt jagab oma sõltumatut arvamust ja teeb ettevalmistusi liidu poliitikameetmete ja õiguse arendamise ja läbivaatamise jaoks küberturvalisuse valdkonnas, aga ka valdkonnaspetsiifiliste poliitiliste ja õiguslike algatuste jaoks, kui need puudutavad küberturvalisusega seotud küsimusi.

2. Aitab liikmesriikidel järjekindlalt rakendada küberturvalisusega seotud liidu poliitikameetmeid ja õigusakte eeskätt seoses direktiiviga (EL) 2016/1148, kasutades selleks muu hulgas arvamusi, juhiseid, nõuandeid ja parimaid tavasid sellistes küsimustes nagu riskihaldus, intsidentidest teatamine ja teabe jagamine ning aidates kaasa selle valdkonna parimate tavade jagamisele pädevate asutuste vahel.

3. Annab oma panuse direktiivi (EL) 2016/1148 artikliga 11 loodud koostöörühma töösse, pakkudes selleks oma oskusteavet ja abi.

4. Toetab:

   1) liidu poliitikameetmete arendamist ja rakendamist e-identimise ja usaldusteenuste valdkonnas, eeskätt pakkudes nõu ja tehnilisi juhiseid ning aidates kaasa parimate tavade vahetamisele pädevate asutuste vahel;

   2) elektroonilise side suurema turvalisuse edendamist, muu hulgas oskusteabe ja nõu pakkumisega ning pädevate asutuste vaheliste parimate tavade jagamise soodustamisega.

5. Toetab liidu poliitikameetmetega seotud tegevuse regulaarset läbivaatamist ning esitab selleks igal aastal aruande vastava õigusraamistiku rakendamise seisu kohta seoses järgmisega:

   a) liikmesriikide teated intsidentide kohta, mille ühtsed kontaktpunktid on esitanud koostöörühmale vastavalt direktiivi (EL) 2016/1148 artikli 10 lõikele 3;

   b) teated usaldusteenuse osutajaid puudutavate turvalisuse rikkumiste ja tervikluse kadude kohta, mille järelevalveasutused esitavad ametile vastavalt määruse (EL) 910/2014 artikli 19 lõikele 3;

   c) üldkasutatavaid sidevõrke või üldkasutatavaid elektroonilise side teenuseid pakkuvate ettevõtjate edastatud teated [...] turva**intsidentide** kohta, mille pädevad asutused esitavad ametile vastavalt [Euroopa elektroonilise side seadustiku kehtestamise direktiivi] artiklile 40.

Artikkel 6

[...] ***Suutlikkuse arendamine***

1. Amet abistab:

a) liikmesriike nende tegevuses, et parandada küber[...]**ohtude** ja intsidentide ennetamist, avastamist, analüüsimist ja neile reageerimise suutlikkust, pakkudes neile vajalikke teadmisi ja oskusteavet;

b) liidu institutsioone, [...] asutusi **ja organeid** nende tegevuses, et parandada küber[...]**ohtude** ja intsidentide ennetamist, avastamist, analüüsimist ja neile reageerimise suutlikkust, pakkudes **eeskätt** asjakohast toetust liidu institutsioonide, asutuste ja organite CERTile (CERT-EU);

c) liikmesriike, kui need seda taotlevad, et arendada välja riiklikud küberturbe intsidentide lahendamise üksused (CSIRTid) vastavalt direktiivi (EL) 2016/1148 artikli 9 lõikele 5;

d) liikmesriike, kui need seda taotlevad, et arendada välja riiklikud võrgu- ja infosüsteemide turvalisuse strateegiad vastavalt direktiivi (EL) 2016/1148 artikli 7 lõikele 2; ühtlasi edendab amet nende strateegiate levitamist ja [...] **jälgib** nende rakendamisel tehtavaid edusamme kogu liidus, et propageerida parimaid tavasid;

e) liidu institutsioone liidu küberturvalisuse alaste strateegiate arendamisel ja läbivaatamisel, nende levitamisel ja nende rakendamisel tehtavate edusammude jälgimisel;

f) riiklikke ja liidu CSIRTe nende suutlikkuse arendamisel, muu hulgas edendades dialoogi ja teabevahetust tagamaks, et iga CSIRT vastab tehnika taseme osas ühistele miinimumsuutlikkuse nõuetele ning toimib kooskõlas parimate tavadega;

g) liikmesriike, korraldades **korrapäraselt** [...] liidu tasandil artikli 7 lõikes 6 osutatud ulatuslikke küberturvalisuse õppuseid ja andes õppuste hindamise ja õppuste käigus omandatud kogemuste põhjal poliitilisi soovitusi;

h) asjaomaseid avalik-õiguslikke asutusi, pakkudes neile vajaduse korral koostöös sidusrühmadega küberturvalisuse alast koolitust;

i) koostöörühma, [...] parimate tavade vahetamisel eeskätt seoses oluliste teenuste operaatorite identifitseerimisega liikmesriikide poolt, muu hulgas selles osas, mis puudutab riskide ja intsidentidega seotud piiriüleseid sõltuvusseoseid vastavalt direktiivi (EL) 2016/1148 artikli 11 lõike 3 punktile l.

2. Amet **toetab teabe jagamist sektorite siseselt ja sektorite vahel** [...], eeskätt direktiivi (EL) 2016/1148 II lisas loetletud valdkondades, pakkudes parimaid tavasid ja juhiseid kättesaadavate töövahendite ja menetluste kohta ning selle kohta, kuidas lahendada teabe jagamisega seotud regulatiivsed küsimused.

Artikkel 7

[...] ***Operatiivkoostöö liidu tasandil***

1. Amet toetab operatiivkoostööd **liikmesriikide, liidu institutsioonide, asutuste ja** [...] organite ning sidusrühmade vahel.

2. Amet teeb operatiivtasandil koostööd ja loob koostoimet liidu institutsioonide, [...] asutuste **ja organitega** (sealhulgas CERT-EU, need talitused, kelle tegevus puudutab küberkuritegevust, ning järelevalveasutused, kes tegelevad privaatsuse ja isikuandmete kaitsega), et lahendada ühist muret tekitavaid küsimusi, sealhulgas:

   a) oskusteabe ja parimate tavade vahetamine;

   b) nõu andmine ja juhiste jagamine küberturvalisusega seotud asjaomastes küsimustes;

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

3. Amet tagab CSIRTide võrgustiku sekretariaaditeenused vastavalt direktiivi (EL) 2016/1148 artikli 12 lõikele 2 ning soodustab **seda ülesannet täites** [...] teabe jagamist ja koostööd võrgustiku liikmete vahel.

4. Amet [...] **toetab** CSIRTide võrgustikus toimuvat operatiivkoostööd ning toetab liikmesriike **nende taotluse korral** järgmiselt:

   a) annab nõu, kuidas parandada intsidentide vältimise, nende avastamise ja neile reageerimise suutlikkust;

   b) [...] **hõlbustab** märkimisväärse või olulise mõjuga intsidentide [...] tehnilist **lahendamist, sealhulgas toetades eeskätt tehniliste lahenduste vabatahtlikku jagamist liikmesriikide vahel**;

   c) analüüsib nõrkusi [...] ja intsidente;

   ca) toetab nende intsidentide tehnilist järeluurimist, millel on märkimisväärne või oluline mõju vastavalt direktiivile (EL) 2016/1148.

Et saada kasu koostoimest, teevad amet ja CERT-EU neid ülesandeid täites struktureeritud koostööd **ning väldivad tegevuse dubleerimist** [...].

5. [...]

[...]

6. Amet korraldab **korrapäraselt** [...] liidu tasandi küberõppusi ning toetab liikmesriike ja ELi institutsioone, asutusi ja organeid nende taotluse korral õppuste korraldamisel. **Sellised liidu tasandi õppused võivad hõlmata tehnilisi, operatiivseid ja strateegilisi elemente** [...]. **Üks kord iga kahe aasta järel korraldatakse suuremahuline õppus, mis hõlmab kõiki neid elemente.** Lisaks annab amet vajaduse korral oma panuse valdkondlike küberõppuste korraldamisse ja aitab neid korraldada koos asjaomaste [...] **organisatsioonidega, kes võivad** osaleda ka liidu tasandi küberturvalisuse õppustel.

7. Amet koostab **tihedas koostöös liikmesriikidega** korrapäraselt ELi küberturvalisuse tehnilise olukorra aruandeid intsidentide ja ohtude kohta, võttes aluseks avatud allikatest pärit teabe, omaenda tehtud analüüsid ja aruanded, mida jagavad muu hulgas: liikmesriikide CSIRTid [...] või võrgu- ja infosüsteemide direktiivi kohased ühtsed kontaktpunktid (**mõlemad vabatahtlikkuse alusel** [...]); Europoli küberkuritegevuse vastase võitluse Euroopa keskus (EC3), CERT-EU.

8. Amet annab oma panuse, et töötada välja liidu ja liikmesriikide tasandi koostööl põhinev reageering ulatuslikele küberturvalisusega seotud piiriülestele intsidentidele või kriisidele, tehes selleks peamiselt järgmist:

   a) koondab riiklikest allikatest pärit**, vabatahtlikult jagatud** aruandeid, et aidata kaasa ühise olukorrateadlikkuse tekitamisele;

   b) tagab teabe tõhusa liikumise ja eskaleerimismehhanismide olemasolu CSIRTide võrgustiku ning liidu tasandi tehniliste ja poliitiliste otsuste tegijate vahel;

c) [...] **hõlbustab liikmesriikide taotluse korral** intsidendi või kriisi tehnilist lahendamist, sealhulgas **toetades eeskätt** tehniliste lahenduste **vabatahtlikku** jagamist liikmesriikide vahel;

d) toetab **ELi institutsioone, asutusi ja organeid ning taotluse korral liikmesriike** intsidenti või kriisi puudutava avaliku teabevahetuse puhul;

e) **toetab liikmesriike nende taotluse korral**, et [...] testida sellistele intsidentidele või kriisidele reageerimiseks mõeldud koostööplaane.

Artikkel 8

[...] ***Turg, küberturvalisuse sertifitseerimine ja standardimine***

Amet teeb järgmist:

a) toetab ja edendab käesoleva määruse III jaotises kirjeldatud IKT **protsesside,** toodete ja teenuste küberturvalisuse sertifitseerimise alaste liidu poliitikameetmete arendamist ja rakendamist järgmiselt:

1) koostab **koostöös tööstuse esindajatega** IKT **protsesside,** toodete ja teenuste Euroopa küberturvalisuse sertifitseerimise ettevalmistavaid kavasid vastavalt käesoleva määruse artiklile 44;

2) aitab komisjonil pakkuda sekretariaaditeenuseid Euroopa küberturvalisuse sertifitseerimise rühmale vastavalt käesoleva määruse artiklile 53;

3) koostab ja avaldab juhiseid ja töötab välja häid tavasid IKT toodete ja teenuste küberturvalisuse nõuete kohta, tehes selleks koostööd riikide **küberturvalisuse** sertifitseerimise [...] asutuste ja tööstusega;

3a) soovitab asjakohaseid tehnilisi kirjeldusi Euroopa küberturvalisuse sertifitseerimise kavade väljatöötamiseks, kui artikli 47 lõike 1 punktis b osutatud juhtudel standardid puuduvad;

3b) annab panuse hindamise ja sertifitseerimise protsessidega seotud piisava suutlikkuse arendamisse, koostades ja avaldades suuniseid ning toetades liikmesriike nende taotluse korral;

b) hõlbustab riskihalduse ning IKT **protsesside**, toodete ja teenuste turvalisuse Euroopa ja rahvusvaheliste standardite loomist ja kasutuselevõtmist [...];

ba) koostab koostöös liikmesriikidega nõuandeid ja juhiseid oluliste teenuste operaatoritele ja digitaalsete teenuste osutajatele esitatavate turvalisusnõuetega seotud tehniliste valdkondade, aga ka juba olemas olevate standardite, kaasa arvatud liikmesriikide riiklike standardite kohta vastavalt direktiivi (EL) 2016/1148 artikli 19 lõikele 2;

c) analüüsib korrapäraselt nii nõudluse kui ka pakkumise poole peamisi suundumusi küberturvalisuse turul ja levitab analüüsi tulemusi, et arendada küberturvalisuse turgu liidus.

Artikkel 9

[...] ***Teadmised*** **ja** ***teave*** [...]

Amet teeb järgmist:

a) analüüsib kujunemisjärgus tehnoloogiaid ja annab teemapõhiseid hinnanguid sellele, milline on tehnoloogiliste uuenduste eeldatav sotsiaalne, õiguslik, majanduslik ja regulatiivne mõju küberturvalisusele;

b) koostab pikaajalisi strateegilisi analüüse küberturvalisuse ohtude ja intsidentide kohta, et teha kindlaks väljakujunevad suundumused ja aidata vältida küberturvalisuse [...] **intsidente**;

c) jagab koostöös liikmesriikide ametiasutuste ekspertidega nõu, juhiseid ja parimaid tavasid võrgu- ja infosüsteemide turvalisuse kohta, eeskätt selles osas, mis puudutab [...] nende infrastruktuuride turvalisust, mis toetavad direktiivi (EL) 2016/1148 II lisas loetletud valdkondi **ja mida kasutavad kõnealuse direktiivi III lisas loetletud digitaalsete teenuste osutajad**;

d) koondab, korraldab ja teeb avalikkusele spetsiaalse portaali kaudu kättesaadavaks liidu institutsioonide, asutuste ja organite **ning vabatahtlikkuse alusel liikmesriikide ning era- ja avaliku sektori sidusrühmade** esitatud teavet küberturvalisuse kohta;

e) [...]

f) kogub ja analüüsib avalikult kättesaadavat teavet oluliste intsidentide kohta ning koostab aruandeid, et jagada juhiseid ettevõtjatele ja kodanikele kogu liidus.

g) [...].

Artikkel 9a

Teadlikkuse suurendamine ja haridus

Amet teeb järgmist:

a) suurendab üldsuse teadlikkust küberturvalisuse riskidest ja jagab kodanikele ja organisatsioonidele mõeldud juhiseid individuaalsete kasutajate heade tavade kohta;

b) korraldab koostöös liikmesriikidega ja liidu institutsioonide, asutuste ja organitega ning tööstusega korrapäraselt teavituskampaaniaid, et suurendada küberturvalisust ja selle nähtavust liidus;

c) abistab liikmesriike nende jõupingutustes, et suurendada küberturvalisuse alast teadlikkust ja edendada küberturvalisuse alast haridust;

d) toetab liikmesriikidevahelist paremat koordineerimist ja parimate tavade vahetamist küberturvalisuse alase hariduse ja teadlikkuse valdkonnas, hõlbustades riiklike haridusasutuste kontaktpunktide võrgustiku loomist ja haldamist.

Artikkel 10

*[...] **Teadusuuringud ja innovatsioon***

Teadusuuringute ja innovatsiooni vallas teeb amet järgmist:

a) annab liidule ja liikmesriikidele nõu küberturvalisuse valdkonnas vajalike teadusuuringute ja prioriteetide kohta, et võimaldada tulemuslikku reageerimist praegustele ja tulevastele riskidele ja ohtudele, sealhulgas seoses uue ja kujunemisjärgus info- ja kommunikatsioonitehnoloogiaga, ning riskiennetustehnoloogia tõhusat kasutamist;

b) osaleb teadusuuringute ja innovatsiooni rahastamise programmide rakendamisfaasis, kui komisjon on talle delegeerinud asjakohased volitused, või tegutseb toetusesaajana.

Artikkel 11

[...] ***Rahvusvaheline koostöö***

Amet annab panuse liidu jõupingutustesse teha koostööd kolmandate riikide ja rahvusvaheliste organisatsioonidega, et edendada rahvusvahelist koostööd küberturvalisusega seotud küsimustes, sealhulgas:

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

b) hõlbustab **asjaomastes rahvusvahelise koostöö võrgustikes** parimate tavade vahetamist [...];

c) pakub komisjonile taotluse korral oskusteavet**;**

ca) nõustab ja toetab komisjoni koostöös artikli 53 alusel loodud Euroopa küberturvalisuse sertifitseerimise rühmaga küsimustes, mis puudutavad kolmandate riikidega sõlmitavaid küberturvalisuse sertifikaatide vastastikuse tunnustamise lepinguid.

II PEATÜKK
AMETI TÖÖKORRALDUS

Artikkel 12

Struktuur

Ameti haldus- ja juhtimisstruktuur koosneb järgmistest komponentidest:

a) haldusnõukogu, kes täidab artiklis 14 sätestatud ülesandeid;

b) juhatus, kes täidab artiklis 18 sätestatud ülesandeid;

c) tegevdirektor, kes täidab artiklis 19 sätestatud kohustusi; [...]

d) alaline sidusrühm, kes täidab artiklis 20 sätestatud ülesandeid**;**

da) riiklike kontaktametnike võrgustik, kes täidab artiklis 20a sätestatud ülesandeid.

1. JAGU
HALDUSNÕUKOGU

Artikkel 13

Haldusnõukogu koosseis

1. Haldusnõukogusse kuulub igast liikmesriigist üks esindaja ning kaks komisjoni määratud esindajat. Kõigil esindajatel on hääleõigus.

2. Igal haldusnõukogu liikmel on asendusliige, kes asendab liiget tema äraolekul.

3. Haldusnõukogu liikmed ja nende asendusliikmed määratakse ametisse lähtuvalt nende küberturvalisuse alastest teadmistest, võttes arvesse vajalikke juhtimis-, haldus- ja eelarvealaseid oskusi. Komisjon ja liikmesriigid püüavad piirata oma esindajate vahetumist haldusnõukogus, et tagada selle töö järjepidevus. Komisjoni ja liikmesriikide eesmärk on saavutada meeste ja naiste võrdne esindatus haldusnõukogus.

4. Haldusnõukogu liikmete ja asendusliikmete ametiaeg on neli aastat. Neid võib ametisse tagasi nimetada.

Artikkel 14

Haldusnõukogu ülesanded

1. Haldusnõukogu:

a) määrab kindlaks ameti tegevuse üldise suuna ning tagab, et amet töötab kooskõlas käesolevas määruses sätestatud eeskirjade ja põhimõtetega. Haldusnõukogu tagab samuti, et ameti töö on vastavuses liikmesriikide ja liidu tasandi tegevusega;

b) võtab vastu artiklis 21 osutatud ameti ühtse programmdokumendi kavandi enne, kui see esitatakse arvamuse saamiseks komisjonile;

c) võtab komisjoni arvamust arvestades liikmete kahekolmandikulise häälteenamusega vastu ameti ühtse programmdokumendi vastavalt artiklile 17;

ca) teostab järelevalvet ühtses programmdokumendis sisalduva iga-aastase ja mitmeaastase tööprogrammi rakendamise üle;

d) võtab liikmete kahekolmandikulise häälteenamusega vastu ameti aastaeelarve ja täidab muid ameti eelarvega seotud ülesandeid vastavalt III peatükile;

e) annab hinnangu konsolideeritud aastaaruandele ameti tegevuse kohta ja võtab aruande vastu ning saadab nii aruande kui ka hinnangu hiljemalt järgmise aasta 1. juuliks Euroopa Parlamendile, nõukogule, komisjonile ja kontrollikojale. Aastaaruanne hõlmab raamatupidamisaruannet ning selles kirjeldatakse, kuidas amet täitis oma tulemuslikkuse näitajaid. Aastaaruanne avalikustatakse;

f) võtab vastavalt artiklile 29 vastu ameti suhtes kohaldatavad finantseeskirjad;

g) võtab vastu pettusevastase strateegia, mis on proportsionaalses vastavuses pettuseriskiga, pidades silmas rakendatavate meetmete tasuvusanalüüsi;

h) võtab vastu eeskirjad oma liikmete huvide konfliktide vältimiseks ja lahendamiseks;

i) tagab, et Euroopa Pettustevastase Ameti (OLAF) juurdlustest ning erinevatest sise- ja välisauditite aruannetest ja hindamistest tulenevate järelduste ja soovituste põhjal võetakse piisavad järelmeetmed;

j) võtab vastu oma kodukorra;

k) kasutab kooskõlas lõikega 2 ameti personali suhtes volitusi, mis on antud ametisse nimetavale asutusele ametnike personalieeskirjadega ning teenistuslepingute sõlmimise pädevust omavale asutusele Euroopa Liidu muude teenistujate teenistustingimustega (edaspidi „ametisse nimetava asutuse volitused“);

l) võtab personalieeskirjade artiklis 110 sätestatud menetluse korras vastu personalieeskirjade ning muude teenistujate teenistustingimuste rakenduseeskirjad;

m) nimetab kooskõlas käesoleva määruse artikliga 33 ametisse tegevdirektori ning vajaduse korral pikendab tema ametiaega või tagandab ta ametist;

n) nimetab ametisse peaarvepidaja, kes võib olla komisjoni peaarvepidaja, kes on oma ülesannete täitmisel täiesti sõltumatu;

o) teeb kõik otsused ameti sisestruktuuri loomise ja vajaduse korral selle muutmise kohta, võttes arvesse ameti tegevusega seotud vajadusi ja lähtudes usaldusväärsest eelarvehaldusest;

p) lubab määrata kindlaks töökorra vastavalt artiklitele 7 ja 39.

2. Haldusnõukogu võtab kooskõlas personalieeskirjade artikliga 110 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 teha otsuse ajutiselt peatada tegevdirektorile delegeeritud ja tema poolt edasi delegeeritud ametisse nimetava asutuse volitused ning täita kõnealuseid volitusi ise või delegeerida need ühele oma liikmetest või mis tahes töötajale peale tegevdirektori.

Artikkel 15

Haldusnõukogu esimees

Haldusnõukogu valib oma liikmete seast kahekolmandikulise häälteenamusega esimehe ja aseesimehe, kelle ametiaeg on neli aastat ja kelle võib ühe korra ametisse tagasi nimetada. Kui nende liikmesus haldusnõukogus lõpeb mis tahes ajal nende ametiaja jooksul, lõpeb nende ametiaeg automaatselt samal päeval. Aseesimees asendab esimeest *ex officio* juhul, kui esimehel ei ole võimalik oma kohustusi täita.

Artikkel 16

Haldusnõukogu koosolekud

1. Haldusnõukogu koosoleku kutsub kokku esimees.

2. Haldusnõukogul on aastas vähemalt kaks korralist koosolekut. Haldusnõukogu korraldab erakorralisi koosolekuid esimehe, komisjoni või vähemalt ühe kolmandiku liikmete nõudmisel.

3. Tegevdirektor osaleb haldusnõukogu koosolekutel ilma hääleõiguseta.

4. Alalise sidusrühma liikmed võivad esimehe kutsel osaleda haldusnõukogu koosolekutel ilma hääleõiguseta.

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

6. Amet osutab haldusnõukogule sekretariaaditeenust.

Artikkel 17

Haldusnõukogu hääletuskord

1. Haldusnõukogu võtab otsused vastu oma liikmete häälteenamusega.

2. Ühtse programmdokumendi ja aastaeelarve vastuvõtmiseks ning tegevdirektori ametisse nimetamiseks, ametiaja pikendamiseks ja ametist tagandamiseks on vaja kõigi haldusnõukogu liikmete kahekolmandikulist häälteenamust.

3. Igal liikmel on üks hääl. Liikme puudumise korral võib tema hääleõigust kasutada tema asendusliige.

4. Esimees osaleb hääletamisel.

5. Tegevdirektor ei osale hääletamisel.

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

2. JAGU
JUHATUS

Artikkel 18

Juhatus

1. Haldusnõukogu abistab juhatus.

2. Juhatus:

   a) valmistab ette haldusnõukogus vastuvõetavad otsused;

   b) tagab koos haldusnõukoguga, et OLAFi juurdlustest ning erinevatest sise- ja välisauditite aruannetest ja hindamistest tulenevate järelduste ja soovituste põhjal võetakse piisavad järelmeetmed;

   c) abistab ja nõustab tegevdirektorit haldusnõukogu haldus- ja eelarveküsimusi käsitlevate otsuste rakendamisel vastavalt artiklile 19, ilma et see piiraks tegevdirektori kohustusi, mis on sätestatud artiklis 19.

3. Juhatuse moodustavad haldusnõukogu liikmete seast nimetatud viis liiget, nende hulgas haldusnõukogu esimees, kes võib olla ka juhatuse esimees, ning üks komisjoni esindaja. Tegevdirektor osaleb juhatuse koosolekutel, kuid tal ei ole hääleõigust.

4. Juhatuse liikmete ametiaeg on neli aastat. Neid võib ametisse tagasi nimetada.

5. Juhatuse koosolekud toimuvad vähemalt üks kord kolme kuu tagant. Juhatuse esimees kutsub juhatuse liikmete taotlusel kokku täiendavaid koosolekuid.

6. Haldusnõukogu kehtestab juhatuse kodukorra.

7. [...]

3. JAGU
TEGEVDIREKTOR

Artikkel 19

Tegevdirektori kohustused

1. Ametit juhib tegevdirektor, kes on oma ülesannete täitmisel sõltumatu. Tegevdirektor annab aru haldusnõukogule.

2. Tegevdirektor annab Euroopa Parlamendile selle taotluse korral aru oma ülesannete täitmise kohta. Nõukogu võib kutsuda tegevdirektori oma ülesannete täitmisest aru andma.

3. Tegevdirektor vastutab järgmiste valdkondade eest:

a) ameti igapäevane juhtimine;

b) haldusnõukogus vastuvõetud otsuste rakendamine;

c) ühtse programmdokumendi kavandi koostamine ja selle esitamine heakskiitmiseks haldusnõukogule, enne kui see esitatakse komisjonile;

d) ühtse programmdokumendi rakendamine ja haldusnõukogule selle kohta aru andmine;

e) ameti iga-aastase konsolideeritud tegevusaruande koostamine**, sealhulgas iga-aastase tööprogrammi rakendamise kohta,** ja selle esitamine haldusnõukogule hindamiseks ja vastuvõtmiseks;

f) järelhindamise järelduste alusel võetavaid järelmeetmeid sisaldava tegevuskava koostamine ning iga kahe aasta järel komisjonile aruande esitamine edusammude kohta;

g) tegevuskava koostamine sise- või välisauditiaruannete ja hindamiste ning Euroopa Pettustevastase Ameti (OLAF) juurdluste järelduste põhjal järelmeetmete võtmiseks ning tehtud edusammude kohta aru andmine komisjonile kaks korda aastas ja haldusnõukogule korrapäraselt;

h) ameti suhtes kohaldatavate finantseeskirjade kavandi koostamine;

i) ameti tulude ja kulude eelarvestuse projekti koostamine ning ameti eelarve täitmine;

j) liidu finantshuvide kaitsmine ning selleks ennetusmeetmete kohaldamine pettuste, korruptsiooni ja muu ebaseadusliku tegevuse vastu võitlemiseks, tulemusliku kontrolli teostamine, eeskirjade eiramise avastamise korral valesti makstud summade tagasinõudmine ning vajaduse korral tulemuslike, proportsionaalsete ja hoiatavate haldus- ja finantskaristuste kohaldamine;

k) ameti pettustevastase strateegia koostamine ja selle esitamine haldusnõukogule heakskiitmiseks;

l) kontaktide arendamine ja hoidmine äriringkondade ja tarbijaorganisatsioonidega, et tagada korrapärane dialoog asjaomaste sidusrühmadega;

la) korrapärane teabevahetus liidu institutsioonide, asutuste ja organitega seoses nende tegevusega küberturvalisuse vallas, et tagada sidusus ELi poliitika väljatöötamisel ja rakendamisel;

m) muud tegevdirektorile käesoleva määrusega pandud ülesanded.

4. Vajaduse korral ning ameti mandaadi raames ja kooskõlas tema eesmärkide ja ülesannetega võib tegevdirektor luua ajutisi töörühmi, kuhu kuuluvad eksperdid, sealhulgas liikmesriikide pädevate ametiasutuste eksperdid. Haldusnõukogu tuleb sellest ette teavitada. Eeskätt töörühmade koosseisu, töörühmade ekspertide määramist tegevdirektori poolt ja selle töörühma tegevust käsitlev kord täpsustatakse ameti sise-eeskirjades.

5. **Vajaduse korral ja tuginedes asjakohasele kulude-tulude analüüsile võib** tegevdirektor otsustada [...] ameti ülesannete tõhusaks ja tulemuslikuks täitmiseks luua **ühes või mitmes liikmesriigis ühe kohaliku kontori või mitu kohalikku kontorit.** Enne kui tegevdirektor otsustab rajada kohaliku kontori**, peab ta küsima asjaomaste liikmesriikide, sealhulgas ameti asukohaliikmesriigi arvamust** ning saama komisjonilt **ja** haldusnõukogult eelneva nõusoleku [...]. **Kui konsulteerimise käigus lähevad tegevdirektori ja asjaomaste liikmesriikide arvamused lahku, esitatakse küsimus nõukogule arutamiseks.** Otsuses määratakse täpselt kindlaks kohaliku kontori tegevuse ulatus, et vältida tarbetuid kulusid ja ameti haldusülesannete dubleerimist [...]. **Töötajate arv kõigis kohalikes kontorites peab olema minimaalne [...] ega tohi moodustada kokku <u>rohkem kui</u> 40% <u>ameti asukohaliikmesriigis töötava personali koguarvust</u>. Igas kohalikus kontoris töötavate inimeste [...] arv ei tohi olla suurem kui 10% <u>ameti asukohakohaliikmesriigis töötava</u> [...] personali koguarvust.**

4. JAGU
ALALINE SIDUSRÜHM

Artikkel 20

Alaline sidusrühm

1. Haldusnõukogu loob tegevdirektori ettepanekul alalise sidusrühma, mis koosneb asjaomaseid sidusrühmi esindavatest tunnustatud ekspertidest, näiteks IKT tööstuse, avalikkusele kättesaadavate elektroonilise side võrkude või teenuste pakkujate, **oluliste teenuste operaatorite** ja tarbijarühmade ekspertidest, küberturvalisusega tegelevatest akadeemilistest ekspertidest ning [Euroopa elektroonilise side seadustiku kehtestamise direktiivi] alusel teavitatud riiklike reguleerivate asutuste esindajatest, samuti liidu õiguskaitseasutuste ja andmekaitse järelevalveasutuste esindajatest.

2. Eeskätt alalise sidusrühma liikmete arvu, koosseisu ja nimetamist haldusnõukogu poolt, tegevdirektori ettepanekut ja rühma tegevust käsitlev kord täpsustatakse ameti sise-eeskirjades ning see avalikustatakse.

3. Alalist sidusrühma juhatab tegevdirektor või isik, kelle tegevdirektor nimetab iga konkreetse juhtumi korral eraldi.

4. Alalise sidusrühma liikmete ametiaeg on kaks ja pool aastat. Haldusnõukogu liige ei või olla alalise sidusrühma liige. Komisjoni ja liikmesriikide ekspertidel on õigus viibida alalise sidusrühma koosolekutel ning osaleda rühma töös. Kui tegevdirektor peab seda asjakohaseks, võib kutsuda alalise sidusrühma koosolekutel ning selle töös osalema teiste asutuste esindajaid, kes ei ole alalise sidusrühma liikmed.

5. Alaline sidusrühm nõustab ametit tema ülesannete täitmisel. Eelkõige annab rühm tegevdirektorile soovitusi ameti tööprogrammi ettepaneku koostamiseks ning tagab teabevahetuse asjaomaste sidusrühmadega kõikides tööprogrammiga seotud küsimustes.

5a. Alaline sidusrühm teavitab korrapäraselt haldusnõukogu oma tegevusest.

4A. JAGU
RIIKIDE KONTAKTAMETNIKE VÕRGUSTIK

Artikkel 20a

Riikide kontaktametnike võrgustik

1. Haldusnõukogu loob tegevdirektori ettepanekul riikide kontaktametnike võrgustiku, mis koosneb liikmesriikide esindajatest.

2. Riikide kontaktametnike võrgustik koosneb kõigi liikmesriikide esindajatest. Iga liikmesriik nimetab ühe esindaja. Võrgustiku koosolekuid võib pidada erinevates ekspertide formaatides.

3. Riikide kontaktametnike võrgustik hõlbustab eelkõige ENISA ja liikmesriikide vahelist teabevahetust. Ta toetab eelkõige ENISAt oma tegevuse, leidude ja soovituste levitamisel asjaomastele sidusrühmadele ELis.

4. Riikide kontaktametnikud tegutsevad riigi tasandil kontaktpunktidena, et hõlbustada ENISA ja riiklike ekspertide koostööd ENISA tööprogrammi rakendamise raames.

5. Samal ajal kui riikide kontaktametnikud peaksid tegema tihedat koostööd oma vastavate riikide haldusnõukogu esindajatega, ei dubleeri võrgustik ei haldusnõukogu ega mõne teise ELi foorumi tööd.

6. Riikide kontaktametnike võrgustiku funktsioone ja menetlusi täpsustatakse ameti sise-eeskirjades ja need avalikustatakse.

5. JAGU
TEGEVUS

Artikkel 21

Ühtne programmdokument

1. Amet tegutseb kooskõlas ühtse programmdokumendiga, mis sisaldab tema iga-aastast ja mitmeaastast tööprogrammi ja mis hõlmab kõiki ameti kavandatud tegevusi.

2. Tegevdirektor koostab igal aastal ühtse programmdokumendi kavandi, mis sisaldab mitmeaastast ja iga-aastast programmi ja vastavaid inim- ja finantsressursside plaane ning mis on kooskõlas komisjoni delegeeritud määruse (EL) nr 1271/2013[14] artikliga 32 ja milles võetakse arvesse komisjoni kehtestatud suuniseid.

3. Haldusnõukogu võtab lõikes 1 osutatud ühtse programmdokumendi vastu iga aasta 30. novembriks ning esitab Euroopa Parlamendile, nõukogule ja komisjonile hiljemalt järgmise aasta 31. jaanuariks programmdokumendi ja kõik selle hilisemad ajakohastatud versioonid.

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

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

[14] Komisjoni 30. septembri 2013. aasta delegeeritud määrus (EL) nr 1271/2013 raamfinantsmääruse kohta asutustele, millele viidatakse Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) nr 966/2012 artiklis 208 (ELT L 328, 7.12.2013, lk 42).

6. Kui ametile antakse mõni uus ülesanne, muudab haldusnõukogu vastuvõetud aasta tööprogrammi. Kõik aasta tööprogrammi olulised muudatused võetakse vastu sama korra kohaselt nagu algne aasta tööprogramm. Haldusnõukogu võib delegeerida tegevdirektorile õiguse teha aasta tööprogrammis vähetähtsaid muudatusi.

7. Mitmeaastases tööprogrammis esitatakse üldine strateegiline programm, sealhulgas eesmärgid, oodatavad tulemused ja tulemusnäitajad. Selles esitatakse ka vahendite eraldamise programm, sealhulgas mitmeaastase eelarve ja personali jaoks.

8. Vahendite eraldamise programmi ajakohastatakse igal aastal. Strateegilist programmi ajakohastatakse, kui selle järele on vajadus, ja eriti artiklis 56 osutatud hindamise tulemuse arvessevõtmiseks.

Artikkel 22

Huvide deklaratsioon

1. Haldusnõukogu liikmed, tegevdirektor ning liikmesriikide poolt ajutiselt lähetatud ametnikud esitavad kohustuste deklaratsiooni ning deklaratsiooni, milles kinnitavad, et neil puudub või on olemas otsene või kaudne huvi, mida 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 ning ajutistes töörühmades osalevad väliseksperdid teevad 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 ja hääletusest.

3. Amet sätestab oma sise-eeskirjades lõigetes 1 ja 2 osutatud huvide deklaratsioone käsitlevate eeskirjade rakendamise praktilise korra.

Artikkel 23

Läbipaistvus

1. Amet viib oma tegevust läbi maksimaalselt läbipaistvalt ning kooskõlas artikliga 25.

2. Amet tagab üldsusele ja huvitatud isikutele asjakohase, objektiivse, usaldusväärse ja kergesti juurdepääsetava teabe andmise, eelkõige ameti töötulemuste kohta. Ühtlasi avalikustab amet artikli 22 kohaselt esitatud huvide deklaratsioonid.

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

4. Amet sätestab oma sise-eeskirjades lõigetes 1 ja 2 nimetatud läbipaistvuseeskirjade rakendamise praktilise korra.

Artikkel 24

Konfidentsiaalsus

1. Ilma et see piiraks artikli 25 kohaldamist, ei anna amet kolmandatele isikutele teavet, mida ta töötleb või saab ning mille kohta on esitatud põhjendatud taotlus teabe käsitlemiseks täielikult või osaliselt konfidentsiaalsena.

2. Haldusnõukogu liikmed, tegevdirektor, alalise sidusrühma liikmed, ajutistes töörühmades osalevad väliseksperdid ning ameti töötajad, sealhulgas liikmesriikide poolt ajutiselt lähetatud ametnikud järgivad Euroopa Liidu toimimise lepingu (ELi toimimise leping) artiklis 339 sätestatud konfidentsiaalsuse nõudeid, seda isegi pärast nende töökohustuste lõppemist.

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

4. Haldusnõukogu otsustab lubada ametil käidelda salastatud teavet, kui see on vajalik ameti ülesannete täitmiseks. Sellisel juhul võtab haldusnõukogu kokkuleppel komisjoni talitustega vastu sise-eeskirjad, millega kohaldatakse turbepõhimõtteid, mis on sätestatud komisjoni otsustes (EL, Euratom) 2015/443[15] ja 2015/444[16]. Nimetatud eeskirjad hõlmavad salastatud teabe vahetust, töötlemist ja säilitamist käsitlevaid sätteid.

---

15 Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/443 komisjoni julgeoleku kohta (ELT L 72, 17.3.2015, lk 41).

16 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).

Artikkel 25

Juurdepääs dokumentidele

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

2. Haldusnõukogu võtab määruse (EÜ) nr 1049/2001 rakendamiseks vastu menetluse kuue kuu jooksul pärast ameti loomist.

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

III PEATÜKK
EELARVE KOOSTAMINE JA STRUKTUUR

Artikkel 26

Eelarve koostamine

1. Igal aastal koostab tegevdirektor ameti järgmise eelarveaasta tulude ja kulude eelarvestuse projekti ning edastab selle koos ametikohtade loetelu kavaga haldusnõukogule. Tulud ja kulud peavad olema tasakaalus.

2. Haldusnõukogu koostab igal aastal lõikes 1 osutatud tulude ja kulude eelarvestuse projekti põhjal ameti järgmise eelarveaasta tulude ja kulude eelarvestuse projekti.

3. Haldusnõukogu saadab lõikes 2 osutatud eelarvestuse projekti, mis on osa ühtse programmdokumendi kavandist, hiljemalt iga aasta 31. jaanuariks komisjonile ja kolmandatele riikidele, kellega Euroopa Liit on sõlminud kokkulepped kooskõlas artikliga 39.

4. Kõnealusest eelarvestuse projektist lähtudes sisestab komisjon Euroopa Liidu eelarve projekti kalkulatsioonid, mida ta peab ametikohtade loetelu põhjal vajalikuks, ja üldeelarvest makstava toetuse suuruse, ning esitab selle kooskõlas ELi toimimise lepingu artiklitega 313 ja 314 Euroopa Parlamendile ja nõukogule.

5. Euroopa Parlament ja nõukogu kinnitavad ameti toetuseks kasutatavad assigneeringud.

6. Euroopa Parlament ja nõukogu võtavad vastu ameti ametikohtade loetelu.

7. Haldusnõukogu võtab ameti eelarve vastu koos ühtse programmdokumendiga. See muutub lõplikuks pärast liidu üldeelarve lõplikku vastuvõtmist. Haldusnõukogu kohandab vajaduse korral ameti eelarvet ja ühtset programmdokumenti kooskõlas liidu üldeelarvega.

Artikkel 27

Eelarve struktuur

1. Ilma et see piiraks muid sissetulekuallikaid, koosnevad ameti tulud järgmistest vahenditest:

   a) toetus liidu eelarvest;

   b) tulu, mis on ette nähtud konkreetsete kuluartiklite rahastamiseks kooskõlas artiklis 29 osutatud finantseeskirjadega;

   c) liidu rahalised vahendid delegeerimiskokkulepete või sihtotstarbeliste toetuste vormis kooskõlas artiklis 29 osutatud finantseeskirjadega ja liidu poliitikameetmeid toetavate asjakohaste õigusaktide sätetega;

d) ameti töös osalevate kolmandate riikide rahaline osalus vastavalt artiklile 39;

e) liikmesriikide vabatahtlikud rahalised või mitterahalised osamaksed; vabatahtlikke osamakseid tegevad liikmesriigid ei või sellega seoses nõuda mingit kindlat õigust ega teenust.

2. Ameti kulud hõlmavad muu hulgas personali- ja halduskulusid, tehnilise abi kulusid, taristu kulusid, tegevuskulusid ning kulusid, mis tulenevad kolmandate isikutega sõlmitud lepingutest.

Artikkel 28

Eelarve täitmine

1. Tegevdirektor vastutab ameti eelarve täitmise eest.

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

3. Ameti peaarvepidaja esitab järgmise eelarveaasta 1. märtsiks (1. märtsiks aastal N + 1) komisjoni peaarvepidajale ja kontrollikojale esialgse raamatupidamise aastaaruande.

4. Olles kätte saanud kontrollikoja märkused esialgse raamatupidamisaruande kohta, koostab ameti peaarvepidaja omal vastutusel ameti lõpliku raamatupidamisaruande.

5. Tegevdirektor esitab lõpliku raamatupidamisaruande haldusnõukogule arvamuse saamiseks.

6. Hiljemalt N + 1 aasta 31. märtsiks edastab tegevdirektor eelarve täitmise ja finantsjuhtimise aruande Euroopa Parlamendile, nõukogule, komisjonile ja kontrollikojale.

7. Peaarvepidaja edastab N + 1 aasta 1. juuliks lõpliku raamatupidamisaruande ja haldusnõukogu arvamuse Euroopa Parlamendile, nõukogule, komisjoni peaarvepidajale ja kontrollikojale.

8. Lõpliku raamatupidamisaruande esitamise tähtpäevaga samaks kuupäevaks saadab peaarvepidaja kontrollikojale esitiskirja kõnealuse raamatupidamisaruande kohta ning selle koopia komisjoni peaarvepidajale.

9. Tegevdirektor avaldab lõpliku raamatupidamisaruande järgmise aasta 15. novembriks.

10. Tegevdirektor saadab hiljemalt N + 1 aasta 30. septembriks kontrollikojale vastuse selle märkuste kohta ning vastuse koopia haldusnõukogule ja komisjonile.

11. Tegevdirektor esitab taotluse korral Euroopa Parlamendile finantsmääruse artikli 165 lõike 3 kohaselt kogu teabe, mida on vaja kõnealust eelarveaastat käsitleva eelarve täitmise aruande kinnitamismenetluse tõrgeteta rakendamiseks.

12. Euroopa Parlament annab nõukogu soovituse põhjal heakskiidu tegevdirektori tegevusele N aasta eelarve täitmise kohta enne N + 2 aasta 15. maid.

Artikkel 29

Finantseeskirjad

Haldusnõukogu võtab pärast komisjoniga konsulteerimist vastu ameti suhtes kohaldatavad finantseeskirjad. Need ei või lahkneda delegeeritud määrusest (EL) nr 1271/2013, välja arvatud juhul, kui see on konkreetselt vajalik ameti toimimiseks ja komisjon on selleks eelnevalt nõusoleku andnud.

Artikkel 30

Pettuse tõkestamine

1. Selleks et lihtsustada võitlust pettuste, korruptsiooni ja muu ebaseadusliku tegevuse vastu vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL, Euratom) nr 883/2013,[17] ühineb amet kuue kuu jooksul alates oma tegevuse algusest 25. mai 1999. aasta institutsioonidevahelise kokkuleppega Euroopa Pettustevastase Ameti (OLAF) sisejuurdluste kohta ja võtab vastu kõikide oma töötajate suhtes kohaldatavad asjakohased sätted, kasutades kõnealuse kokkuleppe lisas esitatud vormi.

2. Kontrollikojal on õigus auditeerida dokumentide põhjal ja kohapeal kõiki toetusesaajaid, töövõtjaid ja alltöövõtjaid, keda amet on rahastanud liidu vahenditest.

[17] 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).

3. OLAF võib korraldada Euroopa Parlamendi ja nõukogu määruses (EL, Euratom) nr 883/2013 ja nõukogu 11. novembri 1996. aasta määruses (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)[18] sätestatud korras juurdlusi ja kohapealseid kontrolle eesmärgiga teha kindlaks, kas on esinenud pettust, korruptsiooni või muud ebaseaduslikku tegevust, mis mõjutab liidu finantshuve seoses ameti rahastatud toetuse või lepinguga.

4. Ilma et see piiraks lõigete 1, 2 ja 3 kohaldamist, sisaldavad ameti ning kolmandate riikide ja rahvusvaheliste organisatsioonide vahelised koostöölepingud ning lepingud, toetuslepingud ja toetuse määramise otsused sätteid, mis annavad kontrollikojale ja OLAFile sõnaselgelt õiguse selliste auditite ja juurdluste läbiviimiseks vastavalt nende pädevusele.

IV PEATÜKK
AMETI PERSONAL

Artikkel 31

Üldsätted

Ameti personali suhtes kohaldatakse personalieeskirju, muude teenistujate teenistustingimusi ja muid liidu institutsioonide kokkuleppega kõnealuste personalieeskirjade jõustamiseks vastu võetud eeskirju.

[18] 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).

Artikkel 32

Privileegid ja immuniteedid

Ameti ja selle personali suhtes kohaldatakse Euroopa Liidu lepingule ja ELi toimimise lepingule lisatud protokolli nr 7 (Euroopa Liidu privileegide ja immuniteetide kohta).

Artikkel 33

Tegevdirektor

1. Tegevdirektor võetakse tööle ajutise teenistujana vastavalt Euroopa Liidu muude teenistujate teenistustingimuste artikli 2 punktile a.

2. Tegevdirektori nimetab ametisse haldusnõukogu komisjoni esitatud kandidaatide nimekirjast pärast avatud ja läbipaistvat valikumenetlust.

3. Tegevdirektoriga lepingu sõlmimisel esindab ametit haldusnõukogu esimees.

4. Enne ametisse määramist kutsutakse haldusnõukogu valitud kandidaat esinema Euroopa Parlamendi pädeva komisjoni ette ja vastama parlamendiliikmete küsimustele.

5. Tegevdirektori ametiaeg on **neli** [...] aastat. Selle aja lõpuks koostab komisjon hinnangu, milles võetakse arvesse tegevdirektori tegevuse hindamist ning ameti edasisi ülesandeid ja väljakutseid.

6. Tegevdirektori ametisse nimetamise, ametiaja pikendamise ja ametist tagandamise otsused teeb haldusnõukogu hääleõigusega liikmete kahekolmandikulise häälteenamusega.

7. Komisjoni ettepanekul, milles võetakse arvesse lõikes 5 osutatud hinnangut, võib haldusnõukogu pikendada tegevdirektori ametiaega üks kord kuni **nelja**[...] aasta võrra.

8. Haldusnõukogu teatab tegevdirektori ametiaja pikendamise kavatsusest Euroopa Parlamendile. Kolme kuu jooksul enne ametiaja pikendamist esineb tegevdirektor Euroopa Parlamendi pädeva komisjoni kutsel selle ees ja vastab parlamendiliikmete küsimustele.

9. Tegevdirektor, kelle ametiaega on pikendatud, ei või osaleda samale ametikohale uue direktori valiku menetluses.

10. Tegevdirektori võib ametist tagandada üksnes haldusnõukogu otsusega[...].

Artikkel 34

Lähetatud riiklikud eksperdid ja muud töötajad

1. Amet võib kasutada riikide lähetatud eksperte või muid ametiväliseid töötajaid. Sellise personali suhtes ei kohaldata personalieeskirju ega muude teenistujate teenistustingimusi.

2. Haldusnõukogu võtab vastu otsuse, milles sätestatakse riiklike ekspertide ametisse lähetamist käsitlevad eeskirjad.

V PEATÜKK
ÜLDSÄTTED

Artikkel 35

Ameti õiguslik seisund

1. Amet on liidu asutus ja juriidiline isik.

2. Tal on kõikides liikmesriikides kõige ulatuslikum juriidilisele isikule siseriiklike õigusaktidega antud õigus- ja teovõime. Eelkõige võib amet omandada ja võõrandada vallas- ja kinnisasju ning olla kohtus menetlusosaliseks[...].

3. Ametit esindab tegevdirektor.

Artikkel 36

Ameti vastutus

1. Ameti lepingulist vastutust reguleerib vastava lepingu suhtes kohaldatav õigus.

2. Ameti sõlmitud lepingus sisalduva vahekohtuklausli alusel kohtuotsuste tegemine kuulub Euroopa Liidu Kohtu pädevusse.

3. Lepinguvälise vastutuse korral hüvitab amet kõik kahjud, mida amet või selle teenistujad oma kohustuste täitmisel on tekitanud, vastavalt liikmesriikide seaduste ühistele üldpõhimõtetele.

4. Kõikide selliste kahjude hüvitamisega seotud vaidluste lahendamine kuulub Euroopa Liidu Kohtu jurisdiktsiooni alla.

5. Teenistujate vastutust ameti ees reguleerivad ameti töötajate suhtes kohaldatavad sätted.

Artikkel 37

Kasutatavad keeled

1. Ameti suhtes kohaldatakse nõukogu määrust nr 1[19]. Liikmesriigid ja teised nende poolt määratud asutused võivad pöörduda ameti poole ja saada vastuse nende poolt valitud liidu institutsioonide ametlikus keeles.

2. Ameti toimimiseks vajalikke tõlketeenuseid osutab Euroopa Liidu Asutuste Tõlkekeskus.

Artikkel 38

Isikuandmete kaitse

1. Amet kohaldab isikuandmete töötlemise suhtes Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 45/2001[20].

2. Haldusnõukogu võtab vastu määruse (EÜ) nr 45/2001 artikli 24 lõikes 8 osutatud rakendusmeetmed. Haldusnõukogu võib võtta vastu täiendavaid meetmeid, mida amet peab võtma määruse (EÜ) nr 45/2001 kohaldamiseks.

---

19 Määrus nr 1 keelte kasutamise korra kohta Euroopa Aatomienergiaühenduses (EÜT 17, 6.10.1958, lk 401).

20 Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrus (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (EÜT L 8, 12.1.2001, lk 1).

Artikkel 39

Koostöö kolmandate riikide ja rahvusvaheliste organisatsioonidega

1. Niivõrd kui see on vajalik käesoleva määruse eesmärkide saavutamiseks, võib amet teha koostööd kolmandate riikide pädevate asutuste ja/või rahvusvaheliste organisatsioonidega. Selleks võib amet komisjoni eelneval nõusolekul leppida kolmandate riikide asutuste ja rahvusvaheliste organisatsioonidega kokku koostöökorra. Kõnealune koostöökord ei too liidule ega selle liikmesriikidele kaasa õiguslikke kohustusi.

2. Amet on osalemiseks avatud nendele kolmandatele riikidele, kes on sõlminud liiduga vastavad lepingud. Kõnealuste lepingute asjakohaste sätete alusel töötatakse välja kord, milles täpsustatakse eelkõige nende riikide ameti töös osalemise olemust, ulatust ja viisi, sealhulgas sätteid, mis käsitlevad ameti esitatud algatustes osalemist, rahalist panust ja töötajaid. Personaliküsimustes peab kõnealune kord olema igal juhul kooskõlas personalieeskirjadega.

3. Haldusnõukogu võtab vastu strateegia, mis käsitleb kolmandate riikide või rahvusvaheliste organisatsioonidega arendatavaid suhteid ameti pädevusse kuuluvates küsimustes. Komisjon tagab, et amet tegutseb oma mandaadi piires ja olemasolevas institutsioonilises raamistikus, leppides ameti tegevdirektoriga kokku asjakohase töökorra.

Artikkel 40

Julgeolekueeskirjad salastatud teabe ja tundliku, kuid salastamata teabe kaitse kohta

Amet võtab komisjoniga konsulteerides vastu oma julgeolekueeskirjad, kohaldades julgeolekupõhimõtteid, mis sisalduvad komisjoni julgeolekueeskirjades, mis käsitlevad Euroopa Liidu salastatud teabe ja tundliku, kuid salastamata teabe kaitset ning mis on sätestatud komisjoni otsustes (EL, Euratom) 2015/443 ja 2015/444. See hõlmab muu hulgas sellise teabe vahetust, töötlemist ja säilitamist.

Artikkel 41

Peakorterileping ja tegutsemistingimused

1. Vajalikud kokkulepped, milles käsitletakse ametile asukohaliikmesriigis antavaid ruume ja selle liikmesriigi pakutavaid vahendeid ning ameti asukohaliikmesriigis tegevdirektori, haldusnõukogu liikmete, ameti töötajate ja nende perekonnaliikmete suhtes kohaldatavaid erieeskirju, sätestatakse ameti ja vastuvõtva liikmesriigi vahelises peakorterilepingus, mis sõlmitakse pärast haldusnõukogu heakskiidu saamist ja hiljemalt [kaks aastat pärast käesoleva määruse jõustumist].

2. Ameti asukohaliikmesriik tagab ametile [...]tegutsemistingimused, et tagada ameti nõuetekohane toimimine, sealhulgas asukoha ligipääsetavus, sobivate haridusasutuste olemasolu töötajate laste jaoks, laste ja abikaasade piisav juurdepääs tööturule, sotsiaalkindlustusele ja arstiabile.

Artikkel 42

Halduskontroll

Ameti tegevuse üle teostab järelevalvet ombudsman ELi toimimise lepingu artikli 228 kohaselt.

III JAOTIS

KÜBERTURVALISUSE SERTIFITSEERIMISE RAAMISTIK

Artikkel 43

Euroopa küberturvalisuse sertifitseerimise **raamistik[...]**

1. **Luuakse Euroopa küberturvalisuse sertifitseerimise raamistik, et parandada siseturu toimimise tingimusi, suurendades liidus küberturvalisuse taset. Nimetatud raamistiku kaudu kehtestatakse juhtimine, mis võimaldab ELi tasandil ühtlustatud lähenemisviisi Euroopa küberturvalisuse sertifitseerimise kavadele, eesmärgiga luua IKT protsesside, toodete ja teenuste jaoks digitaalne ühtne turg.**

2. **Euroopa küberturvalisuse sertifitseerimise raamistikuga määratletakse mehhanism, et luua** [...] Euroopa küberturvalisuse sertifitseerimise kavad [...] **ning** kinnitada, et selliste kava**de** kohaselt [...] **hinnatud** IKT **protsessid**, tooted ja teenused vastavad kirjeldatud **turva**nõuetele **[...] eesmärgiga kaitsta** salvestatud, edastatud või töödeldud andmete või nende toodete, protsesside **ja** teenuste funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust [...] **kogu olelusringi kestel**.

Artikkel 44

Euroopa küberturvalisuse sertifitseerimise kava ettevalmistamine ja vastuvõtmine

1. Komisjoni **või artikli 53 alusel loodud Euroopa küberturvalisuse sertifitseerimise rühma (edaspidi „rühm“)** taotluse põhjal koostab ENISA Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava, mis vastab käesoleva määruse artiklites 45, 46 ja 47 sätestatud tingimustele.[...]

1a. Liikmesriigid või huvitatud sidusrühmade organisatsioonid võivad teha rühmale Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava koostamise ettepaneku. Rühm hindab selliseid ettepanekuid kriteeriumide alusel, mis on rühma poolt määratletud suuniste abil kooskõlas artikli 53 lõike 3 punktiga ca ning võib taotleda, et ENISA koostaks Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava.

2. Käesoleva artikli lõikes 1 osutatud ettevalmistavat kava koostades konsulteerib ENISA kõigi asjaomaste sidusrühmadega **läbipaistvas konsultatsiooniprotsessis** ja teeb rühmaga tihedat koostööd. Rühm pakub ENISA-le [...] abi ja eksperdinõu seoses ettevalmistava sertifitseerimiskava koostamisega **ja võtab ettevalmistava kava kohta vastu arvamuse enne, kui kava esitatakse komisjonile** [...]. **ENISA tagab, et ettevalmistav kava on vastavuses kohaldatava ühtlustatud standardiga, mida kasutatakse vastavushindamisasutuse akrediteerimiseks.**

3. ENISA võtab **enne** käesoleva artikli lõike 2 kohaselt koostatud [...] ettevalmistava kava **edastamist** [...] komisjonile **täiel määral arvesse rühma arvamust**.

4. Komisjon võib ENISA esitatud ettevalmistava kava põhjal võtta kooskõlas artikli 55 lõikega 2 vastu rakendusaktid, millega nähakse ette Euroopa küberturvalisuse sertifitseerimise kavad IKT protsesside, toodete ja teenuste jaoks, mis vastavad käesoleva määruse artiklite 45, 46 ja 47 nõuetele.

5. [...]

Artikkel 44a

Euroopa küberturvalisuse sertifitseerimise kava haldamine

1. Amet haldab spetsiaalset veebilehte, mis pakub teavet Euroopa küberturvalisuse sertifitseerimise kavade, sertifikaatide ja artikli 47a kohaselt välja antud ELi vastavusdeklaratsioonide kohta ja tutvustab neid.

2. Amet vaatab tihedas koostöös rühmaga vähemalt iga viie aasta tagant vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavad läbi, võttes arvesse huvitatud isikutelt saadud tagasisidet. Kui seda peetakse vajalikuks, võivad komisjon või rühm taotleda, et amet alustaks kooskõlas artikli 44 lõigetega 2 ja 3 muudetud ettevalmistava kava koostamist.

Artikkel 45

Euroopa küberturvalisuse sertifitseerimise kavade turvalisusega seotud eesmärgid

Euroopa küberturvalisuse sertifitseerimise kava peab olema koostatud nii, et [...] **saavutada** vajaduse korral **vähemalt** järgmised turvalisusega seotud eesmärgid:

a) kaitsta salvestatud, edastatud või muul moel töödeldud andmeid juhusliku või volitamata salvestamise, töötlemise, juurdepääsu või avalikustamise eest **kogu protsessi, toote või teenuse olelusringi kestel;**

b) kaitsta salvestatud, edastatud või muul moel töödeldud andmeid juhusliku või volitamata hävitamise, [...] kaotsimineku või muutmise **või ebapiisava kättesaadavuse eest kogu protsessi, toote või teenuse olelusringi kestel;**

c) [...] volitatud kasutajate, programmide ja masinate juurdepääs üksnes neile andmetele, teenustele või funktsioonidele, millele neil on juurdepääsuõigused;

d) talletada, millal ja kes on [...] **pääsenud juurde** millistele andmetele, funktsioonidele või teenustele, **neid kasutanud või muul viisil töödelnud**;

e) [...] võimalus kontrollida, millal ja kes on pääsenud juurde millistele andmetele, teenustele või funktsioonidele, [...] neid kasutanud **või muul viisil töödelnud**;

f) taastada füüsilise või tehnilise intsidendi korral õigeaegselt andmete, teenuste ja funktsioonide käideldavus ja juurdepääs neile;

g) tagada IKT **protsesside**, toodete ja teenuste pakkumine ajakohastatud tark- **ja riist**varaga, mis **ei** sisalda **avalikult** teadaolevaid turvaauke, ning et olemas on mehhanismid turvaliseks [...] uuendamiseks**;**

ga) IKT protsessid, tooted ja teenused töötatakse välja, toodetakse ja tarnitakse vastavalt asjaomases kavas ette nähtud turvanõuetele.

Artikkel 46

Euroopa küberturvalisuse sertifitseerimise kavade usaldusväärsuse tasemed

1. Euroopa küberturvalisuse sertifitseerimise kavas määratakse selle kava raames sertifitseeritud IKT **protsessidele**, toodetele ja teenustele üks või mitu järgmist usaldusväärsuse taset: baastase, märkimisväärne ja/või kõrge tase[...]. **Usaldusväärsuse tase peab vastama IKT protsessi, toote või teenuse ettenähtud kasutamisega seotud riskitasemele.**

2. Baastase, märkimisväärne ja kõrge usaldusväärsuse tase [...] **osutavad sertifikaadile või Euroopa küberturvalisuse sertifitseerimise kava raames välja antud ELi vastavusdeklaratsioonile, milles esitatakse iga usaldusväärsuse taseme kohta vastavad turvanõuded, sealhulgas turvafunktsioonid ja vastav IKT protsessi, toote või teenuse hindamiseks vajalik jõupingutus. Sertifikaadi või ELi vastavusdeklaratsiooni kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on vähendada või vältida küberturvalisuse intsidente järgmiselt:**

a) **Euroopa küberturvalisuse sertifikaat või ELi vastavusdeklaratsioon, mis osutab** usaldusväärsuse baastasemele, **annab kindluse, et IKT protsessid, tooted või teenused täidavad vastavaid turvanõudeid, sealhulgas turvafunktsioone ning et neid on hinnatud tasemeni, mille eesmärk on minimeerida küberintsidentide ja küberrünnete teadaolevaid põhilisi riske. Hindamistegevused hõlmavad vähemalt tehnilise dokumentatsiooni läbivaatamist või, kui see ei ole asjakohane, samaväärse mõjuga asendustegevusi;**

b) **Euroopa küberturvalisuse sertifikaat**, **mis osutab** märkimisväärsele usaldusväärsuse tasemele, annab **kindluse, et IKT protsessid**, **tooted ja teenused täidavad vastavaid turvanõudeid, sealhulgas turvafunktsioone ning et neid on hinnatud tasemeni, mille eesmärk on minimeerida teadaolevaid küberriske, küberintsidente ja küberründeid, mis pannakse toime märkimisväärsete oskuste ja vahenditega tegijate poolt. Hindamistegevused hõlmavad vähemalt järgmisi tegevusi: kontrollimine, et ei esine avalikult teadaolevaid turvaauke ning testimine, et IKT protsessid, tooted ja teenused rakendavad korrektselt vajalikke turvafunktsioone; või kui see ei ole asjakohane, hõlmavad hindamistegevused samaväärse mõjuga asendustegevusi [...];**

c) **Euroopa küberturvalisuse sertifikaat**, **mis osutab** kõrgele usaldusväärsuse tasemele, annab **kindluse, et IKT protsessid**, **tooted ja teenused täidavad vastavaid turvanõudeid, sealhulgas turvafunktsioone ning et neid on hinnatud tasemeni, mille eesmärk on minimeerida selliste tipptasemel küberrünnete riski, mis pannakse toime märkimisväärsete oskuste ja vahenditega tegijate poolt. Hindamistegevused hõlmavad vähemalt järgmisi tegevusi: kontrollimine, et ei esine avalikult teadaolevaid turvaauke ning testimine, et IKT protsessid, tooted ja teenused rakendavad korrektselt vajalikke turvafunktsioone tipptasemel ning nende oskuslikele häkkeritele vastupanemise võime hindamine turvatestimise kaudu; või kui see ei ole asjakohane, hõlmavad hindamistegevused samaväärse mõjuga asendustegevusi [...].**

2a. Euroopa küberturvalisuse sertifitseerimise kavas võidakse täpsustada mitmed hindamise tasemed, sõltuvalt hindamismetoodika rangusest ja põhjalikkusest. Iga hindamistase vastab ühele usaldusväärsuse tasemele ja määratletakse usaldusväärsuse komponentide asjakohase kombinatsiooni kaudu.

Artikkel 47

Euroopa küberturvalisuse sertifitseerimise kavade elemendid

1. Euroopa küberturvalisuse sertifitseerimise kava sisaldab **vähemalt** järgmisi elemente:

a) sertifitseerimise **kava** sisu ja ulatus, sealhulgas hõlmatud IKT **protsesside**, toodete ja teenuste liik või kategooria, **samuti selgitus selle kohta, kuidas sertifitseerimise kava vastab eeldatavate sihtrühmade vajadustele;**

b) [...] viide **hindamises järgitud** rahvusvahelistele, **Euroopa tasandi või riiklikele** standarditele. **Kui standardid ei ole kättesaadavad, osutatakse tehnilisele kirjeldusele, mis täidab määruse 1025/2012 II lisas toodud nõudeid, või kui selline kirjeldus ei ole kättesaadav, kavas määratletud** tehnilisele kirjeldusele **või muudele küberturvalisuse nõuetele [...].**

c) vajaduse korral üks või mitu usaldusväärsuse taset;

ca) vajaduse korral vastavushindamisasutuste suhtes kohaldatavad konkreetsed või täiendavad nõuded, et tagada nende tehniline pädevus hinnata küberturvalisuse nõudeid;

d) konkreetsed hindamiskriteeriumid ja meetodid, sealhulgas hindamise liigid, mida kasutati tõendamaks, et artiklis 45 osutatud konkreetsed eesmärgid on täidetud;

e) **vajaduse korral** sertifitseerimiseks vajalik teave, mille taotleja peab esitama **või muul viisil kättesaadavaks tegema** vastavushindamisasutustele;

f) kui kava näeb ette märgi või märgistuse, tingimused sellise märgi või märgistuse kasutamiseks;

g) [...] eeskirjad sertifikaatide nõuete **või ELi vastavusdeklaratsiooni** nõuete täitmise kontrollimiseks, sealhulgas mehhanismid tõestamaks konkreetsete küberturvalisuse nõuete jätkuvat täitmist;

h) **vajaduse korral** tingimused sertifikaadi väljaandmiseks **ja uuendamiseks ning** säilitamiseks, jätkamiseks ning sertifitseerimise ulatuse laiendamiseks **või** vähendamiseks;

i) eeskirjad sertifitseeritud **või enesehindamise läbinud** IKT toodete ja teenuste [...] **kava** tingimustele mittevastavuse tagajärgede kohta;

j) eeskirjad selle kohta, kuidas tuleks IKT **protsesside**, toodete ja teenuste varem avastamata küberturvalisuse nõrkustest teada anda ja kuidas neid menetleda;

k) **vajaduse korral** eeskirjad andmete säilitamise kohta vastavushindamisasutuste poolt;

l) sama liiki või kategooriasse kuuluvaid IKT **protsesse**, tooteid või teenuseid, **turvanõudeid ja hindamiskriteeriume ja -meetodeid** hõlmavate riiklike **või rahvusvaheliste** küberturvalisuse sertifitseerimise kavade kindlakstegemine;

m) väljastatud sertifikaatide **või ELi vastavusdeklaratsiooni sisu;**

ma) ELi vastavusdeklaratsiooni ning IKT toodete tootja või IKT teenuste osutaja poolt esitatud kogu vajalikku teavet sisaldava tehnilise dokumentatsiooni säilitamisaeg;

mb[...]) sertifikaatide maksimaalne kehtivusaeg;

mc[...]) avalikustamispoliitika väljaantud, muudetud ja tagasivõetud sertifikaatide jaoks;

md[...]) sertifitseerimise kavade kolmandate riikidega vastastikuse tunnustamise tingimused;

me[...]) vajaduse korral vastastikuse hindamise mehhanismi käsitlevad eeskirjad asutuste jaoks, kes väljastavad kooskõlas artikli 48 lõikega 4a Euroopa küberturvalisuse sertifikaate kõrge usaldusväärsuse taseme jaoks.

2. Kavas kirjeldatud nõuded ei tohi minna vastuollu kohaldatavate õiguslike nõuetega, eelkõige liidu ühtlustatud õigusaktidest tulenevate nõuetega.

3. Kui konkreetses liidu õigusaktis on nii sätestatud, võib Euroopa küberturvalisuse sertifitseerimise kava kohast sertifitseerimist **või ELi vastavusdeklaratsiooni** kasutada tõendamaks kõnealuse õigusakti nõuetele vastavuse eeldust.

4. Liidu ühtlustatud õigusaktide puudumisel võib liikmesriikide õigusaktides sätestada, et Euroopa küberturvalisuse sertifitseerimise kava võib kasutada selleks, et teha kindlaks, kas võib eeldada vastavust õiguslikele nõuetele.

Artikkel 47a

Vastavuse enesehindamine

1. Euroopa küberturvalisuse sertifitseerimise kavas võidakse lubada vastavushindamise läbiviimist IKT toodete tootjate või IKT teenuste osutajate ainuvastutusel. Selline vastavuse enesehindamine on kohaldatav ainult madala riskiga IKT toodete ja teenuste suhtes, mis vastavad usaldusväärsuse baastasemele.

2. IKT toodete tootja või IKT teenuste osutaja võib anda välja ELi vastavusdeklaratsiooni, milles antakse kinnitus, et kavas esitatud nõuded on täidetud. Sellise deklaratsiooni koostamisega võtab IKT toodete tootja või IKT teenuste osutaja vastutuse IKT toote või teenuse vastavuse eest kavas sätestatud nõuetele.

3. IKT toodete tootja või IKT teenuste osutaja hoiab ELi vastavusdeklaratsiooni ja asjaomast tehnilist dokumentatsiooni, mis puudutab kogu teavet IKT toodete või teenuste vastavuse kohta kavale, vastavas Euroopa küberturvalisuse sertifitseerimise kavas määratletud perioodi jooksul artikli 50 lõikes 1 osutatud riikliku küberturvalisuse sertifitseerimise asutuse jaoks kättesaadavana. ELi vastavusdeklaratsiooni koopia esitatakse riiklikule küberturvalisuse sertifitseerimise asutusele ja ENISA-le.

4. ELi vastavusdeklaratsiooni väljaandmine on vabatahtlik, kui liidu õigusnormides ega liikmesriikide õiguses ei ole sätestatud teisiti.

5. Käesoleva artikli kohaselt välja antud ELi vastavusdeklaratsiooni tunnustatakse kõigis liikmesriikides.

Artikkel 48

Küberturvalisuse sertifitseerimine

1. Kui IKT **protsessid**, tooted ja teenused on sertifitseeritud Euroopa küberturvalisuse sertifitseerimise kava kohaselt, mis on vastu võetud kooskõlas artikliga 44, eeldatakse, et nad vastavad sellise kava nõuetele.

2. Sertifitseerimine on vabatahtlik, kui liidu õigusnormides **või liikmesriikide õiguses** ei ole sätestatud teisiti.

3. Käesoleva artikli kohase Euroopa küberturvalisuse sertifikaadi, **milles osutatakse kas usaldusväärsuse baastasemele või märkimisväärsele tasemele**, annavad välja artiklis 51 osutatud vastavushindamisasutused artikli 44 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavas sisalduvate kriteeriumide alusel.

4. Erandina lõikest 3 võib nõuetekohaselt põhjendatud juhtudel teatavas Euroopa küberturvalisuse **sertifitseerimise** kavas ette näha, et sellest kavast tuleneva Euroopa küberturvalisuse sertifikaadi võib välja anda üksnes avalik-õiguslik asutus. Selline [...] asutus on üks järgnevatest asutustest:

a) artikli 50 lõikes 1 osutatud riiklik **küberturvalisuse** sertifitseerimise [...]asutus;

b) artikli 51 lõike 1 kohaselt vastavushindamisasutusena akrediteeritud **avalik** asutus [...]

c) [...].

4a. Juhul kui artikli 44 kohane Euroopa küberturvalisuse sertifitseerimise kava nõuab kõrget usaldusväärsuse taset, võib sertifikaadi väljastada ainult artikli 50 lõikes 1 osutatud riiklik küberturvalisuse sertifitseerimise asutus või artiklis 51 osutatud vastavushindamisasutus, kui täidetud on järgmised tingimused:

a) riikliku küberturvalisuse sertifitseerimise asutuse eelneval heakskiidul iga üksiku vastavushindamisasutuse poolt välja antud sertifikaadi puhul; või

b) riikliku küberturvalisuse sertifitseerimise asutuse poolt kõnealuse ülesande eelneval delegeerimisel vastavushindamisasutusele.

5. Füüsiline või juriidiline isik, kes esitab oma IKT **protsessid**, tooted või teenused sertifitseerimiseks, peab [...] **tegema** artiklis 51 osutatud vastavushindamisasutusele **või artiklis 50 osutatud riiklikule küberturvalisuse sertifitseerimise asutusele**, **juhul kui nimetatud asutus on sertifikaati väljastav asutus, kättesaadavaks** kogu sertifitseerimismenetluse läbiviimiseks vajaliku teabe.

5a. Sertifikaadi omanik teavitab sertifikaati väljaandvat asutust mis tahes hiljem avastatud haavatavustest või nõuete rikkumistest, mis puudutavad sertifitseeritud IKT protsessi, toote või teenuse turvalisust ja millel võib olla mõju sertifitseerimisega seotud nõuetele. Asutus edastab selle teabe põhjendamatu viivituseta riiklikule küberturvalisuse sertifitseerimise asutusele.

6. Sertifikaat antakse [...] **konkreetses sertifitseerimise kavas määratletud perioodiks** ja selle kehtivust võib pikendada [...], kuni asjakohased nõuded on täidetud.

7. Käesoleva artikli kohaselt välja antud Euroopa küberturvalisuse sertifikaati tunnustatakse kõigis liikmesriikides.

Artikkel 49

Riiklikud küberturvalisuse sertifitseerimise kavad ja sertifikaadid

1. Ilma et see piiraks lõike 3 kohaldamist, lõpeb riiklike küberturvalisuse sertifitseerimise kavade ja Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT **protsesside**, toodete ja teenustega seotud menetluste õiguslik toime artikli 44 lõike 4 kohaselt vastu võetud rakendusaktis sätestatud kuupäeval. Olemasolevad riiklikud küberturvalisuse sertifitseerimise kavad ja Euroopa küberturvalisuse sertifitseerimise kavaga hõlmamata IKT **protsesside**, toodete ja teenustega seotud menetlused jäävad alles.

2. Liikmesriigid ei kehtesta uusi riiklikke küberturvalisuse sertifitseerimise kavasid IKT **protsesside**, toodete ja teenuste jaoks, mis on kaetud kehtiva Euroopa küberturvalisuse sertifitseerimise kavaga.

3. Riiklike küberturvalisuse sertifitseerimise kavade alusel väljastatud sertifikaadid, **mis on hõlmatud Euroopa küberturvalisuse sertifitseerimise kavaga**, jäävad kehtima kuni oma kehtivusaja lõpuni.

Artikkel 50

Riiklikud* küberturvalisuse *sertifitseerimise [...] asutused

1. Iga liikmesriik **[...] määrab oma territooriumil ühe või mitu** riiklikku **küberturvalisuse** sertifitseerimise [...] asutust **või vastastikusel kokkuleppel teise liikmesriigiga ühe või mitu asutust, mis luuakse nimetatud teises liikmesriigis ja mis vastutavad järelevalveülesannete eest määravas liikmesriigis.**

2. Iga liikmesriik teatab komisjonile **[...] määratud asutuste andmed ja neile antud ülesanded.**

3. **Ilma et see piiraks artikli 48 lõike 4 punkti a ja artikli 48 lõike 4a** kohaldamist, on [...]iga riiklik **küberturvalisuse** sertifitseerimise [...] asutus oma organisatsiooni, rahastamisotsuste, õigusliku struktuuri ja otsuste tegemise poolest sõltumatu üksustest, mille üle ta järelevalvet teostab.

3a. Liikmesriigid tagavad, et riikliku küberturvalisuse sertifitseerimise asutuse tegevus seoses sertifikaatide väljastamisega kooskõlas artikli 48 lõike 4 punktiga a ja artikli 48 lõikega 4a peab kinni rollide ja vastutusalade rangest lahususest käesolevas artiklis nimetatud järelevalvetegevustega ning et mõlemad tegevused toimivad üksteisest sõltumatult.

4. Liikmesriigid tagavad, et riiklikel **küberturvalisuse** sertifitseerimise [...] asutustel on piisavad ressursid oma volituste rakendamiseks ning oma ülesannete tulemuslikuks ja tõhusaks täitmiseks.

5. Määruse tõhusaks rakendamiseks on asjakohane, et need asutused osaleksid aktiivselt, tõhusalt, tulemuslikult ja turvaliselt artikli 53 kohaselt asutatud Euroopa küberturvalisuse sertifitseerimise rühma töös.

6. Riiklikud **küberturvalisuse** sertifitseerimise [...] asutused:

a) [...]

aa) jälgivad ja jõustavad nende riigi territooriumil asutatud IKT toodete tootja või IKT teenuste osutaja artikli 47a lõigetes 2 ja 3 sätestatud kohustusi ning vastavas Euroopa küberturvalisuse sertifikaadi kavas toodud kohustusi;

b) [...] **ilma et see piiraks artikli 51 lõike 1b kohaldamist, aitavad riiklikke akrediteerimisasutusi** vastavushindamisasutuste tegevuse **jälgimisel ja kontrollimisel** käesoleva määruse kohaldamisel [...];

ba) jälgivad ja kontrollivad artikli 48 lõikes 4 osutatud asutuste tegevust;

bb) volitavad artikli 51 lõikes 1b osutatud vastavushindamisasutusi ning piiravad, peatavad või võtavad tagasi olemasolevaid volitusi juhul, kui käesoleva määruse nõudeid ei täideta;

c) käsitlevad füüsiliste või juriidiliste isikute esitatud kaebusi seoses sertifikaatidega, mille on väljastanud **riiklik küberturvalisuse sertifitseerimise asutus [...] või kooskõlas artikli 48 lõikega 4a vastavushindamisasutused**, uurivad asjakohasel määral kaebuse sisu ja teavitavad kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest;

d) teevad koostööd teiste riiklike **küberturvalisuse** sertifitseerimise [...]asutuste või muude avaliku sektori asutusega, sealhulgas jagades teavet IKT **protsesside**, toodete ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele;

e) jälgivad küberturvalisuse sertifitseerimise valdkonna asjakohaseid arenguid.

7. Igal riiklikul **küberturvalisuse** sertifitseerimise [...]asutusel on vähemalt järgmised volitused:

a) anda vastavushindamisasutustele, [...] Euroopa küberturvalisuse sertifikaadi omanikele **ja ELi vastavusdeklaratsiooni väljastajatele** korraldus esitada teavet, mis on vajalik tema ülesannete täitmiseks;

b) teostada auditi vormis vastavushindamisasutuste, Euroopa küberturvalisuse sertifikaadi omanike **ja ELi vastavusdeklaratsiooni väljastajate** uurimist, et kontrollida nende vastavust III jaotise sätetele;

c) võtta asjakohaseid meetmeid vastavalt siseriiklikele õigusaktidele tagamaks, et vastavushindamisasutused, sertifikaadi omanikud **ja ELi [...] vastavusdeklaratsiooni väljastajad** järgivad käesoleva määruse või Euroopa küberturvalisuse sertifitseerimise kava nõudeid;

d) saada juurdepääs kõigile vastavushindamisasutuste ja Euroopa küberturvalisuse sertifikaadi omanike ruumidele, et teostada uurimisi kooskõlas liidu või liikmesriigi menetlusõigusega;

e) võtta siseriiklike õigusaktide kohaselt tagasi sertifikaadid, **mille on väljastanud riiklik küberturvalisuse sertifitseerimise asutus või kooskõlas artikli 48 lõikega 4a vastavushindamisasutus** ning mis ei ole kooskõlas käesoleva määrusega või Euroopa küberturvalisuse sertifitseerimise kavaga;

f) määrata karistusi vastavalt artiklile 54, kooskõlas siseriikliku õigusega ning nõuda käesolevas määruses sätestatud kohustuste rikkumise viivitamatut lõpetamist.

8. Riiklikud **küberturvalisuse** sertifitseerimise [...]asutused teevad omavahel ja komisjoniga koostööd ning vahetavad eelkõige teavet, kogemusi ja häid tavasid seoses küberturvalisuse sertifitseerimisega ning IKT **protsesside**, toodete ja teenuste küberturvalisust puudutavate tehniliste küsimustega.

Artikkel 51

Vastavushindamisasutused

1. Vastavushindamisasutused akrediteeritakse määruse (EÜ) nr 765/2008 kohaselt nimetatud riikliku akrediteerimisasutuse poolt ainult siis, kui nad vastavad käesoleva määruse lisas sätestatud nõuetele.

1a. Juhul kui Euroopa küberturvalisuse sertifikaat antakse välja riikliku küberturvalisuse sertifitseerimise asutuse poolt vastavalt artikli 48 lõike 4 punktile a ja artikli 48 lõikele 4a, akrediteeritakse käesoleva artikli lõike 1 kohaselt riikliku küberturvalisuse sertifitseerimise asutuse sertifitseerimise organ vastavushindamisasutuseks.

1b. Vajaduse korral volitatakse vastavushindamisasutused riikliku küberturvalisuse sertifitseerimise asutuse poolt viima ellu selle ülesandeid, kuid nad täidavad artikli 47 lõike 1 punkti ca kohaseid Euroopa sertifitseerimise kavas sätestatud konkreetseid või täiendavaid nõudeid.

2. Akrediteering antakse maksimaalselt viieks aastaks ja selle kehtivust võib pikendada samadel tingimustel senikaua, kuni vastavushindamisasutus vastab käesolevas artiklis sätestatud nõuetele. Akrediteerimisasutus **võtab mõistliku aja jooksul kõik asjakohased meetmed, et piirata, peatada või** tühistada käesoleva artikli lõikes 1 osutatud vastavushindamisasutuse akrediteerimine, kui akrediteerimise tingimused ei ole täidetud või ei ole enam täidetud või asutuse poolt võetavad meetmed rikuvad käesolevat määrust.

Artikkel 52

Teavitamine

1. Riiklikud **küberturvalisuse** sertifitseerimise [...] asutused teatavad iga artikli 44 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava puhul komisjonile, millised akrediteeritud, **ja vajaduse korral artikli 51 lõike 1b kohaselt** volitatud vastavushindamisasutused võivad anda välja artiklis 46 osutatud usaldusväärsuse tasemel sertifikaate, ning teatavad põhjendamatu viivituseta kõigist hilisematest muudatustest.

2. Üks aasta pärast Euroopa küberturvalisuse sertifitseerimise kava jõustumist avaldab komisjon teatatud vastavushindamisasutuste nimekirja *Euroopa Liidu Teatajas*.

3. Kui komisjoni teavitatakse pärast lõikes **2**[...] osutatud ajavahemiku möödumist, avaldab ta Euroopa Liidu Teatajas lõikes 2 osutatud nimekirja muudatused kahe kuu jooksul alates kõnealuse teate saamise kuupäevast.

4. Riiklik **küberturvalisuse** sertifitseerimise [...]asutus võib esitada komisjonile taotluse eemaldada selle riikliku sertifitseerimise järelevalveasutuse poolt teatatud vastavushindamisasutus käesoleva artikli lõikes 2 osutatud nimekirjast. Komisjon avaldab Euroopa Liidu Teatajas vastavad nimekirja muudatused ühe kuu jooksul alates riikliku **küberturvalisuse** sertifitseerimise [...]asutuse taotluse kättesaamise kuupäevast.

5. Komisjon võib määrata rakendusaktidega kindlaks käesoleva artikli lõikes 1 osutatud teavitamise asjaolud, vormingud ja menetlused. Kõnealused rakendusaktid võetakse vastu vastavalt artikli 55 lõikes 2 osutatud kontrollimenetlusele.

Artikkel 53

Euroopa küberturvalisuse sertifitseerimise rühm

1. Luuakse Euroopa küberturvalisuse sertifitseerimise rühm (edaspidi „rühm“).

2. Rühm koosneb riiklike **küberturvalisuse** sertifitseerimise [...] asutuste **esindajatest või teiste asjakohaste riiklike asutuste esindajatest.** [...] **Rühma iga liige võib esindada ainult ühte teist liikmesriiki.**

3. Rühmal on järgmised ülesanded:

a) nõustada ja abistada komisjoni töös, mille eesmärk on tagada käesoleva jaotise järjepidev rakendamine ja kohaldamine, eelkõige seoses küberturvalisuse sertifitseerimise poliitika küsimuste, poliitika koordineerimise ja Euroopa küberturvalisuse sertifitseerimise kavade ettevalmistamisega;

b) abistada ja nõustada ENISAt ja teha temaga koostööd seoses ettevalmistava kava koostamisega kooskõlas käesoleva määruse artikliga 44;

ba) võtta käesoleva määruse artikli 44 kohaselt vastu arvamus ettevalmistava kava kohta;

c) [...] **paluda** ametil koostada Euroopa küberturvalisuse sertifitseerimise ettevalmistav kava kooskõlas käesoleva määruse artikliga 44;

ca) töötada välja ja võtta vastu suunised kriteeriumide kohta [...]rühmale esitatava ettevalmistava kava koostamise ettepanekute hindamiseks artikli 44 lõike 1a kohaselt;

d) võtta vastu komisjonile suunatud arvamusi seoses olemasolevate Euroopa küberturvalisuse sertifitseerimise kavade alalhoidmise ja läbivaatamisega;

e) analüüsida küberturvalisuse sertifitseerimise valdkonna asjakohaseid arenguid ja vahetada häid tavasid seoses küberturvalisuse sertifitseerimise kavadega;

f) lihtsustada riiklike **küberturvalisuse** sertifitseerimise [...] asutuste käesoleva jaotise kohast koostööd **suutlikkuse suurendamise** ja teabevahetuse kaudu, eelkõige luues meetodid tõhusaks teabevahetuseks kõigis küberturvalisuse sertifitseerimisega seotud küsimustes;

fa) pakkuda tuge vastastikuse hindamise mehhanismi rakendamisele kooskõlas Euroopa küberturvalisuse sertifitseerimise kavas käesoleva määruse artikli 47 lõike 1 punkti md kohaselt kehtestatud eeskirjadega.

4. Komisjon juhatab rühma **vahendajana** ja osutab sellele sekretariaaditeenust, komisjoni abistab ENISA kooskõlas artikli 8 punktiga a.

Artikkel 53a

Õigus esitada riiklikule* küberturvalisuse *sertifitseerimise ...] asutusele kaebus

1. Füüsilistel või juriidilistel isikutel on õigus esitada kaebus riiklikule küberturvalisuse sertifitseerimise asutusele seoses sertifikaadiga, mille on väljastanud nimetatud asutus või kooskõlas artikli 48 lõikega 4a vastavushindamisasutused.

2. Riiklik küberturvalisuse sertifitseerimise asutus, kellele kaebus esitatakse, teavitab kaebuse esitajat kaebuse menetlemise käigust ja tulemusest, sealhulgas artikli 53b kohasest õiguskaitsevahendi kasutamise võimalusest.

Artikkel 53b

Õigus tõhusale õiguskaitsevahendile

1. Füüsilistel või juriidilistel isikutel on õigus kasutada tõhusat õiguskaitsevahendit riikliku küberturvalisuse sertifitseerimise asutuse neid puudutava õiguslikult siduva otsuse vastu.

2. Füüsilistel või juriidilistel isikutel on õigus kasutada tõhusat õiguskaitsevahendit, kui riiklik küberturvalisuse sertifitseerimise asutus ei käsitle kaebust.

3. Riikliku küberturvalisuse sertifitseerimise asutuse vastu algatatakse menetlused selle liikmesriigi kohtus, kus asutus asub.

Artikkel 54

Karistused

Liikmesriigid kehtestavad sätted karistuste kohta, mida rakendatakse käesoleva jaotise ja Euroopa küberturvalisuse sertifitseerimise kavade rikkumise korral, ning võtavad kõik vajalikud meetmed nende rakendamise tagamiseks. Kehtestatud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad. Liikmesriigid teavitavad komisjoni [.../viivitamata] kõnealustest eeskirjadest ja meetmetest ja kõikidest nende hilisematest muudatustest.

IV JAOTIS
LÕPPSÄTTED

Artikkel 55

Komiteemenetlus

1. Komisjoni abistab komitee. See komitee on komitee määruse (EL) nr 182/2011 tähenduses.

2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artikli 5 **lõike 4 punkti b**.

Artikkel 56

Hindamine ja läbivaatamine

1. Hiljemalt viis aastat pärast artiklis 58 osutatud kuupäeva ja seejärel iga viie aasta tagant hindab komisjon ameti ja selle töökorralduse mõju, tulemuslikkust ja tõhusust ning võimalikku vajadust muuta ameti mandaati ja kõigi selliste muudatuste finantsmõju. Hindamisel arvestatakse tagasisidet, mida amet on oma töö kohta saanud. Kui komisjon leiab, et ameti töö jätkamine ei ole ametile seatud eesmärkide, mandaadi ja ülesannete seisukohast enam põhjendatud, võib ta teha ettepaneku käesolevat määrust ametiga seotud sätete osas muuta.

2. Selle hindamise käigus vaadeldakse ka III jaotise sätete mõju, tulemuslikkust ja tõhusust seoses eesmärgiga tagada IKT toodete ja teenuste piisav küberturvalisus ELis ja parandada siseturu toimimist.

3. Komisjon edastab hindamisaruande koos oma järeldustega Euroopa Parlamendile, nõukogule ja haldusnõukogule. Hindamistulemused avalikustatakse.

Artikkel 57

Kehtetuks tunnistamine ja õigusjärglus

1. Määrus (EÜ) nr 526/2013 tunnistatakse kehtetuks alates [...].

2. Viiteid määrusele (EÜ) nr 526/2013 ja ENISA-le tõlgendatakse viidetena käesolevale määrusele ja ametile.

3. Amet on omandiõiguse, lepingute, õiguslike kohustuste, töölepingute, finantskohustuste ja vastutuse osas määrusega (EÜ) nr 526/2013 loodud ameti õigusjärglane. Kõik haldusnõukogu ja juhatuse otsused jäävad kehtima, tingimusel et nad ei ole käesoleva määrusega vastuolus.

4. Amet luuakse määramata ajaks alates [...]

5. Määruse (EÜ) nr 526/2013 artikli 24 lõike 4 alusel ametisse nimetatud tegevdirektor jääb tegevdirektoriks oma ametiaja lõpuni.

6. Määruse (EÜ) nr 526/2013 artikli 6 alusel ametisse nimetatud haldusnõukogu liikmed ja nende asendusliikmed jäävad ameti haldusnõukogu liikmeteks ja nende asendusliikmeteks oma ametiaja lõpuni.

Artikkel 58

Jõustumine

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

1a. Käesolevat määrust kohaldatakse alates […], välja arvatud artiklid 50, 51, 52, 53a, 53b ja 54, mida kohaldatakse alates [24 kuud pärast selle avaldamist *Euroopa Liidu Teatajas]*.

2. Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

VASTAVUSHINDAMISASUTUSTE SUHTES KEHTIVAD NÕUDED

Akrediteeringut saada soovivad vastavushindamisasutused peavad vastama järgmistele nõuetele.

1. Vastavushindamisasutus peab olema asutatud liikmesriigi õiguse kohaselt ning olema juriidiline isik.

2. Vastavushindamisasutus peab olema kolmandast isikust asutus, mis on sõltumatu organisatsioonist või IKT tootest või teenusest, mida ta hindab.

3. Asutust, mis kuulub ettevõtjate ühendusse või kutseliitu, mis esindab ettevõtjaid, kes on seotud nende IKT toodete või teenuste projekteerimise, tootmise, tarnimise, monteerimise, kasutamise või hooldamisega, mida see hindab, võib pidada vastavushindamisasutuseks tingimusel, et tõendatud on selle sõltumatus ning igasugune huvide konflikti puudumine.

4. Vastavushindamisasutus, selle kõrgem juhtkond ja vastavushindamisülesannete täitmise eest vastutavad töötajad ei tohi olla hinnatava IKT toote või teenuse projekteerija, tootja, tarnija, paigaldaja, ostja, omanik, kasutaja, hooldaja ega ühegi nimetatud osalise volitatud esindaja. See ei välista vastavushindamisasutuse tegevuseks vajalike hinnatavate toodete kasutamist ega nende toodete kasutamist isiklikul otstarbel.

5. Vastavushindamisasutus, selle kõrgem juhtkond ja vastavushindamisülesannete täitmise eest vastutavad töötajad ei tohi olla otsesel viisil seotud nimetatud IKT toodete või teenuste disaini või projekteerimise, valmistamise või ehitamise, turustamise, paigaldamise, kasutamise või hooldusega ega esindada ühtegi isikut, kes nimetatud tegevustega tegeleb. Nad ei tohi osaleda tegevuses, mis võib seada kahtluse alla nende otsuste sõltumatuse ja usaldusväärsuse vastavushindamistoimingutes, mille tegemiseks neist on teavitatud. See kehtib eelkõige nõustamisteenuste puhul.

6. Vastavushindamisasutused peavad tagama, et nende tütarettevõtjate või lepingupartnerite tegevus ei mõjuta vastavushindamistoimingute konfidentsiaalsust, objektiivsust ja erapooletust.

7. Vastavushindamisasutused ja nende töötajad peavad tegema vastavushindamistoiminguid suurima erialase usaldusväärsuse ja nõutava erialase tehnilise pädevusega ning ei tohi alluda ühelegi surveavaldusele ega ahvatlusele, sealhulgas rahalisele, mis võib nende otsuseid või vastavushindamistoimingute tulemusi mõjutada, see on eriti oluline selliste isikute või isikute rühmade puhul, kes on huvitatud nimetatud toimingute tulemustest.

8. Vastavushindamisasutus peab olema võimeline täitma kõiki vastavushindamisülesandeid, mis talle käesoleva määrusega on määratud, seda nii juhul, kui vastavushindamisasutus täidab ülesandeid ise, kui ka juhul, kui neid täidetakse tema nimel ja vastutusel.

9. Vastavushindamisasutuse käsutuses peavad olema alati ja kõigile IKT toodete ja teenuste liikidele, kategooriatele või alamkategooriatele ning kõigile vastavushindamismenetlustele vastavad järgmised vahendid:

a) töötajad, kellel on tehnilised teadmised ning piisav asjakohane kogemus vastavushindamisülesannete täitmiseks;

b) menetluste kirjeldused, mille kohaselt vastavushindamist tehakse ning mis tagavad nende menetluste läbipaistvuse ja kordamise võimaluse. Asutusel peavad olema asjakohased tegevuspõhimõtted ja menetlused, kus eristatakse ülesandeid, mida ta täidab teavitatud asutusena, ja muud tegevust;

c) menetlused toimingute tegemiseks, mis võtavad asjakohaselt arvesse ettevõtja suurust, tegutsemisvaldkonda, tema struktuuri, IKT toote või teenuse tehnoloogia keerukuse astet ning seda, kas tegemist on mass- või seeriatootmisega.

10. Vastavushindamisasutusel peavad olema vajalikud vahendid vastavushindamistoimingute nõuetekohase teostamisega seotud tehniliste ja haldusülesannete täitmiseks ning juurdepääs vajalikule varustusele ja vahenditele.

11. Vastavushindamistoimingute teostamise eest vastutavatel töötajatel peavad olema järgmised oskused:

a) heal tasemel tehniline ja kutseõpe, mis hõlmab kõiki vastavushindamistegevusi;

b) piisavad teadmised nende poolt tehtavate hindamistoimingute nõuetest ning piisav pädevus nimetatud hindamistoiminguteks;

c) sobilikud teadmised ja arusaam kehtivatest nõuetest ja katsestandarditest;

d) oskus koostada sertifikaate, protokolle ja aruandeid, mis tõendavad hindamistoimingute läbiviimist.

12. Tuleb tagada vastavushindamisasutuste, nende kõrgema juhtkonna ja hindamistöötajate erapooletus.

13. Vastavushindamisasutuse kõrgema juhtkonna ja hindamistöötajate tasu suurus ei tohi sõltuda tehtud hindamiste arvust ega nimetatud hindamiste tulemustest.

14. Vastavushindamisasutus peab sõlmima vastutuskindlustuslepingu, välja arvatud juhul, kui vastutust kannab liikmesriigi õiguse kohaselt riik või kui vastavushindamine on liikmesriigi enda otsene ülesanne.

15. Vastavushindamisasutuse töötajad peavad hoidma ametisaladust teabe osas, mis on saadud käesoleva määruse või selle jõustamiseks vastuvõetud siseriiklike õigusaktide kohaselt täidetud ülesannete käigus, välja arvatud teabevahetus selle liikmesriigi pädevate asutustega, kus asutus tegutseb.

16. Vastavushindamisasutus peab vastama **asjakohase** standardi nõuetele, **mis on ühtlustatud määruse (EÜ) 765/2008 kohaselt protsesside, toodete või teenuste sertifitseerimisprotsessi läbiviivate vastavushindamisasutuste akrediteerimiseks** [...].

17. Vastavushindamisasutus peab tagama, et vastavushindamiseks kasutatavad katselaborid vastavad **asjakohase** standardi nõuetele, **mis on ühtlustatud määruse (EÜ) 765/2008 alusel katselaborite akrediteerimiseks**[...].