Euroopa Liidu
Nõukogu

Brüssel, 1. märts 2018
(OR. en)

Institutsioonidevaheline dokument:
2017/0225 (COD)

12183/2/17
REV 2

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139
CSC 276
CSCI 68

ETTEPANEK

Komisjoni dok nr:	COM(2017) 477 final/3
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“)

Käesolevaga edastatakse delegatsioonidele dokument COM(2017) 477 final/3.

Lisatud: COM(2017) 477 final/3

EUROOPA
KOMISJON

Brüssel, 22.2.2018
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2017

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

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“)

(EMPs kohaldatav tekst)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

SELETUSKIRI

1. ETTEPANEKU TAUST

• Ettepaneku põhjused ja eesmärgid

Euroopa Liit on võtnud mitmeid meetmeid, et suurendada oma vastupidavusvõimet ja valmisolekut küberturvalisuse valdkonnas. 2013. aastal vastu võetud esimeses Euroopa Liidu küberjulgeoleku strateegias[1] sätestati strateegilised eesmärgid ja konkreetsed meetmed, et saavutada vastupidavusvõime, vähendada küberkuritegevust, töötada välja küberkaitse põhimõtted ja suutlikkus, arendada tööstuslikke ja tehnoloogilisi ressursse ning luua ELi jaoks ühtne rahvusvaheline küberruumi poliitika. Selles kontekstis on hiljem toimunud olulisi arenguid, sealhulgas eelkõige Euroopa Liidu Võrgu- ja Infoturbeametile (edaspidi „ENISA“) teise mandaadi andmine[2] ning **võrgu ja infosüsteemide turvalisuse direktiivi**[3] (edaspidi „võrgu- ja infoturbe direktiiv“) vastuvõtmine, mis on käesoleva ettepaneku alus.

Lisaks sellele **võttis Euroopa Komisjon 2016. aastal vastu teatise „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine“**,[4] milles teatati täiendavatest meetmetest, et suurendada koostööd, teavitamist ja teadmiste jagamist ning suurendada ELi vastupidavusvõimet ja valmisolekut, võttes arvesse ka suuremahuliste intsidentide ja üleeuroopalise küberturvalisuse kriisi tekkimise võimalust. Selles kontekstis teatas komisjon, et ta korraldab Euroopa Parlamendi ja nõukogu määruse (EL) nr 526/2013 (mis käsitleb Euroopa Liidu Võrgu- ja Infoturbeametit (ENISA) ning millega tunnistatakse kehtetuks määrus (EÜ) nr 460/2004, edaspidi „ENISA määrus“) **hindamise** ja **läbivaatamise**. Hindamise tulemusena võidakse ametit reformida ning suurendada selle suutlikkust ja võimet toetada liikmesriike jätkusuutlikul viisil. Seega saaks amet hindamise tulemusena operatiivsema ja kesksema rolli küberturvalisuse vastupidavusvõime saavutamisel ning ameti uues mandaadis võetaks arvesse selle uusi kohustusi võrgu- ja infoturbe direktiivi alusel.

Võrgu- ja infoturbe direktiiv on esimene oluline etapp, et edendada riskijuhtimise kultuuri, kehtestades turvanõuded juriidilise kohustusena peamistele majandustegevuses osalejatele, eelkõige olulisi teenuseid osutavatele operaatoritele (edaspidi „oluliste teenuste operaator“) ja peamiste digitaalsete teenuste osutajatele (edaspidi „digitaalse teenuse osutaja“). Kuna turvanõuded on üliolulised, et kaitsta ühiskonna üha suuremast digitaaltehnoloogiale üleminekust saadavat kasu, ja võttes arvesse ühendatud seadmete kiiret levikut (asjade internet), esitatakse 2016. aasta teatises ka mõte luua IKT toodete ja teenuste turvalisuse sertifitseerimise raamistik, et suurendada usaldust ja turvalisust digitaalsel ühtsel turul. IKT küberturvalisuse sertifitseerimine muutub eriti oluliseks, võttes arvesse kõrgetasemelist

---

1 Euroopa Komisjoni ja Euroopa välisteenistuse ühisteatis: „Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum“ (JOIN(2013)).

2 Määrus (EL) nr 526/2013, mis käsitleb Euroopa Liidu Võrgu- ja Infoturbeametit (ENISA) ning millega tunnistatakse kehtetuks määrus (EÜ) nr 460/2004.

3 Direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus.

4 Komisjoni teatis „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine“ (COM(2016) 0410 final).

küberturvalisust eeldava tehnoloogia suuremat kasutamist, näiteks internetiühendusega ja automatiseeritud autod, e-tervis ning tööstuslikud automatiseeritud juhtimissüsteemid.

Neid poliitikameetmeid ja teadaandeid toetati veelgi **nõukogu** 2016. aasta **järeldustes**, milles kinnitati, et „küberohud ja -haavatavused arenevad edasi ja muutuvad intensiivsemaks, mis nõuab jätkuvat ja tihedamat koostööd, eriti laiaulatuslike piiriüleste küberintsidentide käsitlemisel“. Järeldustes kinnitati, et ENISA määrus on üks ELi kübervastupidavusvõime raamistiku põhielementidest,[5] ning kutsuti komisjoni üles võtma täiendavaid meetmeid, et tegeleda sertifitseerimise küsimusega Euroopa tasandil.

Sertifitseerimissüsteemi loomiseks oleks vaja luua ELi tasandil nõuetekohane juhtimissüsteem, sealhulgas sõltumatu ELi ameti kaudu antavate oskusteadmiste abil. Selles kontekstis määratakse käesoleva ettepanekuga kindlaks, et ENISA kui küberturvalisuse küsimustes pädev ELi tasandi amet peaks hakkama täitma seda ülesannet, et tuua kokku sertifitseerimise valdkonnas pädevad liikmesriikide asutused ja nende tööd koordineerida.

Komisjon täpsustas oma **2017. aasta mai digitaalse ühtse turu strateegia vahekokkuvõtet** käsitlevas teatises veelgi, et ta vaatab ENISA mandaadi läbi 2017. aasta septembriks. Selle eesmärk on määrata kindlaks ENISA roll muutunud küberturvalisuse keskkonnas ja töötada välja küberturvalisuse standardeid, sertifitseerimist ja märgistamist käsitlevad meetmed, et parandada IKT-põhiste süsteemide, sealhulgas ühendatud seadmete küberturvalisust[6]. 2017. aasta juunis toimunud **Euroopa Ülemkogu järeldustes**[7] tunnustati komisjoni kavatsust vaadata septembris läbi küberjulgeoleku strateegia ning esitada enne 2017. aasta lõppu ettepanekud täiendavate sihipäraste meetmete võtmiseks.

Väljapakutud määruses sätestatakse terviklik meetmete komplekt, mis tugineb varasematele meetmetele ja edendab järgmisi üksteist toetavaid erieesmärke:

- arendada liikmesriikide ja ettevõtjate **suutlikkust ja valmisolekut**;
- parandada k**oostööd ja koordineerimist** liikmesriikides ning ELi institutsioonides, organites ja asutustes;
- suurendada **ELi tasandil suutlikkust täiendada liikmesriikide võetavaid meetmeid**, eelkõige piiriüleste küberkriiside puhul;
- suurendada kodanike ja ettevõtjate **teadlikkust** küberturvalisusega seotud küsimustest;
- suurendada IKT toodete ja teenuste **küberturvalisuse alase usaldusväärsuse**[8] üldist **läbipaistvust**, et tugevdada usaldust digitaalse ühtse turu ja digitaalse uuendustegevuse vastu, ning

---

5 Nõukogu järeldused Euroopa kübervastupidavusvõime süsteemi tugevdamise ning konkurentsivõimelise ja uuendusliku küberjulgeolekusektori toetamise kohta, 15. november 2016.

6 Komisjoni teatis digitaalse ühtse turu strateegia rakendamise vahekokkuvõtte kohta (COM(2017) 228).

7 Euroopa Ülemkogu kohtumine (22. ja 23. juuni 2017) – järeldused (EUCO 8/17).

8 Küberturvalisuse alase usaldusväärsuse läbipaistvus tähendab seda, et kasutajatele antakse piisavalt teavet küberturvalisuse omaduste kohta, tänu millele saavad nad määrata objektiivselt kindlaks konkreetse IKT toote, teenuse või protsessi turvalisuse taseme.

- vältida **sertifitseerimiskavade killustatust** ELis ning nendega seotud turvanõuete ja hindamiskriteeriumide killustatust liikmesriikides ja sektorites.

Seletuskirja järgmises osas selgitatakse üksikasjalikumalt selle algatuse põhjusi seoses ENISA ja küberturvalisuse sertifitseerimise jaoks välja pakutud meetmetega.

ENISA

ENISA on eksperdikeskus, mille eesmärk on täiustada võrgu- ja infoturvet liidus ning toetada liikmesriikide suutlikkuse arendamist.

ENISA loodi 2004. aastal,[9] et aidata kaasa üldise eesmärgi saavutamisele, milleks on tagada ELis võrgu- ja infoturbe kõrge tase. 2013. aastal anti ametile määrusega (EL) nr 526/2013 uus seitsmeaastane mandaat kuni 2020. aastani. Amet asub Kreekas, selle juhatuse asukoht on Irákleios (Kreetal) ja peamine tegevuskoht Ateenas.

ENISA on teiste ELi ametitega võrreldes väike amet, millel on väike eelarve ja töötajate arv. Selle mandaat on tähtajaline.

ENISA toetab Euroopa Liidu institutsioone, liikmesriike ja äriringkondi **võrgu- ja infoturbe probleemidega tegelemisel, neile reageerimisel ja eelkõige nende vältimisel**. Ta teeb seda, võttes mitmeid meetmeid oma strateegias kindlaks määratud viies tegevusvaldkonnas[10]:

- oskusteadmised: peamistes võrgu- ja infoturbe küsimustes teabe ja oskusteadmiste jagamine;
- poliitika: toetus liidu poliitika kujundamisele ja rakendamisele;
- suutlikkus: toetus suutlikkuse arendamisele kogu liidus (näiteks koolituste, soovituste ja teadlikkuse suurendamise tegevuste abil);
- kogukond: võrgu- ja infoturbe kogukonna edendamine (näiteks toetus infoturbeintsidentidega tegelevatele rühmadele (edaspidi „CERT“), üleeuroopaliste küberõppuste koordineerimine);
- võimaldamine (näiteks suhtlus sidusrühmadega ja rahvusvahelised suhted).

ELi kaasseadusandjad otsustasid võrgu- ja infoturbe direktiivi üle peetavate läbirääkimiste käigus anda ENISA-le olulise rolli selle direktiivi rakendamisel. Eelkõige tagab amet sekretariaaditeenused CSIRTide võrgustikule (mis luuakse, et edendada liikmesriikide vahel kiiret ja tõhusat operatiivkoostööd konkreetsete küberturvalisuse intsidentide puhul ja jagada teavet riskide kohta) ja aitab koostöörühmal täita oma ülesandeid. Lisaks selle nõutakse direktiivis, et ENISA abistaks liikmesriike ja komisjoni, pakkudes neile oma oskusteadmisi ja andes nõu ning toetades parimate tavade vahetamist.

Komisjon on teinud ENISA määruse kohaselt ameti hindamise, mis hõlmab sõltumatut uuringut ja avalikku konsultatsiooni. Hindamise käigus analüüsiti ameti asjakohasust, mõju, tulemuslikkust, tõhusust, sidusust ja sellest saadavat ELi lisaväärtust seoses ameti tulemuste,

---

9 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).

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy

juhtimise, asutusesisese organisatsioonilise struktuuri ja töötavadega ajavahemikus 2013–2016.

ENISA üldisele tulemuslikkusele andis positiivse hinnangu enamik avalikule konsultatsioonile vastanutest[11] (74 %). Enamik vastanutest oli ka seisukohal, et ENISA saavutab oma erinevaid eesmärke (vähemalt 63 % iga eesmärgi puhul). ENISA teenuseid ja tooteid kasutavad korrapäraselt (kord kuus või sagedamini) peaaegu pooled vastanutest (46 %) ning neid hinnatakse seetõttu, et neid pakub ELi tasandi asutus (83 %) ja need on kvaliteetsed (62 %).

Samas oli valdav enamik vastanutest (88 %) seisukohal, et ELi tasandil praegu saadaval olevad vahendid ja mehhanismid ei ole piisavad, et tegeleda praeguste küberturvalisuse probleemidega, või sobivad selleks ainult osaliselt. Valdav enamik vastanutest (98 %) märkis, et nende küsimustega peaks tegelema ELi asutus, ning 99 % vastanutest pidas ENISAt selle jaoks õigeks organisatsiooniks. Lisaks sellele oli 67,5 % vastanutest seisukohal, et ENISA võiks osaleda IT toodete ja teenuste turvalisuse sertifitseerimise ühtlustatud raamistiku loomises.

Üldise hindamise käigus (mis ei põhine ainult avalikul konsultatsioonil vaid ka mitmel individuaalsel küsitlusel, täiendavatel sihtotstarbelistel uuringutel ja seminaridel) jõuti järgmistele järeldustele.

- ENISA eesmärgid on ka praegu asjakohased. Tehnoloogia kiire arengu ja muutvate ohtude kontekstis ning suurenevaid ülemaailmseid küberturvalisuse riske arvesse võttes on selgelt vaja edendada ja tugevdada ELi kõrgetasemelisi tehnilisi oskusteadmisi küberturvalisuse valdkonnas. Tuleb suurendada liikmesriikide suutlikkust mõista ohte ja neile reageerida ning sidusrühmad peavad tegema koostööd temaatiliste valdkondade ja institutsioonide üleselt.

- Ameti väikesest eelarvest hoolimata on see olnud operatiivselt tõhus oma ressursside kasutamisel ja ülesannete täitmisel. Nii Ateenas kui ka Irákleios paiknemine on siiski tekitanud täiendavaid halduskulusid.

- Tõhususe seisukohast on ENISA täitnud oma eesmärgid osaliselt. Amet on edukalt aidanud parandada võrgu- ja infoturvet Euroopas, pakkudes suutlikkuse arendamist 28 liikmesriigis,[12] tõhustades koostööd liikmesriikide ning võrgu- ja infoturbe sidusrühmade vahel ning jagades oskusteadmisi, kujundades kogukonda ja toetades

[11] Konsultatsioonile vastas 90 sidusrühma 19 liikmesriigist (88 vastust ja kaks kirjalikku seisukohavõttu), sealhulgas 15 liikmesriigi ametiasutused ja kaheksa katusorganisatsiooni, kes esindavad märkimisväärset osa Euroopa ettevõtjatest.

[12] Avalikule konsultatsioonile vastanutelt küsiti, mida nad peavad ENISA peamisteks saavutusteks aastatel 2013–2016. Kõigist rühmadest vastanud (kokku 55, sealhulgas 13 riigi ametiasutust, 20 vastanut erasektorist ja 22 muud vastanut) pidasid peamisteks ENISA järgmisi saavutusi: 1) õppuste Cyber Europe koordineerimine; 2) CERTide/CSIRTide toetamine koordineerimist ja vahetusi edendavate seminaride ja koolituse kaudu; 3) ENISA väljaanded (suunised ja soovitused, ohtude kaardistamise aruanded, intsidentidest teatamise ja kriisijuhtimise strateegiad jne), mida peeti kasulikuks, et luua ja ajakohastada riiklikke turvaraamistikke, ning lähtealusena poliitikakujundajatele ja kübervaldkonnas tegutsejatele; 4) võrgu- ja infoturbe direktiivi edendamisele kaasa aitamine; 5) küberturvalisuse kuu raames küberturvalisuse alase teadlikkuse suurendamiseks tehtavad jõupingutused.

tegevuspõhimõtete väljatöötamist. Kokkuvõttes keskendus ENISA põhjalikult oma tööprogrammi täitmisele ja oli oma sidusrühmadele usaldusväärne partner valdkonnas, mille puhul on selle tähtsat piiriülest mõju tunnustatud alles hiljuti.

- ENISA suutis avaldada vähemalt teatavas ulatuses mõju väga mahukas võrgu- ja infoturbe valdkonnas, aga ei olnud täiesti edukas tugeva kaubamärgi väljakujundamisel ning piisava märgatavuse saamisel, et olla tunnustatud peamise eksperdikeskusena Euroopas. Selle põhjus seisneb ENISA ulatuslikus mandaadis, mille jaoks ei eraldatud proportsionaalselt piisavalt ressursse. Lisaks sellele on ENISA ainus ELi amet, millel on tähtajaline mandaat, mis piirab tema võimet koostada pikaajalist strateegiat ja toetada oma sidusrühmi jätkusuutlikul viisil. See on ka vastuolus võrgu- ja infoturbe direktiivi sätetega, mis annavad ENISA-le ülesanded, millel ei ole lõppkuupäeva. Hindamise käigus leiti, et see piiratud tulemuslikkus on osaliselt põhjustatud tuginemisest asutusesiseste oskusteadmiste asemel suurel määral asutusevälistele oskusteadmistele ning spetsialistide värbamise ja tööl hoidmisega seotud probleemidest.

- Hindamise tulemusena järeldati, et ENISA lisaväärtus seisneb peamiselt ameti võimes tõhustada koostööd liikmesriikide vahel ning eelkõige asjaomaste võrgu- ja infoturbe kogukondadega (eriti CSIRTidega). ELi tasandil ei ole ühtegi teist osalejat, kes toetaks sedavõrd laialdast võrgu- ja infoturbe sidusrühmade võrgustikku. Samas kuna ENISA peab määrama oma tegevuse jaoks rangeid prioriteete, lähtub selle tööprogramm peamiselt liikmesriikide vajadustest. Seetõttu ei tegele ta piisavalt teiste sidusrühmade, eelkõige tööstusvaldkonna vajadustega. Samuti peab amet sellest tulenevalt täitma oma peamiste sidusrühmade vajadusi ja ei saa avaldada suuremat mõju. Seega andis amet erinevat lisaväärtust lähtuvalt oma sidusrühmade erinevatest vajadustest ja võimest neile reageerida (näiteks suured liikmesriigid võrreldes väikeste liikmesriikidega ja liikmesriigid võrreldes tööstusvaldkonnaga).

Kokkuvõttes nähtus sidusrühmadega konsulteerimise ja hindamise tulemustest, et ENISA ressursse ja mandaati tuleb kohandada, et amet saaks nõuetekohaselt täita oma osa praegustele ja tulevastele probleemidele reageerimisel.

Neid tulemusi arvesse võttes vaadatakse käesolevas ettepanekus läbi ENISA praegune mandaat ning määratakse kindlaks uued ülesanded eesmärgiga toetada tulemuslikult ja tõhusalt liikmesriikide, ELi institutsioonide ja muude sidusrühmade jõupingutusi Euroopa Liidus turvalise küberruumi tagamiseks. Uue välja pakutud mandaadi eesmärk on anda ametile tugevam ja kesksem osa, eelkõige toetades ka liikmesriike aktiivsemalt võrgu- ja infoturbe direktiivi rakendamisel ning konkreetsete ohtude vastases võitluses (tegevussuutlikkus) ning saades liikmesriike ja komisjoni küberturvalisuse sertifitseerimise valdkonnas toetavaks eksperdikeskuseks. Käesoleva ettepanekuga tehtaks järgmised muudatused.

- ENISA saaks alalise mandaadi ja seega kindla tuleviku. Mandaati, eesmärke ja ülesandeid tuleks siiski korrapäraselt läbi vaadata.

- Välja pakutud mandaadi puhul täpsustatakse veelgi ENISA rolli küberturvalisuse ELi ametina ja ELi küberturvalisuse ökosüsteemi võrdlusalusena, kes tegutseb tihedas koostöös kõnealuse ökosüsteemi kõigi teiste asjaomaste asutustega.

- Ameti korraldus ja juhtimine, mida peeti hindamise käigus positiivseks, vaadatakse piiratud ulatuses läbi, eelkõige veendumaks, et ameti töös kajastuvad paremini laiema sidusrühmade kogukonna vajadused.

- Mandaadi soovituslik ulatus piiritletakse, tugevdades neid valdkondi, kus amet on näidanud selget lisaväärtust, ja lisades valdkonnad, kus vajatakse tuge, võttes arvesse uusi poliitilisi prioriteete ja vahendeid, eelkõige võrgu- ja infoturbe direktiivi, Euroopa Liidu küberjulgeoleku strateegia läbivaatamist, tulevast ELi küberturvalisuse tegevuskava küberkriiside valdkonnas tehtava koostöö jaoks ning IKT turvalisuse sertifitseerimist.

    - **ELi põhimõtete arendamine ja rakendamine:** ENISA-le antaks ülesandeks aidata enesealgatuslikult kaasa poliitikakujundamisele võrgu- ja infoturbe valdkonnas ning erinevates valdkondades (näiteks energeetika, transport ja rahandus) tehtud teistele poliitilistele algatustele, millel on küberturvalisuse elemente. Selleks peaks tal olema tugev nõustav roll, mida ta saaks täita, esitades sõltumatuid arvamusi ja tehes ettevalmistavat tööd tegevuspõhimõtete ja õigusaktide väljatöötamiseks ning ajakohastamiseks. ENISA toetaks ka ELi põhimõtteid ja õigusakte elektroonilise side, elektroonilise identiteedi ja usaldusteenuste valdkonnas, et suurendada küberturvalisust. Rakendamise etapis ning eelkõige võrgu- ja infoturbe koostöörühma kontekstis aitaks ENISA liikmesriikidel võtta kasutusele lähenemisviisi, mille alusel rakendataks võrgu- ja infoturbe direktiivi ning teisi asjaomaseid tegevuspõhimõtteid ja õigusakte ühtselt piiride ja valdkondade üleselt. Selleks et toetada küberturvalisuse valdkonna tegevuspõhimõtete ja õigusaktide korrapärast läbivaatamist, esitab ENISA ka korrapäraseid aruandeid ELi õigusraamistiku rakendamise olukorra kohta.

    - **Suutlikkuse arendamine:** ENISA aitab suurendada ELi ja riigi ametiasutuste suutlikkust ja oskusteadmisi, sealhulgas intsidentidele reageerimise ning küberturvalisusega seotud regulatiivsete meetmete järelevalve valdkonnas. Ametilt nõutakse ka seda, et ta aitaks luua erinevates valdkondades teabe jagamise ja analüüsimise keskused (ISACid), tutvustades parimaid tavasid ja andes suuniseid saadaolevate vahendite ja menetluste kohta ning tegeledes nõuetekohaselt teabe jagamisega seotud regulatiivsete küsimustega.

    - **Teadmised, teave ja teadlikkuse suurendamine:** ENISAst saaks ELi teabekeskus. See tähendaks parimate tavade ja algatuste edendamist ning jagamist ELis, koondades ELi ning riiklikelt institutsioonidelt, asutustelt ja organitelt saadud küberturvalisust käsitleva teabe. Amet annaks ka nõuandeid ja suuniseid ning tutvustaks parimaid tavasid elutähtsa taristu turvalisuse valdkonnas. Pärast olulisi piiriüleseid küberturvalisuse intsidente koostaks ENISA ka aruanded, et anda suuniseid ettevõtjatele ja kodanikele kogu ELis. Selle töövoo raames korraldataks ka koostöös liikmesriikide ametiasutustega korrapäraselt teadlikkuse suurendamise tegevusi.

    - **Turuga seotud ülesanded (standardimine ja küberturvalisuse sertifitseerimine):** ENISA täidaks mitmeid ülesandeid, täpsemalt toetaks siseturgu ja küberturvalisuse turu vaatlusrühma, analüüsides küberturvalisuse turu asjaomaseid suundumusi, et reageerida paremini nõudlusele ja pakkumisele, ning toetades ELi poliitika kujundamist IKT standardimise ja

IKT küberturvalisuse sertifitseerimise valdkonnas. Standardimise valdkonnas aitaks ENISA täpsemalt koostada ja võtta kasutusele küberturvalisuse standardeid. ENISA täidaks ka tulevase sertifitseerimisraamistiku (vt jaotis allpool) kontekstis ette nähtud ülesandeid.

- **Teadusuuringud ja innovatsioon:** ENISA kasutaks oma oskusteadmisi, et nõustada ELi ja riigi ametiasutusi teadus- ja arendustegevuse valdkonnas prioriteetide määramisel, sealhulgas küberturvalisuse alase lepingulise avaliku ja erasektori partnerluse kontekstis. Teadusuuringute valdkonnas ENISA antud nõuandeid kasutataks järgmise mitmeaastase finantsraamistiku alusel uue Euroopa küberturvalisuse uurimis- ja pädevuskeskuse huvides. ENISA osaleks komisjoni taotluse korral ka ELi teadusuuringute ja innovatsiooni rahastamisprogrammide rakendamises.

- **Operatiivkoostöö ja kriisiohjamine:** see töövoog peaks põhinema olemasoleva vältimise tegevussuutlikkuse tugevdamisel, eelkõige täiustades üleeuroopalisi küberturvalisuse õppusi (Cyber Europe), muutes need iga-aastasteks, ning toetades operatiivkoostööd CSIRTide võrgustiku sekretariaadina (võrgu- ja infoturbe direktiivi nõuete kohaselt), tagades muu hulgas, et CSIRTide võrgustiku IT taristu ja sidekanalid toimivad hästi. Selles kontekstis on vajalik struktureeritud koostöö CERT-EU, küberkuritegevuse vastase võitluse Euroopa keskuse ja teiste asjaomaste ELi asutustega. Lisaks sellele peaks CERT-EUga füüsiliselt lähestikku tehtav struktureeritud koostöö võimaldama anda oluliste intsidentide korral tehnilist abi ja toetada intsidentide analüüsi. Vastava taotluse esitanud liikmesriigid saaksid abi intsidentidega tegelemiseks ning toetust nõrkuste, moonutuste ja intsidentide analüüsimiseks, et tugevdada oma vältimis- ja reageerimissuutlikkust.

- ENISA-l oleks ka osa **ELi küberturvalisuse tegevuskavas**, mida tutvustatakse selle paketi osana ja milles esitatakse komisjoni soovitused liikmesriikidele, et reageerida koordineeritud viisil suurtele piiriülestele küberturvalisuse intsidentidele ja kriisidele ELi tasandil[13]. ENISA edendaks hädaolukordadele reageerimise käigus individuaalsete liikmesriikide vahelist koostööd, analüüsides ja koondades riiklikke olukorraaruandeid lähtuvalt teabest, mille liikmesriigid ja muud üksused on ametile vabatahtlikult esitanud.

- **IKT toodete ja teenuste küberturvalisuse sertifitseerimine**

Selleks et luua ja säilitada usaldust ja turvalisust, tuleb IKT toodetesse ja teenustesse otseselt inkorporeerida turvaomadused nende tehnilise projekteerimise ja arendamise algetappides (sisseprojekteeritud turve). Lisaks sellele peab klientidel ja kasutajatel olema võimalik kindlaks teha nende hangitud või ostetud toodete ja teenuste turvalisuse alase usaldusväärsuse tase.

[13] Tegevuskava rakendatakse küberturvalisuse intsidentide suhtes, mille põhjustatud häired on liiga laialdased, et neist mõjutatud liikmesriik üksi suudaks nendega toime tulla, või millel on mitmes liikmesriigis niivõrd laiaulatuslik ja märkimisväärne tehniline või poliitiline mõju, et need eeldavad õigeaegset poliitika koordineerimist ja reageerimist liidu poliitilisel tasandil.

Sertifitseerimine, mille puhul sõltumatu ja akrediteeritud asutus hindab ametlikult tooteid, teenuseid ja protsesse kindlaks määratud standardikriteeriumide alusel ning väljastatakse vastavust tõendav sertifikaat, on oluline, et suurendada toodete ja teenuste turvalisust ning usaldust nende vastu. Kuigi turvalisuse hindamine on üpris tehniline valdkond, on sertifitseerimise abil võimalik teavitada ostjaid ja kasutajaid nende ostetud või kasutatavate IKT toodete ja teenuste turvaomadustest ning neid selles valdkonnas julgustada. Nagu eespool märgitud, kehtib see eelkõige suurel määral digitehnoloogiat kasutavate ja väga heal tasemel turvalisust eeldavate uute süsteemide suhtes, nt internetiühendusega ja automatiseeritud autod, e-tervis, tööstuslikud automatiseeritud juhtimissüsteemid[14] või arukad võrgud.

Praegu on IKT toodete ja teenuste küberturvalisuse sertifitseerimine ELis üpris lünklik. On mitmeid rahvusvahelisi algatusi, näiteks infotehnoloogia turvalisuse hindamise nn ühiskriteeriumid (ISO 15408), mille puhul on tegemist arvuti turvalisuse hindamise rahvusvahelise standardiga. See põhineb kolmanda isiku tehtaval hindamisel ja sellega nähakse ette seitse hindamise usaldusväärsuse taset. Ühiskriteeriumid ja nendega kaasnev infotehnoloogia turvalisuse hindamise ühine metoodika on tehniline alus rahvusvahelisele kokkuleppele Common Criteria Recognition Arrangement (ühiskriteeriumide tunnustamise kokkulepe, edaspidi „CCRA“), millega tagatakse, et ühiskriteeriumide sertifikaate tunnustavad kõik CCRA allakirjutanud. Samas tunnustatakse CCRA kehtiva versiooni alusel vastastikku ainult hindamisi kuni tasemeni EAL 2. Lisaks sellele on kokkuleppe allkirjastanud ainult 13 liikmesriiki.

12 liikmesriigi sertifitseerimisasutused on sõlminud vastastikuse tunnustamise kokkuleppe nende sertifikaatide kohta, mis on väljastatud lähtuvalt ühiskriteeriumidest ja kokkuleppe kohaselt[15]. Liikmesriikides on praegu tehtud või hakatakse tegema mitmeid IKT sertifitseerimise algatusi. Kuigi need on olulised, kaasneb nende algatustega ka risk, et turg killustub ja tekivad probleemid koostalitusvõimega. Seetõttu võib ettevõtjal olla vaja hankida mitu sertifikaati mitmes liikmesriigis, et ta saaks oma tooteid mitmel turul pakkuda. Näiteks nutiarvestite tootja, kes soovib müüa oma tooteid kolmes liikmesriigis, näiteks Saksamaal, Prantsusmaal ja Ühendkuningriigis, peab praegu täitma kolme erineva sertifitseerimiskava nõudeid. Need on Commercial Product Assurance (CPA) Ühendkuningriigis, Certification de Sécurité de Premier Niveau (CSPN) Prantsusmaal ja ühiskriteeriumidel põhinev konkreetne kaitseprofiil Saksamaal.

See olukord tekitab suuremad kulud ja põhjustab märkimisväärset halduskoormust ettevõtjatele, kes tegutsevad mitmes liikmesriigis. Kuigi sertifitseerimise kulud võivad olenevalt tootest/teenusest, soovitud hindamise usaldusväärsuse tasemest ja/või muudest asjaoludest märkimisväärselt erineda, on see summa ettevõtjate jaoks üldjuhul üpris suur. BSI „Smart Meter Gateway“ sertifikaadi saamine maksab rohkem kui 1 miljon eurot (kõrgeim katsetus- ja usaldusväärsuse tase, mis kehtib lisaks tootele ka kogu seda ümbritseva taristu

---

[14] Teadusuuringute Ühiskeskus on avaldanud aruande, milles pakutakse välja ühiste Euroopa nõuete esialgne komplekt ja üldised suunised, mis on seotud tööstuslike automatiseerimis- ja juhtimissüsteemide komponentide küberturvalisuse sertifitseerimisega. Kättesaadav aadressil https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

[15] Kõrgemate ametnike infosüsteemide turbe rühma (edaspidi „SOG-IS“) kuulub 12 liikmesriiki ja Norra ning see on välja töötanud teatavad kaitseprofiilid piiratud arvule toodetele, näiteks digitaalallkirjale, digitaalsele sõidumeerikule ja kiipkaartidele. Osalejad teevad koostööd, et koordineerida ühiskriteeriumide kaitseprofiilide standardimist ning kaitseprofiilide väljatöötamist. Liikmesriigid küsivad riigihangete pakkumuste puhul sageli SOG-ISi sertifikaati.

kohta). Nutiarvestite sertifitseerimise maksumus Ühendkuningriigis on peaaegu 150 000 eurot. Prantsusmaal on see maksumus Ühendkuningriigiga sarnane (ligikaudu 150 000 eurot või rohkem).

Peamised avaliku ja erasektori sidusrühmad kinnitasid, et kuna puudub ELi-ülene küberturvalisuse sertifitseerimise kava, on ettevõtjad pidanud mitmel juhul hankima sertifikaadi individuaalselt igas liikmesriigis, mis põhjustab turu killustatuse. Kõige olulisem on, et ELi ühtlustatud õigusaktide puudumise tõttu IKT toodete ja teenuste valdkonnas võivad küberturvalisuse sertifitseerimise standardite ja tavade erinevused liikmesriikides luua ELis tegelikkuses 28 eraldi turvalisuse turgu, millest igaühel on oma tehnilised nõuded, katsemeetodid ja küberturvalisuse sertifitseerimise menetlused. Kui ELi tasandil nõuetekohaseid meetmeid ei võeta, siis võivad need erinevad lähenemisviisid riiklikul tasandil põhjustada märkimisväärse tagasilöögi digitaalse ühtse turu saavutamisel, aeglustades või takistades majanduskasvu ja töökohtade loomise seisukohast ühendatud positiivse mõju tekkimist.

Eespool nimetatust lähtuvalt luuakse määruse ettepanekuga IKT toodete ja teenuste Euroopa küberturvalisuse sertifitseerimise raamistik (edaspidi „**raamistik**“) ning täpsustatakse ENISA olulised ülesanded küberturvalisuse sertifitseerimise valdkonnas. Käesoleva ettepanekuga kehtestatakse Euroopa küberturvalisuse sertifitseerimise kavasid reguleerivate õigusnormide üldine raamistik. Ettepanekuga ei võeta kasutusele otseselt kasutusvalmis sertifitseerimiskavasid, vaid luuakse süsteem (raamistik) konkreetsete IKT toodete/teenuste jaoks konkreetsete sertifitseerimiskavade koostamiseks (edaspidi „Euroopa küberturvalisuse sertifitseerimise kavad“). Raamistiku kohaselt Euroopa küberturvalisuse sertifitseerimise kavade loomine võimaldab tagada nende kavade alusel väljastatud sertifikaatide kehtivuse ja tunnustamise kõikides liikmesriikides ning vähendada praegust turu killustatust.

Euroopa küberturvalisuse sertifitseerimise kava üldeesmärk on kinnitada, et selle kava kohaselt sertifitseeritud IKT tooted ja teenused vastavad kindlaksmääratud küberturvalisuse nõuetele. See hõlmaks näiteks nende võimet kaitsta (salvestatud, edastatud või muul viisil töödeldud) andmeid juhusliku või lubamatu salvestamise, töötlemise, juurdepääsu, avaldamise, hävitamise, juhusliku kaotamise või muutmise eest. ELi küberturvalisuse sertifitseerimise kavad kasutaksid tehniliste nõuete ja hindamismenetluste valdkonnas kehtivaid standardeid, millele tooted peavad vastama, ja nende raames ei koostataks uusi tehnilisi standardeid[16]. Näiteks selleks, et tagada selliste toodete nagu kiipkaartide ELi-ülene sertifitseerimine, mida katsetatakse praegu mitmepoolse SOG-ISi kava alusel ühiskriteeriumide rahvusvaheliste standarditega võrreldes (ja mida on eespool kirjeldatud), oleks vaja muuta see kava kehtivaks kogu ELi ulatuses.

Lisaks sellele, et ettepanekus kirjeldatakse konkreetsete turvaeesmärkide komplekti, mida tuleb võtta arvesse konkreetse Euroopa küberturvalisuse sertifitseerimise kava koostamisel, esitatakse selles nõuded kõnealuste kavade miinimumsisule. Nendes kavades tuleb muu hulgas määrata kindlaks konkreetsed nõuded küberturvalisuse sertifitseerimise ulatusele ja eesmärgile. See hõlmab asjakohaste toodete ja teenuste kategooriate kindlaksmääramist, küberturvalisuse nõuete üksikasjalikku kirjeldamist (näiteks osutades asjakohastele standarditele või tehnilistele kirjeldustele), konkreetseid hindamiskriteeriume ja -meetodeid

[16] Euroopa standardite puhul toimub see läbi Euroopa standardiorganisatsioonide ning seda toetab Euroopa Komisjon Euroopa Liidu Teatajas avaldamise teel (vt määrus (EL) nr 1025/2012).

ning usaldusväärsuse taset, mida nendega soovitakse tagada (näiteks baastase, märkimisväärne või kõrge tase).

Euroopa küberturvalisuse sertifitseerimise kavad koostab ENISA, kasutades eksperdiabi ja tehes tihedat koostööd Euroopa küberturvalisuse sertifitseerimise rühmaga (vt allpool) ning need võtab vastu komisjon rakendusaktide alusel. Kui küberturvalisuse sertifitseerimise kava peetakse vajalikuks, siis esitab komisjon ENISA-le taotluse, et ta koostaks kava konkreetse IKT toote või teenuse jaoks. ENISA koostab kava tihedas koostöös rühmas esindatud riiklike sertifitseerimise järelevalveasutustega. Liikmesriigid ja rühm võivad teha komisjonile ettepaneku, et ta taotleks ENISA-lt konkreetse kava koostamist.

Sertifitseerimine võib olla väga kulukas protsess, mis võib suurendada klientidelt ja tarbijatelt küsitavaid hindu. Sertifitseerimisvajadus võib ka märkimisväärselt erineda, lähtuvalt toodete ja teenuste kasutamise konkreetsest kontekstist ning tehniliste muutuste kiirest tempost. Euroopa küberturvalisuse sertifitseerimise kasutamine peaks seega jääma vabatahtlikuks, kui liidu õigusaktides, millega kehtestatakse IKT toodete ja teenuste turvanõuded, ei ole sätestatud teisiti.

Selleks et tagada ühtlustamine ja vältida killustatust, lõpetatakse Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT toodete ja teenuste puhul riiklike küberturvalisuse sertifitseerimise kavade või menetluste kasutamine alates Euroopa küberturvalisuse sertifitseerimise kava vastuvõtmise rakendusaktis sätestatud kuupäevast. Liikmesriigid ei tohiks ka kehtestada uusi riiklikke küberturvalisuse sertifitseerimise kavasid IKT toodetele ja teenustele, mis on kaetud kehtiva Euroopa küberturvalisuse sertifitseerimise kavaga.

Kui Euroopa küberturvalisuse sertifitseerimise kava on vastu võetud, saavad IKT toodete tootjad või IKT teenuste osutajad esitada enda valitud vastavushindamisasutusele taotluse oma toodete või teenuste sertifitseerimiseks. Akrediteerimisasutus peaks vastavushindamisasutused akrediteerima, kui need vastavad teatavatele konkreetsetele nõuetele. Akrediteering antakse maksimaalselt viieks aastaks ja selle kehtivust võib pikendada samadel tingimustel senikaua, kuni vastavushindamisasutus vastab nõuetele. Akrediteerimisasutus tühistab vastavushindamisasutuse akrediteerimise, kui akrediteerimise tingimused ei ole täidetud või ei ole enam täidetud või asutuse poolt võetavad meetmed rikuvad käesolevat määrust.

Ettepaneku kohaselt täidavad seire, järelevalve ja täitmise tagamise ülesandeid liikmesriigid. Liikmesriigid peavad tagama ühe sertifitseerimise järelevalveasutuse olemasolu. See asutus peab kontrollima, et vastavushindamisasutused ja nende territooriumil asutatud vastavushindamisasutuste väljastatud sertifikaadid vastavad käesoleva määruse ning asjakohaste Euroopa küberturvalisuse sertifitseerimise kavade nõuetele. Riiklikud sertifitseerimise järelevalveasutused on pädevad tegelema füüsiliste või juriidiliste isikute esitatud kaebustega, mis käsitlevad nende territooriumil asutatud vastavushindamisasutuste väljastatud sertifikaate. Nad uurivad nõuetekohases ulatuses kaebuse sisu ja annavad kaebuse esitajale mõistliku aja jooksul teada tehtud edusammudest ning uurimise tulemusest. Lisaks sellele teevad nad koostööd teiste sertifitseerimise järelevalveasutuste või muude avaliku sektori asutusega, näiteks jagades teavet IKT toodete ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele.

Ettepaneku alusel luuakse Euroopa küberturvalisuse sertifitseerimise rühm (edaspidi „rühm“), kuhu kuuluvad kõigi liikmesriikide riiklikud sertifitseerimise järelevalveasutused. Rühma

põhiülesanne on nõustada komisjoni küberturvalisuse sertifitseerimise poliitikaga seotud küsimustes ning teha koostööd ENISAga, et koostada Euroopa küberturvalisuse sertifitseerimise kavade projektid. ENISA aitab komisjoni, tagades rühma sekretariaaditeenused ja hoides käigus Euroopa küberturvalisuse sertifitseerimise raamistiku alusel heaks kiidetud kavade ajakohastatud avalikku andmikku. ENISA suhtleks ka standardiorganisatsioonidega, et tagada heakskiidetud kavades kasutatud standardite asjakohasus ja määrata kindlaks küberturvalisuse standardeid vajavad valdkonnad.

Euroopa küberturvalisuse sertifitseerimise raamistik (edaspidi „raamistik“) annab kodanikele ja ettevõtjatele mitmeid eeliseid. Need eelised on eelkõige järgmised.

- Konkreetsete toodete ja teenuste jaoks ELi-üleste küberturvalisuse sertifitseerimise kavade loomine tagab ettevõtjatele ühtse kontaktpunkti ELis küberturvalisuse sertifikaadi hankimiseks. Kõnealustel ettevõtjatel tekib võimalus sertifitseerida oma toode ainult korra ja saada sertifikaat, mis kehtib kõikides liikmesriikides. Nad ei pea sertifitseerima oma tooteid uuesti teiste riiklike sertifitseerimisasutuste juures. See vähendab märkimisväärselt ettevõtjatele tekkivaid kulusid, lihtsustab piiriülest tegevust ning lõppkokkuvõttes vähendab ja aitab vältida asjaomaste toodete siseturu killustatust.

- Raamistikuga kehtestatakse Euroopa küberturvalisuse sertifitseerimise kavade ülimuslikkus riiklike kavade suhtes: selle tingimuse kohaselt muutub Euroopa küberturvalisuse sertifitseerimise kava selle vastuvõtmisel ülimuslikuks kõigi samal usaldusväärsuse tasemel sama IKT toote või teenuse puhul kehtivate riiklike kavade suhtes. See suurendab selgust ning vähendab kattuvate ja vahel ka vastandlike riiklike küberturvalisuse sertifitseerimise kavade praegust levikut.

- Ettepanekuga toetatakse ja täiendatakse ka võrgu- ja infoturbe direktiivi rakendamist, andes ettevõtjatele, kelle suhtes seda direktiivi kohaldatakse, väga kasulikud vahendid, mille abil nad saavad tõendada vastavust võrgu- ja infoturbe nõuetele kogu liidus. Komisjon ja ENISA pööravad uute küberturvalisuse sertifitseerimise kavade väljatöötamisel eritähelepanu vajadusele tagada, et võrgu- ja infoturbe direktiivi nõuded kajastuvad küberturvalisuse sertifitseerimise kavades.

- Ettepanekuga toetatakse ja edendatakse Euroopa küberturvalisuse poliitika väljatöötamist, ühtlustades tingimusi ja sisulisi nõudeid IKT toodete ja teenuste küberturvalisuse sertifitseerimisele ELis. Euroopa küberturvalisuse sertifitseerimise kavad osutavad hindamis- ja katsemeetodite ühistele standarditele või kriteeriumidele. See aitab märkimisväärselt (kuigi kaudselt) kaasa ühiste turvalahenduste kasutuselevõtule ELis, kõrvaldades ka tõkked siseturul.

- Raamistik on koostatud selliselt, et tagada küberturvalisuse sertifitseerimise kavade jaoks vajalik paindlikkus. Olenevalt konkreetsetest küberturvalisuse vajadustest võidakse toode või teenus sertifitseerida kõrgemal või madalamal turvalisuse tasemel. Euroopa küberturvalisuse sertifitseerimise kavad koostatakse seda paindlikkust arvesse võttes ja nendega tagatakse seetõttu erinevad usaldusväärsuse tasemed (s.o baastase, märkimisväärne või kõrge tase), et neid saaks kasutada erinevas kontekstis erineval otstarbel.

- Kõik eespool märgitud elemendid muudavad küberturvalisuse sertifitseerimise ettevõtjatele atraktiivsemaks kui tõhusa vahendi, mille abil saab anda teavet IKT

toodete või teenuste küberturvalisuse usaldusväärsuse taseme kohta. Kuna küberturvalisuse sertifitseerimine muutub odavamaks, tõhusamaks ja ärilises mõistes atraktiivsemaks, on ettevõtjatel suurem ajend sertifitseerida oma tooteid küberturvalisuse riskide vältimiseks, aidates seeläbi kaasa paremate küberturvalisuse tavade levikule IKT toodete ja teenuste projekteerimisel (sisseprojekteeritud küberturvalisus).

- **Kooskõla poliitikavaldkonnas praegu kehtivate õigusnormidega**

Võrgu- ja infoturbe direktiivi kohaselt peavad meie majanduse ja ühiskonna jaoks elutähtsates sektorites (näiteks energeetika, vesi, pangandus, finantsturutaristud, tervishoid ja digitaalne taristu) tegutsevad operaatorid ning digitaalsete teenuste (näiteks otsingumootorid, pilvandmetöötlusteenused ja internetipõhised kauplemiskohad) osutajad võtma meetmeid, et juhtida nõuetekohaselt turvariske. Käesoleva ettepaneku uued õigusnormid täiendavad võrgu- ja infoturbe direktiivi sätteid ja tagavad nendega kooskõla, et suurendada veelgi ELi kübervastupidavusvõimet tänu suuremale suutlikkusele, koostööle, riskijuhtimisele ja küberteadlikkusele.

Lisaks sellele on küberturvalisuse sertifitseerimise õigusnormid ülioluline vahend ettevõtjatele, kelle suhtes kohaldatakse võrgu- ja infoturbe direktiivi, kuna nad saavad sertifitseerida oma IKT tooteid ja teenuseid küberturvalisuse riskide vastu, kasutades selleks kogu ELis kehtivaid ja tunnustatud küberturvalisuse sertifitseerimise kavasid. Need täiendavad ka e-identimise ja e-tehingute jaoks vajalike usaldusteenuste määruses[17] ning raadioseadmete direktiivis[18] sätestatud turvanõudeid.

- **Kooskõla muude liidu tegevuspõhimõtetega**

Määrus (EL) 2016/679 (edaspidi „**isikuandmete kaitse üldmäärus**“)[19] sisaldab sätteid sertifitseerimismehhanismide ning andmekaitsepitserite ja -märgiste kasutuselevõtuks eesmärgiga tõendada, et vastutavate töötlejate ja volitatud töötlejate isikuandmete töötlemise toimingud vastavad kõnealusele määrusele. Käesolev määrus ei piira andmetöötlustoimingute sertifitseerimist isikuandmete kaitse üldmääruse kohaselt, sealhulgas juhul, kui sellised toimingud sisalduvad toodetes või teenustes.

---

17 Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ.

18 Euroopa Parlamendi ja nõukogu 16. aprilli 2014. aasta direktiiv 2014/53/EL raadioseadmete turul kättesaadavaks tegemist käsitlevate liikmesriikide õigusaktide ühtlustamise kohta ja millega tunnistatakse kehtetuks direktiiv 1999/5/EÜ.

19 Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1–88).

Määruse ettepaneku puhul tagatakse kooskõla määrusega (EÜ) nr 765/2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded,[20] osutades selle riiklikke akrediteerimisasutusi ja vastavushindamisasutusi käsitleva raamistiku õigusnormidele. Järelevalveasutuste puhul nõutakse välja pakutud määrusega, et liikmesriigid nimetaksid riiklikud sertifitseerimise järelevalveasutused, kes vastutavad õigusnormide järelevalve, seire ja täitmise tagamise eest. Need asutused on eraldiseisvad määrusega (EÜ) nr 765/2008 ette nähtud vastavushindamisasutustest.

2. ÕIGUSLIK ALUS, SUBSIDIAARSUS JA PROPORTSIONAALSUS

- **Õiguslik alus**

ELi meetme õiguslik alus on Euroopa Liidu toimimise lepingu artikkel 114, mis käsitleb liikmesriikide õigusaktide ühtlustamist, et saavutada Euroopa Liidu toimimise lepingu artiklis 26 seatud eesmärk, nimel siseturu nõuetekohane toimimine.

Siseturu õiguslikku alust ENISA loomiseks on kinnitanud Euroopa Kohus (kohtuasjas C-217/04 Ühendkuningriik *vs.* Euroopa Parlament ja nõukogu) ning seda toetati veelgi 2013. aasta määrusega, millega anti ametile praegune mandaat. Lisaks sellele kuuluvad tegevused, mille eesmärk on suurendada liikmesriikide koostööd ja koordineerimist ning mis lisavad ELi tasandi suutlikkust, et täiendada liikmesriikide võetavaid meetmeid, operatiivkoostöö kategooria alla. See on määratud kindlaks võrgu- ja infoturbe direktiivis (mille õiguslik alus on Euroopa Liidu toimimise lepingu artikkel 114) CSIRTide võrgustiku kontekstis seatud eesmärgina, mille puhul „ENISA tagab sekretariaadi töö ja toetab aktiivselt [...] koostööd“ (artikli 12 lõige 2). Eelkõige tuuakse artikli 12 lõike 3 punktis f veelgi esile CSIRTide võrgutikule ülesandeks antud operatiivkoostöö täiendavaid vorme, sealhulgas seoses i) riskide ja intsidentide kategooriatega, ii) varajaste hoiatustega, iii) vastastikuse abiga ning iv) koostöö põhimõtete ja korraga juhtudeks, kui liikmesriigid reageerivad piirülestele riskidele ja intsidentidele.

- IKT toodete ja teenuste sertifitseerimise kavade praegune killustatus on ka põhjustatud liikmesriikide suhtes kohaldatava ühise õiguslikult siduva ja tõhusa raamistiku protsessi puudumisest. See takistab IKT toodete ja teenuste siseturu loomist ning piirab Euroopa tööstuse konkurentsivõimet selles sektoris. Käesoleva ettepaneku eesmärk on tegeleda praeguse killustatuse ja sellest siseturule tekkivate takistustega, tagades ühise raamistiku, et luua kogu ELis kehtivad küberturvalisuse sertifitseerimise kavad.

[20] Määrus (EÜ) nr 765/2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93.

Subsidiaarsus (liidu ainupädevusse mittekuuluva valdkonna puhul)

Subsidiaarsuse põhimõtte kohaselt on vaja hinnata ELi meetme vajalikkust ja lisaväärtust. Subsidiaarsuse põhimõtte järgimist selles valdkonnas kinnitati juba kehtiva ENISA määruse[21] vastuvõtmise ajal.

Küberturvalisus on liidule ühist huvi pakkuv küsimus. Võrkude ja infosüsteemide omavaheline seotus on selline, et üksikud osalejad (avalikust ja erasektorist, sealhulgas kodanikud) ei saa sageli üksi toime tulla küberturvalisuse intsidentide ohtudega, juhtida nende riske ega hallata nende võimalikku mõju. Ühest küljest muudab liikmesriikide omavaheline seotus, sealhulgas elutähtsa taristu (muu hulgas energeetika, transport, vesi) käitamise puhul Euroopa tasandil avaliku sekkumise mitte ainult kasulikuks, aga ka vajalikuks. Teisest küljest võib ELi sekkumine avaldada positiivset kõrvalmõju lähtuvalt heade tavade jagamisest liikmesriikides, mis võib anda tulemuseks parema küberturvalisuse liidus.

Kokkuvõttes nähtub praeguses kontekstis ja tulevikustsenaariume arvesse võttes, et **ELi liikmesriikide individuaalsetest meetmetest ja küberturvalisuse puhul killustatud lähenemisviisi rakendamisest** ei piisa **liidu ühise kübervastupidavusvõime suurendamiseks**.

ELi meetmeid peetakse ka vajalikuks, et tegeleda küberturvalisuse sertifitseerimise kavade praeguse killustatusega. See annaks tootjatele võimaluse saada siseturust täielikku kasu, hoides märkimisväärselt kokku katsetamise ja ümberkujundamise kulusid. Kuigi näiteks kõrgemate ametnike infosüsteemide turbe rühma (edaspidi „SOG-IS“) vastastikuse tunnustamise kokkulepe on saavutanud selles valdkonnas märkimisväärseid tulemusi, on selle tegevuse käigus ilmnenud ka märkimisväärseid piiranguid, mille tõttu see ei saa pakkuda pikaajalisi jätkusuutlikke lahendusi siseturu täieliku potentsiaali saavutamiseks.

ELi tasandil tegutsemise lisaväärtust, eelkõige et suurendada koostööd liikmesriikide vahel, aga ka võrgu- ja infoturbe kogukondade vahel, on kinnitatud nõukogu 2016. aasta järeldustes[22] ja see ilmneb ka selgelt ENISA tehtud hindamisest.

- **Proportsionaalsus**

Kavandatud meede ei lähe kaugemale sellest, mis on vajalik selle poliitikaeesmärkide saavutamiseks. ELi sekkumise ulatus ei takista riikliku julgeoleku valdkonnas täiendavate riiklike meetmete võtmist. ELi meede on seega subsidiaarsuse ja proportsionaalsuse seisukohast põhjendatud.

- **Vahendi valik**

Käesoleva ettepanekuga vaadatakse läbi määrus (EL) nr 526/2013, milles sätestatakse ENISA kehtiv mandaat ja ülesanded. Võttes arvesse ENISA olulist rolli ELi küberturvalisuse

[21] 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.

[22] Nõukogu järeldused Euroopa kübervastupidavusvõime süsteemi tugevdamise ning konkurentsivõimelise ja uuendusliku küberjulgeolekusektori toetamise kohta, 15. november 2016.

sertifitseerimise raamistiku loomisel ja haldamisel, on kõige parem luua ENISA uus mandaat ja kõnealune raamistik ühe õigusakti alusel, kasutades selleks määrust.

3. JÄRELHINDAMISE, SIDUSRÜHMADEGA KONSULTEERIMISE JA MÕJU HINDAMISE TULEMUSED

Praegu kehtivate õigusaktide järelhindamine või toimivuse kontroll

Komisjon analüüsis hindamise tegevuskava[23] alusel tehtud hindamise käigus ameti **asjakohasust, mõju, tulemuslikkust, tõhusust, sidusust ja sellest saadavat lisaväärtust** seoses ameti tulemuste, juhtimise, asutusesisese organisatsioonilise struktuuri ja töötavadega ajavahemikus 2013–2016. Põhitulemused on järgmised (lisateavet leiate mõjuhinnangule lisatud komisjoni talituste töödokumendist).

- **Asjakohasus:** tehnika arengu ja muutuvate ohtude kontekstis ning võttes arvesse märkimisväärset vajadust suurema küberturvalisuse järele ELis, osutusid ENISA eesmärgid asjakohaseks. Liikmesriigid ja ELi asutused tuginevad selle märkimisväärsetele oskusteadmistele küberturvalisuse küsimustes. Tuleb suurendada liikmesriikide suutlikkust mõista paremini ohte ja neile reageerida ning sidusrühmad peavad tegema koostööd temaatiliste valdkondade ja institutsioonide üleselt. Küberturvalisus on jätkuvalt ELi peamine poliitiline prioriteet, millega ENISA peab eeldatavasti tegelema, kuid kuna ENISA on tähtajalise mandaadiga ELi amet: i) ei saa ta teha pikaajalisi plaane ega toetada jätkusuutlikult liikmesriike ja ELi institutsioone; ii) võib tekkida õiguslik vaakum, sest võrgu- ja infoturbe direktiivi sätted, millega pandi ENISA-le tema ülesanded, on oma olemuselt alalised[24]; iii) puudub sidusus arusaamaga, mille kohaselt seostatakse ENISAt ELi parema küberturvalisuse keskkonnaga.

- **Tulemuslikkus:** ENISA on kokkuvõttes saavutanud oma eesmärgid ja täitnud oma ülesanded. Ta panustas oma põhitegevuse kaudu (suutlikkuse arendamine, oskusteadmiste pakkumine, kogukonna loomine ja poliitika toetamine) suuremasse võrgu- ja infoturbesse Euroopas. Saamas oleks selle tegevust saanud kõigis neis valdkondades parandada. Hindamise käigus jõuti järeldusele, et ENISA on tulemuslikult loonud tugevad ja usaldusväärsed suhted teatavate sidusrühmadega, eelkõige liikmesriikide ja CSIRTide kogukonnaga. Suutlikkuse arendamise valdkonnas tehtud sekkumisi peeti tulemuslikuks eelkõige vähemate ressurssidega liikmesriikide puhul. Ulatusliku koostöö edendamine on olnud üks peamistest saavutustest ning enamik sidusrühmadest on nõus, et ENISA-l on olnud inimeste kokku toomisel positiivne roll. Samas oli ENISA-l keerukas avaldada suurt mõju võrgu- ja infoturbe väga ulatuslikus valdkonnas. See oli ka põhjustatud asjaolust, et tal olid oma väga ulatusliku mandaadi täitmiseks suhteliselt piiratud inimressursid ja rahalised vahendid. Hindamise käigus jõuti ka järeldusele, et ENISA täitis oskusteabe pakkumise eesmärgi osaliselt, kuna tal oli probleeme ekspertide värbamisega (mida on käsitletud ka tõhususe jaotises allpool).

---

23 http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_et.pdf

24 Viited võrgu- ja infosüsteemide turvalisuse direktiivi (edaspidi „võrgu- ja infoturbe direktiiv“) artiklitele 7, 9, 11, 12 ja 19.

- **Tõhusus:** ENISA on hoolimata oma piiratud eelarvest, mis on teiste ELi ametitega võrreldes üks väiksemaid, suutnud aidata kaasa sihtotstarbeliste eesmärkide saavutamisele, kasutades oma ressursse kokkuvõttes tõhusalt. Hindamise tulemusena järeldati, et protsessid olid üldiselt tõhusad ning selge vastutusvaldkondade jaotus ameti piires võimaldas töö hästi ellu viia. Üks ameti peamistest probleemidest tõhususe valdkonnas seisneb selles, et ENISA-l on probleeme kõrgetasemelise kvalifikatsiooniga ekspertide värbamisel ja tööl hoidmisel. Tulemuste kohaselt seisneb selle põhjus mitme teguri koosmõjus, sealhulgas avaliku sektori üldised probleemid erasektoriga konkureerimisel, kui proovitakse värvata väga suure erialase pädevusega eksperte, ameti pakutavate lepingute liik (tähtajaline leping) ning ENISA asukoha suhteliselt väikse atraktiivsus, näiteks abikaasadel töö leidmisel tekkivate probleemide tõttu. Samal ajal Ateenas ja Irákleios tegutsemise tõttu oli vaja täiendavat koordineerimist ja tekkisid lisakulud, aga ameti põhitegevuse osakonna 2013. aastal Ateenasse viimine suurendas ameti tegevuslikku tõhusust.

- **Sidusus:** ENISA tegevus on olnud üldjoontes kooskõlas selle sidusrühmade põhimõtete ja tegevusega riiklikul ja ELi tasandil, aga vajatakse paremini koordineeritud küberturvalisuse lähenemisviisi ELi tasandil. ENISA ja teiste ELi asutuste vahelise koostöö potentsiaali ei ole täielikult kasutatud. ELi õigus- ja poliitilise keskkonna muutumise tõttu ei ole kehtiv mandaat enam sidus.

- **ELi lisaväärtus**: ENISA lisaväärtus seisneb peamiselt ameti võimes tõhustada koostööd, eelkõige liikmesriikide vahel, aga ka asjaomaste võrgu- ja infoturbe kogukondadega. ELi tasandil ei ole ühtegi teist osalejat, kes toetaks kõnealuste võrgu- ja infoturbe sidusrühmade koostööd. Ametist saadav lisaväärtus erines olenevalt selle sidusrühmade erinevatest ressurssidest ja vajadustest (näiteks suured liikmesriigid võrreldes väikeste liikmesriikidega, liikmesriigid võrreldes tööstusvaldkonnaga) ning ameti vajadusest tähtsustada oma tegevust tööprogrammi alusel. Hindamise tulemusena jõuti järeldusele, et ENISA tegevuse võimalik lõpetamine oleks kaotatud võimalus kõigi liikmesriikide jaoks. Küberturvalisuse valdkonnas ei oleks võimalik tagada samal määral kogukonna loomist ja koostööd liikmesriikide vahel. Ilma kesksema ELi ametita oleks olukord rohkem killustatud ning ENISA jäetud tühimikku hakkaks täitma kahepoolne või piirkondlik koostöö.

Võttes konkreetselt arvesse ENISA varasemaid tulemusi ja tulevikku, on 2017. aasta konsultatsioonist ilmnevad peamised suundumused järgmised[25].

- Enamik vastanutest (74 %) hindas ENISA üldist tulemuslikkust ajavahemikus 2013–2016 positiivselt. Enamik vastanutest oli ka seisukohal, et ENISA saavutab oma erinevaid eesmärke (vähemalt 63 % iga eesmärgi puhul). ENISA teenuseid ja tooteid kasutavad korrapäraselt (kord kuus või sagedamini) peaaegu pooled vastanutest

[25] Konsultatsioonile vastas 90 sidusrühma 19 liikmesriigist (88 vastust ja kaks kirjalikku seisukohavõttu), sealhulgas 15 liikmesriigi (muu hulgas Prantsusmaa, Itaalia, Iirimaa ja Kreeka) ametiasutused ja kaheksa katusorganisatsiooni, kes esindavad märkimisväärset arvu Euroopa organisatsioone (näiteks European Banking Federation, Digital Europe (kes esindab digitaaltehnoloogia tööstust Euroopas) ja European Telecommunications Network Operators' Association (edaspidi „ETNO“)). ENISA avalikku konsultatsiooni täiendati mitme teise allika abil, sealhulgas: i) küberturvalisuse kogukonna 50 peamise osalejaga korraldatud põhjalikud küsitlused; ii) CSIRTide võrgustiku uuring; iii) ENISA haldusnõukogu, juhatuse ja alalise sidusrühma uuring.

(46 %) ning neid hinnatakse seetõttu, et neid pakub ELi tasandi asutus (83 %) ja need on kvaliteetsed (62 %).

- Vastanud nimetasid ELi küberturvalisuse tuleviku mitut lünka ja probleemi, millest peamised (16 lüngast ja probleemist koosnevast nimekirjast) olid: liikmesriikide koostöö, võime ära hoida, avastada ja lahendada suuremahulisi küberrünneid; liikmesriikide koostöö küberturvalisusega seotud küsimustes; koostöö ja teabe jagamine erinevate sidusrühmade vahel, sealhulgas avaliku ja erasektori koostöö; elutähtsa taristu kaitse küberrünnete eest.

- Valdav enamik vastanutest (88 %) oli seisukohal, et ELi tasandil praegu saadaval olevad vahendid ja mehhanismid ei ole piisavad nende küsimustega tegelemiseks või sobivad selleks ainult osaliselt. Valdav enamik vastanutest (98 %) märkis, et nende küsimustega peaks tegelema ELi asutus, ning 99 % neist pidas ENISAt selle jaoks õigeks organisatsiooniks.

Konsulteerimine sidusrühmadega

- Komisjon korraldas ENISA läbivaatamiseks 12. aprillist 5. juulini 2016 avaliku konsultatsiooni, millele laekus 421 vastust[26]. Tulemuste kohaselt oli 67,5 % vastanutest seisukohal, et ENISA võiks aidata luua IT toodete ja teenuste turvalisuse sertifitseerimise ühtlustatud raamistikku.

Küberturvalisuse alast lepingulist avaliku ja erasektori partnerlust käsitleva 2016. aasta avaliku konsultatsiooni[27] sertifitseerimist käsitleva osa tulemused näitavad järgmist.

- 50,4 % vastanutest (121 vastanut 240st) ei tea, kas riiklikke sertifitseerimiskavasid tunnustatakse vastastikku ELi liikmesriikides. 25,8 % (62 vastanut 240st) vastas „Ei“ ja 23,8 % (57 vastanut 240st) vastas „Jah“.

- 37,9 % vastanutest (91 vastanut 240st) arvab, et olemasolevad sertifitseerimiskavad ei toeta Euroopa tööstuse vajadusi. Teisest küljest 17,5 % (42 vastanut 240st, kes olid peamiselt Euroopa turul tegutsevad ülemaailmsed ettevõtjad) olid vastupidisel seisukohal.

- 49,6 % vastanutest (119 vastanut 240st) oli arvamusel, et ei ole lihtne tõendada standardite, sertifitseerimiskavade ja märgiste samaväärsust. 37,9 % (91 vastanut 240st) vastas „Ei oska öelda“ ja 12,5 % (30 vastanut 240st) vastas „Jah“.

[26] 162 vastust kodanikelt, 33 kodanikuühiskonnalt ja tarbijaorganisatsioonidelt; 186 vastust tööstussektorilt ja 40 avaliku sektori asutustelt, sealhulgas e-privaatsuse direktiivi täitmise tagamisega tegelevatelt pädevatelt ametiasutustelt.

[27] Sertifitseerimist käsitlevale osale vastas 240 sidusrühma, sealhulgas riigi haldusasutused, suurettevõtjad, VKEd, mikroettevõtjad ja teadusasutused.

Eksperdiarvamuste kogumine ja kasutamine

Komisjon tugines järgmisele asutusevälisele eksperdiabile.

- Study on the Evaluation of ENISA (ENISA hindamist käsitlev uuring) (Ramboll/Carsa 2017; SMART 2016/0077);
- Study on ICT Security Certification and Labelling – Evidence gathering and impact assessment (IKT turvalisuse sertifitseerimist ja märgistamist käsitlev uuring – tõendite kogumine ja mõjuhinnang) (PriceWaterhouseCoopers 2017; SMART 2016/0029).

Mõjuhinnang

- Käesoleva algatuse mõjuhinnangus määrati kindlaks järgmised peamised probleemid, mis tuleb lahendada:
- liikmesriikide killustatud tegevuspõhimõtted ja lähenemisviisid küberturvalisuse valdkonnas,
- ELi institutsioonide, organite ja asutuste poolt küberturvalisuse jaoks eraldatavate ressursside hajusus ja kasutatavate lähenemisviiside killustatus ning
- kodanike ja ettevõtjate ebapiisav teadlikkus ja teave, samal ajal kui võetakse kasutusele mitmeid riiklikke ja valdkondlikke sertifitseerimiskavasid.

Mõjuhinnangus analüüsiti ENISA mandaadi puhul järgmisi võimalikke variante:

- praeguse olukorra säilitamine, mille puhul pikendatakse mandaati, aga jäetakse see tähtajaliseks (lähtestsenaariumi variant);
- ENISA kehtiva mandaadi aegumine ilma seda uuendamata ja ENISA tegevuse lõpetamine (poliitilisi meetmeid ei võeta);
- reformitud ENISA ning
- täieliku tegevusvõimega ELi küberturvalisuse amet.

Mõjuhinnangus analüüsiti küberturvalisuse sertifitseerimise puhul järgmisi võimalikke variante:

- poliitilisi meetmeid ei võeta (lähtestsenaarium);
- muud kui seadusandlikud (pehme õiguse) meetmed;
- ELi õigusakt, millega luuakse SOG-ISi süsteemi alusel kõikide liikmesriikide jaoks kohustuslik süsteem, ning
- ELi üldine IKT küberturvalisuse sertifitseerimise raamistik.

Analüüsi tulemusena järeldati, et eelistatud variant on reformitud ENISA koos ELi üldise IKT küberturvalisuse sertifitseerimise raamistikuga.

Eelistatud varianti peeti ELi jaoks kõige tõhusamaks, et saavutada järgmised kindlaks määratud eesmärgid: küberturvalisuse suutlikkuse, valmisoleku, koostöö, teadlikkuse ja läbipaistvuse suurendamine ning turu killustatuse vältimine. Seda peeti ka kõige sidusamaks Euroopa Liidu küberjulgeoleku strateegia ja sellega seotud poliitikameetmete (näiteks võrgu- ja infoturbe direktiiv) ning digitaalse ühtse turu strateegia poliitiliste prioriteetidega. Lisaks sellele ilmnes konsultatsiooniprotsessi käigus, et eelistatud varianti toetab enamik sidusrühmadest. Mõjuhinnangu käigus tehtud analüüs näitas ka seda, et eelistatud variandi puhul saaks eesmärgid saavutada, kasutades selleks mõistlikus koguses ressursse.

Komisjoni õiguskontrollikomitee esitas esialgu 24. juulil negatiivse arvamuse ja 25. augustil 2017 pärast mõjuhinnangu uuesti esitamist positiivse arvamuse. Muudetud mõjuhinnang sisaldas lisatõendusmaterjali, ENISA hindamise lõplikke järeldusi ning poliitikavariantide ja nende mõju täiendavaid selgitusi. Lõpliku mõjuhinnangu 1. lisas esitatakse kokkuvõte selle kohta, kuidas on võetud arvesse komitee teises arvamuses esitatud märkusi. Eelkõige ajakohastati mõjuhinnangut, et kirjeldada üksikasjalikumalt ELi küberturvalisuse konteksti, sealhulgas meetmeid, mis on lisatud ühisteatisesse „Vastupidavusvõime, heidutus ja kaitse – tugeva küberturvalisuse tagamine ELis“ (JOIN(2017) 450) ning mis omavad ENISA jaoks erilist tähtsust: ELi küberturvalisuse tegevuskava ning Euroopa küberturvalisuse uurimis- ja pädevuskeskus, millega amet oleks seotud ELi teadusuuringute vajaduste kohta antavate nõuannete puhul.

Mõjuhinnangus selgitatakse, kuidas ameti reformimine, sealhulgas uued ülesanded, paremad tööhõive tingimused ja struktuurne koostöö ELi sama valdkonna asutustega, parandaks ameti atraktiivsust tööandjana ning aitaks tegeleda ekspertide värbamisel tekkivate probleemiga. Mõjuhinnangu 6. lisas esitatakse ka ENISA poliitikavariantidest tekkivate kulude läbivaadatud prognoos. Sertifitseerimise puhul on mõjuhinnangut muudetud, et selgitada eelistatud varianti üksikasjalikumalt, sealhulgas graafiliselt, ning esitada liikmesriikidele ja komisjonile uuest sertifitseerimisraamistikust tekkivate kulude prognoos. On põhjalikumalt selgitatud mõttekäiku, mille alusel valiti ENISA selle raamistiku võtmetähtsusega osalejaks, lähtuvalt ameti eksperditeadmistest selles valdkonnas ning asjaolust, et see on ainus küberturvalisusega tegelev ELi tasandi asutus. Sertifitseerimist käsitlevad jaotised vaadati läbi, et selgitada erinevusi praeguse SOG-ISi süsteemiga, erinevatest poliitikavariantidest saadavat kasu ning et Euroopa sertifitseerimiskavaga hõlmatud IKT toote või teenuse liik määratakse kindlaks heaks kiidetud kavas endas.

Õigusnormide toimivus ja lihtsustamine

Ei kohaldata.

Põhiõigused

Küberturvalisus on ülioluline, et kaitsta üksikisikute privaatsust ja isikuandmeid kooskõlas Euroopa Liidu põhiõiguste harta artiklitega 7 ja 8. Küberturvalisuse intsidendid mõjutavad selgelt meie privaatsust ja isikuandmete kaitset. Seetõttu on küberturvalisus meie isikuandmete privaatsuse ja konfidentsiaalsuse austamise eeltingimus. Sellest lähtuvalt

täiendab ettepanek, seades eesmärgiks küberturvalisuse suurendamise Euroopas, märkimisväärselt kehtivaid õigusakte, millega kaitstakse privaatsuse ja isikuandmetega seotud põhiõigust. Küberturvalisus on ka ülioluline, et kaitsta meie elektroonilise side konfidentsiaalsust ja et me saaksime kasutada oma sõna- ja teabevabadust ning nendega seotud muid õigusi, näiteks mõtte-, südametunnistuse- ja usuvabadust.

4. MÕJU EELARVELE

Vt finantsselgitus.

5. MUU TEAVE

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

Komisjon teeb määruse kohaldamise järelevalvet ja esitab selle hindamise aruande Euroopa Parlamendile ja nõukogule ning Euroopa Majandus- ja Sotsiaalkomiteele iga viie aasta tagant. Need aruanded on avalikud ja kirjeldavad käesoleva määruse tegelikku kohaldamist ja täitmist.

- **Ettepaneku sätete üksikasjalik selgitus**

Määruse I jaotis sisaldab üldsätteid: reguleerimisese (artikkel 1), mõisted (artikkel 2), sealhulgas viited asjakohastele mõistetele sellistes teistes ELi õigusaktides nagu Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (edaspidi „võrgu- ja infoturbe direktiiv), Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 765/2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93, ning Euroopa Parlamendi ja nõukogu määrus (EL) nr 1025/2012, mis käsitleb Euroopa standardimist.

II jaotis sisaldab ENISA kui ELi küberturvalisuse ametiga seotud peamisi sätteid.

Selle jaotise I peatükis sätestatakse ameti mandaat (artikkel 3), eesmärgid (artikkel 4) ja ülesanded (artiklid 5–11).

II peatükis sätestatakse ENISA töökorraldus ja see sisaldab selle struktuuri suhtes kehtivaid olulisi nõudeid (artikkel 12). Selles peatükis käsitletakse haldusnõukogu koosseisu, hääletuskorda ja ülesandeid (1. jao artiklid 13–17), juhatust (2. jao artikkel 18) ja tegevdirektorit (3. jao artikkel 19). See sisaldab ka sätteid alalise sidusrühma koosseisu ja rolli kohta (4. jao artikkel 20). Selle peatüki 5. jaos kirjeldatakse ameti tegevuskorda, sealhulgas tegevuse programmi koostamist, huvide konflikte, läbipaistvust, konfidentsiaalsust ja juurdepääsu dokumentidele (artiklid 21–25).

III peatükis käsitletakse ameti eelarve koostamist ja struktuuri (artiklid 26 ja 27) ning selle täitmise eeskirju (artiklid 28 ja 29). Peatükk sisaldab ka sätteid pettuste, korruptsiooni ja muu ebaseadusliku tegevuse tõkestamise kohta (artikkel 30).

IV peatükk käsitleb ameti personali. See sisaldab üldsätteid personalieeskirjade ja muude teenistujate teenistustingimuste kohta ning privileege ja immuniteete reguleerivaid norme (artiklid 31 ja 32). Selles sätestatakse ka ameti tegevdirektori töölevõtmist ja ametisse

nimetamist reguleerivad normid (artikkel 33). See sisaldab samuti sätteid, mis reguleerivad lähetatud riiklike ekspertide või muude ametiväliste töötajate kasutamist (artikkel 34).

V peatükk sisaldab ametiga seotud üldsätteid. Selles kirjeldatakse ameti õiguslikku seisundit (artikkel 35) ja see sisaldab sätteid, millega reguleeritakse vastutust, kasutatavaid keeli ja isikuandmete kaitset (artiklid 36–38) ning julgeolekueeskirju salastatud teabe ja tundliku, kuid salastamata teabe kaitse kohta (artikkel 40). Selles on esitatud normid, mis reguleerivad ameti koostööd kolmandate riikide ja rahvusvaheliste organisatsioonidega (artikkel 39). See sisaldab ka sätteid ameti peakorteri ja tegutsemistingimuste ning ombudsmani tehtava halduskontrolli kohta (artiklid 41 ja 42).

Määruse III jaotisega luuakse üldise õigusnormina (*lex generalis*) IKT toodete ja teenuste Euroopa küberturvalisuse sertifitseerimise raamistik (edaspidi „**raamistik**“) (artikkel 1). Selles määratakse kindlaks Euroopa küberturvalisuse sertifitseerimise kavade üldeesmärk, s.o tagada, et IKT tooted ja teenused vastavad kindlaks määratud küberturvalisuse nõuetele selles osas, mis puudutab nende võimet pidada teataval usaldusväärsuse tasemel vastu tegevustele, mille eesmärk on rikkuda salvestatud, edastatud või töödeldud andmete või nendega seotud funktsioonide või teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust (artikkel 43). Seal loetletakse ka Euroopa küberturvalisuse sertifitseerimise kavade turvalisusega seotud eesmärgid (artikkel 45), näiteks võime kaitsta andmeid juhusliku või volitamata juurdepääsu või avalikustamise, hävitamise või muutmise eest, ning Euroopa küberturvalisuse sertifitseerimise kavade sisu (s.o elemendid), näiteks nende ulatuse, turvalisusega seotud eesmärkide, hindamiskriteeriumide jms üksikasjalik kirjeldus (artikkel 47).

III jaotisega kehtestatakse ka Euroopa küberturvalisuse sertifitseerimise kavade peamine õiguslik mõju, nimelt i) kohustus rakendada kava riiklikul tasandil ja sertifitseerimise vabatahtlikkus ning ii) et Euroopa küberturvalisuse sertifitseerimise kavade vastuvõtmine muudab samade toodete või teenuste puhul kasutatavad riiklikud kavad kehtetuks (artiklid 48 ja 49).

Selles jaotises sätestatakse ka Euroopa küberturvalisuse sertifitseerimise kavade vastuvõtmise menetlus ning komisjoni, ENISA ja Euroopa küberturvalisuse sertifitseerimise rühma (edaspidi „rühm“) vastavad rollid (artikkel 44). Selle jaotisega reguleeritakse ka vastavushindamisasutusi, sealhulgas neile seatavaid nõudeid, nende volitusi ja ülesandeid, riiklikke sertifitseerimise järelevalveasutusi ning karistusi.

Selle jaotise alusel luuakse rühm olulise organina, mis koosneb riiklike sertifitseerimise järelevalveasutuste esindajatest ja mille peamine ülesanne on teha ENISAga koostööd Euroopa küberturvalisuse sertifitseerimise kavade koostamisel ning nõustada komisjoni küberturvalisuse sertifitseerimise poliitikaga seotud üldistes ja konkreetsetes küsimustes.

IV jaotis sisaldab lõppsätteid, mis kirjeldavad delegeeritud õiguste kasutamist, hindamisnõudeid, kehtetuks tunnistamist ja õigusjärglust ning jõustumist.

2017/0225 (COD)

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“)

(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[28],

võttes arvesse Regioonide Komitee arvamust[29],

toimides seadusandliku tavamenetluse kohaselt

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

[28] ELT C ..., ..., lk …
[29] ELT C ..., ..., lk …

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) Küberründe 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,[30] 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,[31] millega pikendati ameti mandaati 2012. aasta

[30] 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).

[31] 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).

märtsini. Määrusega (EL) nr 580/2011[32] pikendati ameti mandaati 13. septembrini 2013. 2013. aastal võtsid Euroopa Parlament ja nõukogu vastu määruse (EL) nr 526/2013,[33] mis käsitleb ENISAt ja millega tunnistati kehtetuks määrus (EÜ) nr 460/2004, millega oli ameti mandaati pikendatud kuni 2020. aasta juunikuuni.

(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 muutnud 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 põhimõttelisi ettepanekuid, tegutsedes küberturvalisuse küsimustes liidu valdkondliku poliitika algatuste kontaktüksusena ning soodustades nii liikmesriikide omavahelist kui ka liikmesriikide ja Euroopa Liidu institutsioonide, organite ja asutuste vahelist operatiivkoostööd.

---

[32] 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).

[33] 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).

(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, organite ja asutuste, aga ka liikmesriikidega, peaks amet andma ennetava panuse riikide ja 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, sealhulgas elutähtsa sideinfrastruktuuri kaitse ja kübervastupidavusvõime alase poliitika ja õigusaktide väljatöötamisega. 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, organeid ja asutusi töös, mida nad teevad, et luua ja suurendada suutlikkust ja valmisolekut ennetada ja avastada küberturvalisuse intsidente ja neile reageerida, ning seoses võrgu- ja infosüsteemide turvalisusega. Eeskätt peaks amet toetama riiklike CSIRTide arendamist ja tõhustamist, et neil oleks kogu liidus ühtemoodi kõrge küpsuse aste. Samuti peaks amet abistama liidu ja liikmesriikide võrgu- ja infosüsteemide turvalisuse strateegiate väljatöötamist ja uuendamist, edendama nende levitamist ja hoidma silma peal nende rakendamisel. Lisaks peaks amet pakkuma koolitusi ja koolitusmaterjali avalikele asutustele ning koolitama vajaduse korral koolitajaid, et aidata liikmesriikidel välja kujundada 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 ja koostööd erasektori sees, pidades silmas eeskätt toetust elutähtsate infrastruktuuride kaitsele, peaks amet hõlbustama valdkondlike teabe jagamise ja analüüsimise keskuste (ISACide) loomist, pakkudes parimaid tavasid ja juhiseid kättesaadavate töövahendite ja menetluste kohta ning selle kohta, kuidas lahendada teabe jagamisega seotud regulatiivsed küsimused.

(18) Amet peaks koondama ja analüüsima riikide CSIRTide ja CERT-EU aruandeid ning koostama teabevahetuse jaoks ühised eeskirjad, keele ja terminoloogia. Võrgu- ja infoturbe direktiiviga loodud CSIRTide võrgustikuga loodi alus vabatahtlikuks tehnilise teabe vahetamiseks operatiivtasandil – selle raames peaks amet kaasama ka erasektori.

(19) Amet peaks andma oma panuse sellesse, kuidas ELi tasandil reageeritakse mastaapsetele piiriülestele küberturvalisuse intsidentidele ja kriisidele. See funktsioon peaks hõlmama 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 iga-aastaste küberturvalisuse õppuste käigus.

(20) Operatiivülesannete täitmisel peaks amet tegema CERT-EUga füüsiliselt lähestikku olles struktureeritud koostööd ja kasutama nende kättesaadavat oskusteavet. Struktureeritud koostöö soodustab vajalikku koosmõju ja ENISA oskusteabe kasvu. Vajaduse korral tuleks kahe organisatsiooni vahel kehtestada erikord, et määrata kindlaks sellise koostöö praktiline kulg.

(21) Amet peaks kooskõlas oma operatiivülesannetega suutma pakkuda liikmesriikidele toetust, näiteks jagama nõu ja tehnilist abi või tagama ohtude ja intsidentide analüüsimise. 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 oma operatiivülesannete täitmisel täiendavat abi.

(22) Amet peaks liidu olukorrateadlikkust toetava tehnilise tasandi korrapärase koostöö raames korrapäraselt 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 (vabatahtlikkuse alusel) või võrgu- ja infosüsteemide direktiivi kohased ühtsed kontaktpunktid, Europoli juures tegutsev küberkuritegevuse vastase võitluse Euroopa keskus (EC3) ja 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) Kui intsidendil on oluline mõju mitmes liikmesriigis, peaks tehniline järeluurimine, mida amet toetab või teostab asjaomaste liikmesriikide taotluse korral või nende nõusolekuga, keskenduma edasiste intsidentide ärahoidmisele ning see tuleks ellu viia ilma, et see piiraks süüd või vastutust omistavaid kohtu-või haldusmenetlusi.

(24) Asjaomased liikmesriigid peaksid uurimise käigus pakkuma ametile vajalikku teavet ja abi, ilma et see piiraks Euroopa Liidu toimimise lepingu artikli 346 sätteid või muid avaliku poliitikaga seotud põhjuseid.

(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 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, organeid ja asutusi esilekerkivate suundumuste kindlakstegemisel ja küberturvalisusega seotud probleemide vältimisel.

(27) Amet peaks liidu vastupidavuse suurendamiseks arendama internetitaristu ja elutähtsate infrastruktuuride turvalisuse alaseid teadmisi, 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, organitelt ja asutustelt.

(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 liikmesriikide ja liidu institutsioonide, organite, asutuste ja ametitega 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, organite ja asutustega, 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) 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 on CSIRTide võrgustiku liige ja pakub neile ka sekretariaaditeenuseid ning 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 igal aastal liidu tasandi küberturvalisuse õppusi ning toetama liikmesriike ja ELi institutsioone, organeid ja asutusi 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 põhimõtted peaksid tuginema hästi väljatöötatud riskihindamismeetoditele, seda nii avalikus kui ka erasektoris. Riskihindamisemeetodeid 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 suurendab 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 teadusuuringuid, arendustegevust ja tehnoloogilisi hindamisi, eelkõige neid, mida tehakse mitmesuguste Euroopa Liidu teadusalgatuste raames, et nõustada liidu institutsioone, organeid ja asutusi ning kui see on asjakohane, liikmesriike nende taotlusel seoses vajadusega teadusuuringute järele võrgu- ja infoturbe, eelkõige küberturvalisuse valdkonnas.

(37) Küberturvalisusega seotud probleemid on ülemaailmsed. Vaja on teha tihedamat rahvusvahelist koostööd, et parandada turbestandardeid, (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, organitele ja asutustele vajalikku oskusteavet ja analüüsi.

(38) Amet peaks suutma reageerida liikmesriikide ja ELi institutsioonide, ametite 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 juulis 2012 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 kindlaks määrama 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, 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 teadureksperdid.

(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[34]. 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[35]. Amet peaks teabe käitlemisel, eelkõige tundliku kuid salastamata teabe ja ELi salastatud teabe käitlemisel järgima liidu institutsioonide kohta kehtivaid sätteid ja liikmesriikide õigusakte.

(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) Vastavushindamine on hindamisprotsess, mille käigus hinnatakse, kas toote, protsessi, teenuse, süsteemi, isiku või asutusega seotud erinõuded on täidetud. Käesoleva

---

[34] 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).

[35] EÜT L 8, 12.1.2001, lk 1.

määruse kohaldamisel tuleks sertifitseerimist käsitada teatavat liiki vastavushindamisena, mis puudutab toote, protsessi, teenuse, süsteemi või nende kombinatsiooni (edaspidi „IKT tooted ja teenused“) küberturvalisuse elemente ja mida teostab sõltumatu kolmas isik, mitte tootja või teenusepakkuja. 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.

(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 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, esineb SOG-IS vastastikuse tunnustamise kokkuleppes siiski märkimisväärseid puudujääke seoses selle suurte kulude ja piiratud ulatusega. Praeguseks on välja arendatud vaid mõned digitaalsete toodete kaitseprofiilid, näiteks digitaalallkiri, digitaalne sõidumeerik ja kiipkaardid. Kõige olulisem on aga see, et SOG-IS hõlmab 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 IKT toodete ja teenuste sertifikaate 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 ELi 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 toodete ja teenuste rühmade kohta. Neid kavu peaksid rakendama ja nende üle järelevalvet teostama riiklikud sertifitseerimise järelevalveasutused 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 tooted ja teenused vastavad kirjeldatud nõuetele. Nimetatud nõuded puudutavad võimet pidada teataval usaldusväärsuse tasemel vastu tegevustele, mille eesmärk on rikkuda 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 käesoleva määruse tähenduses. Käesolevas

määruses ei ole võimalik üksikasjalikult kirjeldada kõigi IKT toodete ja teenuste suhtes kohaldatavaid küberturvalisuse nõudeid. IKT 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 toodete ja teenuste puhul tuleks täpsustada üksikasjalikult igas individuaalses sertifitseerimiskavas, mille komisjon vastu võtab, näiteks viidates standarditele või tehnilistele kirjeldustele.

(56) Komisjonile tuleks anda volitused paluda ENISA-l koostada ettevalmistav sertifitseerimiskava konkreetsete IKT 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 sertifikaadi ulatust ja sisu, sealhulgas hõlmatud IKT 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.

(57) Euroopa küberturvalisuse sertifitseerimise kasutamine peaks jääma vabatahtlikuks, kui liidu või siseriiklikes õigusaktides pole sätestatud teisiti. 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.

(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 akrediteerimise tühistama, kui akrediteerimise tingimused ei ole täidetud või ei ole enam täidetud või asutuse poolt võetavad meetmed rikuvad käesolevat määrust.

(59) Liikmesriike tuleb kohustada määrama ühe küberturvalisuse sertifitseerimise järelevalveasutuse, kes jälgiks nende territooriumil asutatud vastavushindamisasutuste ja nende väljastatud sertifikaatide vastavust käesoleva määruse ja vastavate küberturvalisuse sertifitseerimise kavade nõuetele. Riiklikud sertifitseerimise järelevalveasutused peavad käsitlema füüsiliste või juriidiliste isikute esitatud kaebusi seoses nende riigi territooriumil asutatud vastavushindamisasutuste väljastatud

sertifikaatidega, uurima asjakohasel määral kaebuse sisu ja teavitama kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest. Lisaks peavad nad tegema koostööd teiste riiklike sertifitseerimise järelevalveasutuste 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 riiklikest sertifitseerimise järelevalveasutustest. 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 komisjonile suunatud arvamusi seoses olemasolevate Euroopa küberturvalisuse sertifitseerimise kavade alalhoidmise ja läbivaatamisega;

(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.

(62) Ameti toetus küberturvalisuse sertifitseerimisele peaks hõlmama ka teabevahetust nõukogu julgeolekukomitee ja asjaomaste riiklike asutustega seoses turvaklassvõrkudes kasutatavate toodete krüptograafilise heakskiiduga.

(63) Et vastavushindamisasutuste akrediteerimise kriteeriume veelgi täpsustada, peaks komisjonil olema õigus võtta kooskõlas Euroopa Liidu toimimise lepingu artikliga 290 vastu delegeeritud õigusakte. Komisjon peaks oma ettevalmistustöö jooksul pidama asjakohaseid konsultatsioone, sh ekspertide tasandil. Need konsultatsioonid tuleb läbi viia kooskõlas 13. aprilli 2016. aasta institutsioonidevahelise parema õigusloome kokkuleppes sätestatud põhimõtetega. Eelkõige selleks, et tagada võrdne osalemine delegeeritud õigusaktide ettevalmistamises, peaksid Euroopa Parlament ja nõukogu saama kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel peaks olema pidev juurdepääs komisjoni eksperdirühmade koosolekutele, millel arutatakse delegeeritud õigusaktide ettevalmistamist.

(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 sertifitseerimise järelevalveasutused teavitavad komisjoni akrediteeritud vastavushindamisasutustest.

(66) Ameti tööd tuleks hinna 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 proportsionaalsuspõhimõtte kohaselt ei lähe käesolev direktiiv kaugemale sellest, mis on vajalik nimetatud eesmärgi saavutamiseks,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I JAOTIS
ÜLDSÄTTED

Artikkel 1
Reguleerimisese ja kohaldamisala

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

(a) sätestatakse ENISA ehk nn ELi küberturvalisuse ameti (edaspidi „amet“) eesmärgid, ülesanded ja organisatsioonilised aspektid ning

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

Artikkel 2
Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

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

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

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

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

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

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

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

(9) „küberoht“ – mistahes võimalik asjaolu või sündmus, mis võib kahjustada võrgu- ja infosüsteeme, nende kasutajaid ja mõjutatud isikuid.

(10) „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) toodete ja teenuste sertifitseerimiseks;

(11) „Euroopa küberturvalisuse sertifikaat“ – dokument, mille annab välja vastavushindamisasutus ja mis tõendab, et asjaomane IKT toode või teenus vastab Euroopa küberturvalisuse sertifitseerimise kavas sätestatud konkreetsetele nõuetele;

(12) „IKT toode ja teenus“ – võrgu- ja infosüsteemide mistahes element või elementide rühm;

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

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

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

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

(17) „standard“ – määruse (EL) nr 1025/2012 artikli 2 punktis 1 määratletud standard.

II JAOTIS
ENISA – ELi küberturvalisuse amet

I PEATÜKK
MANDAAT, EESMÄRGID JA ÜLESANDED

Artikkel 3
Mandaat

1. Amet hakkab tegelema ülesannetega, mis talle käesoleva määrusega pannakse, et panustada kõrgetasemelisse küberturvalisusse liidus.

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

3. Ameti eesmärgid ja ülesanded ei piira liikmesriikide küberturvalisuse alast pädevust ning samuti ei piira need mingil juhul tegevusi, mis on seotud avaliku julgeoleku, riigikaitse, riikliku julgeoleku ja riigi tegevusega kriminaalõiguse valdkonnas.

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, ametitel ja asutustel ning liikmesriikidel töötada välja küberturvalisuse valdkonna põhimõtted ja neid rakendada.

3. Amet toetab suutlikkuse ja valmisoleku arendamist kogu liidus sellega, et aitab liidul, liikmesriikidel ning avaliku ja erasektori sidusrühmadel suurendada võrgu- ja infosüsteemide kaitset, arendada küberturvalisuse valdkonna oskusi ja pädevusi ning saavutada kübervastupidavusvõime.

4. Amet edendab liidu tasandil küberturvalisusega seotud küsimuste alast koostööd ja koordineerimist liikmesriikide, liidu institutsioonide, ametite ja asutuste ning asjaomaste sidusrühmade seas, kaasa arvatud erasektoris.

5. Amet suurendab liidu tasandil küberturvalisuse alast suutlikkust, et täiendada liikmesriikide tegevust küberohtude ennetamisel ja neile reageerimisel, seda eeskätt piiriüleste intsidentide puhul.

6. Amet propageerib sertifitseerimist muu hulgas sellega, et aitab 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.

Artikkel 5

Liidu põhimõtete ja õiguse arendamise ja rakendamisega seotud ülesanded

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

1. Abistab ja annab nõu, eeskätt jagab oma sõltumatut arvamust ja teeb ettevalmistusi liidu põhimõtete 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 põhimõtteid 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 põhimõtete 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 põhimõtetega seotud tegevuse regulaarset läbivaatamist ning esitab selleks igal aastal aruande vastava õigusraamistiku rakendamise seisu kohta seoses järgmisega:

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

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

(d) üldkasutatavaid sidevõrke või üldkasutatavaid elektroonilise side teenuseid pakkuvate ettevõtjate edastatud teated turvalisuse rikkumise kohta, mille pädevad asutused esitavad ametile vastavalt [Euroopa elektroonilise side seadustiku kehtestamise direktiivi] artiklile 40.

Artikkel 6
Suutlikkuse arendamisega seotud ülesanded

1. Amet abistab:

(b) liikmesriike nende tegevuses, et parandada küberturvalisuse probleemide ja intsidentide ennetamist, avastamist, analüüsimist ja neile reageerimise suutlikkust, pakkudes neile vajalikke teadmisi ja oskusteavet;

(c) liidu institutsioone, organeid ja asutusi nende tegevuses, et parandada küberturvalisuse probleemide ja intsidentide ennetamist, avastamist, analüüsimist ja neile reageerimise suutlikkust, pakkudes asjakohast toetust liidu institutsioonide, organite ja asutuste CERTile (CERT-EU);

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

(e) 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;

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

(g) 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;

(h) liikmesriike, korraldades igal aastal liidu tasandil artikli 7 lõikes 6 osutatud ulatuslikud küberturvalisuse õppused ja andes õppuste hindamise ja õppuste käigus omandatud kogemuste põhjal poliitilisi soovitusi;

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

(j) koostöörühma, vahetades parimaid tavasid 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 soodustab valdkondlike teabe jagamise ja analüüsimise keskuste (ISACide) loomist ja toetab neid pidevalt 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

Liidu tasandi operatiivkoostööga seotud ülesanded

1. Amet toetab operatiivkoostööd pädevate avalik-õiguslike asutuste seas ja sidusrühmade vahel.

2. Amet teeb operatiivtasandil koostööd ja loob koostoimet liidu institutsioonide, organite ja asutustega (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 aktiivselt teabe jagamist ja koostööd võrgustiku liikmete vahel.

4. Amet annab oma panuse CSIRTide võrgustikus toimuvasse operatiivkoostöösse ning toetab liikmesriike järgmiselt:

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

   (e) pakub liikmesriikidele nende taotlusel tehnilist abi märkimisväärse või olulise mõjuga intsidentide korral;

   (f) analüüsib nõrkusi, moonutusi ja intsidente.

Et saada kasu koostoimest, teevad amet ja CERT-EU neid ülesandeid täites struktureeritud koostööd, eeskätt operatiivaspektides.

5. Kahe või enama asjaomase liikmesriigi taotluse korral ja üksnes selleks, et anda nõu edasiste intsidentide vältimiseks, teeb amet tehnilise järeluurimise või pakub selleks vajalikku toetust pärast seda, kui mõjutatud ettevõtjad on teatanud märkimisväärse

või olulise mõjuga intsidendist vastavalt direktiivile (EL) 2016/1148. Amet teeb sellise uurimise ka juhul, kui selline intsident on mõjutanud rohkem kui kaht liikmesriiki ning kui komisjon esitab asjaomaste liikmesriikide nõusolekul põhjendatud taotluse.

Sellise uurimise ulatuses ja selle teostamise korras lepivad kokku asjaomased liikmesriigid ja amet ning see ei piira ühtegi sama intsidendi kohta pooleli olevat kriminaaluurimist. Uurimise lõpuks koostab amet eeskätt asjaomaste liikmesriikide ja ettevõtjate esitatud teabe ja kommentaaride põhjal lõpliku tehnilise aruande, mis lepitakse kokku asjaomaste liikmesriikidega. Aruande kokkuvõtet, milles keskendutakse soovitustele selle kohta, kuidas edaspidi intsidente vältida, jagatakse CSIRTide võrgustikuga.

6. Amet korraldab iga-aastaseid liidu tasandi küberõppusi ning toetab liikmesriike ja ELi institutsioone, organeid ja asutusi nende taotluse korral õppuste korraldamisel. Iga-aastased liidu tasandi õppused sisaldavad tehnilisi, operatiivseid ja strateegilisi elemente, et aidata ette valmistada liidu tasandi koostööl põhinevat reageerimist ulatuslikele piiriülestele küberturvalisuse intsidentidele. Lisaks annab amet vajaduse korral oma panuse valdkondlike küberõppuste korraldamisse ja aitab neid korraldada koos asjaomaste teabe jagamise ja analüüsimise keskustega ning lubab keskustel osaleda ka liidu tasandi küberturvalisuse õppustel.

7. Amet koostab 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 (vabatahtlikkuse alusel) või ELi võrgu- ja infoturbe direktiivi alusel loodud ühtsed kontaktpunktid (vastavalt võrgu- ja infoturbe direktiivi artiklit 14 lõikele 5); 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:

   (g) koondab riiklikest allikatest pärit aruandeid, et aidata kaasa ühise olukorrateadlikkuse tekitamisele;

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

   (i) toetab intsidendi või kriisi tehnilist lahendamist, hõlbustades muu hulgas tehniliste lahenduste jagamist liikmesriikide vahel;

   (j) toetab intsidenti või kriisi puudutavat avalikku teabevahetust;

   (k) testib sellistele intsidentidele või kriisidele reageerimiseks mõeldud koostööplaane.

Artikkel 8

Turu, küberturvalisuse sertifitseerimise ja standardimisega seotud ülesanded

Amet teeb järgmist:

(k) toetab ja edendab käesoleva määruse III jaotises kirjeldatud IKT toodete ja teenuste küberturvalisuse sertifitseerimise alaste liidu põhimõtete arendamist ja rakendamist järgmiselt:

(1) koostab IKT toodete ja teenuste Euroopa küberturvalisuse sertifitseerimise ettevalmistavad kavad 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 sertifitseerimisega tegelevate järelevalveasutuste ja tööstusega;

(l) hõlbustab riskihalduse ning IKT toodete ja teenuste turvalisuse Euroopa ja rahvusvaheliste standardite loomist ja kasutuselevõtmist ning 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;

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

Artikkel 9

Teadmiste, teabe ja teadlikkuse suurendamisega seotud ülesanded

Amet teeb järgmist:

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

(o) koostab pikaajalisi strateegilisi analüüse küberturvalisuse ohtude ja intsidentide kohta, et teha kindlaks väljakujunevad suundumused ja aidata vältida küberturvalisusega seotud probleeme;

(p) jagab koostöös liikmesriikide ametiasutuste ekspertidega nõu, juhiseid ja parimaid tavasid võrgu- ja infosüsteemide turvalisuse kohta, eeskätt selles osas, mis puudutab internetitaristu ja nende taristute turvalisust, mis toetavad direktiivi (EL) 2016/1148 II lisas loetletud sektoreid;

(q) koondab, korraldab ja teeb avalikkusele spetsiaalse portaali kaudu kättesaadavaks liidu institutsioonide, ametite ja organite esitatud teavet küberturvalisuse kohta;

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

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

(t) korraldab koostöös liikmesriikide ja liidu institutsioonide, organite ja asutustega korrapäraselt teavituskampaaniaid, et suurendada küberturvalisust ja selle nähtavust liidus.

Artikkel 10

Teadus- ja uuendustegevusega seotud ülesanded

Teadus- ja uuendustegevuse vallas teeb amet järgmist:

(u) 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;

(v) osaleb teadus- ja uuendustegevuse rahastamise programmide rakendamisfaasis, kui komisjon on talle delegeerinud asjakohased volitused, või tegutseb toetusesaajana.

Artikkel 11

Rahvusvahelise koostööga seotud ülesanded

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

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

(x) aitab komisjoni taotlusel kaasa parimate tavade vahetamisele asjaomaste rahvusvaheliste organisatsioonide vahel;

(y) pakub komisjonile taotluse korral oskusteavet.

II PEATÜKK
AMETI TÖÖKORRALDUS

Artikkel 12
Struktuur

Ameti haldus- ja juhtimisstruktuur koosneb järgmistest komponentidest:

(z) haldusnõukogu, kes täidab artiklis 14 sätestatud ülesandeid;

(aa) juhatus, kes täidab artiklis 18 sätestatud ülesandeid;

(bb) tegevdirektor, kes täidab artiklis 19 sätestatud kohustusi, ning

(cc) alaline sidusrühm, kes täidab artiklis 20 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;

(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:

   (b) valmistab ette haldusnõukogus vastuvõetavad otsused;

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

   (d) 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. Kiireloomulistel juhtudel võib juhatus vajaduse korral teha haldusnõukogu nimel teatavaid esialgseid otsuseid, eelkõige halduskü simustes, sealhulgas ametisse nimetava asutuse volituste delegeerimise peatamise ja eelarveküsimuste kohta.

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 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;

(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. Tegevdirektor otsustab, kas ameti ülesannete tõhusaks ja tulemuslikuks täitmiseks on vaja paigutada töötajaid ühte või mitmesse liikmesriiki. Enne kui tegevdirektor otsustab rajada kohaliku kontori, peab ta saama komisjonilt, haldusnõukogult ja asjaomaselt liikmesriigilt (asjaomastelt liikmesriikidelt) eelneva nõusoleku. Otsuses määratakse täpselt kindlaks kohaliku kontori tegevuse ulatus, et vältida tarbetuid kulusid ja ameti haldusülesannete dubleerimist. Vajaduse korral või kui seda nõutakse, tuleb saavutada kokkulepe asjaomaste liikmesriikidega.

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 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.

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[36] 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.

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.

---

36 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).

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[37] ja 2015/444[38]. Nimetatud eeskirjad hõlmavad salastatud teabe vahetust, töötlemist ja säilitamist käsitlevaid sätteid.

Artikkel 25
Juurdepääs dokumentidele

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

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

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

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

[38] 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).

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:

   (b) toetus liidu eelarvest;

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

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

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

   (f) 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,[39] 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.

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[40] (mis käsitleb komisjoni tehtavat kohapealset kontrolli ja inspekteerimist, et kaitsta Euroopa ühenduste finantshuve pettuste ja igasuguse muu eeskirjade eiramiste eest) 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.

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).

---

39 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).

40 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 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 viis aastat. Selle aja lõpuks koostab komisjon hinnangu, milles võetakse arvesse tegevdirektori tegevuse hindamist ning ameti edasisi ülesandeid ja probleeme.

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 viie 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 otsusega, mille haldusnõukogu teeb komisjoni ettepaneku alusel.

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 kinnisvara 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[41].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.

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

Artikkel 38

Isikuandmete kaitse

1. Amet kohaldab isikuandmete töötlemise suhtes Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 45/2001[42].

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.

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

[42] 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).

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 parimad võimalikud 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 kavad

Euroopa küberturvalisuse sertifitseerimise kava kinnitab, et selle kava kohaselt sertifitseeritud IKT tooted ja teenused vastavad kirjeldatud nõuetele selles osas, mis puudutab nende võimet pidada teataval usaldusväärsuse tasemel vastu tegevustele, mille eesmärk on rikkuda salvestatud, edastatud või töödeldud andmete või nende toodete, protsesside, teenuste ja süsteemide funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust.

Artikkel 44

Euroopa küberturvalisuse sertifitseerimise kava ettevalmistamine ja vastuvõtmine

1. Komisjoni taotluse põhjal koostab ENISA Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava, mis vastab käesoleva määruse artiklites 45, 46 ja 47 sätestatud tingimustele. Liikmesriigid või artikliga 53 loodud Euroopa küberturvalisuse sertifitseerimise rühm (edaspidi „rühm“) võivad teha komisjonile ettepaneku koostada Euroopa küberturvalisuse sertifitseerimise ettevalmistav kava.

2. Käesoleva artikli lõikes 1 osutatud ettevalmistavat kava koostades konsulteerib ENISA kõigi asjaomaste sidusrühmadega ja teeb rühmaga tihedat koostööd. Rühm pakub ENISA-le viimase taotluse korral abi ja eksperdinõu seoses ettevalmistava sertifitseerimiskava koostamisega, esitades vajaduse korral ka arvamusi.

3. ENISA edastab käesoleva artikli lõike 2 kohaselt koostatud Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava komisjonile.

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

5. ENISA haldab spetsiaalset veebilehte, mis pakub teavet Euroopa küberturvalisuse sertifitseerimise kavade kohta ja tutvustab neid.

Artikkel 45

Euroopa küberturvalisuse sertifitseerimise kavade turvalisusega seotud eesmärgid

Euroopa küberturvalisuse sertifitseerimise kava peab olema koostatud nii, et võtta vajaduse korral arvesse järgmisi turvalisusega seotud eesmärke:

(e) kaitsta salvestatud, edastatud või muul moel töödeldud andmeid juhusliku või volitamata salvestamise, töötlemise, juurdepääsu või avalikustamise eest;

(f) kaitsta salvestatud, edastatud või muul moel töödeldud andmeid juhusliku või volitamata hävitamise ja juhusliku kaotsimineku või muutmise eest;

(g) tagada, et volitatud kasutajatel, programmidel ja masinatel oleks juurdepääs üksnes neile andmetele, teenustele või funktsioonidele, millele neil on juurdepääsuõigused;

(h) talletada, milliseid andmeid, teenuseid või funktsioone on edastatud, millal ja kelle poolt;

(i) tagada võimalus kontrollida, millal ja kes on pääsenud juurde millistele andmetele, teenustele või funktsioonidele või neid kasutanud;

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

(k) tagada, et IKT tooteid ja teenuseid pakutakse ajakohastatud tarkvaraga, mis ei sisalda teadaolevaid turvaauke, ning et olemas on mehhanismid turvaliseks tarkvara uuendamiseks.

Artikkel 46

Euroopa küberturvalisuse sertifitseerimise kavade usaldusväärsuse tasemed

1. Euroopa küberturvalisuse sertifitseerimise kavas määratakse selle kava raames sertifitseeritud IKT toodetele ja teenustele üks või mitu järgmist usaldusväärsuse taset: baastase, märkimisväärne ja/või kõrge tase.

2. Baastase, märkimisväärne ja kõrge usaldusväärsuse tase vastavad järgmistele tingimustele:

(l) usaldusväärsuse baastase osutab Euroopa küberturvalisuse sertifitseerimise kava raames väljastatud sertifikaadile, mis annab piiratud usalduse IKT toote või teenuse väidetavate või kinnitatud küberturvalisuse omaduste vastu ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on vähendada küberturvalisuse intsidentide riski;

(m) märkimisväärne usaldusväärsuse tase osutab Euroopa küberturvalisuse sertifitseerimise kava raames väljastatud sertifikaadile, mis annab märkimisväärse usalduse IKT toote või teenuse väidetavate või kinnitatud küberturvalisuse omaduste vastu ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on vähendada märkimisväärselt küberturvalisuse intsidentide riski;

(n) kõrge usaldusväärsuse tase osutab Euroopa küberturvalisuse sertifitseerimise kava raames väljastatud sertifikaadile, mis annab kõrgema usalduse IKT toote või teenuse väidetavate või kinnitatud küberturvalisuse omaduste vastu kui

märkimisväärse usaldusväärsuse tasemega sertifikaat ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on vältida küberturvalisuse intsidente.

Artikkel 47

Euroopa küberturvalisuse sertifitseerimise kavade elemendid

1. Euroopa küberturvalisuse sertifitseerimise kava sisaldab järgmisi elemente:

(o) sertifitseerimise sisu ja ulatus, sealhulgas hõlmatud IKT toodete ja teenuste liik või kategooria;

(p) konkreetsete IKT toodete ja teenuste puhul hinnatavate küberturvalisuse nõuete üksikasjalik kirjeldus , näiteks viidates liidu või rahvusvahelistele standarditele või tehnilistele kirjeldustele;

(q) vajaduse korral üks või mitu usaldusväärsuse taset;

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

(s) sertifitseerimiseks vajalik teave, mille taotleja peab esitama vastavushindamisasutustele;

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

(u) kui kava osaks on järelevalve, eeskirjad sertifikaatide nõuete täitmise kontrollimiseks, sealhulgas mehhanismid tõestamaks konkreetsete küberturvalisuse nõuete jätkuvat täitmist;

(v) tingimused sertifitseerimise võimaldamiseks, säilitamiseks, jätkamiseks ning sertifitseerimise ulatuse laiendamiseks ja vähendamiseks;

(w) eeskirjad sertifitseeritud IKT toodete ja teenuste sertifitseerimistingimustele mittevastavuse tagajärgede kohta;

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

(y) eeskirjad andmete säilitamise kohta vastavushindamisasutuste poolt;

(z) sama liiki või kategooriasse kuuluvaid IKT tooteid või teenuseid hõlmavate riiklike küberturvalisuse sertifitseerimise kavade kindlakstegemine;

(aa) väljastatud sertifikaatide sisu.

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 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 48

Küberturvalisuse sertifitseerimine

1. Kui IKT 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 ei ole sätestatud teisiti.

3. Käesoleva artikli kohase Euroopa küberturvalisuse sertifikaadi 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 avalik-õiguslik asutus on üks järgnevatest asutustest:

   (bb) artikli 50 lõikes 1 osutatud riiklik sertifitseerimise järelevalveasutus,

   (cc) artikli 51 lõike 1 kohaselt vastavushindamisasutusena akrediteeritud asutus või

   (dd) asjaomase liikmesriigi õigusaktide, seadusandlike dokumentide või muude ametlike haldusmenetluste kohaselt loodud asutus, mis vastab standardi ISO/IEC 17065:2012 nõuetele asutustele, kes sertifitseerivad tooteid, protsesse ja teenuseid.

5. Füüsiline või juriidiline isik, kes esitab oma IKT tooted või teenused sertifitseerimiseks, peab esitama artiklis 51 osutatud vastavushindamisasutusele kogu sertifitseerimismenetluse läbiviimiseks vajaliku teabe.

6. Sertifikaat antakse maksimaalselt kolmeks aastaks ja selle kehtivust võib pikendada samadel tingimustel senikaua, 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 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 toodete ja teenustega seotud menetlused jäävad alles.

2. Liikmesriigid ei kehtesta uusi riiklikke küberturvalisuse sertifitseerimise kavasid IKT toodetele ja teenustele, mis on kaetud kehtiva Euroopa küberturvalisuse sertifitseerimise kavaga.

3. Riiklike küberturvalisuse sertifitseerimise kavade alusel väljastatud sertifikaadid jäävad kehtima kuni oma kehtivusaja lõpuni.

Artikkel 50
Riiklikud sertifitseerimise järelevalveasutused

1. Iga liikmesriik määrab riikliku sertifitseerimise järelevalveasutuse.

2. Iga liikmesriik teatab komisjonile määratud asutuse andmed.

3. Iga riiklik sertifitseerimise järelevalveasutus on oma organisatsiooni, rahastamisotsuste, õigusliku struktuuri ja otsuste tegemise poolest sõltumatu üksustest, mille üle ta järelevalvet teostab.

4. Liikmesriigid tagavad, et riiklikel sertifitseerimise järelevalveasutustel 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 sertifitseerimise järelevalveasutused:

(ee) jälgivad käesoleva jaotise sätete kohaldamist riiklikul tasandil ja tagavad nende täitmise ning teevad järelevalvet nende riigi territooriumil asutatud vastavushindamisasutuse poolt välja antud sertifikaatide vastavuse üle käesolevas jaotises ja vastavas Euroopa küberturvalisuse sertifikaadi kavas sätestatud nõuetele;

(ff) jälgivad ja kontrollivad vastavushindamisasutuste tegevust käesoleva määruse kohaldamisel, sealhulgas seoses käesoleva määruse artiklis 52 sätestatud vastavushindamisasutustest teavitamise ja sellega seotud ülesannetega;

(gg) käsitlevad füüsiliste või juriidiliste isikute esitatud kaebusi seoses nende riigi territooriumil asutatud vastavushindamisasutuste väljastatud sertifikaatidega, uurivad asjakohasel määral kaebuse sisu ja teavitavad kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest;

(hh) teevad koostööd teiste riiklike sertifitseerimise järelevalveasutuste või muude avaliku sektori asutusega, sealhulgas jagades teavet IKT toodete ja teenuste

võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele;

(ii) jälgivad küberturvalisuse sertifitseerimise valdkonna asjakohaseid arenguid.

7. Igal riiklikul sertifitseerimise järelevalveasutusel on vähemalt järgmised volitused:

(jj) anda vastavushindamisasutustele ja Euroopa küberturvalisuse sertifikaadi omanikele korraldus esitada teavet, mis on vajalik tema ülesannete täitmiseks;

(kk) teostada auditi vormis vastavushindamisasutuste ja Euroopa küberturvalisuse sertifikaadi omanike uurimist, et kontrollida nende vastavust III jaotise sätetele;

(ll) võtta asjakohaseid meetmeid vastavalt siseriiklikele õigusaktidele tagamaks, et vastavushindamisasutused ja sertifikaadi omanikud järgivad käesoleva määruse või Euroopa küberturvalisuse sertifitseerimise kava nõudeid;

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

(nn) võtta siseriiklike õigusaktide kohaselt tagasi sertifikaadid, mis ei ole kooskõlas käesoleva määrusega või Euroopa küberturvalisuse sertifitseerimise kavaga;

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

8. Riiklikud sertifitseerimise järelevalveasutused teevad omavahel ja komisjoniga koostööd ning vahetavad eelkõige teavet, kogemusi ja häid tavasid seoses küberturvalisuse sertifitseerimisega ning IKT 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.

2. Akrediteering antakse maksimaalselt viieks aastaks ja selle kehtivust võib pikendada samadel tingimustel senikaua, kuni vastavushindamisasutus vastab käesolevas artiklis sätestatud nõuetele. Akrediteerimisasutus tühistab käesoleva artikli lõikes 1 osutatud vastavushindamisasutuse akrediteerimise, kui akrediteerimise tingimused ei ole täidetud või ei ole enam täidetud või asutuse poolt võetavad meetmed rikuvad käesolevat määrust.

Artikkel 52
Teavitamine

1. Riiklikud sertifitseerimise järelevalveasutused teatavad iga artikli 44 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava puhul komisjonile, millised akrediteeritud 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 sertifitseerimise järelevalveasutus 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 sertifitseerimise järelevalveasutuse 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 riiklikest sertifitseerimise järelevalveasutustest. Riiklikke sertifitseerimise järelevalveasutusi esindavad nende juhid või muud kõrgetasemelised esindajad.

3. Rühmal on järgmised ülesanded:

(pp) 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;

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

(rr) teha komisjonile ettepanek, et ta paluks ametil koostada Euroopa küberturvalisuse sertifitseerimise ettevalmistav kava kooskõlas käesoleva määruse artikliga 44;

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

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

(uu) lihtsustada riiklike sertifitseerimise järelevalveasutuste käesoleva jaotise kohast koostööd teabevahetuse kaudu, eelkõige luues meetodid tõhusaks teabevahetuseks kõigis küberturvalisuse sertifitseerimisega seotud küsimustes.

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

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. Nimetatud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad. Liikmesriigid teavitavad komisjoni [.../viivitama] 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 artiklit 5.

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 (EL) nr 526/2013 tunnistatakse kehtetuks alates [...].

2. Viiteid määrusele (EL) 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 (EL) 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 (EL) nr 526/2013 artikli 24 lõike 4 alusel ametisse nimetatud tegevdirektor jääb tegevdirektoriks oma ametiaja lõpuni.

6. Määruse (EL) 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.

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

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

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 turvalisuse sertifitseerimist („küberturvalisust käsitlev õigusakt/määrus“)

1.2. Asjaomased poliitikavaldkonnad

Poliitikavaldkond: 09. Sidevõrgud, sisu ja tehnoloogia

Tegevusala: 09.02. Digitaalne ühtne turg

1.3. Ettepaneku/algatuse liik

☒ Ettepanek/algatus käsitleb **uut meedet (III jaotis – sertifitseerimine)**

☐ Ettepanek/algatus käsitleb **uut meedet, mis tuleneb katseprojektist / ettevalmistavast meetmest**[43]

☒ Ettepanek/algatus käsitleb **olemasoleva meetme pikendamist (II jaotis – ENISA mandaat)**

☐ Ettepanek/algatus käsitleb **ümbersuunatud meedet**

1.4. Eesmärgid

1.4.1. Komisjoni mitmeaastased strateegilised eesmärgid, mida ettepaneku/algatuse kaudu täidetakse

1. Liikmesriikide, ettevõtjate ja ELi kui terviku vastupidavusvõime suurendamine

2. ELi IKT toodete ja teenuste siseturu nõuetekohase toimimise tagamine

3. IKT valdkonnas tegutsevate ELi ettevõtjate ülemaailmse konkurentsivõime suurendamine

4. Liikmesriikide nende õigus- ja haldusnormide ühtlustamine, mille puhul on vaja tagada küberturvalisus

1.4.2. Erieesmärgid

Üldeesmärki arvesse võttes on instrumendi eesmärk saavutada läbivaadatud küberturvalisuse strateegia laiemas kontekstis järgmised erieesmärgid, määrates kindlaks ENISA haldusala ja mandaadi ning kehtestades IKT toodete ja teenuste Euroopa

[43] Vastavalt finantsmääruse artikli 54 lõike 2 punktile a või b.

sertifitseerimise raamistiku:

1. arendada liikmesriikide ja ettevõtjate **suutlikkust ja valmisolekut**;

2. parandada k**oostööd ja koordineerimist** liikmesriikides, ELis ning institutsioonides, organites ja asutustes;

3. suurendada **ELi tasandil suutlikkust täiendada liikmesriikide võetavaid meetmeid**, eelkõige piirüleste küberkriiside puhul;

4. suurendada kodanike ja ettevõtjate **teadlikkust** küberturvalisusega seotud küsimustest;

5. suurendada usaldust digitaalse ühtse turu ja digitaalse uuendustegevuse vastu, suurendades IKT toodete ja teenuste **küberturvalisuse alase usaldusväärsuse**[44] üldist **läbipaistvust**.

ENISA aitab saavutada eespool nimetatud eesmärgid järgmiselt:

suurem toetus poliitikakujundamisele – annab komisjonile ja liikmesriikidele juhiseid ja nõuandeid, et töötada küberturvalisuse valdkonnas välja terviklik normatiivne raamistik ning sektoripõhised poliitika- ja seadusandlikud algatused ning neid ajakohastada; panustab koostöörühma (direktiivi (EL) 2016/1148 artikkel 11) töösse, andes oskusteavet ja abi; toetab poliitikakujundamist ja rakendamist e-identimise ja usaldusteenuste valdkonnas; edendab parimate tavade jagamist pädevate asutuste vahel;

suurem toetus suutlikkuse arendamisele – aitab liikmesriikidel ning Euroopa Liidu institutsioonidel, organitel ja asutustel töötada välja ja parandada küberturvalisuse probleemide ja intsidentide ärahoidmise, avastamise, analüüsimise ja neile reageerimise suutlikkust; aitab liikmesriikidel, kui nad seda taotlevad, arendada välja riiklikud küberturbe intsidentide lahendamise üksused (CSIRTid) ja riiklikud küberturvalisuse strateegiad; aitab Euroopa Liidu institutsioonidel arendada välja ja vaadata läbi Euroopa Liidu küberturvalisuse strateegiad; pakub küberturvalisuse alast koolitust; aitab liikmesriikidel tutvustada koostöörühma kaudu parimaid tavasid; soodustab valdkondlike teabe jagamise ja analüüsimise keskuste (ISACide) loomist;

operatiivkoostöö ja kriisiohje toetamine – toetab koostööd pädevate avalik-õiguslike asutuste seas ja sidusrühmade vahel, luues süsteemse koostöö Euroopa Liidu institutsioonide, organite ja ametitega, kelle tegevus puudutab küberturvalisust, küberkuritegevust ning eraelu puutumatuse ja isikuandmete kaitset; tagab CSIRTide võrgustiku sekretariaaditeenused (direktiivi (EL) 2016/1148 artikli 12 lõige 2) ja panustab operatiivkoostöösse võrgustikuga, tagades koostöös CERT-EUga liikmesriikide taotluse korral neile vajaliku toe; korraldab korrapäraselt küberturvalisuse õppusi; aitab töötada välja koostööl põhinevat reageerimist ulatuslikele piirülestele küberturvalisuse intsidentidele ja kriisidele; viib koostöös CSIRTide võrgustikuga ellu oluliste intsidentide tehnilised järeluurimised ja annab edasisi soovitusi;

[44] Küberturvalisuse alase usaldusväärsuse läbipaistvus tähendab seda, et kasutajatele antakse piisavalt teavet küberturvalisuse omaduste kohta, tänu millele saavad nad määrata objektiivselt kindlaks konkreetse IKT toote, teenuse või protsessi turvalisuse taseme.

turuga seotud ülesanded (standardimine ja sertifitseerimine) – täidab mitmeid ülesandeid, et toetada siseturgu: tegutseb küberturvalisuse turu vaatlusrühmana, analüüsides küberturvalisuse turu asjaomaseid suundumusi, et reageerida paremini nõudlusele ja pakkumisele; toetab ja edendab Euroopa Liidu tegevuspõhimõtete väljatöötamist ja rakendamist IKT toodete ja teenuste küberturvalisuse sertifitseerimise valdkonnas, koostades IKT toodete ja teenuste jaoks ettevalmistavad Euroopa küberturvalisuse sertifitseerimise kavad, tagades Euroopa Liidu küberturvalisuse sertifitseerimise rühma sekretariaaditeenused ning IKT toodete ja teenuste turvanõuete juhised ja head tavad koostöös riiklike sertifitseerimise järelevalveasutuste ja tööstusega; **suurem toetus teadmiste, teabe ja teadlikkuse suurendamisele** – annab komisjonile ja liikmesriikidele abi ja nõu kogu liidus võrgu- ja infoturbe küsimustes kõrgetasemeliste teadmiste omandamiseks ja nende rakendamiseks tööstusvaldkonna sidusrühmade suhtes. Selleks tuleb ka spetsiaalse portaali kaudu koondada, korraldada ja teha avalikkusele kättesaadavaks võrgu- ja infosüsteemide turvalisust [või küberturvalisust] käsitlevat teavet. Teine tähtis element on küberturvalisuse riske käsitlevad teadlikkuse suurendamise tegevused ja teavituskampaaniad, mis on suunatud laiemale avalikkusele;

suurem toetus teadus- ja uuendustegevusele – annab nõuandeid vajalike teadusuuringute ja prioriteetide kohta küberturvalisuse valdkonnas;

rahvusvahelise koostöö toetamine – toetab jõupingutusi, mida Euroopa Liit teeb kolmandate riikide ja rahvusvaheliste organisatsioonidega koostöö tegemiseks, et edendada küberturvalisuse valdkonnas tehtavat rahvusvahelist koostööd.

SERTIFITSEERIMINE

Sertifitseerimisraamistik aitab saavutada eesmärke, suurendades IKT toodete ja teenuste küberturvalisuse alase usaldusväärsuse[45] üldist läbipaistvust ja seeläbi ka usaldust digitaalse ühtse turu ja digitaalse uuendustegevuse vastu. Selle abil peaks ka olema võimalik vältida sertifitseerimise kavade killustatust ELis ning nendega seotud turvanõuete ja hindamiskriteeriumide killustatust liikmesriikides ja sektorites.

1.4.3. Oodatavad tulemused ja mõju

Täpsustage, milline peaks olema ettepaneku/algatuse oodatav mõju toetusesaajatele/sihtrühmale.

Tugevam ENISA (mis toetab suutlikkust, ennetamist, koostööd ja teadlikkust ELi tasandil ja on seega kujundatud suurendama ELi üldist kübervastupidavusvõimet) ning IKT toodete ja teenuste ELi sertifitseerimisraamistiku toetamine annab eeldatavasti järgmised tulemused (loetelu ei ole ammendav).

Üldine mõju

- Üldine positiivne mõju siseturule tänu väiksemale turu killustatusele ja parema koostöö abil usalduse suurendamisele digitaaltehnoloogia vastu, paremini ühtlustatud

[45] Küberturvalisuse alase usaldusväärsuse läbipaistvus tähendab seda, et kasutajatele antakse piisavalt teavet küberturvalisuse omaduste kohta, tänu millele saavad nad määrata objektiivselt kindlaks konkreetse IKT toote, teenuse või protsessi turvalisuse taseme.

lähenemisviisidele ELi küberturvalisuse valdkonna põhimõtete puhul ja suuremale suutlikkusele ELi tasandil. See peaks avaldama positiivset majanduslikku mõju, aidates vähendada küberturvalisuse / küberkuritegevuse intsidentide kulusid, mille hinnanguline majanduslik mõju liidus on 0,41 % ELi SKPst (s.o ligikaudu 55 miljardit eurot).

Konkreetsed tulemused

Liikmesriikide ja ettevõtjate parem küberturvalisuse alane suutlikkus ja valmisolek

- Liikmesriikide parem küberturvalisuse alane suutlikkus ja valmisolek (tänu küberohtude ja -intsidentide pikaajalisele strateegilisele analüüsile, juhistele ja aruannetele, oskusteabe ja heade tavade vahendamisele, koolitustele ja õppematerjalide kättesaadavusele ning täiustatud õppustele Cyber Europe).

- Erasektori osalejate parem suutlikkus tänu teabe jagamise ja analüüsimise keskuste (ISACide) loomisele eri valdkondades.

- ELi ja liikmesriikide parem küberturvalisuse alane valmisolek tänu sellele, et õppuste Cyber Europe raames katsetatud suuremahuliste piiriüleste küberturvalisuse intsidentide puhul on kättesaadavad hästi läbi harjutatud ja kokkulepitud kavad.

Parem koostöö ja koordineerimine liikmesriikides ning ELi institutsioonides, organites ja asutustes

- Parem koostöö nii avaliku ja erasektori piires kui ka nende vahel.

- ELi võrgu- ja infoturbe direktiivi piiriülese ja valdkondliku rakendamise puhul ühtsema lähenemisviisi kasutamine.

- Parem koostöö sertifitseerimise valdkonnas tänu institutsioonilisele raamistikule, mis võimaldab töötada välja Euroopa küberturvalisuse sertifitseerimise kavad ja ühised tegevuspõhimõtted selles valdkonnas.

Suurem ELi tasandi suutlikkus täiendada liikmesriikide võetavaid meetmeid

- Parem ELi tegevussuutlikkus täiendada liikmesriikide võetavaid meetmeid ja toetada liikmesriike piiritletud ja eelnevalt kindlaks määratud teenustega, kui nad esitavad vastava taotluse. Need avaldavad tõenäoliselt positiivset mõju intsidentide edukale ärahoidmisele, avastamisele ja lahendamisele nii liikmesriigi kui ka liidu tasandil.

Kodanike ja ettevõtjate suurem teadlikkus küberturvalisusega seotud küsimustest

- Kodanike ja ettevõtjate suurem üldine teadlikkus küberturvalisusega seotud küsimustest.

- Tänu küberturvalisuse sertifitseerimisele on võimalik teha paremini IKT toodete ja teenuste teadlikke ostuotsuseid.

Suurem usaldus digitaalse ühtse turu ja digitaalse uuendustegevuse vastu, suurendades IKT toodete ja teenuste küberturvalisuse alase usaldusväärsuse läbipaistvust

- IKT toodete ja teenuste küberturvalisuse alase usaldusväärsuse[46] suurem läbipaistvus tänu turvalisuse sertifitseerimise menetluste lihtsustamisele ELi-ülese raamistiku abil.

- IKT toodete ja teenuste turvaomadused on usaldusväärsemad.

- Turvalisuse sertifitseerimine võetakse laialdasemalt kasutusele tänu lihtsustatud menetlustele, väiksematele kuludele ja kogu ELi hõlmavatele ärivõimalustele, mida ei takista turu killustatus.

- ELi küberturvalisuse turu parem konkurentsivõime tänu VKEde väiksematele kuludele ja halduskoormusele ning mitmest riiklikust sertifitseerimissüsteemist põhjustatud potentsiaalsete turule sisenemise tõkete kõrvaldamisele.

Muud

- Ühegi eesmärgi puhul ei eeldata märkimisväärse keskkonnamõju tekkimist.

- ELi eelarve puhul võib eeldada, et tõhusus suureneb tänu paremale koostööle ja tegevuse koordineerimisele ELi institutsioonide, organite ja asutuste vahel.

1.4.4. Tulemus- ja mõjunäitajad

Täpsustage, milliste näitajate alusel hinnatakse ettepaneku/algatuse elluviimist.

(vv)

Eesmärk: arendada liikmesriikide ja ettevõtjate suutlikkust ja valmisolekut

- ENISA korraldatud koolituste arv.
- ENISA antud otsese abi geograafiline hõlmavus (riikide ja piirkondade arv).
- Liikmesriikide valmisoleku tase CSIRTide valmisoleku ning küberturvalisuse järelevalvega seotud regulatiivsete meetmete seisukohast.
- ENISA jagatud kogu ELi hõlmavate heade tavade arv elutähtsa taristu jaoks.
- ENISA jagatud kogu ELi hõlmavate heade tavade arv VKEde jaoks.
- ENISA poolt küberohtude ja -intsidentide iga-aastase strateegilise analüüsi avaldamine, et määrata kindlaks tekkivad seaduspärad.
- ENISA pidev panus Euroopa standardiorganisatsioonide küberturvalisuse töörühmade töösse.

Eesmärk: parandada koostööd ja koordineerimist liikmesriikides ning ELi institutsioonides, organites ja asutustes

- Oma poliitika kujundamise protsessis ENISA soovitusi ja arvamusi kasutanud liikmesriikide arv.

[46] Küberturvalisuse alase usaldusväärsuse läbipaistvus tähendab seda, et kasutajatele antakse piisavalt teavet küberturvalisuse omaduste kohta, tänu millele saavad nad määrata objektiivselt kindlaks konkreetse IKT toote, teenuse või protsessi turvalisuse taseme.

- Oma poliitika kujundamise protsessis ENISA soovitusi ja arvamusi kasutanud ELi institutsioonide, organite ja asutuste arv.
- CSIRTide võrgustiku tööprogrammi korrapärane rakendamine ning CSIRTide võrgustiku IT taristu ja teabevahetuskanalite hea toimimine.
- Koostöörühmale kättesaadavaks tehtud ja rühma kasutatud tehniliste aruannete arv.
- Võrgu- ja infoturbe direktiivi piiriülese ja valdkondliku rakendamise puhul ühtse lähenemisviisi kasutamine.
- ENISA ellu viidud regulatiivsetele nõuetele vastavuse hindamiste arv.
- Erinevates valdkondades ja eriti elutähtsa taristu puhul kasutusel olevate ISACide arv.
- ELi institutsioonidest, organitest ja asutustest saadavat küberturvalisuse teavet levitava teabeplatvormi loomine ja korrapärane käitamine.
- Korrapärane panustamine ELi teadus- ja uuendustegevuse tööprogrammide koostamisse.
- ENISA, küberkuritegevuse vastase võitluse Euroopa keskuse (EC3) ja CERT-EU vahel koostöölepingu sõlmimine.
- Raamistiku alla kuuluvate ja selle piires välja töötatud sertifitseerimiskavade arv.

Eesmärk: suurendada ELi tasandil liikmesriikide võetavate meetmete täiendamise suutlikkust, eelkõige piirüleste küberkriiside puhul

- ENISA poolt küberohtude ja -intsidentide iga-aastase strateegilise analüüsi avaldamine, et määrata kindlaks tekkivad seaduspärad.
- Koondteabe avaldamine nende intsidentide kohta, millest ENISA on teatanud vastavalt võrgu- ja infoturbe direktiivile.
- Ameti poolt koordineeritud üleeuroopaliste õppuste arv ning nendes osalevate liikmesriikide ja organisatsioonide arv.
- Nende taotluste arv, mille liikmesriigid on ENISA-le hädaolukorrale reageerimise käigus toetuse saamiseks esitanud ja millele amet on reageerinud.
- Nõrkuste, moonutuste ja intsidentide analüüside arv, mille ENISA on koostöös CERT-EUga ellu viinud.
- Nende üleeuroopaliste olukorra aruannete kättesaadavus, mis põhinevad teabel, mille liikmesriigid ja muud üksused on esitanud ENISA-le suuremahulise piiriülese küberintsidendi korral.

Eesmärk: suurendada kodanike ja ettevõtjate teadlikkust küberturvalisusega seotud küsimustest

- Kogu ELi hõlmavate ja riiklike teadlikkuse suurendamise kampaaniate korrapärane korraldamine ning teemade korrapärane ajakohastamine lähtuvalt tekkivatest õppevajadustest.
- ELi kodanike kübervaldkonnaga seotud teadlikkuse suurendamine
- Küberturvalisuse alast teadlikkust käsitlevate viktoriinide korrapärane korraldamine ja aja jooksul õigete vastuste protsendi suurendamine.

- Töötajatele ja organisatsioonidele suunatud küberturvalisuse ja küberhügieeni alaste heade tavade korrapärane avaldamine.

Eesmärk: suurendada usaldust digitaalse ühtse turu ja digitaalse uuendustegevuse vastu, suurendades IKT toodete ja teenuste küberturvalisuse alase usaldusväärsuse[47] **üldist läbipaistvust**

- ELi raamistikule vastavate kavade arv.
- IKT turvalisuse sertifikaadi hankimisega kaasnev väiksem kulu.
- Liikmeriikides IKT sertifitseerimisele spetsialiseerunud vastavushindamisasutuste arv.
- Euroopa küberturvalisuse sertifitseerimise rühma loomine ja korrapärane koosolekute korraldamine.
- ELi raamistikule vastavate sertifitseerimise juhiste kasutuselevõtmine.
- ELi küberturvalisuse turu peamisi suundumusi käsitlevate analüüside korrapärane avaldamine.
- Euroopa IKT turvalisuse sertifitseerimise raamistiku normide kohaselt sertifitseeritud IKT toodete ja teenuste arv.
- Rohkem lõppkasutajaid, kes on teadlikud IKT toodete ja teenuste turvaomadustest.

(ww)

1.4.5. Lühi- või pikaajalises perspektiivis täidetavad vajadused

Võttes arvesse regulatiivseid nõudeid ja kiiresti muutuvat küberturvalisuse ohtude maastikku, tuleb vaadata läbi ENISA mandaat, et määrata kindlaks uued ülesanded eesmärgiga toetada tulemuslikult ja tõhusalt liikmesriikide, ELi institutsioonide ja muude sidusrühmade jõupingutusi Euroopa Liidus turvalise küberruumi tagamiseks. Mandaadi soovituslik ulatus piiritletakse, tugevdades neid valdkondi, kus amet on näidanud selget lisaväärtust, ja lisades valdkonnad, kus vajatakse tuge, võttes arvesse uusi poliitilisi prioriteete ja vahendeid, eelkõige võrgu- ja infoturbe direktiivi, Euroopa Liidu küberjulgeoleku strateegia läbivaatamist, ELi küberturvalisuse tegevuskava küberkriiside valdkonnas tehtava koostöö jaoks ning IKT turvalisuse sertifitseerimist. Uue välja pakutud mandaadi eesmärk on anda ametile tugevam ja kesksem roll, eelkõige toetades ka liikmesriike aktiivsemalt konkreetsete ohtude vastases võitluses (tegevussuutlikkus) ning saades liikmesriike ja komisjoni küberturvalisuse sertifitseerimise valdkonnas toetavaks eksperdikeskuseks.

Samal ajal luuakse ettepanekuga IKT toodete ja teenuste Euroopa küberturvalisuse sertifitseerimise raamistik ning täpsustatakse ENISA olulised ülesanded küberturvalisuse sertifitseerimise valdkonnas. Raamistikuga kehtestatakse ühised sätted ja menetlused, mis võimaldavad luua konkreetsete IKT toodete/teenuste või küberturvalisuse riskide jaoks kogu ELi hõlmavad küberturvalisuse sertifitseerimise kavad. Raamistiku kohaselt Euroopa küberturvalisuse sertifitseerimise kavade loomine võimaldab tagada nende kavade alusel väljastatud sertifikaatide kehtivuse ja tunnustamise kõikides liikmesriikides ning

[47] Küberturvalisuse alase usaldusväärsuse läbipaistvus tähendab seda, et kasutajatele antakse piisavalt teavet küberturvalisuse omaduste kohta, tänu millele saavad nad määrata objektiivselt kindlaks konkreetse IKT toote, teenuse või protsessi turvalisuse taseme.

vähendada praegust turu killustatust.

1.4.6. ELi meetme lisaväärtus

Küberturvalisus on tõeliselt ülemaailmne probleem, mis on juba oma olemuselt piiriülene ja muutub võrkude ja infosüsteemide omavahelise seotuse tõttu üha valdkonnaülesemaks. Küberturvalisuse intsidentide arv, keerukus ja ulatus ning neist majandusele ja ühiskonnale tekkiv mõju kasvab aja jooksul ning suureneb tehnoloogia arengu mõjul eeldatavasti veelgi, näiteks asjade interneti laialdase kasutuselevõtu tulemusena. See tähendab, et eeldatavasti ei vähene tulevikus vajadus liikmesriikide, ELi institutsioonide ja erasektori sidusrühmade ühiste jõupingutuste järele, mille eesmärk on võidelda küberturvalisusega seotud ohtude vastu. Alates ENISA loomisest 2004. aastal on selle eesmärk olnud edendada koostööd liikmesriikide ning võrgu- ja infoturbealaste sidusrühmade vahel, toetades muu hulgas avaliku ja erasektori koostööd. See koostöö toetamine hõlmas tehnilist tööd, et saada kogu ELi hõlmav arusaam ohukeskkonnast, eksperdirühmade loomist ja üleeuroopaliste küberintsidentide ja kriisiohjeõppuste korraldamist avalikule ja erasektorile mõeldud õppuste raames (eelkõige Cyber Europe). Võrgu- ja infoturbe direktiiviga anti ENISA-le lisaülesanded, sealhulgas CSIRTide võrgustiku sekretariaadi roll liikmesriikidevahelise operatiivkoostöö jaoks. ELi tasandil tegutsemise lisaväärtust, eelkõige et suurendada koostööd liikmesriikide, aga ka võrgu- ja infoturbe kogukondade vahel, on tunnustatud nõukogu 2016. aasta järeldustes[48] ja see ilmneb selgelt ka ENISA 2017. aasta hindamisest, mille kohaselt seisneb ameti lisaväärtus peamiselt tema võimes suurendada koostööd nende sidusrühmade vahel. ELi tasandil ei ole ühtegi teist osalejat, kes toetaks kõnealuste võrgu- ja infoturbe sidusrühmade koostööd. ENISA lisaväärtus, mis seisneb küberturvalisuse kogukondade ja sidusrühmade kokkutoomises, kehtib ka sertifitseerimise valdkonnas. Küberkuritegevuse ja küberturvalisuse ohtude suurenemise tõttu on loodud riiklikud algatused, millega kehtestatakse tavapärases taristus kasutatavatele IKT komponentidele kõrgetasemelised küberturvalisuse ja sertifitseerimise nõuded. Kuigi kõnealused algatused on olulised, võivad need põhjustada ühtse turu killustatust ja takistusi koostalitlusvõimele. IKT müüjale võib tekkida vajadus läbida mitu sertifitseerimisprotsessi, et ta saaks oma tooteid ja teenuseid mitmes liikmesriigis müüa. Ei ole tõenäoline, et praeguste sertifitseerimiskavade ebatulemuslikkust/-tõhusust on võimalik kõrvaldada ilma ELi sekkumiseta. Kui meetmeid ei võeta, siis suureneb turu killustatus suure tõenäosusega lühikeses ja keskpikas perspektiivis (järgmise viie kuni kümne aasta jooksul) uute sertifitseerimiskavade kasutuselevõtu tõttu. Nende kavade koordineerituse ja koostalitlusvõime puudumise tõttu väheneb digitaalse ühtse turu potentsiaal. See tõendab IKT toodete ja teenuste jaoks Euroopa küberturvalisuse sertifitseerimise raamistiku loomise lisaväärtust, tagades õiged tingimused, et tegeleda tulemuslikult eri liikmesriikides mitme sertifitseerimismenetluse samaaegse olemasoluga seotud probleemiga, vähendades sertifitseerimise kulusid ja muutes seega sertifitseerimise ELis ärilisest ja konkurentsi seisukohast kokkuvõttes atraktiivsemaks.

[48] Nõukogu järeldused Euroopa kübervastupidavusvõime süsteemi tugevdamise ning konkurentsivõimelise ja uuendusliku küberjulgeolekusektori toetamise kohta, 15. november 2016.

1.4.7. Samalaadsetest kogemustest saadud õppetunnid

Komisjon on teinud ENISA õigusliku aluse kohaselt ameti hindamise, mis hõlmas sõltumatut uuringut ja avalikku konsultatsiooni. Hindamise käigus jõuti järeldusele, et ENISA eesmärgid on ka praegu asjakohased. Võttes arvesse tehnoloogia arengut, muutuvaid ohte ja märkimisväärset vajadust suurema võrgu- ja infoturbe järele ELis, on vaja tehnilisi erialateadmisi võrgu- ja infoturbe küsimuste muutumise kohta. Tuleb suurendada liikmesriikide suutlikkust mõista ohte ja neile reageerida ning sidusrühmad peavad tegema koostööd temaatiliste valdkondade ja institutsioonide üleselt.

Amet on edukalt aidanud parandada võrgu- ja infoturvet Euroopas, pakkudes suutlikkuse suurendamist 28 liikmesriigis ning tõhustades koostööd liikmesriikide ning võrgu- ja infoturbe sidusrühmade vahel, pakkudes oskusteavet, aidates kogukonna väljakujundamisel ja toetades poliitikat.

Kuigi ENISA suutis avaldada vähemalt teatavas ulatuses mõju väga mahukas võrgu- ja infoturbe valdkonnas, ei olnud ta täiesti edukas tugeva kaubamärgi väljakujundamisel ning piisava märgatavuse saamisel, et olla tunnustatud peamise eksperdikeskusena Euroopas. Selle põhjus seisneb ENISA ulatuslikus mandaadis, mille jaoks ei eraldatud proportsionaalselt piisavalt ressursse. Lisaks sellele on ENISA ainus ELi amet, millel on tähtajaline mandaat, mis piirab tema võimet koostada pikaajalist strateegiat ja toetada oma sidusrühmi jätkusuutlikul viisil. See on ka vastuolus võrgu- ja infoturbe direktiivi sätetega, mis annavad ENISA-le ülesanded, millel ei ole lõppkuupäeva.

IKT toodete ja teenuste küberturvalisuse sertifitseerimiseks ei ole praegu mingit Euroopa raamistikku. Samas on küberkuritegevuse ja turvaohtude suurenemise tõttu tehtud riiklikke algatusi, mille tõttu tekib ühtse turu killustumise oht.

1.4.8. Kooskõla ja võimalik koostoime muude asjaomaste meetmetega

Algatus on suurel määral kooskõlas kehtiva poliitikaga, eelkõige siseturu valdkonnas. See on koostatud, võttes arvesse digitaalse ühtse turu strateegia läbivaatamise käigus kindlaks määratud üldist lähenemisviisi küberturvalisusele, et täiendada terviklikku meetmete komplekti, näiteks Euroopa Liidu küberjulgeoleku strateegia läbivaatamist, kübervaldkonna kriiside puhul koostöö tegemise tegevuskava ja küberkuritegevuse vastase võitluse algatusi. See tagaks kooskõla kehtivate küberturvalisuse õigusaktidega (eelkõige võrgu- ja infoturbe direktiiv) ja tugineks neile, et suurendada ELi kübervastupidavusvõimet suurema suutlikkuse, koostöö, riskijuhtimise ja kübervaldkonnast teadlikkuse abil.

Soovitatud sertifitseerimismeetmete abil peaks olema võimalik tegeleda olemasolevatest ja loodavatest riiklikest sertifitseerimiskavadest tekkiva võimaliku killustatusega, aidates seeläbi kaasa digitaalne ühtse turu arengule. Algatus toetab ja täiendab ka võrgu- ja infoturbe direktiivi rakendamist, andes ettevõtjatele, kelle suhtes seda direktiivi kohaldatakse, vahendid, mille abil nad saavad tõendada vastavust võrgu- ja infoturbe nõuetele kogu liidus.

Välja pakutud Euroopa IKT küberturvalisuse sertifitseerimise raamistiku puhul ei piirata isikuandmete kaitse üldmääruse[49] ja eelkõige selle sertifitseerimist käsitlevate sätete[50] kohaldamist, kuna neid kohaldatakse isikuandmete töötlemisel järgitavate turvanõuete suhtes. Tulevases Euroopa raamistikus välja pakutavad kavad peaksid toetuma võimalikult palju rahvusvahelistele standarditele, et mitte luua kaubandustõkkeid ja tagada kooskõla rahvusvaheliste algatustega.

[49] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).

[50] Näiteks artikkel 42 („Sertifitseerimine“) ja artikkel 43 („Sertifitseerimisasutused“) ning artiklid 57, 58 ja 70, mis käsitlevad vastavalt sõltumatute järelevalveasutuste asjaomaseid ülesandeid ja volitusi ning Euroopa Andmekaitsenõukogu ülesandeid.

1.5. Meetme kestus ja finantsmõju

☐ **Piiratud kestusega** ettepanek/algatus

– ☐ Ettepanek/algatus hõlmab ajavahemikku [PP/KK]AAAA–[PP/KK]AAAA

– ☐ Finantsmõju avaldub ajavahemikul AAAA–AAAA

☒ **Piiramatu kestusega** ettepanek/algatus

– rakendamise käivitumisperiood hõlmab ajavahemikku 2019–2020,

– millele järgneb täieulatuslik rakendamine.

1.6. Ettenähtud eelarve täitmise viisid[51]

☒ **Otsene eelarve täitmine** komisjoni poolt (III jaotis – sertifitseerimine)

– ☐ rakendusametite kaudu

☐ **Eelarve täitmine koostöös** liikmesriikidega

☒ **Kaudne eelarve täitmine**, mille puhul eelarve täitmise ülesanded on delegeeritud:

☐ rahvusvahelistele organisatsioonidele ja nende allasutustele (täpsustage);

☐ Euroopa Investeerimispangale (EIP) ja Euroopa Investeerimisfondile (EIF);

☒ artiklites 208 ja 209 osutatud asutustele (II jaotis – ENISA);

☐ avalik-õiguslikele asutustele;

☐ avalikke teenuseid osutavatele eraõiguslikele asutustele, kuivõrd nad esitavad piisavad finantstagatised;

☐ liikmesriigi eraõigusega reguleeritud asutustele, kellele on delegeeritud avaliku ja erasektori partnerluse rakendamine ja kes esitavad piisavad finantstagatised;

☐ isikutele, kellele on delegeeritud Euroopa Liidu lepingu V jaotise kohaste ÜVJP erimeetmete rakendamine ja kes on kindlaks määratud asjaomases alusaktis.

Märkused

Määrust kohaldatakse järgmise suhtes: - välja pakutud määruse II jaotise alusel vaadatakse läbi Euroopa Liidu Võrgu- ja Infoturbeameti (ENISA) mandaat, andes talle sertifitseerimise käigus olulise rolli, ning - III jaotise alusel luuakse raamistik IKT toodete ja teenuste Euroopa küberturvalisuse sertifitseerimise kavade loomiseks, milles ENISA-l on ülioluline roll.

[51] Eelarve täitmise viise koos viidetega finantsmäärusele on selgitatud veebisaidil: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

Täpsustage tingimused ja sagedus.

Järelevalve algab kohe pärast õigusakti vastuvõtmist ja keskendub selle kohaldamisele. Komisjon korraldab kohtumised ENISA, liikmesriikide esindajate (näiteks ekspertide rühm) ja asjaomaste sidusrühmadega, eelkõige et edendada sertifitseerimist käsitlevate õigusnormide rakendamist (näiteks haldusnõukogu loomist).

Esimene hindamine peaks toimuma õigusakti jõustumisest viie aasta möödumisel, kui saadaval on piisavalt andmeid. Õigusakt sisaldab sõnaselget hindamis- ja läbivaatamisklauslit [artikkel XXX], mille alusel komisjon viib ellu sõltumatu hindamise. Komisjon esitab seejärel Euroopa Parlamendile ja nõukogule hindamise kohta aruande, lisades sellele vajaduse korral läbivaatamise ettepaneku, et mõõta määruse mõju ja selle lisaväärtust. Uus hindamine tuleks korraldada iga viie aasta tagant. Selle suhtes kohaldatakse komisjoni parema õigusloome hindamismetoodikat. Need hindamised viiakse ellu ekspertidega peetavate sihtotstarbeliste arutelude, uuringute ja ulatuslike sidusrühmadega konsulteerimiste abil.

ENISA tegevdirektor peaks esitama haldusnõukogule iga kahe aasta tagant ENISA tegevuse järelhindamise. Amet peaks ka koostama järelmeetmete tegevuskava, mis sisaldab järelhindamise järeldusi, ja esitama iga kahe aasta järel komisjonile aruande tehtud edusammude kohta. Haldusnõukogu peaks tagama, et nende järelduste alusel võetakse nõuetekohased järelmeetmed.

Kui ameti tegevuses esineb väidetavat haldusomavoli, siis uurib seda Euroopa Ombudsman vastavalt aluslepingu artiklile 228.

Kavandatud järelevalve peamised andmeallikad on ENISA, Euroopa küberturvalisuse sertifitseerimise rühm, koostöörühm, CSIRTide võrgustik ja liikmesriikide ametiasutused. Lisaks ENISA, Euroopa küberturvalisuse sertifitseerimise rühma, koostöörühma ja CSIRTide võrgustiku aruannetest (sealhulgas iga-aastastest tegevusaruannetest) saadud andmetele kasutatakse vajaduse korral konkreetseid andmete kogumise vahendeid (näiteks riigi ametiasutuste ja Eurobaromeetri uuringuid, küberturvalisuse kuu kampaania ja üleeuroopaliste õppuste käigus laekunud aruandeid).

2.2. Haldus- ja kontrollisüsteem

2.2.1. Tuvastatud ohud

Tuvastatud ohud on väikesed: liidu amet on juba olemas ja selle mandaati piiritletakse, tugevdades neid valdkondi, kus amet on näidanud selget lisaväärtust, ja lisades valdkonnad, kus vajatakse tuge, võttes arvesse uusi poliitilisi prioriteete ja vahendeid, eelkõige võrgu- ja infoturbe direktiivi, Euroopa Liidu küberjulgeoleku strateegia läbivaatamist, tulevast ELi

küberturvalisuse tegevuskava küberkriiside valdkonnas tehtava koostöö jaoks ning IKT turvalisuse sertifitseerimist.

Ettepanekuga kirjeldatakse seega üksikasjalikult ameti ülesandeid ja suurendatakse selle tõhusust. Suuremad operatiivsed pädevused ja ülesanded ei tekita tegelikku riski, kuna need täiendaksid liikmesriikide võetavaid meetmeid ja toetaksid liikmesriike piiritletud ja eelnevalt kindlaks määratud teenustega, kui nad esitavad vastava taotluse.

Lisaks sellele tagatakse ühise lähenemisviisi kaudu ameti välja pakutud mudeli abil, et piisavalt kontrollitakse seda, kas ENISA tegutseb oma eesmärkide saavutamise nimel. Kavandatavate muudatuste operatsiooni- ja finantsriskid näivad olevat väikesed.

Samal ajal on vaja tagada piisavad rahalised vahendid, et ENISA saaks täita talle uue mandaadi alusel antud ülesandeid, muu hulgas sertifitseerimise valdkonnas.

2.2.2. Ettenähtud kontrollimeetodid

Ameti raamatupidamisaruanded esitatakse heakskiitmiseks Euroopa Kontrollikojale ning nende suhtes kohaldatakse eelarve täitmisele heakskiidu andmise menetlust ja auditeerimist.

Ameti tegevust kontrollib ombudsman kooskõlas asutamislepingu artikliga 228.

Vt punkt 2.1 ja punkt 2.2.1

2.3. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

Täpsustage rakendatavad või kavandatud ennetus- ja kaitsemeetmed

Kohaldatakse ENISA ennetus- ja kaitsemeetmeid, eelkõige järgmiselt.

- Ameti personal kontrollib kõiki makseid mis tahes teenuse või uuringu eest enne makse sooritamist, võttes arvesse kõiki lepingulisi kohustusi, majanduslikke põhimõtteid ning head finantstegevus- ja juhtimistava. Pettusevastased sätted (järelevalve, aruandlusnõuded jms) lisatakse kõikidesse ameti ja mis tahes makse saajate vahelistesse kokkulepetesse ning lepingutesse.

- Pettuse, korruptsiooni ja muude õigusvastaste tegude vastu võitlemiseks kohaldatakse piiranguteta Euroopa Pettustevastase Ameti (OLAF) juurdlusi käsitleva Euroopa Parlamendi ja nõukogu 11. septembri 2013. aasta määruse (EL, Euratom) nr 883/2013 sätteid.

- Amet ühineb kuue kuu jooksul alates käesoleva määruse jõustumisest Euroopa Parlamendi, Euroopa Liidu Nõukogu ja Euroopa Ühenduste Komisjoni 25. mai 1999. aasta institutsioonidevahelise kokkuleppega Euroopa Pettustevastase Ameti (OLAF) sisejuurdluste kohta ja võtab viivitamata vastu kõikide oma töötajate suhtes kohaldatavad asjakohased sätted.

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

- Olemasolevad eelarveread

Järjestage mitmeaastase finantsraamistiku rubriikide ja iga rubriigi sees eelarveridade kaupa.

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Assigneeringute liik	Rahaline osalus			
		Liigendatud/liigendamata[52]	EFTA riigid[53]	Kandidaatriigid[54]	Kolmandad riigid	finantsmääruse artikli 21 lõike 2 punkti b tähenduses
1a. Konkurentsivõime majanduskasvu ja tööhõive tagamiseks	09.0203 ENISA ning info- ja kommunikatsioonitehnoloogia turvalisuse sertifitseerimine	Liigendatud	JAH	EI	EI	EI
5 Halduskulud]	09.0101 Sidevõrkude, sisu ja tehnoloogia valdkonnas tegutseva personaliga seotud kulud 09.0102 Sidevõrkude, sisu ja tehnoloogia	Liigendamata	EI	EI	EI	EI

[52] Liigendatud assigneeringud / liigendamata assigneeringud.
[53] EFTA: Euroopa Vabakaubanduse Assotsiatsioon.
[54] Kandidaatriigid ja vajaduse korral Lääne-Balkani potentsiaalsed kandidaatriigid.

	valdkonnas tegutsevate koosseisuväliste töötajatega seotud kulud 09.010211 Muud juhtimiskulud					

3.2. Hinnanguline mõju kuludele

3.2.1. Üldine hinnanguline mõju kuludele

miljonites eurodes (kolm kohta pärast koma)

Mitmeaastase finantsraamistiku rubriik	1a	Konkurentsivõime majanduskasvu ja tööhõive tagamiseks

ENISA			**Lähteolukord** **2017 (31.12.2016)**		**2019** ***(alates 1.7.2019)***	**2020**	**2021**	**2022**	**KOKKU**
Jaotis 1: personalikulud *(sealhulgas töötajate värbamise, väljaõppe, sotsiaal-meditsiinilise taristu ja välisteenustega seotud kulud)*	Kulukohustused	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Maksed	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Jaotis 2: infrastruktuuri- ja tegevuskulud	Kulukohustused	(1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Maksed	(2 a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Jaotis 3: tegevuskulud	Kulukohustused	(3a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Maksed	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
ENISA assigneeringud	Kulukohustused	=1+1a +3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**

KOKKU	Maksed	=2+2a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Mitmeaastase finantsraamistiku rubriik	**5**	„Halduskulud“

miljonites eurodes (kolm kohta pärast koma)

		2019 *(alates 1.7.2019)*	**2020**	**2021**	**2022**	**KOKKU**
Sidevõrkude, sisu ja tehnoloogia peadirektoraat						
• Inimressursid		0,216	0,846	0,846	0,846	**2,754**
• Muud halduskulud		0,102	0,235	0,238	0,242	**0,817**
Sidevõrkude, sisu ja tehnoloogia **peadirektoraat KOKKU**	Assigneeringud	0,318	1,081	1,084	1,088	**3,571**

Personalikulud arvutati lähtuvalt kavandatavast värbamiskuupäevast (tööhõive algab eeldatavasti 1. juulil 2019).

Ressursside väljavaade pärast 2020. aastat on hinnanguline ja see ei piira 2020. aasta järgset mitmeaastast finantsraamistikku käsitlevate komisjoni ettepanekute kohaldamist

Mitmeaastase finantsraamistiku **RUBRIIGI 5 assigneeringud KOKKU**	(Kulukohustuste kogusumma = maksete kogusumma)	0,318	1,081	1,084	1,088	**3,571**

miljonites eurodes (kolm kohta pärast koma)

		2019	**2020**	**2021**	**2022**	**KOKKU**
Mitmeaastase finantsraamistiku **rubriikide 1–5 assigneeringud KOKKU**	Kulukohustused	16,868	21,727	23,332	24,11	**86,038**
	Maksed	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Hinnanguline mõju ameti assigneeringutele

– ☐ Ettepanek/algatus ei hõlma tegevusassigneeringute kasutamist

– ☒ Ettepanek/algatus hõlmab tegevusassigneeringute kasutamist, mis toimub järgmiselt:

kulukohustuste assigneeringud miljonites eurodes (kolm kohta pärast koma)

Täpsustage eesmärgid ja väljundid[55] ⇩	**2019**	**2020**	**2021**	**2022**	**KOKKU**
Liikmesriikide ja ettevõtjate suutlikkuse ja valmisoleku arendamine.	1,408	1,900	1,931	1,969	7,208
Koostöö ja koordineerimise parandamine liikmesriikides ning ELi institutsioonides, organites ja asutustes.	0,939	1,266	1,288	1,313	4,806
ELi tasandil liikmesriikide võetavate meetmete täiendamise suutlikkuse parandamine, eelkõige piiriüleste küberkriiside puhul.	0,704	0,950	0,965	0,985	3,604
Kodanike ja ettevõtjate teadlikkuse suurendamine küberturvalisusega seotud küsimustest.	0,704	0,950	0,965	0,985	3,604
Usalduse suurendamine digitaalse ühtse turu ja digitaalse uuendustegevuse vastu, suurendades IKT toodete ja teenuste küberturvalisuse alase usaldusväärsuse üldist läbipaistvust.	0,939	1,266	1,288	1,313	4,806
KULUD KOKKU	4 694	6,332	6,437	6,565	24,028

[55] Tabelis on esitatud vaid 3. jaotise kohased tegevuskulud.

3.2.3. Hinnanguline mõju ameti inimressurssidele

3.2.3.1. Kokkuvõte

– ☐ Ettepanek/algatus ei hõlma haldusassigneeringute kasutamist

– ☒ Ettepanek/algatus hõlmab haldusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes (kolm kohta pärast koma)

	2019. aasta kolmas ja neljas kvartal	**2020**	**2021**	**2022**
Ajutised ametnikud (AD palgaastmed)	4,242	5,695	6,381	6,709
Ajutised ametnikud (AST palgaastmed)	1,601	1,998	2,217	2,217
Lepingulised töötajad	2,041	2,041	2,041	2,041
Riikide lähetatud eksperdid	0,306	0,447	0,656	0,796
KOKKU	**8,190**	**10,181**	**11,295**	**11,763**

Personalikulud arvutati lähtuvalt kavandatavast värbamiskuupäevast (praeguste ENISA töötajate puhul eeldati täielikku tööhõivet alates 1.1.2019). Uute töötajate puhul nähti ette järkjärguline tööhõive alates 1.7.2019 ja täielik tööhõive 2022. aastal. Ressursside väljavaade pärast 2020. aastat on hinnanguline ja see ei piira 2020. aasta järgset mitmeaastast finantsraamistikku käsitlevate komisjoni ettepanekute kohaldamist.

Hinnanguline mõju inimressurssidele (täiendavad täistööajale taandatud töötajad) – ametikohtade loetelu

Tegevusüksus ja palgaaste	2017 **Praegune ENISA**	2019. aasta kolmas ja neljas kvartal	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			

AD11 AD10 AD9 AD8 AD7 AD6 AD5	 5 10 15	 2 4	 2 3 3	 3 3	 1 2
AD kokku	34	9	8	6	3
AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
AST kokku	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
AST/SC kokku					
KÕIK KOKKU	48	12	10	7	3

Palgaastme AD/AST täiendavate töötajate ülesanded instrumendi eesmärkide saavutamiseks, nagu on kirjeldatud jaotises 1.4.2:

Ülesanded	AD	AST	Riikide läheta tud eksperdid	Kokku
Põhimõtted ja suutlikkuse arendamine	8	1		9
Operatiivkoostöö	8	1	7	16
Sertifitseerimine (turuga seotud ülesanded)	9	3	2	14
Teadmised, teave ja teadlikkus	1	1		2
KOKKU	26	6	9	41

Ülesannete kirjeldus:

Ülesanded	**Vajalikud lisaressursid**
ELi põhimõtete arendamine ja rakendamine ning suutlikkuse arendamine	Ülesanded hõlmaksid koostöörühma abistamist, võrgu- ja infoturbe piiriülese järjepideva rakendamise toetamist, korrapärast aruandlust ELi õigusraamistiku rakendamise olukorra kohta, valdkondlike küberturvalisuse algatuste nõustamist ja koordineerimist muu hulgas energeetika, transpordi (näiteks lennundus, auto- ja merevedu, ühendatud sõidukid), tervishoiu ja rahanduse valdkonnas ning erinevates valdkondades teabe jagamise ja analüüsimise keskuste (ISACide) loomise toetamist.
Operatiivkoostöö ja kriisiohjamine	**Ülesanded hõlmaksid järgmist.** CSIRTide võrgustikule sekretariaaditeenuste võimaldamine, millega tagatakse muu hulgas CSIRTide võrgustiku IT taristu ja sidekanalite hea toimimine. Struktureeritud koostöö tagamine CERT-EU, küberkuritegevuse vastase võitluse Euroopa keskuse ja teiste asjaomaste ELi asutustega. **Õppuste Cyber Europe**[56] korraldamine – ülesanded, mille abil muudetakse õppus iga kahe aasta tagant toimuvast üritusest kord aastas toimuvaks ürituseks ja veendutakse, et õppuse käigus käsitletakse intsidenti selle algusest kuni lõpuni. **Tehniline abi** – ülesanded hõlmaksid struktureeritud koostööd CERT-EUga, et anda tehnilist abi oluliste intsidentide puhul ja toetada intsidentide analüüsi. See hõlmaks liikmesriikidele abi andmist, et tegeleda intsidentidega ja analüüsida nõrkusi, moonutusi ja intsidente. Hädaolukordadele reageerimise käigus individuaalsete liikmesriikide vahelise koostöö edendamine, analüüsides ja koondades riiklikke olukorraaruandeid lähtuvalt teabest, mille liikmesriigid ja muud üksused on ametile

[56] Cyber Europe on siiani kõige suurem ja terviklikum ELi küberturvalisuse õppus, kus osaleb rohkem kui 700 küberturvalisuse spetsialisti kõigist 28 liikmesriigist. Seda korraldatakse iga kahe aasta tagant. ENISA hinnang ja 2013. aasta Euroopa Liidu küberjulgeoleku strateegia näitavad, et mitmed sidusrühmad soovivad muuta õppuse Cyber Europe kord aastas toimuvaks sündmuseks, võttes arvesse küberohtude kiiresti muutuvat olemust. See ei ole ameti piiratud ressursside tõttu praegu siiski otstarbekas.

	esitanud. **Suuremahulistele piiriülestele küberintsidentidele koordineeritud reageerimise tegevuskava** – amet aitab töötada liidu ja liikmesriikide tasandil välja koostööl põhinevat reageerimist küberturvalisusega seotud suuremahulistele piiriülestele intsidentidele või kriisidele, täites mitmeid ülesandeid alates liidu tasandil olukorrateadlikkuse saavutamisele kaasa aitamisest kuni intsidentide puhul kasutatavate koostööplaanide katsetamiseni. **Intsidentide tehnilised järeluurimised** – amet teeb või aitab teha intsidentide tehnilisi järeluurimisi koostöös CSIRTide võrgustikuga, et avaldada edasiste intsidentide parema ärahoidmise eesmärgil avalikke aruandeid, milles esitatakse soovitusi ja millega arendatakse suutlikkust.
Turuga seotud ülesanded (standardimine ja sertifitseerimine)	Ülesanded hõlmaksid sertifitseerimisraamistiku alusel tehtava töö aktiivset toetamist, sealhulgas tehniliste erialateadmiste andmist, et koostada ettevalmistavad küberturvalisuse sertifitseerimise Euroopa kavad. Ülesanded hõlmavad ka standardimist, sertifitseerimist ja turu vaatlusrühma käsitlevate liidu põhimõtete väljatöötamist ja rakendamist, milleks on vaja edendada elektroonikatoodete, võrkude ja teenuste riskijuhtimise standardite kasutuselevõttu ning anda elutähtsate teenuste operaatoritele ja digitaalteenuste osutajatele nõuandeid tehnilistest turvanõuete valdkonnas. Ülesanded hõlmavad ka analüüsi esitamist küberturvalisuse turu peamiste suundumuste kohta.
Teadmised, teave ja teadlikkuse suurendamine	Et tagada lihtsam juurdepääs küberturvalisuse riske ja võimalikke lahendusi käsitlevale paremini struktureeritud teabele, antakse käesoleva ettepanekuga ametile uus ülesanne töötada välja liidu teabekeskus ja seda hallata. Ülesanded hõlmaksid selle teabe koondamist, korraldamist ja avalikkusele spetsiaalse portaali kaudu kättesaadavaks tegemist, mille ELi institutsioonid, ametid ja organid on võrgu- ja infosüsteemide turvalisuse ning eelkõige küberturvalisuse kohta esitanud. Ülesanded hõlmaksid ka ENISA tegevuse toetamist teadlikkuse suurendamise valdkonnas, et amet

	saaks tehtavaid jõupingutusi suurendada.

3.2.3.2. Vastutava peadirektoraadi hinnanguline personalivajadus

– ☐ Ettepanek/algatus ei hõlma personali kasutamist

– ☒ Ettepanek/algatus hõlmab personali kasutamist, mis toimub järgmiselt:

hinnanguline väärtus täisarvuna (või maksimaalselt ühe kohaga pärast koma)

		Lisatöötajad			
	Lähteol ukord 2017	Kolmas ja neljas kvartal 2019	2020	2021	2020
• **Ametikohtade loeteluga ette nähtud ametikohad (ametnikud ja ajutised töötajad)**					
09 01 01 01 (komisjoni peakorteris ja esindustes)	1	2	3		
• **Koosseisuväline personal (täistööajale taandatud töötajad)**[57]					
09 01 02 01 (üldvahenditest rahastatavad lepingulised töötajad, riikide lähetatud eksperdid, renditööjõud)	1	2			
KOKKU		**4**	**3**		

Ülesannete kirjeldus:

Ametnikud ja ajutised töötajad	Komisjoni esindamine ameti haldusnõukogus. Komisjoni arvamuse koostamine ENISA ühtse programmidokumendi kohta ja selle rakendamise jälgimine. Ameti eelarve koostamise kontrollimine ja selle täitmise jälgimine. Aidata ametil arendada oma tegevust kooskõlas liidu tegevuspõhimõtetega, sealhulgas osaledes asjasse puutuvatel kohtumistel. Teha IKT toodete ja teenuste Euroopa küberturvalisuse

[57] Lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud, noored eksperdid delegatsioonides.

	sertifitseerimise kavade raamistiku rakendamise järelevalvet. Säilitada sertifitseerimisega seoses kontakte liikmesriikide ja teiste asjaomaste sidusrühmadega. Teha ettevalmistavate kavade asjus koostööd ENISAga. Koostada ettevalmistavad Euroopa küberturvalisuse kavad.
Koosseisuvälised töötajad	Vt eespool

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

– ☐ Ettepanek/algatus on kooskõlas kehtiva mitmeaastase finantsraamistikuga.

– ☒ Ettepanekuga/algatusega kaasneb mitmeaastase finantsraamistiku asjaomase rubriigi ümberplaneerimine.

Ettepanekuga kaasneb eelarveartikli 09 02 03 ümberplaneerimine, kuna muudetakse ENISA mandaati, millega antakse ametile uued ülesanded, mis on muu hulgas seotud võrgu- ja infoturbe direktiivi rakendamisega ning Euroopa küberturvalisuse sertifitseerimise raamistikuga. Vastavad summad:

Aasta	Eeldatav	Taotletud
2019	10,739	16,550
2020	10,954	20,646
2021	Ei kohaldata	22,248*
2022	Ei kohaldata	23,023*

* See on hinnanguline näitaja. Pärast 2020. aastat ELi poolt antavad rahalised vahendid vaadatakse läbi seoses kõikide pärast 2020. aastat algavaks perioodiks esitatud ettepanekute arutamisega komisjonis. See tähendab, et kohe, kui komisjon on teinud ettepaneku järgmise mitmeaastase finantsraamistiku kohta, esitab ta muudetud finantsselgituse, kus on arvesse võetud mõjuhinnangu järeldusi[58].

– ☐ Ettepanek/algatus eeldab paindlikkusinstrumendi kohaldamist või mitmeaastase finantsraamistiku läbivaatamist[59].

3.2.5. Kolmandate isikute rahaline osalus

– ☐ Ettepanek/algatus ei hõlma kolmandate isikute poolset kaasrahastamist.

[58] Link mõjuhinnangule.

[59] Vt nõukogu määruse (EL, Euratom) nr 1311/2013 (millega määratakse kindlaks mitmeaastane finantsraamistik aastateks 2014–2020) artiklid 11 ja 17.

– ☒ Ettepanek/algatus hõlmab kaasrahastamist, mille hinnanguline summa on järgmine:

	Aasta **2019**	Aasta **2020**	Aasta **2021**	Aasta **2022**
EFTA	p.m.[60]	p.m.	p.m.	p.m.

3.3. Hinnanguline mõju tuludele

– ☒ Ettepanekul/algatusel puudub finantsmõju tuludele

– ☐ Ettepanekul/algatusel on järgmine finantsmõju:

  – ☐ omavahenditele

  – ☐ mitmesugustele tuludele

[60] Järgnevate aastate täpne summa saadakse teada, kui EFTA suhtarv asjaomase aasta kohta kindlaks määratakse.