EUROOPA
KOMISJON

Strasbourg, 20.1.2026
COM(2026) 13 final

2026/0012 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV

millega muudetakse direktiivi (EL) 2022/2555 seoses lihtsustamismeetmetega ja vastavusse viimisega [küberturvalisuse 2. määruse ettepanekuga]

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

(EMPs kohaldatav tekst)

SELETUSKIRI

1. ETTEPANEKU TAUST

• Ettepaneku põhjused ja eesmärgid

Käesolev ettepanek kuulub meetmepaketti, mille eesmärk on viia liidu küberturvalisuse raamistik kooskõlla sidusrühmade vajadustega aina keerukamate küberohtudega keskkonnas ja keerulises geopoliitilises reaalsuses. Aina sagedamini on küberrünnete sihtmärkideks kriitilise tähtsusega sektoritesse kuuluvad elutähtsad ja olulised üksused,[1] samal ajal kui riiklikud ohusubjektid kasutavad oma rünnete võimendamiseks ja optimeerimiseks kujunemisjärgus tehnoloogiat, näiteks tehisintellekti. Sellega seoses käsitatakse elutähtsa taristu vastupidavust küberohtudele meie demokraatia ja liidu majandusjulgeoleku strateegilise tugisambana. Küberturvalisus on seatud liidu vastupanuvõime tegevuskava keskmesse nii ELi kriisivalmiduse strateegias[2] kui ka Euroopa sisejulgeoleku strateegias (ProtectEU)[3]. Samuti on teatises „ELi majandusjulgeoleku tugevdamine“[4] nimetatud prioriteetsete eesmärkidena juurdepääsu takistamist tundlikule teabele ja andmetele, mis võib kahjustada liidu majandusjulgeolekut, ning liidu majandust mõjutavate liidu elutähtsa taristu häirete ennetamist ja leevendamist, milles on tähtsal kohal tulemuslikud küberturvalisuse meetmed. Lisaks rõhutati Draghi aruandes vajadust suurendada julgeolekut ja vähendada sõltuvust kui üht peamist liidus vajalikku tegevusvaldkonda[5]. Oma teatises „Lihtsam ja kiirem Euroopa“[6] teatas komisjon oma pühendumisest ambitsioonikale programmile, et edendada tulevikku vaatavaid uuenduslikke poliitikameetmeid, mis tugevdavad liidu konkurentsivõimet ning vähendavad inimeste, ettevõtete ja haldusasutuste regulatiivset koormust, säilitades samal ajal liidu väärtuste edendamisel kõrgeima standardi.

Käesolev ettepanek võtta vastu direktiiv, millega muudetakse direktiivi (EL) 2022/2555 seoses lihtsustamismeetmetega ja vastavusse viimisega [ettepanekuga võtta vastu Euroopa Parlamendi ja nõukogu määrus, mis käsitleb Euroopa Liidu Küberturvalisuse Ametit (ENISA), Euroopa küberturvalisuse sertifitseerimise raamistikku ja IKT tarneahela turvalisust ning millega tunnistatakse kehtetuks määrus (EL) 2019/881 (küberturvalisuse 2. määrus)], on kirjeldatud asjaolusid arvestades loodud eesmärgiga lahendada liidu turvaolekut mõjutava küberturvalisusega seotud poliitika keerukuse ja mitmekesisuse probleem, eelkõige täpsustuste lisamisega ja reguleeritud üksuste jaoks nõuete täitmise lihtsustamisega.

Käesoleva direktiivi eesmärki tuleks käsitada osana küberturvalisuse määruse läbivaatamise paketi üldistest eesmärkidest; pakett sisaldab ettepanekut võtta vastu Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse Euroopa Liidu Küberturvalisuse Ametit (ENISA), Euroopa küberturvalisuse sertifitseerimise raamistikku ja IKT tarneahela turvalisust ning millega tunnistatakse kehtetuks määrus (EL) 2019/881. Kõnealuse määruse ettepaneku eesmärk on käsitleda järgmisi probleeme: i) liidu küberturvalisuse poliitikaraamistiku ja sidusrühmade vajaduste kooskõlastamatus üha vaenulikumas keskkonnas; ii) Euroopa küberturvalisuse sertifitseerimise raamistiku rakendamise seiskumine; iii) liidu turvaolekut

---

1 ENISA, ENISA ohtude kaardistamise aruanne 2025.
2 JOIN/2025/130 final.
3 COM/2025/148 final.
4 JOIN(2025) 977 final.
5 Euroopa Komisjon, „Euroopa konkurentsivõime tulevik“, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.
6 COM(2025) 47 final.

mõjutava küberturvalisusega seotud poliitika keerukus ja mitmekesisus ning iv) IKT tarneahelate turvariskide suurenemine. Seoses liidu turvaolekut mõjutava küberturvalisusega seotud poliitika keerukuse ja mitmekesisusega on küberturvalisuse määruse läbivaatamise paketis tehtud Euroopa küberturvalisuse sertifitseerimise raamistiku reformi raames ettepanek edendada sertifitseerimist kui ettevõtjate nõuetele vastavuse tagamise vahendit ning võimaldada üksuste turvaolekut käsitleva kava väljatöötamist, et vähendada nõuete täitmisega seotud kulusid üksustele, kelle suhtes kohaldatakse küberturvalisuse 2. direktiivi ja muid asjakohaseid liidu küberturvalisuse õigusakte. See lähenemisviis lihtsustab märkimisväärselt paljusid vastavusnõudeid täitma pidavate üksuste regulatiivseid kohustusi ja tagab ressursside tulemuslikuma kasutamise riikide ametiasutustes.

Küberturvalisuse 2. määruse ettepaneku seletuskirjas kirjeldatakse ettepaneku aluseks olevaid peamisi probleeme ja konkreetseid eesmärke nende lahendamiseks. Direktiivi ettepanekus käsitletakse küberturvalisuse määruse läbivaatamise mõjuhinnangu 4. erieesmärki, st luua mehhanismid ja tingimused, mis aitavad hõlbustada küberturvalisuse nõuete täitmist ning muuta seeläbi nende rakendamine sidusamaks ja tulemuslikumaks. Küberturvalisuse 2. direktiivi sihipäraste muudatuste eesmärk on lihtsustada küberturvalisuse raamistiku konkreetsete aspektide järgimist ning tagada nende sujuv ja sidus rakendamine, sealhulgas seoses kohaldamisala, määratluste, lunavaraintsidentidest teatamise ja piiriüleseid teenuseid osutavate üksuste järelevalvega.

Ettepanek võtta vastu direktiiv, millega muudetakse direktiivi (EL) 2022/2555 seoses lihtsustamismeetmega ja vastavusse viimisega [küberturvalisuse 2. määrusega], kuulub õigusloome kvaliteedi ja tulemuslikkuse programmi (REFIT) alla. Koos küberturvalisuse määruse läbivaatamisega aitab see oluliselt kaasa selguse parandamisele, ebatõhususe kõrvaldamisele ja eri õigusraamistike menetluste ühtlustamisele. See aitab kaasa siseturu nõuetekohasele toimimisele, tagades samal ajal liidu julgeoleku ja strateegilise autonoomia.

- **Kooskõla poliitikavaldkonnas praegu kehtivate õigusnormidega**

Liit on laiendanud oma õiguslikke ja poliitilisi vahendeid mitme õigusakti ja poliitikameetme vastuvõtmisega: i) küberturvalisuse 2. direktiivi eesmärk on tugevdada elutähtsa taristu küberturvalisust; ii) selle nn sõsardirektiivis, elutähtsa teenuse osutajate toimepidevuse direktiivis, on määratletud füüsilise turvalisuse meetmed; iii) küberkerksuse määrusega suurendatakse toodete küberturvalisust; iv) kübersolidaarsuse määrusega parandatakse kogu ELis reageerimisvõimekust; v) ELi kübervaldkonna tegevuskavaga[7] toetatakse ELi tasandi koostööd kriisiohje valdkonnas; vi) 5G küberturvalisuse meetmepaketiga (5G meetmepakett) toetatakse 5G-võrkude küberturvalisust; vii) Euroopa haiglate ja tervishoiuteenuse osutajate küberturvalisuse tegevuskava[8] aitab suurendada nende küberturvalisust ning viii) küberturbeoskuste akadeemia[9] kaudu lahendatakse üha suuremat küberturvalisuse valdkonna talendinappuse probleemi.

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

---

7 COM/2025/66 final.
8 COM(2025) 10 final.
9 COM(2023) 207 final.
10 Komisjoni rakendusmäärus (EL) 2023/203 ja komisjoni delegeeritud määrus (EL) 2022/1645.

Käesolev direktiivi ettepanek, nagu ka sellega kaasnev määruse ettepanek, on osa laiemast õiguslike ja poliitiliste algatuste kogumist, mille liit võtab vastu, et parandada üksuste vastupanuvõimet julgeoleku- ja küberohtudele. Selles keskendutakse küberturvalisuse 2. direktiivi sihipärastele muudatustele, mille eesmärk on muu hulgas täpsustada teatavaid kohaldamisala, määratluste ja jurisdiktsiooninormidega seotud aspekte, vähendada elutähtsate ja oluliste üksuste järelevalve koormust ning hõlbustada piiriüleste üksuste järelevalvet, tugevdades ENISA rolli operatiivkoostöö toetamisel. Peale selle loovad käesolev ettepanek ja määruse ettepanek ühiselt tugeva sünergia, mis tuleneb küberturvalisuse 2. direktiivi kohase turvaoleku sertifitseerimise väljatöötamisest ning võib hõlbustada muude asjakohaste liidu õigusaktide, näiteks isikuandmete kaitse üldmääruse järgimist, ilma et see piiraks nende konkreetseid sertifitseerimisnõudeid. Need lihtsustamismeetmed peaksid vabastama vahendeid, et tugevdada liidu kriitilise tähtsusega sektorite üksuste operatiivset küberturvalisuse alast valmisolekut.

- **Kooskõla muude liidu tegevuspõhimõtetega**

Käesoleva ettepanekuga tugevdatakse ettevõtluskukru teenuseid pakkuvate üksuste turvanõudeid, mis on sätestatud ettepanekus võtta vastu Euroopa Parlamendi ja nõukogu määrus Euroopa ettevõtluskukrute loomise kohta[11]. Lisaks tagab komisjon kooskõla tulevaste algatustega, näiteks digivõrkude õigusaktiga. Käesolev ettepanek on kooskõlas digivaldkonna õigusaktide lihtsustamist käsitleva määruse ettepanekuga (digivaldkonna koondpakett), mis sisaldab muudatusi küberturvalisuse 2. direktiivis ja muudes liidu õigusaktides. Digivaldkonna koondpaketis tehakse ettepanek hõlbustada muu hulgas küberturvalisuse 2. direktiivi kohaste küberturvalisuse aruandlusnõuete täitmist, nii et teatamiseks kasutataks intsidentidest teatamise ühtset kontaktpunkti, mille töötab välja ja mida haldab ENISA. Ettepanek on ühtlasi kooskõlas ettepanekuga võtta vastu Euroopa Parlamendi ja nõukogu määrus liidus toimuva kosmosetegevuse ohutuse, kerksuse ja kestlikkuse kohta[12].

Nagu eespool rõhutatud, on ettepanek kooskõlas ka Mario Draghi aruandega Euroopa konkurentsivõime tuleviku kohta.

2. ÕIGUSLIK ALUS, SUBSIDIAARSUS JA PROPORTSIONAALSUS

- **Õiguslik alus**

Käesoleva direktiivi õiguslik alus on Euroopa Liidu toimimise lepingu (ELi toimimise leping) artikkel 114, mille kohaselt soovitakse rajada siseturg ja tagada selle toimimine riigisiseste normide ühtlustamise meetmete tõhustamise abil. Käesoleva ettepanekuga muudetakse direktiivi (EL) 2022/2555, mis võeti vastu ELi toimimise lepingu artikli 114 alusel.

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

Subsidiaarsuse põhimõtte kohaselt on vaja hinnata liidu meetme vajalikkust ja lisaväärtust. Subsidiaarsuse põhimõtte järgimist selles valdkonnas tunnistati juba käesoleva ettepanekuga muudetava direktiivi (EL) 2022/2555 vastuvõtmisel.

Käesolev ettepanek soodustab liidu küberturvalisuse õigusaktide järgimist, vähendades mõjutatud üksuste nõuete täitmisega seotud kulusid ja õiguskindlusetust ning hõlbustades ja

[11] COM/2025/838 final.
[12] COM/2025/335 final.

parandades küberturvalisuse nõuete täitmise määra. Samuti aitab see liikmesriikides ühtlustada lähenemisviise järelevalvele ja vastavuskontrollile.

- **Proportsionaalsus**

Käesoleva direktiivi kavandatud eeskirjadega reguleeritakse üksnes seda, mis on vajalik, et saavutada kindlad eesmärgid rahuldaval tasemel. Kavandatav kohaldamisala, turvameetmete ja teatamiskohustuste vastavusse viimine ja ühtlustamine lähtub liikmesriikide ja ettevõtjate taotlustest praegust raamistikku parandada.

- **Vahendi valik**

Ettepanekuga muudetakse kehtivat küberturvalisuse 2. direktiivi ja ühtlustatakse veelgi ettevõtjatele kehtestatud kohustusi, tagades seega kogu liidus ühtlasema taseme. Käesoleva ettepaneku jaoks valitud vahend on vastab muudetavale õigusaktile, s.t küberturvalisuse 2. direktiivile. Käesolevas ettepanekus tuginetakse küberturvalisuse 2. direktiivi eesmärgile anda liikmesriikidele paindlikkus, mida on vaja riiklike eripärade arvessevõtmiseks.

3. JÄRELHINDAMISE, SIDUSRÜHMADEGA KONSULTEERIMISE JA MÕJU HINDAMISE TULEMUSED

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

Vt [küberturvalisuse 2. määruse ettepaneku] seletuskiri.

- **Konsulteerimine sidusrühmadega**

Vt [küberturvalisuse 2. määruse ettepaneku] seletuskiri.

- **Eksperdiarvamuste kogumine ja kasutamine**

Vt [küberturvalisuse 2. määruse ettepaneku] seletuskiri.

- **Mõjuhinnang**

Vt [küberturvalisuse 2. määruse ettepanekule] lisatud seletuskiri ja mõjuhinnang.

- **Õigusnormide toimivus ja lihtsustamine**

Vt [küberturvalisuse 2. määruse ettepaneku] seletuskiri.

- **Põhiõigused**

Vt [küberturvalisuse 2. määruse ettepaneku] seletuskiri.

4. MÕJU EELARVELE

Vt [küberturvalisuse 2. määruse ettepaneku] finantsselgitus.

5. MUU TEAVE

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

Küberturvalisuse 2. direktiivi artikli 40 kohaselt vaatab komisjon direktiivi toimimise läbi ja esitab iga 36 kuu järel Euroopa Parlamendile ja nõukogule aruande.

- **Ettepaneku sätete üksikasjalik selgitus**

Ettepaneku eesmärk on hõlbustada küberturvalisuse kohustuste täitmist ja vabastada vahendeid, et tugevdada liidu kriitilise tähtsusega sektorite üksuste operatiivset küberturvalisuse alast valmisolekut.

Ettepanekuga tehakse küberturvalisuse 2. direktiivis sihipäraseid muudatusi, et lihtsustada küberturvalisuse raamistiku konkreetseid aspekte, suurendada õiguskindlust ja ühtlustada rakendamist.

Selleks et üksustel ja tarnijatel oleks lihtsam tõendada vastavust küberturvalisuse 2. direktiivile, on küberturvalisuse 2. direktiiviga reguleeritud üksustel võimalik saada sertifikaate organisatsioonide küberturvalisuse sertifitseerimise kavade alusel, mis on välja töötatud Euroopa küberturvalisuse sertifitseerimise raamistikus kooskõlas käesoleva ettepanekuga kaasneva määruse ettepanekuga.

Et veelgi hõlbustada küberturvalisuse riskijuhtimismeetmete järgimist mitme riigiga seotud üksustes, mille üle teevad järelevalvet mitme liikmesriigi pädevad asutused, antakse ENISA-le uus roll toetada liikmesriike nende üksuste järelevalves, hõlbustades vastastikust abi ja luues parema ülevaate küberturvalisuse 2. direktiivi kohaldamisalasse kuuluvatest üksustest.

Lisaks pakutakse ettepanekus välja, et komisjon võtaks vastu suunised selliste tarneahela turvanõuete kohaldamise kohta, mida küberturvalisuse 2. direktiivi kohaldamisalasse kuuluvad üksused nõuavad oma tarnijatelt, et tagada õiguskindlus ja vältida kohustuste põhjendamatut edasiandmist üksustele, mis ei kuulu küberturvalisuse 2. direktiivi kohaldamisalasse.

Küberturvalisuse 2. direktiivi sihipäraste muudatuste hulka kuuluvad ka järgmised:

- kohaldamisala ja määratluste täpsustamine;
- mikro- ja väikeettevõtjatest domeeninimede süsteemi teenuse osutajate väljajätmine kohaldamisalast;
- artikli 21 lõike 5 kohaste rakendusaktide (milles täpsustatakse küberturvalisuse riskijuhtimismeetmed) võimalikult suur ühtlustamine, et hõlbustada üksuste jaoks nõuete täitmist ja ametiasutuste jaoks järelevalve tegemist;
- väikeste keskmise turukapitalisatsiooniga ettevõtjate uue kategooria kasutuselevõtt kooskõlas komisjoni 2025. aasta soovitusega väikeste keskmise turukapitalisatsiooniga ettevõtjate määratluse kohta[18]; väikesteks keskmise turukapitalisatsiooniga ettevõtjateks kvalifitseeruvad üksused tuleb määrata olulisteks üksusteks, vähendades nende nõuete täitmisega seotud koormust ja pädevate asutuste järelevalvekoormust;
- nõue, et liikmesriigid võtaksid oma riikliku küberturvalisuse strateegia osana vastu postkvantkrüptograafiale ülemineku poliitika, ning
- lunavarareründeid käsitlevate andmete ühtlustatud kogumine.

2026/0012 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV

millega muudetakse direktiivi (EL) 2022/2555 seoses lihtsustamismeetmetega ja vastavusse viimisega [küberturvalisuse 2. määruse ettepanekuga]

(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[1],

võttes arvesse Regioonide Komitee arvamust[2],

toimides seadusandliku tavamenetluse kohaselt

ning arvestades järgmist:

(1) Euroopa Parlamendi ja nõukogu direktiivis (EL) 2022/2555[3] on sätestatud meetmed, mille eesmärk on saavutada küberturvalisuse ühtlaselt kõrge tase kogu liidus, et parandada siseturu toimimist. Alates direktiivi (EL) 2022/2555 jõustumisest on liidu kübervastupidavusvõime suurendamisel tehtud edusamme. Samal ajal on liikmesriikides tekkinud rakendamisel teatavad probleemid, sealhulgas seoses direktiivi kohaldamisalaga, küberturvalisuse riskijuhtimise ja intsidentidest teatamise kohustuste rakendamisega ning piiriüleste üksuste järelevalvega. Tuginedes [küberturvalisuse 2. määruse ettepanekule], tuleks nende probleemide lahendamiseks teha direktiivis (EL) 2022/2555 sihipäraseid muudatusi, lihtsustades konkreetseid aspekte, et suurendada õiguskindlust ja tagada direktiivi (EL) 2022/2555 ühetaoline rakendamine.

(2) Selleks et vähendada üksuste nõuete täitmisega seotud koormust ja pädevate asutuste järelevalvekoormust, tuleks direktiivi (EL) 2022/2555 lisada väikeste keskmise turukapitalisatsiooniga ettevõtjate uus kategooria kooskõlas komisjoni soovitusega (EL) 2025/1099[4]. Direktiivi (EL) 2022/2555 I lisas osutatud liiki üksused, mis

---

1 ELT C [...], [...], lk [...].

2 ELT C [...], [...], lk [...].

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

4 Komisjoni 21. mai 2025. aasta soovitus (EL) 2025/1099, mis käsitleb väikeste keskmise turukapitalisatsiooniga ettevõtjate määratlust (ELT L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).

kvalifitseeruvad kõnealuse soovituse kohaselt väikesteks keskmise turukapitalisatsiooniga ettevõtjateks, tuleks reeglina määrata olulisteks üksusteks. Selleks et toetada komisjoni eesmärki vähendada halduskulusid kokku 25 % ning väikeste ja keskmise suurusega ettevõtjate puhul 35 %, tuleks domeeninimede süsteemi teenuse osutajate suhtes kohaldada direktiivis (EL) 2022/2555 sätestatud suuruse ülemmäära üldreeglit, mille kohaselt kõik üksused, kes kvalifitseeruvad komisjoni soovituse 2003/361/EÜ[5] lisa artikli 2 kohaselt keskmise suurusega ettevõtjateks või ületavad kõnealuse artikli lõikes 1 esitatud keskmise suurusega ettevõtja ülemmäärasid, kuuluvad direktiivi (EL) 2022/2555 kohaldamisalasse.

(3) Direktiivi (EL) 2022/2555 rakendamisel on esinenud probleeme selle kohaldamisala käsitlevate sätete tõlgendamisel. Seepärast tuleks täpsustada teatavaid kohaldamisalaga seotud sätteid tervishoiuteenuste osutajate, elektritootjate, vesinikuettevõtjate ja keemiasektori üksuste kohta, et tagada õiguskindlus ja vähendada nõuete täitmisega seotud koormust nii üksuste kui ka riiklike ametiasutuste jaoks.

(4) Selleks et tagada proportsionaalsus elektritootjate puhul, kes on määratletud Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/944[6] artikli 2 punktis 38, tuleks direktiivis (EL) 2022/2555 elutähtsateks või olulisteks üksusteks pidada üksnes neid elektritootjaid, kelle kogu tootmisvõimsus ületab 1 MW, tingimusel et nad vastavad suuruse ülemmäära reeglile. Siia alla peaksid kuuluma nii elektritootjad, kelle üks elektritootmisrajatis ületab 1 MW, kui ka elektritootjad, kes käitavad mitut tootmisrajatist, mille tootmisvõimsus kokku ületab 1 MW. Selline lähenemisviis võimaldab saavutada tasakaalu, kus ühel pool on vajadus hõlmata need üksused, mille võrgu- ja infosüsteemi häirimine võib tähendada tootmisvõimsuse kadu, kontrollimatust või välist kontrolli, kusjuures see tootmisvõimsus on iseenesest oluline elektrivõrgu turvalisuse ja stabiilsuse seisukohast, ning teisel pool on vajadus mitte tekitada ettevõtjatele direktiivi (EL) 2022/2555 alusel ebaproportsionaalset halduskoormust.

(5) Euroopa Parlamendi ja nõukogu määruses (EL) nr 910/2014[7] sätestatud Euroopa digiidentiteedikukrud on liidu digitaristu vajalik osa, mis võimaldab turvalist identimist ja autentimist ning elektrooniliste dokumentide, sealhulgas elektrooniliste tõendite vahetamist. Arvestades digiidentiteedikukrute tähtsust üldsusele ning avalike ja erateenuste osutamisele, võib neid digiidentiteedikukruid mõjutavatel küberintsidentidel olla ulatuslik mõju. Selleks et tagada digiidenteedikukrute teenuste osutamine, tuleks nõuda, et Euroopa digiidentiteedikukrute pakkujad rakendaksid asjakohaseid tehnilisi, tegevuslikke ja korralduslikke meetmeid küberriskide juhtimiseks ning intsidentide ennetamiseks ja neile reageerimiseks ja teeksid pädevate asutustega koostööd vastavalt direktiivile (EL) 2022/2555. Seepärast tuleks olenemata nende suurusest lisada nad kõnealuse direktiiviga hõlmatud üksuste hulka ja kvalifitseerida elutähtsateks üksusteks. ELi digiidentiteedi raamistikule tuginedes pakuvad Euroopa ettevõtluskukrud sarnaseid funktsioone ja teenuseid, mis on

---

5 Komisjoni 6. mai 2003. aasta soovitus 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratluse kohta (ELT L 124, 20.5.2003, lk 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

6 5. juuni 2019. aasta direktiiv (EL) 2019/944 elektrienergia siseturu ühiste normide kohta ja millega muudetakse direktiivi 2012/27/EL (ELT L 158, 14.6.2019, lk 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).

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

kohandatud ettevõtjate ja avaliku sektori asutuste vajadustega, ning on sama tähtsad digimajanduse turvalisuse ja terviklikkuse seisukohast. Järelikult tuleks vastavalt [ettepanekule võtta vastu määrus Euroopa ettevõtluskukrute loomise kohta][8] loodud Euroopa ettevõtluskukrute pakkujate suhtes kohaldada samu küberturvalisuse nõudeid ja kohustusi kui Euroopa digiidentiteedikukrute pakkujate suhtes, et tagada kogu digiidentiteedi ökosüsteemis järjepidev ja kõrge turvalisuse tase.

(6) Merealusesse andmeedastustaristusse kuulub lisaks kaablitele ka nende käitamisega seotud taristu. Selline taristu sisaldab merekaabli maabumiskohti ja selle maa peal asuvaid osi, mis on nendega ühendatud, nt maismaateed rannikul asuvate sidekaevude juurest maabumiskohtadeni, andmekeskused või ühenduspunktid. Merealust andmeedastustaristut käitavad tavaliselt üksused, mis juba kuuluvad direktiivi (EL) 2022/2555 kohaldamisalasse, sealhulgas üldkasutatavate elektroonilise side võrkude ja teenuste pakkujad või pilvandmetöötlusteenuse osutajad. Merealust andmeedastustaristut võivad aga käitada ka muud liiki üksused, mis ei kuulu praegu direktiivi (EL) 2022/2555 kohaldamisalasse, näiteks üldsusele suletud elektroonilise side võrkude pakkujad või üksused, mis on andnud merealuse andmeedastustaristu käitamise kas täielikult või osaliselt rendile üldkasutatavate elektroonilise side võrkude pakkujatele. Arvestades üha suurenevaid riske merealusele andmeedastustaristule ja nendest tulenevat suurt kriitilist tähtsust, on vaja tagada, et direktiiv (EL) 2022/2555 hõlmaks merealuse andmeedastustaristu igat liiki käitajaid. Muud kriitilise tähtsusega meretaristud, nagu merealused elektrikaablid ja gaasi-, vesiniku- ja naftajuhtmed enamasti juba kuuluvad direktiivi (EL) 2022/2555 alla, kuna neid käitavad elektri, gaasi, vesiniku ja nafta allsektorite ülekandesüsteemi haldurid.

(7) Selleks et mitmes liikmesriigis teenuseid osutavad üksused saaksid siseturul kasu sidusamatest ja vähem koormavatest järelevalvealastest lähenemisviisidest, peaks sellistel üksustel olema võimalik tõendada direktiivis (EL) 2022/2555 sätestatud konkreetsete või kõigi küberriskide juhtimisega seotud kohustuste täitmist turvaoleku sertifikaadiga, mis kuulub Euroopa küberturvalisuse sertifitseerimise kava alla. Sellise kava väljatöötamiseks võetakse vastu rakendusaktid tehniliste, metoodiliste ja valdkondlike nõuete kohta seoses direktiivi (EL) 2022/2555 kohaste küberturvalisuse riskijuhtimismeetmetega, mis põhinevad võimalikult suurel ühtlustamisel.

(8) Arvestades meie ühiskonna ja majanduse üha suuremat sõltuvust digitehnoloogiast, on vaja võtta leevendusmeetmeid kvantohu vastu. Võimalikud „kogu nüüd, dekrüpteeri hiljem“ (*harvest now, decrypt later*) ründed, mis tõenäoliselt toimuvad juba praegu, ning tulevased kvantrünnetest tulenevad allkirjade võltsimise riskid, teatavate algoritmide teostuse kavandatud mittesoovitavaks kuulutamine ja praeguste avaliku võtmega krüptoalgoritmide täielik keelamine suurendavad postkvantkrüptograafiale ülemineku meetmete võtmise vajaduse kiireloomulisust. Seetõttu tuleks nõuda, et liikmesriigid võtaksid oma riikliku küberturvalisuse strateegia osana vastu postkvantkrüptograafiale ülemineku poliitika. Selline poliitika peaks hõlbustama strateegilise kavandamise kiirendamist ning toetusmeetmete ja abivahendite loomist, et hinnata krüptograafiliste varade avatust kvantarvutitest tulenevatele riskidele. Lisaks peaks see aitama koostada üleminekukava ja katsetada postkvantkrüptograafia kasutuselevõttu digirakendustes ja -võrkudes ning samal ajal soodustama selliste ametlikult kontrollitud ja hinnatud Euroopa postkvantkrüptograafia lahenduste teket ja kasutuselevõttu, mis järgivad toodete ja teenuste vastavusraamistikke. See poliitika

[8] COM(2025) 838 final.

peaks olema kooskõlas vahe-eesmärkidega, mis on sätestatud liidu õigusaktides ja liidu poliitikas ning võrgu- ja infoturbe koostöörühma vastu võetud dokumentides, eelkõige koostöörühma 2025. aasta juunis vastu võetud postkvantkrüptograafiale ülemineku koordineeritud rakendamise tegevuskavas, saavutades seega kriitilise tähtsusega kasutusjuhtumite puhul postkvantkrüptograafiale ülemineku 2030. aastaks ning keskmise ja madala taseme kasutusjuhtumite puhul 2035. aastaks.

(9) Direktiivi (EL) 2022/2555 artikli 21 lõike 2 punkti d kohaselt peavad elutähtsad ja olulised üksused tagama oma tarneahelas asjakohase turvalisuse taseme. Praktikas on see kohustus tekitanud olukorra, kus paljud üksused küsivad oma tarnijatelt ulatuslikku teavet erinevate küsimustike, vormingute ja protsesside kaudu. Kuigi selliste taotluste eesmärk on toetada hoolsuskohustust ja riskijuhtimist, võivad need ühtlasi tekitada elutähtsate ja oluliste üksuste tarnijatele märkimisväärset halduskoormust, eriti kui sarnast teavet tuleb esitada korduvalt eri vormides. Selle koormuse leevendamiseks ning tarneahela turvalisuse hindamise järjepideva, proportsionaalse ja tõhusa lähenemisviisi edendamiseks peaks komisjon välja töötama suunised, et soovitada, milline on selliste teabenõuete asjakohane üksikasjalikkus, struktuur ja vorm. Sellised suunised peaksid hõlbustama ühtlustamist, vähendama tarbetut dubleerimist ning aitama nii üksustel kui ka nende tarnijatel tulemuslikult täita direktiivist (EL) 2022/2555 tulenevaid kohustusi.

(10) Endiselt on üks peamisi ohte elutähtsatele ja olulistele üksustele lunavararünded, mille puhul pahavara krüpteerib andmeid ja süsteeme ning nõuab vabastamiseks lunaraha maksmist. Küberintsidentidele reageerimise üksustele (edaspidi „CSIRTid“) ja riikide ametiasutustele annaks mõjutatud elutähtsatelt ja olulistelt üksustelt lunavararünnete kohta andmete kogumise ühtlustamine ja parendamine teavet, mis võimaldab neil tagada, et tulevased lunavaraga seotud sekkumised on asjakohased ja tulemuslikud, toetada üksusi nende vastupanuvõime suurendamisel ja tulevaste rünnete ennetamisel ning koguda luureandmeid ja tõendeid, mida õiguskaitseasutused vajavad lunavararündeid korraldavate grupeeringute tabamiseks ja kõrvaldamiseks ning nende liikmete karistamiseks. Võttes arvesse lunavararünnete kohta jagatava teabe võimalikku tundlikku laadi, eelkõige seda, kas üksus on maksnud lunaraha, ning kui on, siis kui palju ja kellele, tuleks selline teave esitada üksnes CSIRTidele või asjakohasel juhul pädevatele asutustele nende taotluse korral. Sellise teabevahetuse eesmärgil soovitatakse elutähtsatel ja olulistel üksustel määrata isik, kes tegutseb kontaktpunktina ning tagab teabevahetuse konfidentsiaalsuse ja usaldusväärsuse. Rahvusvahelise lunavaravastase algatuse raames on liit heaks kiitnud mittesiduva rahvusvahelise poliitilise avalduse, mille kohaselt osalevate riikide valitsuste alluvusse kuuluvad asjaomased asutused ei tohiks maksta lunavaraga väljapressimise korral lunaraha.

(11) Lunavaraintsidentide kohta asjakohase teabe esitamise kohustuse täitmine ei tohiks kaasa tuua lisakohustuste kehtestamist direktiivi (EL) 2022/2555 alusel, mida üksuse suhtes ei oleks kohaldatud, kui ta ei oleks teavet esitanud. Selleks peaksid liikmesriigid oma riigisisese õiguskorra piires käsitlema võimalikke riske, mis tulenevad suuremast vastutusest seoses lunavaraintsidente puudutava asjakohase teabe esitamisega.

(12) Arvestades siseturu paljude elutähtsate ja oluliste üksuste piiriülest mõõdet ja vajadust tagada järelevalvealaste lähenemisviiside sidusus ning toetada nende lähenemist ja tõhusust, peaks ENISA toetama liikmesriike vastastikuse abi andmisel elutähtsatele ja olulistele üksustele, kes osutavad teenuseid rohkem kui ühes liikmesriigis või kes osutavad teenuseid ühes või mitmes liikmesriigis ja kelle võrgu- ja infosüsteemid

asuvad ühes või mitmes muus liikmesriigis. Selleks peaksid liikmesriigid esitama lisateavet ENISA hallatavale üksuste registrile. ENISA peaks elutähtsate ja oluliste üksuste registri teabe alusel põhjalikult analüüsima elutähtsate ja oluliste üksustega seotud piiriüleseid küberriske. Analüüs peaks põhinema metoodikal, mis on välja töötatud koos komisjoni ning võrgu- ja infoturbe koostöörühmaga. Selle metoodika puhul võiks arvesse võtta, millisel määral elutähtsad ja olulised üksused kasutavad oma teenuseid laialdaselt piiriüleselt, sõltuvad piiriülestest teenustest, on avatud tarneahela kontsentratsiooniriskile, võivad ise osutuda tarneahela kontsentratsiooniriski allikaks, on avatud intsidentidele, millel võib olla märkimisväärne häiriv mõju piiriülestele teenustele, või tuginevad oma teenuste osutamisel võrgu- ja infosüsteemidele, mis asuvad eri liikmesriikides ja väljaspool liitu. ENISA peaks riskianalüüsi aruande põhjal soovitama asjaomastel pädevatel asutustel moodustada ühised kontrollirühmad, et toetada intsidentide korral selliste üksuste järelevalvet, kelle siseturu sujuva toimimise takistamise risk on suurem, ning abistada pädevaid asutusi nende taotluse korral ühiste järelevalvemeetmete võtmisel.

(13) Kuna käesoleva direktiivi eesmärki – lihtsustada meetmete rakendamist, et tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus – ei suuda liikmesriigid eraldi piisavalt saavutada, küll aga saab seda meetme toimet arvestades paremini saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev direktiiv nimetatud eesmärgi saavutamiseks vajalikust kaugemale.

(14) Euroopa Andmekaitseinspektori ja Euroopa Andmekaitsenõukoguga konsulteeriti kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725[9] artikli 42 lõikega 2 ning nad esitasid ühisarvamuse [kuupäev],

ON VASTU VÕTNUD KÄESOLEVA DIREKTIIVI:

Artikkel 1

Direktiivi (EL) 2022/2555 muutmine

Direktiivi (EL) 2022/2555 muudetakse järgmiselt.

(1) Artiklit 2 muudetakse järgmiselt:

(a) lõike 2 punkti a muudetakse järgmiselt:

i) alapunkt iii asendatakse järgmisega:

„iii) tippdomeeninimede registrid;“;

ii) lisatakse punktid iv ja v:

„iv) määruses (EL) nr 910/2014 nimetatud Euroopa digiidentiteedikukrute pakkujad;

v) määruse (EL) [...]* kohaselt loodud Euroopa ettevõtluskukrute pakkujad.

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

_____

* Määrus (EL) [...] [ettepanek võtta vastu määrus Euroopa ettevõtluskukrute loomise kohta].“;

(b) lisatakse lõige 3a:

„3a. Käesolevat direktiivi kohaldatakse üksuste suhtes, kes on määruse (EL) [...]** kohaselt kindlaks määratud strateegilise kahesuguse kasutusega taristu omanike, haldajate ja käitajatena, olenemata nende suurusest.

_____

** Määrus (EL) [...] [Ettepanek võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega kehtestatakse meetmete raamistik, et hõlbustada kaitseotstarbelise varustuse, sõjaliste kaupade ja sõjaväelaste transporti liidus].“

(2) Artiklit 3 muudetakse järgmiselt:

(a) lõiget 1 muudetakse järgmiselt:

i) punktid a ja b asendatakse järgmisega:

„a) I lisas osutatud liiki üksused, mis ületavad väikeste keskmise turukapitalisatsiooniga ettevõtjate ülemmäärasid;

b) kvalifitseeritud usaldusteenuse osutajad, Euroopa digiidentiteedikukrute pakkujad, Euroopa ettevõtluskukrute pakkujad ja tippdomeeninimede registrid, olenemata nende suurusest;“;

ii) lisatakse punkt h:

„h) üksused, mis on määruse (EL) [...] [ettepanek võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega kehtestatakse meetmete raamistik, et hõlbustada kaitseotstarbelise varustuse, sõjaliste kaupade ja sõjaväelaste transporti liidus] kohaselt kindlaks määratud strateegilise kahesuguse kasutusega taristu omanike, haldajate ja käitajatena.“;

(b) lõike 4 esimene lõik asendatakse järgmisega:

„Lõikes 3 osutatud loetelu koostamiseks nõuavad liikmesriigid, et nimetatud lõikes osutatud üksused esitaksid pädevatele asutustele vähemalt järgmise teabe:

a) üksuse nimi;

b) I või II lisas osutatud asjakohane sektor, allsektor ja üksuse liik, kui see on kohaldatav;

c) üksuse aadress või üksuse peamise tegevuskoha ja liidus asuvate muude ametlike tegevuskohtade aadress, kui see on kohaldatav, või kui tal liidus tegevuskohta ei ole või ta ei ole seal asutatud, tema artikli 26 lõike 3 kohaselt määratud esindaja aadress;

d) kui see on kohaldatav, üksuse Euroopa ettevõtluskukru ja asjakohasel juhul selle artikli 26 lõike 3 kohaselt määratud esindaja ajakohased kontaktandmed, sealhulgas e-posti aadressid, telefoninumbrid, kordumatu tunnus ja digiaadressid;

e) liikmesriigid, kus üksus teenust osutab;

f) üksuse IP-vahemikud.“

(3) Artikkel 5 asendatakse järgmisega:

„*Artikkel 5*

Minimaalne ühtlustamine

Ilma et see piiraks artikli 21 lõike 5 viienda lõigu kohaldamist, ei takista käesolev direktiiv liikmesriike tarbijate kaitseks vastu võtmast või kehtima jätmast sätteid, millega tagatakse kõrgem küberturvalisuse tase, tingimusel et sellised sätted on kooskõlas liikmesriikide kohustustega, mis on sätestatud liidu õiguses.“

(4) Artiklisse 6

lisatakse punktid 42 ja 43:

„42) „väike keskmise turukapitalisatsiooniga ettevõtja“ – komisjoni soovituse (EL) 2025/1099*** lisas määratletud ettevõtja;

43) „merealune andmeedastustaristu“ – andmeid edastavad merekaablid, nendega seotud taristu ja muud andmeedastusega seotud rajatised või elemendid.

_____

*** Komisjoni 21. mai 2025. aasta soovitus (EL) 2025/1099, mis käsitleb väikeste keskmise turukapitalisatsiooniga ettevõtjate määratlust (ELT L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).“

(5) Artikli 7 lõikesse 2 lisatakse punkt k:

„k) postkvantkrüptograafiale üleminekuks, võttes arvesse kohaldatavates liidu õigusaktides ja poliitikas sätestatud ülemineku tähtaegu ja asjakohaseid nõudeid.“

(6) Artikli 15 lõike 2 esimene lause asendatakse järgmisega:

„CSIRTide võrgustik luuakse artikli 10 kohaselt määratud või asutatud CSIRTide, liidu institutsioonide ja ametite infoturbeintsidentidega tegeleva rühma (CERT-EU) ja ENISA esindajatest.“

(7) Artikli 21 lõiget 5 muudetakse järgmiselt:

(a) teine lõik asendatakse järgmisega:

„Komisjon võib võtta vastu rakendusakte, milles sätestatakse lõikes 2 osutatud meetmete tehnilised ja metoodilised ning vajaduse korral valdkondlikud nõuded seoses muude kui käesoleva lõike esimeses lõigus osutatud elutähtsate ja oluliste üksustega. Siseturu toimimise parandamiseks hindab komisjon korrapäraselt, kas käesolevas lõigus osutatud rakendusaktid võetakse vastu konkreetsete sektorite või üksuste liikide kohta. Selliste hindamiste ettevalmistamisel keskendub komisjon eelkõige sektorite või üksuste liikide piiriülesusele ning korraldab avatud, läbipaistva ja kaasava konsultatsiooniprotsessi asjaomaste sidusrühmade ja liikmesriikidega.“;

(b) lisatakse viies lõik:

„Kui komisjon võtab vastu käesoleva lõike esimeses ja teises lõigus osutatud rakendusaktid, ei kehtesta liikmesriigid nende rakendusaktide kohaldamisalasse kuuluvatele üksustele direktiivi (EL) 2022/2555 artikli 21

lõikes 2 osutatud meetmetega seoses täiendavaid tehnilisi, metoodilisi ega valdkondlikke nõudeid.“

(8) Artiklisse 23 lisatakse lõiked 12 ja 13:

„12. Lõike 11 esimese lõigu kohase rakendusakti vastuvõtmisel lisab komisjon nõude, et lunavararünnete kohta esitatakse lõike 1 kohaselt järgmine teave:

(a) kas üksus avastas lunavararünde;

(b) lunavararünde ründevektor;

(c) kas on rakendatud leevendusmeetmeid.

13. Liikmesriigid tagavad, et lunavararündest põhjustatud olulise intsidendi korral teatavad asjaomased üksused CSIRTi või asjakohasel juhul pädeva asutuse taotlusel CSIRTi või asjakohasel juhul pädeva asutuse pakutava sidekanali kaudu järgmisest:

(a) kas üksus on saanud lunarahanõude ja asjakohasel juhul nõude esitaja;

(b) kas lunaraha on makstud ja kui on, siis milline summa, millise maksevahendi kaudu ja millisele saajale, sealhulgas asjakohasel juhul krüptovara ja krüptovarateenuse osutaja.“

(9) Artiklisse 24 lisatakse lõiked 4, 5 ja 6:

„4. Liikmesriigid võivad nõuda, et elutähtsad ja olulised üksused esitaksid artiklile 21 vastavuse tõendamiseks määruse (EL) XXX/XXX**** [ettepanek võtta vastu küberturvalisuse 2. määrus] artikli 75 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava kohase turvaoleku sertifikaadi.

5. Kui elutähtsa või olulise üksuse turvaolek on määruse (EL) XXX/XXX**** [ettepanek võtta vastu küberturvalisuse 2. määrus] artikli 74 alusel vastu võetud Euroopa küberturvalisuse sertifitseerimise kava kohaselt sertifitseeritud ja kui sertifikaat tõendab vastavust käesoleva direktiivi artikli 21 lõike 5 kohaselt vastu võetud rakendusaktis või käesoleva direktiivi artikli 21 lõikeid 1 ja 2 ülevõtvas riigisiseses seaduses sätestatud nõuetele, ei kohalda pädevad asutused üksuse suhtes kas artikli 32 lõike 2 punkti b või artikli 33 lõike 2 punkti b kohaseid lisameetmeid seoses sertifikaadiga hõlmatud nõuetega, olenevalt sellest, kumb punkt on asjakohane.

6. Lõike 4 kohane sertifitseerimine ei mõjuta elutähtsa või olulise üksuse vastutust käesoleva direktiivi järgimise eest.

_____

**** Määrus (EL) XXX/XXX [ettepanek võtta vastu küberturvalisuse 2. määrus].“

(10) Artiklit 26 muudetakse järgmiselt:

(a) lõikesse 1 lisatakse punkt d:

„d) lennuettevõtjaid loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kelle lennutegevuslube väljaandev pädev asutus andis üksusele lennutegevusloa vastavalt Euroopa Parlamendi ja nõukogu määrusele (EÜ) nr 1008/2008*****, või kui kõnealuse määruse kohast lennutegevusluba või samaväärset luba ei ole antud, loetakse neid selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on nende lõike 2 kohane peamine tegevuskoht liidus.

_____

***** Euroopa Parlamendi ja nõukogu 24. septembri 2008. aasta määrus (EÜ) nr 1008/2008 ühenduses lennuteenuste osutamist käsitlevate ühiseeskirjade kohta (ELT L 293, 31.10.2008, lk 3, ELI: http://data.europa.eu/eli/reg/2008/1008/oj).“;

(b) lõige 3 asendatakse järgmisega:

„3. Kui elutähtsa või olulise üksuse tegevuskoht ei ole liidus või ta ei ole seal asutatud, kuid ta pakub liidus oma teenuseid, määrab ta endale liidus esindaja. Esindaja tegevuskoht peab olema ühes nendest liikmesriikidest, kus teenuseid osutatakse, või ta peab olema seal asutatud. Kõnealust üksust loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on esindaja tegevuskoht või kus ta on asutatud. Kui selline üksus on lõike 1 punktis a osutatud üksus, loetakse ta selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus ta oma teenuseid osutab. Kui käesoleva lõike kohast esindajat liidus määratud ei ole, võib üksuse vastu, kes rikub käesolevat direktiivi, võtta õiguslikke meetmeid iga liikmesriik, kus üksus teenuseid osutab.“

(11) Artiklit 27 muudetakse järgmiselt:

(a) lõige 1 asendatakse järgmisega:

„1. ENISA loob ühtsetelt kontaktpunktidelt lõike 4 kohaselt saadud teabe põhjal elutähtsate ja oluliste üksuste ning domeeninimede registreerimise teenuseid osutavate üksuste registri ja haldab seda. Taotluse korral võimaldab ENISA pädevatele asutustele juurdepääsu selle registri teabele domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, domeeninimede registreerimise teenuseid osutavate üksuste, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate, hallatud teenuse osutajate ja hallatud turbeteenuse osutajate ning internetipõhiste kauplemiskohtade, veebipõhiste otsingumootorite, sotsiaalvõrguteenuse platvormide pakkujate ja lennuettevõtjate kohta, tagades samal ajal teabe konfidentsiaalsuse kaitse, kui see on kohaldatav.“;

(b) lõige 2 jäetakse välja;

(c) lõiked 3, 4 ja 5 asendatakse järgmisega:

„3. Liikmesriigid tagavad, et elutähtsad ja olulised üksused teavitavad pädevat asutust viivitamata artikli 3 lõike 4 kohaselt esitatud teabe muutumisest, tehes seda igal juhul hiljemalt kahe nädala jooksul alates muudatuse kuupäevast.

4. Artikli 3 lõikes 4 osutatud teabe kättesaamisel edastab asjaomase liikmesriigi ühtne kontaktpunkt selle põhjendamatu viivituseta ENISA-le.

5. Kui see on kohaldatav, esitatakse artikli 3 lõike 4 esimeses lõigus osutatud teave artikli 3 lõike 4 neljandas lõigus osutatud riikliku mehhanismi kaudu.“

(12) Lisatakse artikkel 37a:

„Artikkel 37a

ENISA roll vastastikuses abis

1. ENISA abistab liikmesriike vastastikuse abi osutamisel artikli 37 tähenduses ning aitab hõlbustada selliseid koostööprotsesse elutähtsate ja oluliste üksuste puhul, kes osutavad teenuseid rohkem kui ühes liikmesriigis või osutavad teenuseid ühes või

mitmes liikmesriigis ning kelle võrgu- ja infosüsteemid asuvad ühes või mitmes muus liikmesriigis.

2. Lõikes 1 sätestatud eesmärkidel analüüsib ENISA hiljemalt ... [15 kuud pärast käesoleva määruse jõustumist] põhjalikult piiriüleseid küberriske, mis on seotud elutähtsate ja oluliste üksustega, kes osutavad teenuseid rohkem kui ühes liikmesriigis või osutavad teenuseid ühes või mitmes liikmesriigis ja kelle võrgu- ja infosüsteemid asuvad ühes või mitmes muus liikmesriigis. Analüüsi käigus hinnatakse selliseid elutähtsaid ja olulisi üksuseid mõjutavate intsidentide võimalike piiriüleste ja siseturule avalduvate tagajärgede ulatust. ENISA töötab nimetatud analüüsi metoodika välja koostöös komisjoni ja koostöörühmaga. Analüüsi põhjal koostab ENISA põhjaliku piiriülese küberriski hindamise aruande, mida ajakohastatakse igal aastal.

3. ENISA teeb põhjaliku piiriülese küberriski hindamise aruande põhjal järgmist:

(a) kui see on asjakohane, soovitab asjaomastel pädevatel asutustel moodustada ühised kontrollirühmad, et toetada kindlate üksuste järelevalvet;

(b) töötab välja suunised ühiste järelevalvemeetmete kohta;

(c) kehtestab asjaomaste liikmesriikide pädevate asutuste taotluse korral praktilise korra ühiste järelevalvemeetmete võtmiseks;

(d) osaleb asjaomaste liikmesriikide pädevate asutuste taotluse korral ja tema omavahenditega proportsionaalselt ühistes järelevalvemeetmetes;

(e) aitab asjaomaste liikmesriikide pädevate asutuste taotluse korral hinnata, millisel määral on elutähtis või oluline üksus rakendanud artiklis 21 sätestatud küberturvalisuse riskide juhtimise meetmeid.

4. Käesoleva artikli lõike 3 punkti e kohaldamisel esitavad asjaomaste liikmesriikide pädevad asutused ENISA-le elutähtsa või olulise üksuse poolt artikli 21 kohaselt võetud küberturvalisuse riskijuhtimismeetmete loetelu, kui see on kättesaadav, võetud järelevalve- või täitmise tagamise meetmete loetelu ning asjakohased dokumendid, sealhulgas tõendid küberturvalisuse alase poliitika rakendamise kohta, näiteks selliste turvaauditite tulemused, mille pädevad asutused on selle üksuse suhtes artiklite 32 ja 33 kohaselt läbi viinud.

5. Kui liikmesriik saab artikli 37 lõike 1 esimese lõigu punktis c osutatud vastastikust abi, teavitab ühtne kontaktpunkt ENISAt vastastikuse abi osutamisest. Kui see on kohaldatav, märgib ühtne kontaktpunkt, milline artikli 23 lõikes 6 osutatud piiriülene intsident oli seotud vastastikuse abi juhtumiga.“

(13) I ja II lisa muudetakse vastavalt käesoleva direktiivi lisale.

Artikkel 2
Ülevõtmine

1. Liikmesriigid võtavad käesoleva direktiivi järgimiseks vajalikud meetmed vastu ja avaldavad need hiljemalt … [12 kuud pärast käesoleva direktiivi jõustumist]. Liikmesriigid teatavad nendest viivitamata komisjonile.

Nad kohaldavad kõnealuseid meetmeid alates … [esimeses lõigus osutatud kuupäevale järgnevast päevast].

2. Kui liikmesriigid lõikes 1 osutatud meetmed vastu võtavad, lisavad nad nende ametlikul avaldamisel nendesse või nende juurde viite käesolevale direktiivile. Sellise viitamise viisi näevad ette liikmesriigid.

Artikkel 3
Jõustumine

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

Artikkel 4
Adressaadid

Käesolev direktiiv on adresseeritud liikmesriikidele.

Strasbourg,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*
[...]	*[...]*