Euroopa Liidu
Nõukogu

Brüssel, 26. november 2021
(OR. en)

14337/21

Institutsioonidevaheline dokument: 2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

MÄRKUS

Saatja:	Nõukogu peasekretariaat
Saaja:	Nõukogu
Eelmise dok nr:	9583/2/21, 11724/21
Komisjoni dok nr:	14150/20
Teema:	Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148 *– Üldine lähenemisviis*

I. SISSEJUHATUS

1. Komisjon võttis 16. detsembril 2020 vastu direktiivi ettepaneku, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus (muudetud küberturvalisuse direktiiv, ehk „küberturvalisuse 2. direktiiv“),[1] et asendada praegune võrgu- ja infosüsteemide turvalisust käsitlev direktiiv („küberturvalisuse direktiiv“)[2].

[1] Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148.

[2] Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus.

Ettepanek on üks meetmetest, mis on ette nähtud ELi küberturvalisuse strateegias digikümnendi jaoks,[3] mille eesmärk on tagada, et kodanikud ja ettevõtjad saaksid kasutada usaldusväärset digitehnoloogiat.

2. Ettepanek põhineb Euroopa Liidu toimimise lepingu (edaspidi „ELi toimimise leping“) artiklil 114 ja selle eesmärk on täiendavalt suurendada avaliku ja erasektori üksuste, pädevate asutuste ja liidu kui terviku vastupidavusvõimet ja intsidentidele reageerimise suutlikkust.

3. Euroopa Parlamendis vastutab ettepaneku eest tööstuse, teadusuuringute ja energeetikakomisjon (ITRE). ITRE komisjon võttis raportööri raporti vastu 28. oktoobril 2021.

4. Euroopa Majandus- ja Sotsiaalkomitee võttis oma arvamuse vastu 28. aprillil 2021.

5. 3. veebruaril 2021 otsustas alaliste esindajate komitee konsulteerida ettepaneku osas Regioonide Komiteega[4]. Seni ei ole Regioonide Komitee oma arvamust esitanud.

6. Euroopa andmekaitseinspektor võttis oma arvamuse vastu 11. märtsil 2021[5].

7. Oma 22. märtsi 2021. aasta järeldustes,[6] milles käsitletakse Euroopa Liidu küberturvalisuse strateegiat digikümnendi jaoks, võttis nõukogu teadmiseks küberturvalisuse direktiivile tugineva uue ettepaneku ning kordas oma toetust riiklike küberturvalisuse raamistike tugevdamisele ja ühtlustamisele ning liikmesriikidevahelisele püsivale koostööle.

8. Oma 21.–22. oktoobri 2021. aasta järeldustes kutsus Euroopa Ülemkogu üles jätkama tööd võrgu- ja infosüsteemide turvalisust käsitleva muudetud direktiivi ettepanekuga.

---

[3] 14133/20
[4] 5573/21
[5] Arvamus 5/2021, mis käsitleb küberturvalisuse strateegiat ja küberturvalisuse 2. direktiivi (NIS 2.0).
[6] 6722/21

II. TÖÖ NÕUKOGU ETTEVALMISTAVATES ORGANITES

9. Nõukogus toimub ettepaneku läbivaatamine horisontaalses küberküsimuste töörühmas (edaspidi „HWPCI“). Ettepaneku läbivaatamine algas Portugali eesistumise ajal 19. jaanuaril, kui ettepanek põhjalikult läbi vaadati, võimaldades liikmesriikidel esitada oma küsimused ja tuua välja oma peamised mureküsimused ning saada komisjonilt üksikasjalikke selgitusi muudetud direktiivis sisalduvate muudatuste kohta.

10. Portugali eesistumise ajal on HWPCI pühendanud ettepaneku tutvustamisele ja läbivaatamisele 17 koosolekut. Läbivaatamise eduaruanne esitati transpordi, telekommunikatsiooni ja energeetika nõukogule 4. juunil 2021.

11. Sloveenia eesistumise ajal on töö jätkunud ja intensiivistunud, eesmärgiga leppida nõukogu (transport, telekommunikatsioon ja energeetika) 3. detsembri 2021. aasta istungil kokku üldine lähenemisviis. Eesistujariik Sloveenia pühendas küberturvalisuse 2. direktiivi ettepaneku läbivaatamisele ja paljudele kahepoolsetele aruteludele kõigil tasanditel 15 koosolekut.

12. HWPCI keskendus oma töös ettepaneku teksti ümbersõnastamisele, kõigepealt küberturvalisuse 2. direktiivi koostoimele valdkondlike õigusaktidega ja kohaldamisalale, eelkõige avaliku halduse, domeeninimede süsteemi juurserverite ja välistava klausli osas, ning seejärel käsitleti muude teemade hulgas vastastikust hindamist, jurisdiktsiooni ja vastastikust abi, nõrkuste koordineeritud avalikustamist, domeeninimede ja registreerimisandmete andmebaase ning rahvusvahelist koostööd.

13. Esimene kompromissettepanek kavandatava direktiivi teksti kohta esitati 21. septembril 2021,[7] tuginedes liikmesriikidelt saadud kirjalikele märkustele ja mitteametlikele dokumentidele ning varasematele kompromissettepanekutele, mis käsitlevad küberturvalisuse 2. direktiivi koostoimet valdkondlike õigusaktidega ning küberturvalisuse 2. direktiivi kohaldamisala.

---

[7] 12019/21

14. Eesistujariigi kompromissettepaneku viimast versiooni[8] arutati töörühma tasandil 22. novembril 2021. Kuigi delegatsioonid üldiselt tervitasid kompromissteksti, esitasid mõned delegatsioonid siiski analüüsi reservatsiooni või esitasid kommentaare kompromissettepaneku osade kohta. Teksti teatavate osade puhul pakuti endiselt välja mõningast tehnilist ümbersõnastamist.

III. SISU

15. Töörühma tasandil peetud arutelude põhjal tehti kindlaks, et peamised poliitilised küsimused on järgmised:

a) Kohaldamisala (artikkel 2)

Alates arutelude algusest küberturvalisuse 2. direktiivi ettepaneku üle oli liikmesriikide väljendatud peamine mure direktiivi kohaldamisalasse kuuluvate üksuste arvu märkimisväärne suurenemine ning eelkõige suuruse ülempiiri reegli kehtestamine, mille kohaselt kuuluvad direktiivi kohaldamisalasse kõik keskmise suurusega ja suured üksused, kes tegutsevad küberturvalisuse 2. direktiivi kohaldamisalasse kuuluvates sektorites või osutavad selle kohaldamisalasse kuuluvaid teenuseid. Kuigi kompromissettepanekus see üldreegel säilitatakse, sisaldab see täiendavaid sätteid, et tagada vajalik proportsionaalsus, riskijuhtimise kõrgem tase ja selged kriitilisuse kriteeriumid direktiivi kohaldamisalasse kuuluvate üksuste kindlaksmääramiseks. Lisaks sisaldab kompromissettepanek erisätteid järelevalvemeetmete kasutamise prioriseerimise kohta, järgides riskipõhist lähenemisviisi.

[8] 12019/5/21 REV 5

b) Avalik haldus (artikli 2 lõige 2a)

Avaliku halduse lisamine küberturvalisuse 2. direktiivi kohaldamisalasse tekitas palju vaidlusi, kuna avaliku halduse sektor on väga erinev teistest küberturvalisuse 2. direktiiviga hõlmatud sektoritest. Eesistujariik on püüdnud saavutada tasakaalustatud lähenemisviisi, mille puhul võetakse arvesse riiklike avaliku halduse raamistike eripärasid ja tagatakse liikmesriikidele teatav paindlikkus küberturvalisuse 2. direktiivi kohaldamisalasse kuuluvate avaliku halduse üksuste kindlaksmääramisel. Seetõttu on kompromissteksti kohaselt küberturvalisuse 2. direktiiv kohaldatav keskvalitsuste avaliku halduse üksuste suhtes, samas kui liikmesriigid võivad sätestada, et seda direktiivi kohaldatakse ka piirkondliku ja kohaliku tasandi avaliku halduse üksuste suhtes.

c) Välistav klausel (artikli 2 punktid 3a ja 3aa)

Liikmesriigid soovisid muuta välistavat klauslit selgemaks selles osas, et direktiivi ei kohaldata üksuste suhtes, kes tegutsevad peamiselt kaitse, riikliku julgeoleku, avaliku julgeoleku või õiguskaitse valdkonnas, ega riikliku julgeoleku ja kaitse valdkondades toimuva tegevuse suhtes. Kohaldamisalast on välja jäetud ka kohtud, parlamendid ja keskpangad.

d) Koostoime valdkondlike õigusaktidega

Liikmesriigid rõhutasid vajadust viia küberturvalisuse 2. direktiiv vastavusse valdkondlike õigusaktidega, eelkõige finantssektori digitaalset tegevuskerksust käsitleva määrusega (DORA) ja kriitilise tähtsusega üksuste vastupidavusvõimet käsitleva direktiiviga (CER-direktiiv). Küberturvalisuse 2. direktiiv, mis peaks olema küberturvalisuse valdkonnas minimaalse ühtlustamise alus, sisaldab eraldi artiklit valdkondlike liidu õigusaktide kohta (artikkel 2b). Mis puudutab koostoimet CER-direktiiviga, siis kompromissettepanek tagab suurema selguse „kõiki ohte hõlmava“ lähenemisviisi osas. Muud olulised täiendused on seotud asjaomaste õigusaktide alusel pädevate asutuste vahel sõlmitud koostöökokkulepetega.

e) Vastastikune õpe (artikkel 16)

Peaaegu kõik liikmesriigid olid vastu komisjoni soovile kehtestada kohustuslikud vastastikused eksperdihinnangud. Väljapakutud kompromiss tagab, et uus vastastikuse õppimise mehhanism põhineb vastastikusel usaldusel ning on vabatahtlik ja liikmesriikide juhitav protsess.

f) Jurisdiktsioon ja territoriaalsus (artikkel 24) ning vastastikune abi (artikkel 34)

Liikmesriigid on väljendanud muret seoses selle tagajärgedega, kui IKT sektori üksustel on erinevad jurisdiktsioonid, nagu nähakse ette komisjoni ettepanekus. Kompromisstekstis on üksuste liigist tulenevat jurisdiktsiooni selgemaks muudetud, ning tugevdatud vastastikust abi käsitleva teksti sõnastust.

g) Teatamiskohustused (artikkel 20)

Arvestades liikmesriikide väljendatud muret, et see koormaks liigselt küberturvalisuse 2. direktiiviga hõlmatud üksusi ja tooks kaasa liigse teavitamise, on olulistest küberohtudest teatamine kompromisstekstist välja jäetud.

IV. KOKKUVÕTE

16. Alaliste esindajate komitee jõudis 24. novembril 2021 kompromissteksti suhtes lisas esitatud kujul kokkuleppele ja otsustas esitada selle nõukogule (transport, telekommunikatsioon ja energeetika) üldise lähenemisviisi vastuvõtmiseks.

17. Nõukogul palutakse lisas esitatud eesistujariigi kompromisstekst heaks kiita ning võtta oma 3. detsembri 2021. aasta istungil vastu osaline üldine lähenemisviis.

LISA

Ettepanek

EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV,

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

(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,[9]

võttes arvesse Regioonide Komitee arvamust,[10]

toimides seadusandliku tavamenetluse kohaselt

[9] ELT C , , lk .
[10] ELT C , , lk .

ning arvestades järgmist:

(1) Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148[11] eesmärgiks seati suurendada küberturvalisuse alast suutlikkust kogu liidus, vähendada peamistes sektorites elutähtsate teenuste osutamiseks kasutatavaid võrgu- ja infosüsteeme ähvardavaid ohte ning tagada selliste teenuste katkematu osutamine küberturvalisuse intsidentide esinemise korral ning aidata seeläbi kaasa liidu majanduse ja ühiskonna tõhusale toimimisele.

(2) Alates direktiivi (EL) 2016/1148 jõustumisest on liidu küberturvalisuse alase vastupidavusvõime suurendamisel tehtud märkimisväärseid edusamme. Kõnealuse direktiivi läbivaatamisest nähtub, et see on kannustanud liidu küberturvalisust käsitleva institutsionaalse ja regulatiivse lähenemisviisi kujunemist ning sillutanud seeläbi teed märkimisväärsele muutusele mõtteviisis. Kõnealuse direktiiviga on tagatud riiklike raamistike ülesehitamine, mis on hõlmanud riiklike [...] **võrgu- ja infosüsteemide turvalisuse** strateegiate määratlemist, riikliku suutlikkuse kujundamist ning regulatiivsete meetmete kohaldamist iga liikmesriigi määratud elutähtsate taristute ja osalejate suhtes. Samuti on see aidanud kaasa koostöö edendamisele liidu tasandil koostöörühma[12] ja riiklike küberturbe intsidentide lahendamise üksuste võrgustiku (CSIRTide võrgustik) loomise kaudu[13]. Vaatamata nendele saavutustele on direktiivi (EL) 2016/1148 läbivaatamisel tuvastatud olemuslikke puudusi, mis takistavad praeguste ja esilekerkivate küberturvalisuse alaste probleemide tõhusat lahendamist.

---

[11] Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194/1, 19.7.2016, lk 1).

[12] Direktiivi (EL) 2016/1148 artikkel 11.

[13] Direktiivi (EL) 2016/1148 artikkel 12.

(3) Võrgu- ja infosüsteemidest on saanud keskne osa igapäevaelus, mida iseloomustab kiire digiüleminek ja ühiskonnaosaliste vastastikune seotus, sealhulgas piiriüleses tegevuses. Sellise arenguga koos on laienenud küberturvalisusega seotud ohtude maastik ning kerkinud esile uued probleemid, mis nõuavad kohandatud, koordineeritud ja uuenduslikku reageerimist kõigis liikmesriikides. Küberturvalisuse intsidentide arv, ulatus, keerukus, sagedus ja mõju suurenevad ning see kujutab endast suurt ohtu võrgu- ja infosüsteemide toimimisele. Selle tulemusena võivad küberintsidendid tõkestada siseturu majandustegevust, põhjustada rahalist kahju, õõnestada kasutajate usaldust ning tekitada suurt kahju liidu majandusele ja ühiskonnale. Küberturvalisuse alane valmisolek ja tõhusus on seega praegu siseturu nõuetekohaseks toimimiseks olulisem kui kunagi varem.

(4) Direktiivi (EL) 1148/2016 õiguslik alus oli Euroopa Liidu toimimise lepingu („ELi toimimise leping“) artikkel 114, mille eesmärk on siseturu rajamine ja toimimise tagamine siseriiklike eeskirjade ühtlustamise meetmete tõhustamise kaudu. Teenuseid osutavatele või majanduslikult oluliste toimingutega tegelevatele üksustele kehtestatud küberturvalisuse nõuded erinevad liikmesriigiti märkimisväärselt nii nõuete liigi, üksikasjalikkuse astme kui ka järelevalvemeetodi poolest. Need erinevused põhjustavad lisakulusid ja tekitavad raskusi piiriüleselt kaupu või teenuseid pakkuvatele ettevõtjatele. Ühe liikmesriigi kehtestatud nõuded, mis erinevad teise liikmesriigi kehtestatud nõuetest või on nendega vastuolus, võivad kõnealust piiriülest tegevust oluliselt pärssida.

Lisaks mõjutab küberturvalisuse [...] **meetmete** ebatõhus kavandamine või rakendamine ühes liikmesriigis tõenäoliselt küberturvalisuse taset ka teistes liikmesriikides, kui piiriülene tegevus on sedavõrd intensiivne. Direktiivi (EL) 2016/1148 läbivaatamise käigus selgus, et liikmesriigid kohaldavad seda väga erinevalt; muu hulgas erineb selle kohaldamisala, mille piiritlemine jäeti suuresti liikmesriikide otsustada. Direktiiviga (EL) 2016/1148 anti liikmesriikidele ka väga ulatuslik kaalutlusõigus direktiivis sätestatud turvalisuse tagamise ja intsidentidest teatamise kohustuste rakendamisel. Seega rakendati neid kohustusi siseriiklikul tasandil väga erinevalt. Samuti esines erinevusi kõnealuse direktiivi järelevalve- ja täitmise tagamise sätete rakendamisel.

(5) Kõik need erinevused põhjustavad siseturu killustumist ja võivad kahjustada selle toimimist, mõjutades eelkõige teenuste piiriülest osutamist ja küberturvalisuse alase vastupidavusvõime taset, kuna rakendatavad [...] **meetmed** on erinevad. Käesoleva direktiivi eesmärk on kõrvaldada kirjeldatud suured erinevused liikmesriikide vahel, sätestades koordineeritud reguleeriva raamistiku toimimisega seotud miinimumeeskirjad, kehtestades liikmesriikide vastutavate asutuste tõhusaks koostööks vajalikud mehhanismid, ajakohastades loetelu sektoritest ja tegevustest, mille suhtes küberturvalisusega seotud kohustusi kohaldatakse, ning nähes ette tõhusad õiguskaitsevahendid ja karistused, mis on olulised nende kohustuste tõhusa täitmise tagamiseks. Seega tuleks direktiiv (EL) 2016/1148 kehtetuks tunnistada ja asendada käesoleva direktiiviga.

(6) [...] Liikmesriigid **peaksid saama** võtta vajalikke meetmeid, et tagada oma oluliste julgeolekuhuvide kaitse, tagada avalik kord ja julgeolek ning võimaldada kriminaalkuritegude uurimist, avastamist ja nende eest vastutusele võtmist [...]. [...] **Direktiivi ei peaks kohaldama teatavate nimetatud valdkondades tegutsevate avaliku ja erasektori üksuste suhtes. Seda ei peaks kohaldama ka nimetatud valdkondades toimuva üksuste tegevuse suhtes. Lisaks** ei tohi liikmesriike kohustada andma sellist teavet, mille avalikustamine kahjustaks tema olulisi avaliku julgeolekuga seotud huve. Olulised on salastatud teabe kaitset käsitlevad siseriiklikud ja liidu eeskirjad, ametlikud ja mitteametlikud mitteavalikustamise kokkulepped, nagu fooritulede analoogial põhinev protokoll teabe tundlikkuse märgistamiseks[14].

(6a) Käesoleva direktiivi alusel toimuva isikuandmete töötlemise suhtes kohaldatakse isikuandmete ja eraelu puutumatuse kaitset käsitlevaid liidu õigusakte. Eelkõige ei piira käesolev direktiiv Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ kohaldamist ning seetõttu ei tohiks see eelkõige mõjutada nende sõltumatute järelevalveasutuste ülesandeid ja volitusi, kes on pädevad teostama asjaomase liidu andmekaitseõiguse järgimise üle järelevalvet.

---

[14] Fooritulede analoogial põhinev protokoll teabe tundlikkuse märgistamiseks on vahend, mille abil teavet jagav isik teavitab teabe saajaid kõnealuse teabe edasise levitamise piirangutest. Seda kasutatakse peaaegu kõigis CSIRTi kogukondades ning mõnes teabe jagamise ja analüüsimise keskuses (ISAC).

(7) Direktiivi (EL) 2016/1148 kehtetuks tunnistamisega tuleks sektoripõhist kohaldamisala laiendada, et hõlmata suurem osa majandusest, võttes arvesse põhjendustes 4–6 esitatud kaalutlusi. Direktiivi (EL) 2016/1148 sektoripõhist kohaldamisala tuleks seega laiendada, et hõlmata võimalikult täielikult need sektorid ja teenused, mis on siseturu peamise ühiskondliku ja majandustegevuse jaoks elutähtsad. Õigusnormid ei tohiks erineda selle alusel, kas üksused on oluliste teenuste operaatorid või digiteenuse osutajad. Selline eristamine on iganenud, kuna see ei võta arvesse sektorite või teenuste tegelikku tähtsust siseturu ühiskondliku ja majandustegevuse jaoks.

(8) Direktiivi (EL) 2016/1148 kohaselt oli liikmesriikidel endal kohustus määratleda, millised üksused vastavad oluliste teenuste operaatorite kriteeriumidele („identifitseerimisprotsess"). Et kõrvaldada sellest tulenevad liikmesriikidevahelised suured erinevused ning tagada kõigile asjaomastele üksustele riskijuhtimisnõuete ja teatamiskohustustega seoses õiguskindlus, tuleks kehtestada ühine kriteerium, mille alusel määratletakse käesoleva direktiivi kohaldamisalasse kuuluvad üksused. See kriteerium peaks põhinema suuruse ülempiiri reegli kohaldamisel, nii et kohaldamisalasse jääksid kõik komisjoni soovituses 2003/361/EÜ[15] määratletud keskmise suurusega ja suured ettevõtjad, kes tegutsevad käesoleva direktiivi kohaldamisalasse kuuluvates sektorites või osutavad käesoleva direktiivi kohaldamisalasse kuuluvaid teenuseid. [...]

[15] 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).

(8a) Selleks et tagada selge ülevaade käesoleva direktiivi kohaldamisalasse kuuluvatest üksustest, peaks liikmesriikidel olema võimalik kehtestada riiklikud enesest teavitamise mehhanismid, millega nõutakse, et kõik käesolevat direktiivi kohaldamisalasse kuuluvad üksused teataksid käesoleva direktiivi kohastele pädevatele asutustele või liikmesriikide poolt selleks määratud asutustele vähemalt oma nime, aadressi ja kontaktandmed, samuti sektori, milles nad tegutsevad, või osutatava teenuse liigi ning vajaduse korral loetelu liikmesriikidest, kus üksus oma teenuseid osutab. Liikmesriigid võivad otsustada asjakohaste mehhanismide üle, kui riikide tasandil on olemas registrid, mis võimaldavad kindlaks määrata käesoleva direktiivi kohaldamisalasse kuuluvaid üksusi.

(9) Käesolev direktiiv peaks [...] hõlmama ka **mikro- või** väikeettevõtjaid, kes vastavad teatavatele kriteeriumidele, mis annavad märku võtmetähtsusega rolli täitmisest liikmesriikide majanduse või ühiskonna või kindlate sektorite või teenuseliikide jaoks. Liikmesriikidele tuleks panna kohustus esitada [...] komisjonile **vähemalt asjakohase teabe, mis käsitleb kindlaks määratud üksuste arvu, sektorit, millesse need üksused kuuluvad, või nende üksuste poolt osutatavate teenuste liiki ning konkreetseid kriteeriume, mille alusel nad kindlaks määrati**. **Liikmesriigid võivad, kui see on kooskõlas riiklike julgeolekunormidega, samuti otsustada esitada komisjonile nende üksuste nimed.**

(9a) Käesoleva direktiivi kohaldamisalast jäetakse välja avaliku halduse üksused, kes tegutsevad riikliku julgeoleku, riigikaitse, avaliku julgeoleku ja õiguskaitse valdkonnas, ning samuti kohtud, parlamendid ja keskpangad. Käesoleva direktiivi kohaldamisel ei loeta regulatiivse pädevusega üksusi õiguskaitse valdkonnas tegutsevateks üksusteks ja seetõttu ei ole nad sel põhjusel käesoleva direktiivi kohaldamisalast välja jäetud. Lisaks ei kuulu käesoleva direktiivi kohaldamisalasse need keskvalitsuse avaliku halduse üksused, mis on asutatud ühiselt kolmanda riigiga kooskõlas rahvusvahelise lepinguga.

(9aa) Liikmesriikidel peaks olema võimalik kehtestada, et üksusi, kes on direktiivi (EL) 2016/1148 kohaselt tunnistatud oluliste teenuste operaatoriteks enne käesoleva direktiivi jõustumist, käsitatakse elutähtsate üksustena.

(9aaa) Käesolevat direktiivi ei kohaldata liikmesriikide välismaal asuvate diplomaatiliste ja konsulaaresinduste suhtes ega nende info- ja kommunikatsioonitehnoloogia taristu suhtes, mida sellised esindused kasutavad, kui selline taristu asub välismaal või kui seda kasutatakse välismaal asuvate kasutajate jaoks.

(10) Komisjon võib koostöös koostöörühmaga anda välja mikro- ja väikeettevõtjate suhtes kohaldatavate kriteeriumide rakendamise suunised.

(11) [...] **Käesoleva direktiivi reguleerimisalasse kuuluvad üksused tuleks liigitada kahte kategooriasse: elutähtis ja oluline, mille puhul võetakse arvesse sektori või pakutava teenuse liigi kriitilisust ning üksuse suurust. Sellega seoses tuleks nõuetekohaselt arvesse võtta ka kõiki asjakohaseid valdkondlikke riskihindamisi või pädevate asutuste suuniseid, kui see on asjakohane.** Nii elutähtsate kui ka oluliste üksuste suhtes tuleks kohaldada [...] riskijuhtimisnõudeid ja teatamiskohustusi. Nende kahe üksuseliigi järelevalve- ja karistuskord peaks olema erinev, et tagada õiglane tasakaal kohaldatavate **riskipõhiste** nõuete ja kohustuste ning nõuete täitmise järelevalvega seotud halduskoormuse vahel.

(12) **Käesolevas direktiivis sätestatakse küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuste alused kõigis selle kohaldamisalasse kuuluvates sektorites. Selleks et vältida liidu õigusaktide küberturvalisuse sätete killustumist, kui küberturvalisuse kõrge taseme tagamiseks peetakse vajalikuks täiendavaid valdkondlikke sätteid, mis käsitlevad** küberturvalisusega seotud riskijuhtimismeetmeid **ja teatamiskohustust, peaks komisjon hindama, kas sellised sätted võiks ette näha rakendusaktis käesolevas direktiivis sätestatud volituse alusel. Kui sellised õigusaktid ei ole selleks sobivad, võiksid** valdkondlikud õigusaktid aidata tagada küberturvalisuse kõrge taseme, võttes ühtlasi täielikult arvesse asjaomaste sektorite eripära ja keerukust [...]. **Põhjendused, miks käesolevas direktiivis sätestatud volituse alusel vastu võetud rakendusakt ei olnud asjakohane, tuleb esitada valdkondlikes õigusaktides. Samas tuleks sellistes liidu õigusaktide valdkondlikes sätetes võtta nõuetekohaselt arvesse vajadust tervikliku ja ühtlustatud küberturvalisuse raamistiku järele.** [...] See [...] ei piira komisjonile mitmes sektoris, sealhulgas transpordi- ja energeetikasektoris antud rakendusvolitusi.

(12a) Kui valdkondlikus liidu õigusaktis **on sätted**, mis **nõuavad** elutähtsatelt või olulistelt üksustelt **käesolevas direktiivis sätestatud kohustustega vähemalt samaväärse mõjuga meetmete** võtmist seoses küberturvalisuse riskijuhtimise ning **olulistest** intsidentidest ja küberohtudest teatamise **kohustustega**, tuleks kohaldada neid valdkondlikke sätteid**, sealhulgas järelevalvet ja täitmise tagamist** käsitlevaid sätteid. **Liidu õigusakti valdkondlike sätetega ette nähtud kohustuste samaväärse mõju kindlaksmääramisel tuleks arvesse võtta järgmisi aspekte: i) küberturvalisuse riskijuhtimismeetmed peaksid hõlmama asjakohaseid ja proportsionaalseid tehnilisi ja korralduslikke meetmeid, et juhtida riske, mis ohustavad asjaomaste üksuste teenuste osutamisel kasutatavate võrgu- ja infosüsteemide turvalisust, ning need peaksid sisaldama vähemalt kõiki käesolevas direktiivis sätestatud elemente; ii) olulistest intsidentidest ja küberohtudest teatamise kohustus peaks olema vähemalt samaväärne käesolevas direktiivis sätestatud kohustustega teadete sisu, vormi ja tähtaegade osas; iii) üksuste ja asjaomaste asutuste poolse teavitamise kord, mis on sätestatud valdkondlikes liidu õigusaktides, peaks olema vähemalt samaväärne käesolevas direktiivis sätestatud nõuetega teadete sisu, vormi ja tähtaegade osas ning selles tuleks arvesse võtta CSIRTide rolli; iv) asjaomaste asutuste piiriülese koostöö nõuded peaksid olema vähemalt samaväärsed käesolevas direktiivis sätestatud nõuetega. Kui liidu õigusakti valdkondlikud sätted ei hõlma kõiki käesoleva direktiivi kohaldamisalasse kuuluva konkreetse valdkonna üksusi, tuleks jätkata käesoleva direktiivi asjakohaste sätete kohaldamist üksuste suhtes, mida need valdkondlikud sätted ei hõlma.**

(12aa) Komisjon **peaks liidu õigusaktide valdkondlike sätetega seotud samaväärse mõju nõude kohaldamise korrapäraselt läbi vaatama** [...]. **Korrapärase läbivaatamise ettevalmistamisel konsulteerib komisjon koostöörühmaga.**

(12aaa) Tulevastes valdkondlikes liidu õigusaktides tuleks nõuetekohaselt arvesse võtta käesoleva direktiivi artiklis 4 esitatud määratlusi ning käesoleva direktiivi VI peatükis sätestatud järelevalve- ja jõustamisraamistikku.

(12ab) Kui liidu õigusaktide valdkondlike sätetega nõutakse elutähtsatelt või olulistelt üksustelt selliste meetmete võtmist, mille mõju on vähemalt samaväärne käesolevas direktiivis sätestatud teatamiskohustustega, tuleks vältida kattuvaid teatamiskohustusi ning tagada küberohte või -intsidente puudutavate teadete käsitlemise sidusus ja tõhusus. Sel eesmärgil võivad need valdkondlikud sätted võimaldada liikmesriikidel kehtestada ühise, automaatse ja otsese teatamise mehhanismi, mille kaudu teatatakse olulistest intsidentidest ja küberohtudest nii ametiasutustele, kelle ülesanded on sätestatud vastavates valdkondlikes sätetes, kui ka käesolevas direktiivis sätestatud küberturvalisuse ülesannete eest vastutavatele pädevatele asutustele, sealhulgas vajaduse korral ühtsele kontaktpunktile ja CSIRTidele, või mehhanismi, mis tagab selliste teadete käsitlemiseks süstemaatilise ja viivitamatu teabevahetuse ja koostöö asjaomaste asutuste ja CSIRTide vahel. Teatamise lihtsustamiseks ning ühise, automaatse ja otsese teatamise mehhanismi rakendamiseks võivad liikmesriigid kooskõlas valdkondlike õigusaktidega kasutada käesoleva direktiivi artikli 11 lõike 5a kohaselt loodud ühtset kontaktpunkti. Ühtlustamise tagamiseks tuleks valdkondlikest liidu õigusaktidest tulenevad teatamiskohustused viia kooskõlla käesolevas direktiivis sätestatud kohustustega. Liikmesriigid võivad otsustada, et valdkondlike õigusaktide kohaselt on teadete adressaadid käesoleva direktiivi kohased pädevad asutused või riiklikud CSIRTid.

(13) Käesoleva direktiiviga seoses tuleks Euroopa Parlamendi ja nõukogu määrust XXXX/XXXX käsitada valdkondliku liidu õigusaktina finantssektori üksuste suhtes. Käesoleva direktiiviga kehtestatud sätete asemel tuleks kohaldada määruse XXXX/XXXX sätteid, mis käsitlevad info- ja kommunikatsioonitehnoloogia (IKT) alaseid riskijuhtimise meetmeid, IKTga seotud intsidentide haldamist ja eriti intsidentidest teatamist, samuti digitaalse operatiivse vastupidavusvõime testimist, teabevahetuskorda ja kolmandate isikutega seotud IKT-riske. Seega ei tohiks liikmesriigid kohaldada käesoleva direktiivi sätteid, mis käsitlevad küberturvalisuse riskijuhtimis- ja teatamiskohustusi, […] järelevalvet ja täitmise tagamist, määruse XXXX/XXXX kohaldamisalasse jäävate finantssektori üksuste suhtes. Samas on käesoleva direktiivi kohaselt oluline säilitada finantssektoriga tugevad suhted ja teabevahetus. Selleks võimaldab määrus XXXX/XXXX [...] finantssektori Euroopa järelevalveasutustel ja määruse XXXX/XXXX kohastel riiklikel pädevatel asutustel osaleda koostöörühma **töös** [...] ning vahetada teavet ja teha koostööd käesoleva direktiivi alusel määratud ühtsete kontaktpunktidega **ning** riiklike CSIRTidega. Määruse XXXX/XXXX kohased pädevad asutused peaksid edastama suurte IKT-intsidentide **ja oluliste küberohtude** üksikasjad ka käesoleva direktiivi alusel määratud ühtsetele kontaktpunktidele, **pädevatele asutustele või riiklikele CSIRTidele**. **Seda on võimalik saavutada intsidente puudutavate teadete automaatse ja otsese edastamise või ühise teavitusplatvormi kaudu.** Lisaks peaksid liikmesriigid jätkuvalt hõlmama finantssektori oma küberturvalisuse strateegiatesse ning riiklikud CSIRTid võivad oma tegevusega hõlmata ka finantssektori.

(13a) Selleks et vältida I lisa punkti 2 alapunktis a osutatud lennundussektori üksustele kehtestatud küberturvalisuse kohustuste vahelisi lünki ja kohustuste dubleerimist, peaksid Euroopa Parlamendi ja nõukogu määruste (EÜ) nr 300/2008[16] ja (EL) 2018/1139[17] alusel määratud riiklikud asutused ning käesoleva direktiivi kohased pädevad asutused tegema koostööd seoses küberturvalisuse riskijuhtimismeetmete rakendamisega ja nende meetmete järelevalvega riiklikul tasandil. Määruse (EÜ) nr 300/2008 ja määruse (EL) 2018/1139 kohaselt määratud riiklikud asutused võivad lugeda seda, kui üksus järgib käesoleva direktiivi kohaseid küberturvalisuse riskijuhtimismeetmeid, kõnealustes määrustes ning nende määruste kohaselt vastu võetud asjakohastes delegeeritud õigusaktides ja rakendusaktides sätestatud nõuetele vastamiseks.

---

16 **Euroopa Parlamendi ja nõukogu 11. märtsi 2008. aasta määrus (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002 (ELT L 97, 9.4.2008, lk 72).**

17 **Euroopa Parlamendi ja nõukogu 4. juuli 2018. aasta määrus (EL) 2018/1139, mis käsitleb tsiviillennunduse valdkonna ühisnorme ja millega luuakse Euroopa Liidu Lennundusohutusamet ning millega muudetakse Euroopa Parlamendi ja nõukogu määrusi (EÜ) nr 2111/2005, (EÜ) nr 1008/2008, (EL) nr 996/2010, (EL) nr 376/2014 ja Euroopa Parlamendi ja nõukogu direktiive 2014/30/EL ning 2014/53/EL ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 552/2004 ja (EÜ) nr 216/2008 ning nõukogu määrus (EMÜ) nr 3922/91 (ELT L 212, 22.8.2018, lk 1).**

(14) Üksuste küberturvalisuse ja füüsilise julgeoleku omavahelisi seoseid arvestades tuleks tagada Euroopa Parlamendi ja nõukogu direktiivi (EL) XXX/XXX ja käesoleva direktiivi lähenemisviiside kooskõla. Selle saavutamiseks peaksid liikmesriigid tagama, et direktiivi (EL) XXX/XXX kohaseid kriitilise tähtsusega üksusi ja samaväärseid üksusi käsitatakse käesoleva direktiivi kohaselt elutähtsate üksustena. Liikmesriigid peaksid samuti tagama, et nende küberturvalisuse strateegiatega nähakse ette poliitikaraamistik käesoleva direktiivi ja direktiivi (EL) XXX/XXX kohaste pädevate asutuste vahelise tegevuse paremaks koordineerimiseks intsidentide ja küberohtude alase teabe vahetamise ning järelevalveülesannete täitmise kontekstis. Kummagi direktiivi kohased **pädevad** asutused peaksid tegema koostööd ja vahetama teavet, eelkõige seoses sellega, mis puudutab kriitilise tähtsusega üksuste, küberohtude, küberturvalisuse riskide ja kriitilise tähtsusega üksusi **[**või **kriitilise tähtsusega üksustega samaväärseid üksusi]** [...] mõjutavate intsidentide **ning muude kui küberriskide, -ohtude ja -intsidentide**, [...] **sealhulgas** kriitilise tähtsusega üksuste võetavaid küberturvalisuse **ja füüsiliste** meetmete määratlemist**, ning selliste üksustega seotud järelevalvetegevuse tulemusi. Lisaks, et ühtlustada mõlema direktiivi alusel määratud pädevate asutuste vahelist järelevalvetegevust ja minimeerida asjaomaste üksuste halduskoormust, peaksid pädevad asutused püüdma ühtlustada intsidenditeadete vorme ja järelevalveprotsesse.** Direktiivi (EL) XXX/XXX [...] kohased pädevad asutused **võivad vajaduse korral taotleda, et** käesoleva direktiivi [...] kohased pädevad asutused kasutaksid oma järelevalve- ja täitmise tagamise volitusi kriitilise tähtsusega üksusena identifitseeritud elutähtsa üksuse **suhtes**. [...]

(14a) Digitaristu sektorisse kuuluvad üksused põhinevad sisuliselt võrgu- ja infosüsteemidel ning seetõttu peaksid neile üksustele käesoleva direktiiviga kehtestatud kohustused osana nende küberturvalisuse riskijuhtimis- ja teatamiskohustustest käsitlema terviklikult selliste süsteemide füüsilist turvalisust. Kuna need küsimused on hõlmatud käesoleva direktiiviga, ei kohaldata selliste üksuste suhtes direktiivi (EL) XXX/XXX [CER] III-VI peatükis sätestatud kohustusi.

(15) Usaldusväärse, vastupidava ja turvalise domeeninimesüsteemi (DNS) tagamine ja hoidmine on võtmetähtsusega, et säilitada interneti usaldusväärsus ning tagada selle pidev ja stabiilne toimimine, millest sõltuvad digimajandus ja -ühiskond. Seepärast tuleks käesolevat direktiivi kohaldada kõigi domeeninimesüsteemi teenuse osutajate suhtes kogu domeeninimesüsteemi teenuse osutamise ja lahendusahela ulatuses, mis on **siseturu jaoks oluline**, sealhulgas [...] tippdomeeninimede **registrite** [...], **domeeninimede registreerimise teenust pakkuvate üksuste**, domeeninimede autoriteetsete nimeserverite **operaatorite** ja rekursiivsete aadressiresolverite **operaatorite** suhtes. **Terminit „domeeninimesüsteemi teenuse osutaja“ ei tohiks kohaldada asjaomase üksuse ja temaga seotud üksuste enda tarbeks kasutatavate domeeninimesüsteemi teenuste suhtes. Käesolevast direktiivi kohaselt sellesse kategooriasse kuuluvate teenuseosutajate suhtes kehtestavad küberturvalisuse kohustused piirduvad rangelt küberturvalisuse riskijuhtimismeetmete ja teavitamisega ning seega ei piira need üleilmse domeeninimesüsteemi juhtimist mitut sidusrühma hõlmava kogukonna poolt.**

(16) Pilvandmetöötlusteenused peaksid hõlmama teenuseid, mis võimaldavad nõudepõhist ja ulatuslikku kaugpääsu jagatavate ja hajusate andmetöötlusressursside skaleeritavale ja paindlikule kogumile. Need andmetöötlusressursid on näiteks võrgud, serverid ja muu taristu, operatsioonisüsteemid, tarkvara, salvestusruum, rakendused ja teenused. **Pilvandmetöötluse teenusemudelid hõlmavad muu hulgas taristut teenusena (IaaS), platvormi teenusena (PaaS), tarkvara teenusena (SaaS) ja võrku teenusena (NaaS).** Pilvandmetöötluse korraldusmudelid peaksid hõlmama privaat-, ühis-, avalikku ja hübriidpilve. Mõistetel „teenusemudel“ ja „korraldusmudel“ on sama tähendus nagu nimetatud mõistetel standardi ISO/IEC 17788:2014 määratluses. Pilvandmetöötlusteenuse kasutaja suutlikkust tagada endale ühepoolselt andmetöötlusvõimekus (nt serveriaeg või võrgu talletusruum), ilma et pilvandmetöötlusteenuse osutaja (inimene) peaks kasutajaga suhtlema, võiks nimetada nõudepõhiseks haldamiseks. Mõistega „ulatuslik kaugpääs“ peetakse silmas seda, et pilvevõimalusi pakutakse võrgu kaudu ja need on kättesaadavad mehhanismide abil, mis toetavad heterogeensete nn kõhna või priske kliendi platvormide (sh mobiiltelefonid, tahvelarvutid, sülearvutid, tööjaamad/kohtarvutid) kasutamist.

Mõiste „skaleeritav“ osutab andmetöötlusressurssidele, mis on nõudluse kõikumisega toimetulekuks pilveteenuse osutaja poolt paindlikult jaotatud, olenemata ressursside geograafilisest asukohast. Mõistet „paindlik kogum“ kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mida pakutakse ja mis tehakse kättesaadavaks vastavalt nõudlusele, et kiiresti suurendada või vähendada kättesaadavaid ressursse vastavalt töökoormusele. Mõistet „jagatav“ kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mida pakutakse paljudele kasutajatele, kellel on ühine juurdepääs teenusele, kuid andmete töötlemine toimub eraldi iga kasutaja jaoks, kuigi teenust osutatakse samade elektrooniliste seadmete abil. Mõistet „hajusad“ kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mis asuvad erinevates võrguga ühendatud arvutites või seadmetes ning mis suhtlevad omavahel ja kooskõlastavad omavahelist tegevust sõnumite edastamise teel.

(17) Kuna maad võtavad uuenduslikud tehnoloogiad ja ärimudelid, tulevad eeldatavasti tarbijate muutuvate vajaduste järgi turule uued pilvandmetöötluse korraldus- ja teenusemudelid. Sellises kontekstis võib pilvandmetöötlusteenuseid osutada väga hajusal kujul, mille puhul töötlus toimub andmete loomise või kogumise kohale veelgi lähemal; seega minnakse nn traditsiooniliselt mudelilt üle väga hajusale mudelile (servtöötlus).

(18) Andmekeskusteenuse osutajate pakutavaid teenuseid ei pakuta alati tingimata pilvandmetöötlusteenusena. Seega ei pruugi andmekeskused alati olla pilvandmetöötlustaristu osa. Kõigi võrgu- ja infosüsteemide turvalisusega seotud riskide juhtimiseks peaks käesoleva direktiivi kohaldamisalasse kuuluma ka selliste andmekeskusteenuste osutajad, mis ei ole pilvandmetöötlusteenused. Käesoleva direktiivi kohaldamisel peaks mõiste „andmekeskusteenus“ kätkema sellise teenuse osutamist, mis hõlmab struktuure või struktuuride rühmi, mis on ette nähtud andmete talletamiseks, töötlemiseks ja edastamiseks kasutatava infotehnoloogia- ja võrguseadmete keskseks majutamiseks, omavahel sidumiseks ja käitamiseks, võttes arvesse ka energiajaotuse ja keskkonnajuhtimisega seotud rajatisi ja taristuid. Mõiste „andmekeskusteenus“ ei hõlma asutusesiseseid andmekeskusi, mis kuuluvad asjaomasele üksusele ja mida käitatakse üksuse enda tarbeks.

(19) Postiteenuse osutajate (Euroopa Parlamendi ja nõukogu direktiivi 97/67/EÜ[18] tähenduses) [...] **sealhulgas** [...] kullerteenuse osutajate suhtes tuleks kohaldada käesolevat direktiivi juhul, kui nad osutavad vähemalt ühe postiteenuseahela etapi teenust, eeskätt kogumis-, sorteerimis- või jaotamisteenust (sh järeletulemise teenused). Transporditeenust, mida ei osutata mõne mainitud etapi raames, ei peaks käsitama postiteenusena.

[18] Euroopa Parlamendi ja nõukogu 15. detsembri 1997. aasta direktiiv 97/67/EÜ ühenduse postiteenuste siseturu arengut ja teenuse kvaliteedi parandamist käsitlevate ühiseeskirjade kohta (EÜT L 15, 21.1.1998, lk 14).

(20) Need kasvavad vastastikused sõltuvused tulenevad üha piiriülesemast ja üha enam vastastikku sõltuvast teenuste osutamise võrgustikust, mis kasutab kogu liidus selliste oluliste sektorite taristuid nagu energeetika, transport, digitaristu, joogi- ja reovesi, tervishoid, avaliku halduse teatavad harud ja ka kosmosetööstus, niivõrd kui viimase teatavate teenuste osutamine sõltub maapealsetest taristutest, mida omavad, haldavad ja käitavad kas liikmesriigid või eraõiguslikud isikud (seega ei peeta siinkohal silmas selliseid taristuid, mida omab, haldab või käitab liit või mida hallatakse või käitatakse liidu nimel osana liidu kosmoseprogrammidest). Need vastastikused sõltuvussuhted tähendavad seda, et mis tahes katkestusel – isegi kui see puudutab algselt vaid üht üksust või sektorit – võib olla laiem astmeline mõju, mis võib avaldada kaugeleulatuvat ja pikaajalist negatiivset mõju teenuste osutamisele kogu siseturul. COVID-19 pandeemia on näidanud meie üha enam üksteisest sõltuvate ühiskondade haavatavust väikese realiseerumisvõimalusega riskide esinemise korral.

(**20a**) **Küberturvalisuse kõrge taseme saavutamiseks ja säilitamiseks peaksid käesoleva direktiiviga nõutavad riiklikud küberturvalisuse strateegiad koosnema sidusatest raamistikest, millega nähakse ette küberturvalisuse valdkonna juhtimine. Need strateegiad võivad koosneda ühest või mitmest seadusandlikust või muust kui seadusandlikust dokumendist.**

(21) Arvestades riikide juhtimisstruktuuride erinevusi ning selleks, et kaitsta juba kehtivat valdkondlikku korda või liidu reguleerivaid ja järelevalveasutusi, peaksid liikmesriigid saama määrata käesoleva direktiivi kohaselt elutähtsate ja oluliste üksuste võrgu- ja infosüsteemide turvalisusega seotud ülesannete täitmiseks rohkem kui ühe riikliku pädeva asutuse. Liikmesriikidel peaks olema võimalik määrata see roll juba tegutsevale asutusele.

(22) Et hõlbustada ametiasutuste piiriülest koostööd ja suhtlust ning käesolevat direktiivi tõhusalt rakendada, on vaja, et iga liikmesriik määraks riikliku ühtse kontaktpunkti, kes vastutab võrgu- ja infosüsteemide turvalisuse küsimuste koordineerimise ning liidu tasandil tehtava piiriülese koostöö eest.

(23) Pädevad asutused või CSIRTid peaksid saama üksuste teateid intsidentide kohta tõhusal ja tulemuslikul viisil, **muuhulgas selleks, et hõlbustada vajaduse korral õigeaegset reageerimist intsidentidele ja anda teavitavale üksusele vastus**. Ühtsetele kontaktpunktidele tuleks teha ülesandeks edastada intsidente käsitlevad teated teiste mõjutatud liikmesriikide ühtsetele kontaktpunktidele. [...]

(23a) Valdkondlikes liidu õigusaktides, milles nõutakse küberturvalisuse riskijuhtimismeetmeid või teatamiskohustusi, mille mõju on vähemalt samaväärne käesolevas direktiivis sätestatuga, võiks ette näha, et nende määratud pädevad asutused kasutavad selliste meetmete või kohustustega seoses oma järelevalve- ja jõustamisvolitusi käesoleva direktiivi kohaselt määratud pädevate asutuste abiga. Asjaomased pädevad asutused võivad sel eesmärgil kehtestada koostöökokkuleppe. Sellistes koostöökokkulepetes võiks muu hulgas täpsustada järelevalvetegevuse koordineerimise, sealhulgas siseriikliku õiguse kohaste uurimiste ja kohapealsete kontrollide korra ning pädevate asutuste vahelise asjakohase järelevalvet ja jõustamist käsitleva teabe vahetamise mehhanismi, sealhulgas juurdepääsu kübervaldkonda puudutavale teabele, mida nõuavad käesoleva direktiivi kohaselt määratud pädevad asutused.

(24) Liikmesriigid peaksid olema nii tehniliselt kui ka töökorralduse mõttes piisavalt varustatud, et vältida ja avastada võrgu- ja infosüsteemidega seotud intsidente ja riske ning neile reageerida ja nende mõju leevendada. Liikmesriigid peaksid seega tagama, et neil oleks hästi toimivad ja olulistele nõuetele vastavad CSIRTid, mida tuntakse ka infoturbeintsidentidega tegelevate rühmadena (CERT), et tagada tulemuslik ja ühilduv suutlikkus tulla toime intsidentide ja riskidega ning tagada liidu tasandil tõhus koostöö. Et tugevdada üksuste ja CSIRTide vahelist usalduslikku suhet olukorras, kus CSIRT on pädeva asutuse osa, [...] **võivad** liikmesriigid kaaluda CSIRTide operatiivülesannete funktsionaalset eraldamist, eelkõige seoses sellega, mis puudutab teabevahetust ja üksuste toetamist ning pädevate asutuste järelevalvetegevust.

(25) Mis puutub isikuandmetesse, siis peaks CSIRTidel olema võimalik kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2016/679[19] teha käesoleva direktiivi kohaldamisalasse jääva üksuse nimel või taotlusel nende teenuste osutamiseks kasutatavate võrgu- ja infosüsteemide ennetavat kontrolli. **Asjakohasel juhul** peaksid liikmesriigid seadma eesmärgiks tagada kõikide valdkondlike CSIRTide võrdsel tasemel tehniline suutlikkus. Liikmesriigid võivad paluda riiklike CSIRTide väljatöötamisel Euroopa Liidu Küberturvalisuse Ameti (ENISA) abi.

(26) Arvestades küberturbealase rahvusvahelise koostöö tähtsust, peaks CSIRTidel olema võimalik lisaks käesoleva direktiivi kohaselt loodud CSIRTide võrgustikule osaleda ka rahvusvahelistes koostöövõrgustikes. **Seetõttu võiksid CSIRTid ja pädevad asutused vahetada teavet, sealhulgas isikuandmeid, kolmandate riikide CSIRTidega või nende ametiasutustega, et täita oma ülesandeid kooskõlas määrusega (EL) 2016/679. Kui puudub määruse (EL) 2016/679 artikli 45 kohane kaitse piisavuse otsus või puuduvad kõnealuse määruse artikli 46 kohased asjakohased kaitsemeetmed, võib isikuandmete vahetamist, mida peetakse vajalikuks oluliste küberohtude leevendamiseks ja asetleidvale olulisele intsidendile reageerimiseks, pidada avalikust huvist tulenevaks kaalukaks põhjuseks määruse (EL) 2016/679 artikli 49 lõike 1 punkti d tähenduses.**

---

[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).

(27) Vastavalt komisjoni soovituse (EL) 2017/1548 (koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral) lisale („Tegevuskava“)[20] tuleks ulatusliku intsidendina mõista intsidenti, millel on märkimisväärne mõju vähemalt kahele liikmesriigile või mille põhjustatud häired on niivõrd laialdased, et ühe liikmesriigi suutlikkusest nendega toimetulekuks ei piisa. Olenevalt nende põhjusest ja mõjust võivad ulatuslikud intsidendid eskaleeruda ning muutuda täieulatuslikuks kriisiks, mis takistab siseturu nõuetekohast toimimist. Võttes arvesse selliste intsidentide ulatuslikku haaret ja (enamikul juhtudel) piiriülest laadi, peaksid liikmesriigid ning asjaomased liidu institutsioonid, organid ja asutused tegema koostööd nii tehnilisel, operatiiv- kui ka poliitilisel tasandil, et reageerimist liidu ulatuses nõuetekohaselt koordineerida.

(28) Kuna võrgu- ja infosüsteemide nõrkade kohtade ärakasutamine võib põhjustada suuri häireid ja olulist kahju, on nende nõrkade kohtade kiire tuvastamine ja kõrvaldamine küberturvalisusega seotud riskide vähendamise tähtis tegur. Üksused, kes selliseid süsteeme välja töötavad **või haldavad**, peaksid seetõttu kehtestama asjakohase menetluskorra, mille alusel lahendada nõrkuste probleemid, kui need tuvastatakse. Kuna nõrkusi avastavad ja neist teatavad (need avalikustavad) sageli kolmandad isikud (teatavad üksused), peaks IKT-toodete või -teenuste tootja/osutaja kehtestama ka vajaliku menetluskorra kolmandatelt isikutelt nõrkusi käsitleva teabe saamiseks. Rahvusvahelistes standardites ISO/IEC 30111 ja ISO/IEC [...] **29147** on selleks esitatud suunised nõrkuste käsitlemiseks ja nende avalikustamiseks. Nõrkuste avalikustamisega seoses on koostöö koordineerimine teavitavate üksuste ning IKT-toodete või -teenuste tootjate või osutajate vahel eriti oluline. Nõrkuste koordineeritud avalikustamise all peetakse silmas struktureeritud protsessi, mille käigus teatatakse organisatsioonidele nõrkustest viisil, mis võimaldab organisatsioonil nõrkust diagnoosida ja selle kõrvaldada enne, kui nõrkusega seotud üksikasjalik teave avalikustatakse kolmandatele isikutele või üldsusele. Nõrkuste koordineeritud avalikustamise protsess peaks hõlmama ka teavitava üksuse ja organisatsiooni vahelist koordineerimist nõrkuste kõrvaldamise ja avalikustamise ajastamise asjus.

---

[20] Komisjoni 13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral (ELT L 239, 19.9.2017, lk 36).

(29) Liikmesriigid peaksid seega võtma meetmeid, et nõrkuste koordineeritud avalikustamist hõlbustada, kehtestades selleks asjakohase riikliku poliitika. **Oma riikliku poliitika raames peaksid liikmesriigid kooskõlas oma siseriikliku õiguskorraga püüdma võimalikult suures ulatuses lahendada probleeme, millega seisavad silmitsi nõrkuste valdkonnas uuringuid läbi viivad isikud, sealhulgas probleeme, mis on seotud nende võimaliku kriminaalvastutusega.** [...] Liikmesriigid peaksid määrama koordineerimise ülesannet täitma CSIRTi, kes hakkab vastavalt vajadusele tegutsema vahendajana teavitavate üksuste ja IKT-toodete või -teenuste tootjate ja osutajate vahel. CSIRTi koordinaatori ülesanded peaks eelkõige olema teha kindlaks asjaomased üksused ja võtta nendega ühendust, toetada teavitavaid üksusi, pidada läbirääkimisi avalikustamise tähtaegade üle ning hallata mitut organisatsiooni mõjutavate nõrkustega seonduvat tegevust (mitut osapoolt puudutavate nõrkuste **koordineeritud** avalikustamine). Kui **teatatud** nõrkus **võib oluliselt mõjutada üksusi** [...] rohkem kui ühes liikmesriigis, peaksid [...] määratud CSIRTid **vajaduse korral** tegema CSIRTide võrgustiku raames koostööd.

(30) Juurdepääs õigele ja õigeaegsele teabele IKT-tooteid ja -teenuseid mõjutavate nõrkuste kohta aitab küberturvalisuse alast riskijuhtimist tõhustada. Seega on nõrkuste kohta avalikult kättesaadava teabe allikad oluline vahend üksuste ja nende kasutajate, aga ka riiklike pädevate asutuste ja CSIRTide jaoks. Sel põhjusel peaks ENISA looma nõrkuste registri, kus elutähtsad ja olulised üksused ja nende tarnijad, aga ka käesoleva direktiivi kohaldamisalast välja jäävad üksused **või määratud CSIRTid** võivad vabatahtlikult avalikustada nõrkusi ning esitada nende kohta teavet, mis võimaldab kasutajatel võtta asjakohaseid leevendusmeetmeid.

(31) Sarnaseid nõrkuste registreid või andmebaase on ka juba loodud, kuid neid majutavad ja haldavad üksused, mille asukoht ei ole liidus. ENISA hallatav Euroopa nõrkuste register tagaks suurema läbipaistvuse nõrkuste ametlikule avalikustamisele eelneva avalikustamisprotsessiga seoses ning suurendaks vastupidavusvõimet sarnaste teenuste osutamist mõjutavate häirete või katkestuste korral. Et vältida topelttööd ja püüda saavutada võimalikult suures ulatuses vastastikune täiendavus, peaks ENISA uurima võimalust sõlmida struktureeritud koostöö lepinguid kolmandate riikide jurisdiktsioonides tegutsevate sarnaste registritega. **Eelkõige peaks ENISA uurima võimalust teha tihedat koostööd ühiste nõrkuste ja riskide (CVE) süsteemi käitajatega, sealhulgas võimalust saada CVE juurnumeratsiooniasutuseks.**

(32) **Koostöörühm peaks jätkuvalt toetama ja hõlbustama strateegilist koostööd ja teabevahetust ning suurendama usaldust ja kindlustunnet liikmesriikide vahel.** Koostöörühm peaks iga kahe aasta järel koostama tööprogrammi kava, mis hõlmab rühma eesmärkide ja ülesannete täitmiseks võetavaid meetmeid. Käesoleva direktiivi alusel vastu võetava esimese programmi ajakava tuleks viia kooskõlla direktiivi (EL) 2016/1148 alusel vastu võetud viimase programmi ajakavaga, et vältida töörühma töö võimalikku häirimist.

(33) Juhenddokumentide väljatöötamisel peaks koostöörühm järjepidevalt kaardistama riiklikud lahendused ja kogemused, hindama koostöörühma tegevuse tulemuste mõju riiklikele lähenemisviisidele, arutama rakendamisega seotud probleeme ning sõnastama konkreetsed soovitused olemasolevate eeskirjade tõhusamaks rakendamiseks.

(34) Koostöörühm peaks jääma paindlikuks foorumiks ning suutma reageerida muutuvatele ja uutele poliitilistele prioriteetidele ja probleemidele, võttes seejuures arvesse vahendite kättesaadavust. Ta peaks korraldama korrapäraseid ühiskoosolekuid asjaomaste erasektori sidusrühmadega kogu liidust, et arutada rühma tegevust ja koguda teavet esilekerkivate poliitiliste probleemide kohta. Et tõhustada koostööd liidu tasandil, peaks rühm kaaluma võimalust kutsuda oma töös osalema küberturvalisuse alase poliitika kujundamisega seotud liidu asutused ja ametid, näiteks küberkuritegevuse vastase võitluse Euroopa keskuse (EC3), Euroopa Liidu Lennundusohutusameti (EASA) ja Euroopa Liidu Kosmoseprogrammi Ameti (EUSPA).

(35) Pädevatel asutustel ja CSIRTidel peaks olema võimalus koostöö parandamiseks osaleda teiste liikmesriikidega ametnike vahetamise programmis. Pädevad asutused peaksid võtma vajalikud meetmed, et võimaldada teiste liikmesriikide ametnikel täita vastuvõtva pädeva asutuse tegevuses tulemuslikku rolli.

(35a) CSIRTide võrgustik peaks jätkuvalt aitama suurendada kindlustunnet ja usaldust ning edendama kiiret ja tõhusat operatiivkoostööd liikmesriikide vahel. Et tõhustada operatiivkoostööd liidu tasandil, peaks CSIRTide võrgustik kaaluma võimalust kutsuda oma töös osalema küberturvalisuse alase poliitika kujundamisega seotud asjaomased liidu asutused ja ametid, näiteks Europoli.

(36) [...]

(36a) Selleks et hõlbustada käesoleva direktiivi selliste sätete tõhusat rakendamist nagu nõrkuste haldamine, küberturvalisuse riskijuhtimine, teatamismeetmed ja teabevahetuse kord, võivad liikmesriigid teha koostööd kolmandate riikidega ja võtta meetmeid, mida peetakse sel eesmärgil asjakohaseks, sealhulgas teabevahetust ohtude, intsidentide, nõrkuste, vahendite ja meetodite, taktika, võtete ja menetluste, küberkriiside ohjamisega seotud valmisoleku ja õppuste, koolituste, usalduse loomise ja struktureeritud teabevahetuse korra kohta. Sellised koostöölepingud peaksid olema kooskõlas andmekaitset käsitlevate liidu õigusaktidega.

(37) Liikmesriigid peaksid aitama luua soovituses (EL) 2017/1584 ette nähtud küberturvalisuse kriisidele reageerimise ELi raamistikku olemasolevate koostöövõrgustike, eelkõige **Euroopa** küberkriisi kontaktasutuste võrgustiku (EU-CyCLONe), CSIRTide võrgustiku ja koostöörühma tegevuse kaudu. EU-CyCLONe ja CSIRTide võrgustik peaksid tegema koostööd menetluskorra alusel, milles määratakse kindlaks kõnealuse koostöö üksikasjad, **ning vältima ülesannete dubleerimist**. EU-CyCLONe menetluskorras tuleks täpsustada võrgustiku toimimist puudutavad üksikasjad, muu hulgas rollid, koostööviisid, teiste asjaomaste osalejatega suhtlemine, teabevahetuse vormid ja kommunikatsioonivahendid. Liidu **poliitilise** tasandi kriisiohje puhul peaksid asjaomased osapooled lähtuma kriisidele poliitilist reageerimist käsitlevast ELi integreeritud korrast (IPCR). Komisjon peaks rakendama üldise kiirhoiatussüsteemi ARGUS kõrgetasemelise valdkondadevahelise kriisikoordineerimise menetlusprotsessi. Kui kriisil on oluline välispoliitiline või ühise julgeoleku- ja kaitsepoliitikaga (ÜJKP) seotud mõõde, tuleks käivitada Euroopa välisteenistuse kriisidele reageerimise mehhanism.

(37a) EU-CyCLONe peaks ulatuslike küberturvalisuse intsidentide ja kriiside korral toimima tehnilise ja poliitilise tasandi vahelise vahendava võrgustikuna. See peaks tõhustama koostööd operatiivtasandil, tuginedes CSIRTide võrgustiku järeldustele ja kasutades oma suutlikkust koostada ulatuslike intsidentide ja kriiside mõjuanalüüs ning toetada otsuste tegemist poliitilisel tasandil. ELi institutsioonid, organid ja asutused peaksid määrama EU-CyCLONe liikmeks ulatuslike julgeolekuintsidentide ja -kriiside ohjamise eest vastutava pädeva asutuse.

(38) [...]

(39) [...]

(39a) Vastutus võrgu- ja infosüsteemi turvalisuse tagamise eest lasub suurel määral elutähtsatel ja olulistel üksustel. Tuleks edendada ja arendada riskijuhtimiskultuuri, mis hõlmab riskihindamist ja ähvardavatele riskidele vastavate turvameetmete rakendamist.

(40) Riskijuhtimismeetmed peaksid **võtma arvesse, mil määral üksus võrgu- ja infosüsteemidest sõltub,** ning hõlmama meetmeid intsidendiriskide tuvastamiseks, intsidentide vältimiseks, tuvastamiseks ja käsitlemiseks ning nende mõju leevendamiseks. Võrgu- ja infosüsteemide turvalisus peaks hõlmama salvestatavate, edastatavate ja töödeldavate andmete turvalisust.

(40a) Kuna võrgu- ja infosüsteemide turvalisust ähvardavatel ohtudel võib olla erinev põhjus, kohaldatakse käesoleva direktiiviga kõiki ohte hõlmavat lähenemisviisi, mis hõlmab võrgu- ja infosüsteemide ning nende füüsilise keskkonna kaitsmist selliste sündmuste eest nagu vargus, tulekahju, üleujutus, telekommunikatsiooni- või elektrikatkestused või loata füüsiline juurdepääs üksuse teabe- ja teabetöötlusrajatistele ning nende kahjustamine ja häirimine, mis võib ohustada võrgu- ja infosüsteemides salvestatud, edastatud või töödeldud andmete või nende süsteemide pakutavate või nende kaudu juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust või konfidentsiaalsust. Seepärast peaksid riskijuhtimismeetmed käsitlema ka füüsilist turvalisust ja keskkonnaohutust, hõlmates meetmeid üksuse võrgu- ja infosüsteemide kaitsmiseks süsteemirikete, inimliku eksimuse, pahatahtliku tegevuse või loodusnähtuste eest kooskõlas Euroopa või rahvusvaheliselt tunnustatud standarditega, näiteks ISO 27000 seerias sisalduvate standarditega. Sellega seoses peaksid üksused oma riskijuhtimismeetmete osana käsitlema ka personali turvalisust ja kehtestama asjakohased juurdepääsukontrollipoliitika meetmed. Need meetmed peaksid olema kooskõlas direktiiviga XXXX [CER-direktiiv].

(40b) Kui puuduvad asjakohased määruse (EL) 2019/881 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavad, võivad liikmesriigid nõuda üksustelt sertifitseeritud IKT-toodete, -teenuste ja -protsesside kasutamist või sertifikaadi saamist olemasolevate riiklike küberturvalisuse kavade alusel, et täita käesoleva direktiivi kohaseid küberturvalisuse riskijuhtimisnõudeid.

(41) Et vältida elutähtsatele ja olulistele üksustele ebaproportsionaalse finants- ja halduskoormuse panemist, peaksid küberturvalisuse riskijuhtimisnõuded olema proportsionaalsed asjaomase võrgu- ja infosüsteemi puhul esineva riski taseme suhtes ning lähtuma meetmete tehnilisest tasemest **ja nende rakendamise kulust**. **Nõuetekohaselt tuleks arvesse võtta ka üksuse suurust, samuti intsidentide esinemise tõenäosust ja nende raskusastet.**

(41a) Regulatiivse koormuse vähendamiseks peaks keskmise suurusega, väikeste ja mikroettevõtjate suhtes kehtestatavad küberturvalisuse riskijuhtimismeetmete rakendamise nõuded olema põhimõtteliselt leebemad, välja arvatud juhul, kui kriitilisuse kriteeriumidest või riiklikust riskihindamisest tulenevalt oleks vaja rangemaid nõudeid, eelkõige üksuste puhul, mis vastavad käesolevas direktiivis sätestatud kriitilisuse kriteeriumidele.

(42) Elutähtsad ja olulised üksused peaksid tagama oma tegevuses kasutatavate võrgu- ja infosüsteemide turvalisuse. Nende puhul on eelkõige tegemist privaatsete võrgu- ja infosüsteemidega, mida haldavad kas üksuse enda IT-töötajad või mille turvalisusega seotud teenused ostetakse sisse. Käesoleva direktiivi kohaseid küberturvalisuse riskijuhtimis- ja teatamisnõudeid tuleks kohaldada asjaomaste elutähtsate ja oluliste üksuste suhtes olenemata sellest, kas nad hooldavad oma võrgu- ja infosüsteeme ise või tellivad hooldusteenuse väljast.

(42aa) Võttes arvesse nende piiriülest olemust, tuleks domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite ja tippdomeenide domeeninimede registreerimise teenuseid osutavate üksuste, pilvandmetöötlusteenuse, andmekeskusteenuse ja sisulevivõrguteenuse ning hallatud teenuse osutajate ja hallatud turbetarnijate suhtes kohaldada liidu tasandil suuremat ühtlustamist. Seetõttu tuleks küberturvalisuse meetmete rakendamise hõlbustamiseks võtta vastu rakendusakt.

(43) Üksuse tarneahelast ja tarnijasuhetest tulenevate küberturvalisuse riskidega tegelemine on eriti oluline, kui võtta arvesse selliste intsidentide esinemise sagedust, mille puhul üksused on langenud küberrünnete ohvriks ning pahatahtlikud osalejad on suutnud kahjustada üksuse võrgu- ja infosüsteemide turvalisust, kasutades ära kolmandate isikute tooteid ja teenuseid mõjutavaid nõrkusi. Seepärast peaksid üksused hindama ja arvesse võtma oma tarnijate ja teenuseosutajate toodete üldist kvaliteeti ja küberturvalisuse tavasid, sealhulgas nende turvalise arenduse korda.

(44) Teenuseosutajate seas mängivad intsidentide tuvastamisel ja neile reageerimisel üksuste jaoks eriti olulist tugirolli turbetarnijad sellistes teenusevaldkondades nagu intsidentidele reageerimine, läbistustestimine, turvarevisjon ja konsultatsioonid. Mainitud turbetarnijad on aga olnud ka ise küberrünnete sihtmärgiks ja kuna nad on operaatorite tegevusse tihedalt lõimitud, kaasneb nendega suurem küberturvalisuse risk. Seega peaksid üksused olema turbetarnija valimisel iseäranis hoolikad.

(44a) Riiklikud pädevad asutused võivad oma järelevalveülesannete täitmisel kasutada ka selliseid küberturvalisuse teenuseid nagu turvaauditid ja läbistustestimine või intsidentidele reageerimine. Selleks, et aidata üksustel ja riiklikel pädevatel asutustel valida kvalifitseeritud ja usaldusväärseid küberturvalisuse teenuse osutajaid, peaks komisjon koostöörühma ja ENISA abiga kaaluma võimalust taotleda vastavalt määruse (EL) 2019/881 artiklile 48 Euroopa küberturvalisuse sertifitseerimise kavasid.

(45) Üksused peaksid tähelepanu pöörama ka sellistele küberturvalisuse riskidele, mis tulenevad nende suhtlemisest ja suhetest teiste sidusrühmadega laiemas ökosüsteemis. Täpsemalt peaksid üksused võtma asjakohaseid meetmeid tagamaks, et nende koostöö akadeemiliste ja teadusasutustega toimub kooskõlas nende küberturvalisuse eeskirjadega ning et selles koostöös järgitakse turvalise juurdepääsu ja levitamisega seotud üldisi häid tavasid ja täpsemalt intellektuaalomandi kaitsega seotud tavasid. Võttes arvesse andmete olulisust ja väärtust üksuste tegevuse jaoks, peaksid üksused kolmandate isikute osutatavatele andmete teisendamise ja analüüsi teenustele tuginedes võtma kõik asjakohased küberturvalisuse meetmed.

(46) Et peamisi tarneahelariske põhjalikumalt käsitleda ja aidata käesoleva direktiivi kohaldamisalasse hõlmatud sektorites tegutsevatel üksustel tarneahela ja tarnijatega seotud küberturvalisuse riske nõuetekohaselt juhtida, peaks asjaomaseid riiklikke asutusi koondav koostöörühm tegema koostöös komisjoni ja ENISAga koordineeritud valdkonnapõhise tarneahela riskihindamise (nagu tehti juba 5G-võrkude kohta vastavalt soovitusele (EL) 2019/534 (5G-võrkude küberturvalisuse kohta)[21]), seades eesmärgiks määratleda iga sektori jaoks kriitilise tähtsusega IKT-teenused, -süsteemid või -tooted, asjaomased ohud ja nõrkused.

[21] Komisjoni 26. märtsi 2019. aasta soovitus (EL) 2019/534 5G-võrkude küberturvalisuse kohta (ELT L 88, 29.3.2019, lk 42).

(47) Tarneahela riskide hindamisel tuleks asjaomase sektori omadusi silmas pidades võtta arvesse nii tehnilisi kui ka (kus asjakohane) mittetehnilisi tegureid, sealhulgas neid, mis on määratletud soovituses (EL) 2019/534, 5G-võrkude küberturvalisusega seotud ELi koordineeritud riskihindamist käsitlevas aruandes ja koostöörühma kokkulepitud ELi 5G-küberturvalisuse meetmepaketis. Et teha kindlaks tarneahelad, mille suhtes peaks kohaldama koordineeritud riskihindamist, tuleks arvesse võtta järgmisi kriteeriume: i) kui suurel määral elutähtsad ja olulised üksused kindlaid kriitilise tähtsusega IKT-teenuseid, -süsteeme või -tooteid kasutavad ning nendele tuginevad; ii) kindlate kriitilise tähtsusega IKT-teenuste, -süsteemide või -toodete asjakohasus kriitiliste või tundlike funktsioonide (sh isikuandmete töötlemine) täitmisel; iii) alternatiivsete IKT-teenuste, -süsteemide või -toodete kättesaadavus; iv) IKT-teenuste, -süsteemide või -toodete tarneahela kui terviku vastupidavusvõime häirivate sündmuste korral või v) kui tegemist on kujunemisjärgus IKT-teenuste, -süsteemide või -toodetega, siis nende potentsiaalne tulevane tähtsus üksuste tegevuse jaoks.

(48) Et ühtlustada üldkasutatavate elektroonilise side võrkude või üldkasutatavate elektroonilise side teenuste pakkujatele ja usaldusteenuse osutajatele pandud võrgu- ja infosüsteemide turvalisusega seotud õiguslikke kohustusi ning võimaldada kõnealustel üksustel ja nende vastavatel pädevatel asutustel käesoleva direktiiviga kehtestatud õigusraamistikust (sh riskide ja intsidentidega seotud tegevuste eest vastutav CSIRT, pädevate asutuste ja organite osalemine koostöörühma tegevuses ja CSIRTide võrgustik) kasu saada, tuleks need üksused hõlmata käesoleva direktiivi kohaldamisalasse. Seega tuleks Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014[22] ning Euroopa Parlamendi ja nõukogu direktiivi (EL) 2018/1972[23] sätted, mis on seotud turva- ja teatamisnõu**ete** kehtestamisega kõnealust liiki üksuste suhtes, kehtetuks tunnistada.

---

[22] 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).

[23] Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (ELT L 321, 17.12.2018, lk 36).

(48a) Käesolevas direktiivis sätestatud turvakohustusi tuleks käsitada täiendusena nõuetele, mis on kehtestatud usaldusteenuse osutajatele määrusega (EL) nr 910/2014 (eIDASe määrus). Usaldusteenuse osutajatelt tuleks nõuda, et nad võtaksid kõik asjakohased ja proportsionaalsed meetmed, et juhtida oma teenuseid ohustavaid riske, sealhulgas seoses klientide ja kolmandate isikutega, ning teataksid käesoleva direktiivi kohaselt turvaintsidentidest. Sellised turva- ja aruandluskohustused peaksid hõlmama osutatava teenuse füüsilist kaitset. Määruse (EL) 910/2014 artiklit 24 kohaldatakse jätkuvalt.

(48aa) Liikmesriigid võivad määrata usaldusteenuste eest vastutavateks pädevateks asutusteks eIDASe järelevalveasutused, et tagada praeguste tavade jätkamine ning kasutada eIDASe määruse kohaldamisel saadud teadmisi ja kogemusi. Kui see roll antakse mõnele teisele asutusele, peaksid käesoleva direktiivi kohased riiklikud pädevad asutused tegema tihedalt ja aegsasti koostööd, vahetades asjakohast teavet, et tagada tulemuslik järelevalve ja see, et usaldusteenuse osutajad täidavad käesolevas direktiivis ja määruses [XXXX/XXXX] sätestatud nõudeid.

Kui see on asjakohane, peaks käesoleva direktiivi kohane riiklik pädev asutus viivitamata teavitama eIDASe järelevalveasutust igast teatatud olulisest küberohust või -intsidendist, mis mõjutab usaldusteenuseid, ning igast juhtumist, mille puhul usaldusteenuse osutaja ei täida käesoleva direktiivi nõudeid. Aruandluseks võivad liikmesriigid vajaduse korral kasutada ühtset kontaktpunkti, mis on loodud selleks, et tagada ühine ja automaatne intsidentidest teatamine nii eIDASe järelevalveasutusele kui käesoleva direktiivi kohasele pädevale asutusele. Teatamiskohustust käsitlevad normid ei tohiks piirata määruse (EL) 2016/679 ning Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ[24] kohaldamist.

[24] Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37).

(49) [...] **Asjakohasel juhul ja selleks, et vältida tarbetute häirete põhjustamist, tuleks olemasolevaid riiklikke suuniseid, mis on vastu võetud direktiivi (EL) 2018/1972 artiklis 40 ja artiklis 41 sätestatud turvameetmetega seotud normide ülevõtmiseks**, **võtta arvesse ülevõtmise korras, mida liikmesriigid kohaldavad seoses käesoleva direktiiviga, kasutades seega direktiivi (EL) 2018/1972 (küberturvalisuse riskijuhtimise meetmete ja intsidentidest teatamise kohta) raames saadud teadmisi ja oskusi. ENISA võib koostada üldkasutatavate elektroonilise side võrkude või üldkasutatavate elektrooniliste side teenuste pakkujate jaoks ka turva- ja aruandlusnõudeid käsitlevad suunised, et hõlbustada ühtlustamist ja üleminekut ning minimeerida häireid. Liikmesriigid võivad anda elektroonilise side eest vastutava pädeva asutuse rolli riigi reguleerivatele asutustele, et tagada praeguste tavade jätkamine ning kasutada direktiivi (EL) 2018/1972 kohaldamisel saadud teadmisi ja kogemusi.**

(50) Võttes arvesse, et numbrivaba isikutevahelise side teenuste olulisus kasvab, tuleb tagada, et ka nende teenuste kohta kehtiksid asjakohased, nende eripära ja majanduslikku tähtsust arvestavad turvalisusnõuded. Selliste teenuste osutajad peaksid seega samuti tagama riskitasemele vastava võrgu- ja infosüsteemide turvalisuse taseme. Arvestades et numbrivaba isikutevahelise side teenuste pakkujatel puudub tavaliselt tegelik kontroll võrkudes signaalide edastamise üle, võib selliste teenuste riske pidada mõnes mõttes väiksemaks kui tavapäraste elektroonilise side teenuste puhul esinevaid riske. Sama kehtib ka selliste isikutevahelise side teenuste kohta, mille puhul kasutatakse numbreid ja millel puudub tegelikult kontroll signaaliedastuse üle.

(51) Siseturg sõltub interneti toimimisest rohkem kui kunagi varem. Peaaegu kõigi elutähtsate ja oluliste üksuste teenused sõltuvad interneti kaudu pakutavatest teenustest. Et tagada elutähtsate ja oluliste üksuste pakutavate teenuste sujuv osutamine, on oluline, et üldkasutatavate elektroonilise side võrkude, näiteks interneti tuumikvõrkude või merealuste sidekaablite puhul rakendataks asjakohaseid küberturvalisuse meetmeid ja et nendega seotud intsidentidest teatataks.

(52) [...] Asjakohasel juhul peaksid üksused teavitama oma teenuse kasutajaid kindlatest [...] meetmetest, mida viimased saavad võtta, et **vähendada neile tõsistest küberohtudest tulenevaid riske**. **Üksused peaksid asjakohasel juhul ja eelkõige juhul, kui oluline küberoht võib realiseeruda, teavitama sellest ka oma teenuse kasutajaid ning pädevaid asutusi või CSIRTe.** Nõue teavitada kasutajaid sellistest ohtudest ei vabasta üksusi kohustusest võtta oma kulul viivitamata sobivaid meetmeid, et võimalikud turvaohud kõrvaldada ja taastada teenuse turvalisuse tavapärane tase. Selline **küber**[...]ohte käsitlev teave tuleks kasutajatele esitada tasuta.

(53) Täpsemalt peaksid üldkasutatavate elektroonilise side võrkude pakkujad või üldkasutatavate elektroonilise side teenuste osutajad teavitama teenuse saajaid konkreetsetest ja tõsistest küberohtudest ning meetmetest, mida viimased saavad oma side turvalisuse kaitseks võtta, kasutades näiteks teatavat liiki tarkvara või krüpteerimistehnoloogiaid.

(54) Artikli 18 kohaldamiseks tuleks elektroonilise side võrkude ja teenuste turvalisuse tagamiseks edendada krüpteerimist ja eelkõige otspunktkrüpteerimist ning teha see vajaduse korral selliste teenuste ja võrkude pakkujatele kohustuslikuks kooskõlas turbe ja privaatsuse vaikesätteid ja sisseprojekteerimist käsitlevate põhimõtetega. Otspunktkrüpteerimise kasutamine tuleks ühildada liikmesriikide volitustega tagada nende oluliste julgeolekuhuvide ja avaliku julgeoleku kaitse ning võimaldada kuritegude uurimist, avastamist ja nende eest vastutusele võtmist kooskõlas liidu õigusega. Lahendused, mis võimaldavad otspunktkrüpteeritud sidekanali kaudu edastatavale teabele seaduslikku juurdepääsu, peaksid võimaldama säilitada krüpteerimise tõhususe side privaatsuse ja turvalisuse kaitsmisel, tagades samas tõhusa reageerimise kuritegevusele.

(55) Käesolevas direktiivis sätestatakse intsidentidest teatamise kaheetapiline lähenemisviis, et saavutada õige tasakaal kahe ülesande vahel: ühelt poolt kiire teatamine, mis aitab vähendada intsidentide võimalikku levikut ja võimaldab üksustel abi otsida, ning teiselt poolt põhjalik aruandlus, mis võimaldab saada üksikutest intsidentidest väärtuslikke õppetunde ja suurendada aja jooksul üksikute ettevõtete ja tervete sektorite vastupanuvõimet küberohtude suhtes. Üksustelt, kes saavad intsidendist teadlikuks, tuleks nõuda esialgse teatise esitamist 24 tunni jooksul ja lõpparuande esitamist hiljemalt ühe kuu pärast. Esialgne teade peaks sisaldama üksnes teavet, mis on pädevate asutuste intsidendist teavitamiseks hädavajalik ja mis võimaldab üksusel vajaduse korral abi hankida. Sellises teates tuleks (kui see on asjakohane) märkida, kas intsident on eeldatavasti põhjustatud ebaseaduslikust või pahatahtlikust tegevusest. Liikmesriigid peaksid tagama, et kõnealuse esialgse teate esitamise nõudega seoses ei võetaks teavitava üksuse ressursse intsidentide käsitlemisega seotud tegevuste arvelt, mis peaksid olema prioriteetsed. Et vältida olukorda, kus intsidentidest teatamise kohustuse tõttu suunatakse vahendid ümber intsidentide lahendamise arvelt või kannatab mainitud tegevus muul moel, peaksid liikmesriigid samuti ette nägema, et nõuetekohaselt põhjendatud juhtudel ja kokkuleppel pädevate asutuste või CSIRTiga võib asjaomane üksus esialgse teatamise 24-tunnisest tähtajast ja lõpparuande esitamise ühekuulisest tähtajast kõrvale kalduda.

(55a) Ennetav lähenemisviis küberohtudele on küberturvalisuse riskijuhtimise oluline osa, mis peaks võimaldama pädevatel asutustel tulemuslikult vältida küberohtude muutumist tegelikeks intsidentideks, mis võivad põhjustada märkimisväärset materiaalset või mittemateriaalset kahju. Seetõttu on olulistest küberohtudest teatamine esmatähtis.

(56) Elutähtsad ja olulised üksused on sageli olukorras, kus kindlast intsidendist tuleb eri õigusaktides sätestatud teatamiskohustuste tõttu teavitada eri asutusi. Sellised olukorrad tekitavad lisakoormust ning võivad põhjustada ebakindlust kõnealuste teadete vormi ja menetluskorraga seoses. Seda silmas pidades ning selleks, et turvaintsidentidest teatamist lihtsustada, [...] **võiksid** liikmesriigid luua *ühtse kontaktpunkti* kõigi käesoleva direktiivi ja muude liidu õigusaktide, näiteks määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ alusel nõutavate teadete edastamise tarbeks. ENISA peaks koostöös koostöörühmaga töötama välja ühised teatevormid ja vastavad suuniseid, mis lihtsustaksid ja ühtlustaksid liidu õigusega nõutava teabe esitamist ning vähendaksid ettevõtjate koormust.

(57) Liikmesriigid peaksid liidu õigusega kooskõlas olevast kriminaalmenetluskorrast lähtuvalt julgustama elutähtsaid ja olulisi üksusi, kes kahtlustavad, et intsident on seotud liidu või liikmesriigi õiguses määratletud raske kuriteoga, teatama nendest arvatavalt raske kuritegevusega seotud intsidentidest asjakohastele õiguskaitseasutustele. Kus asjakohane, võiksid EC3 ja ENISA hõlbustada eri liikmesriikide pädevate asutuste ja õiguskaitseasutuste vahelise koostöö koordineerimist, ilma et see mõjutaks Europoli suhtes kohaldatavaid isikuandmete kaitse eeskirju.

(58) Sageli on intsidendi tagajärjeks isikuandmete kaitstuse rikkumine. Sellega seoses peaksid pädevad asutused tegema koostööd ning vahetama teavet kõigis asjakohastes küsimustes andmekaitseasutuste ja järelevalveasutustega vastavalt direktiivile 2002/58/EÜ.

(59) Domeeninimede ja registreerimisandmete (nn WHOIS-andmed) täpsete ja täielike andmebaaside pidamine ning kõnealustele andmetele seadusliku juurdepääsu võimaldamine on oluline, et tagada domeeninimede süsteemi turvalisus, stabiilsus ja vastupanuvõime, mis omakorda aitab saavutada küberturvalisuse ühtlaselt kõrget taset liidus. Kui töötlemine hõlmab isikuandmete töötlemist, tuleb seda teha kooskõlas liidu andmekaitsealaste õigusaktidega.

(60) Nende andmete kättesaadavus ja nendele õigeaegse juurdepääsu võimaldamine avaliku sektori asutustele, sealhulgas liidu või liikmesriigi õiguse alusel tegutsevatele pädevatele asutustele kuritegude ennetamiseks, uurimiseks või nende eest vastutusele võtmiseks, CERTidele, CSIRTidele ning elektroonilise side võrkude ja teenuste pakkujatele nende klientide andmetega seoses ning nende klientide nimel tegutsevatele küberturvalisuse tehnoloogiate ja teenuste pakkujatele on oluline domeeninimede süsteemi kuritarvitamise ennetamiseks ja selle vastu võitlemiseks, eelkõige küberturvalisuse intsidentide ennetamiseks, tuvastamiseks ja lahendamiseks. Selline juurdepääs tuleks võimaldada kooskõlas liidu andmekaitseõigusega, niivõrd kui see juurdepääs puudutab isikuandmeid.

(61) Et tagada domeeninimede registreerimise täpsete ja täielike andmete kättesaadavus, peaksid tippdomeenide registrid ja tippdomeenide domeeninimede registreerimise teenuseid osutavad üksused (nn registripidajad) koguma domeeninimede registreerimise andmeid ning tagama nende tervikluse ja kättesaadavuse. **Registreerimisandmete puhul peaksid üksused eelkõige kontrollima registreerija nime ja e-posti aadressi.** [...] Tippdomeenide registrid ja tippdomeenide domeeninimede registreerimise teenuseid osutavad üksused **peaksid** kehtestama põhimõtted ja menetluskorra täpsete ja täielike registreerimisandmete kogumiseks ja säilitamiseks ning samuti ebatäpsete registreerimisandmete vältimiseks ja parandamiseks kooskõlas liidu andmekaitse-eeskirjadega.

(62) Tippdomeenide registrid ja neile domeeninimede registreerimise teenuseid osutavad üksused peaksid tegema üldsusele kättesaadavaks liidu andmekaitse-eeskirjade kohaldamisalast välja jäävad domeeninimede registreerimise andmed, näiteks juriidiliste isikutega seotud andmed[25]. Tippdomeenide registrid ja tippdomeenide domeeninimede registreerimise teenuseid osutavad üksused peaksid kooskõlas liidu andmekaitseõigusega võimaldama õiguspärast juurdepääsu õigustatud taotlejatele ka füüsiliste isikutega seotud domeeninimede registreerimise andmetele. Liikmesriigid peaksid tagama, et tippdomeenide registrid ja neile domeeninimede registreerimise teenuseid osutavad üksused vastaksid [...] **põhjendamatu viivituseta domeeninimede registreerimise andmete taotlusele, mille on esitanud õigustatud taotleja, näiteks liidu või liikmesriigi õiguse alusel tegutsev pädev asutus riikliku julgeoleku ja kriminaalõiguse valdkonnas, või CSIRTid.** Tippdomeenide registrid ja domeeninimede registreerimise teenuseid osutavad üksused peaksid kehtestama põhimõtted ja menetluskorra registreerimisandmete avaldamiseks ja avalikustamiseks ning kinnitama seejuures teenustaseme kokkulepped õigustatud juurdepääsu taotlejate juurdepääsutaotluste käsitlemiseks. Juurdepääsumenetlus võib hõlmata ka liidese, portaali või muu tehnilise vahendi kasutamist, mis aitab tagada tõhusa süsteemi registreerimisandmete taotlemiseks ja nendele juurdepääsu võimaldamiseks. **Liikmesriigid peaksid tagama, et igasugune juurdepääs domeeninimede registreerimise andmetele (nii isiku- kui ka isikustamata andmetele) on tasuta.** Et toetada siseturul ühtsete tavade juurutamist, võib komisjon võtta vastu selliseid menetlusi käsitlevad suunised, ilma et sellega piirataks Euroopa Andmekaitsenõukogu pädevust **kooskõlas mitut sidusrühma hõlmava kogukonna välja töötatud rahvusvaheliste standarditega ja neid täiendades**.

[25] Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 põhjendus 14:„Ükski isik ei peaks nõudma käesoleva määrusega ette nähtud kaitset seoses selliste andmete töötlemisega, mis puudutavad juriidilisi isikuid, eelkõige juriidiliste isikutena asutatud ettevõtjaid, sealhulgas juriidilise isiku nime ja vormi ning kontaktandmeid“.

(63) [...] **K**äesoleva direktiivi kohased elutähtsad ja olulised üksused peaksid kuuluma selle liikmesriigi jurisdiktsiooni alla, kus nad oma teenuseid osutavad. **Käesoleva direktiivi I lisa punktides 1–7 ja 10 osutatud üksused, I lisa punktis 8 ja II lisa punktides 1–5 osutatud usaldusteenuse osutajad ja Interneti vahetuspunkti teenuse osutajad peaksid kuuluma selle liikmesriigi jurisdiktsiooni alla, kus asub nende tegevuskoht.** Kui üksus osutab teenuseid **või tal on tegevuskoht** rohkem kui ühes liikmesriigis, peaks ta kuuluma eraldi ja samal ajal iga kõnealuse liikmesriigi jurisdiktsiooni alla. Nende liikmesriikide pädevad asutused peaksid tegema koostööd, üksteist vastastikku abistama ja vajaduse korral võtma ühiseid järelevalvemeetmeid. **Kui liikmesriigid otsustavad jurisdiktsiooni teostada, peaksid nad vältima seda, et käesolevas direktiivis sätestatud kohustuste rikkumise puhul karistataks ühe ja sama tegevuse eest rohkem kui üks kord.**

(64) Võttes arvesse domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, **tippdomeenide domeeninimede registreerimise teenuseid osutavate üksuste**, sisulevivõrgu pakkujate ning pilvandmetöötlusteenuse, andmekeskusteenuse ja digiteenuse osutajate teenuste ja tegevuse piiriülest iseloomu, peaks asjaomased üksused kuuluma vaid ühe liikmesriigi jurisdiktsiooni alla. Üksus peaks kuuluma selle liikmesriigi jurisdiktsiooni alla, kus on tema peamine tegevuskoht liidus. Käesoleva direktiivi kohaldamisel eeldatakse tegevuskohakriteeriumi puhul tulemuslikku tegevust püsiva korra alusel. Sellise korra õiguslik vorm (filiaal või juriidilisest isikust tütarettevõtja) ei ole antud juhul määrav tegur.

Selle kriteeriumi täidetus ei tohiks sõltuda võrgu- ja infosüsteemide füüsilisest paiknemisest teatavas kohas; ainuüksi selliste süsteemide olemasolu ja kasutamine peamist tegevuskohta ei näita ning seega pole need peamise tegevuskoha kindlakstegemisel otsustavad kriteeriumid. Peamine tegevuskoht peaks olema see asukoht liidus, kus tehakse **valdavalt** otsuseid küberturvalisuse riskijuhtimise meetmete kohta. Tavaliselt on see liidu asukoht, kus asub ettevõtja peakontor. Kui **kohta, kus selliseid otsuseid valdavalt tehakse, ei ole võimalik kindlaks määrata või kui** kõnealuseid otsuseid ei tehta liidus, tuleks peamise tegevuskohana käsitada seda liikmesriiki, mille tegevuskohas on üksusel liidus kõige rohkem töötajaid. Kui teenuseid osutab kontsern, tuleks kontserni peamiseks tegevuskohaks lugeda kontrolliva ettevõtja peamine tegevuskoht.

(64a) Kui üldkasutatavate elektroonilise side võrkude või üldkasutatavate elektroonilise side teenuste pakkuja osutab rekursiivset domeeninimede süsteemi teenust üksnes internetiühenduse teenuse osana, peaks asjaomane üksus kuuluma kõigi nende liikmesriikide jurisdiktsiooni alla, kus tema teenuseid osutatakse.

(64aa) Selleks, et tagada selge ülevaade domeeninimede süsteemi teenuse osutajatest, tippdomeeninimede registritest, tippdomeenide domeeninimede registreerimise teenuseid osutavatest üksustest, sisulevivõrgu pakkujatest ning pilvandmetöötlusteenuse, andmekeskusteenuse ja digiteenuse osutajatest, kes pakuvad kogu liidus teenuseid, mis kuuluvad käesoleva direktiivi kohaldamisalasse, peaks ENISA looma selliste üksuste kohta registri ja seda registrit haldama, võttes aluseks liikmesriikidelt saadud teatised, mida liikmesriigid esitavad asjakohasel juhul oma riiklike enesest teavitamise mehhanismide kaudu. Tagamaks, et teave, mis tuleks kõnealusesse registrisse kanda, on täpne ja täielik, peaksid liikmesriigid esitama ENISA-le oma riiklikes registrites nende üksuste kohta olemasoleva teabe. ENISA ja liikmesriigid peaksid võtma meetmeid, et hõlbustada selliste registrite koostalitlusvõimet, tagades samal ajal konfidentsiaalse või salastatud teabe kaitse.

(65) Kui liidus pakub teenuseid domeeninimede süsteemi teenuse, tippdomeeninimede registri, sisulevivõgu, pilvandmetöötlusteenuse, andmekeskusteenuse või digiteenuse osutaja, kelle asukoht pole liidus, peaks ta määrama endale esindaja. Otsustamaks, kas kõnealune üksus pakub teenuseid liidu piires, tuleks kindlaks teha, kas on ilmne, et ta kavatseb osutada teenuseid ühes või mitmes liikmesriigis asuvatele isikutele. Viidatud kavatsuse kinnitamiseks ei piisa vaid faktist, et liidus pääseb juurde digiteenuse osutaja või vahendaja veebisaidile, e-posti aadressile või muudele kontaktandmetele, ega faktist, et kasutatakse üksuse asukohariigiks olevas kolmandas riigis üldiselt kasutatavat keelt. Samas võivad asjaolud, nagu ühes või mitmes liikmesriigis üldiselt kasutatava keele või vääringu kasutamine, millega kaasneb võimalus tellida teenuseid selles teises keeles, või liidus paiknevate klientide või kasutajate mainimine, viidata sellele, et üksus kavatseb pakkuda teenuseid liidus. Esindaja peaks tegutsema üksuse nimel ning pädevatel asutustel või CSIRTidel peaks olema võimalik esindajaga ühendust võtta. Üksus peaks kirjaliku volitusega sõnaselgelt määrama esindaja tema nimel tegutsema seoses käesoleva direktiivi kohaste kohustustega, sealhulgas intsidentidest teatamise kohustusega.

(66) Kui käesoleva direktiivi sätete alusel vahetatakse või edastatakse või jagatakse muul moel teavet, mida käsitatakse riikliku või liidu õiguse alusel salastatud teabena, tuleks järgida asjaomaseid salastatud teabe käitlemise erieeskirju.

(67) Kuna küberohud on muutumas komplekssemaks ja keerukamaks, sõltuvad head tuvastus- ja ennetusmeetmed suuresti ohte ja nõrkusi puudutava teabe korrapärasest jagamisest üksuste vahel. Teabe jagamine aitab suurendada teadlikkust küberohtudest ja see omakorda suurendab üksuste suutlikkust hoida ära ohtude muutumist tegelikeks intsidentideks ning võimaldab üksustel intsidentide mõju paremini piirata ja neil tõhusamini taastuda. Liidu tasandi suuniste puudumise tõttu on sellist teadmuse jagamist pärssinud mitu tegurit, eelkõige ebakindlus konkurentsi ja vastutust käsitlevate normide järgimisega seoses.

(68) Üksuseid tuleks julgustada kasutama kollektiivselt individuaalseid teadmisi ja praktilisi kogemusi strateegilisel, taktikalisel ja operatiivsel tasandil, et suurendada suutlikkust küberohte õigesti hinnata ja jälgida, end nende eest kaitsta ja neile reageerida. Seega on vaja võimaldada luua liidu tasandil vabatahtliku teabevahetuse mehhanismid. Selleks peaksid liikmesriigid aktiivselt toetama ja julgustama ka käesoleva direktiivi kohaldamisalast välja jäävaid asjaomaseid üksusi selliseid teabejagamise mehhanisme kasutama. Neid mehhanisme tuleks rakendada täielikus kooskõlas liidu konkurentsi- ja andmekaitsenormidega.

(69) Isikuandmete töötlemist [...] **elutähtsate ja oluliste üksuste ning** turvatehnoloogiate ja -teenuste pakkujate poolt sellisel määral, mis on rangelt vajalik ja proportsionaalne võrgu- ja infoturbe tagamiseks, [...] **võib pidada vajalikuks, et täita juriidilist kohustust, või** käsitada töötlemisena asjaomase vastutava töötleja õigustatud huvi alusel, nagu on osutatud määruses (EL) 2016/679. See [...] **võiks** hõlmata meetmeid, mis on seotud intsidentide ennetamise, avastamise, analüüsimise ja lahendamisega, meetmeid, millega suurendatakse teadlikkust kindlatest küberohtudest, võimaldatakse teabevahetust nõrkuste vähendamise ja koordineeritud avalikustamise kontekstis, samuti vabatahtlikku teabevahetust seoses kõnealuste intsidentide, küberohtude ja nõrkuste, rikkeindikaatorite, taktikate, meetodite ja menetluskorra, küberturvalisuse hoiatussüsteemide ja konfiguratsioonivahenditega. Sellised meetmed võivad nõuda [...] **erinevat** liiki isikuandmete töötlemist, **näiteks:** IP-aadressid, URLid, domeeninimed ja meiliaadressid. **Isikuandmete töötlemine pädevate asutuste, ühtsete kontaktpunktide ja CSIRTide poolt tuleks sätestada liikmesriigi õigusega ning seda tuleks pidada vajalikuks juriidilise kohustuse täitmiseks või avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks, nagu on osutatud määruse (EL) 2016/679 artikli 6 lõike 1 punktis c või e.**

(69a) Liikmesriikide õigusaktides võib sätestada normid, mis võimaldavad pädevatel asutustel, ühtsetel kontaktpunktidel ja CSIRTidel töödelda kooskõlas määruse (EL) 2016/679 artikliga 9 isikuandmete eriliike sellisel määral, mis on elutähtsate ja oluliste üksuste võrgu- ja infosüsteemide turvalisuse tagamiseks rangelt vajalik ja proportsionaalne, nähes eelkõige ette sobivad ja konkreetsed meetmed füüsiliste isikute põhiõiguste ja huvide kaitsmiseks, sealhulgas tehnilised piirangud seoses selliste andmete taaskasutamisega, ning kõrgeima turvataseme ja privaatsuse säilitamise meetmetega, nagu pseudonümiseerimine või krüpteerimine, kui anonüümimine võib märkimisväärselt mõjutada soovitud eesmärgi saavutamist.

(70) Et tugevdada järelevalvevolitusi ja -meetmeid, mis aitavad tagada nõuete tõhusat täitmist, tuleks käesoleva direktiiviga ette näha minimaalsed järelevalvemeetmed ja -vahendid, mille abil [...] **saavad** pädevad asutused **teha** elutähtsate ja oluliste üksuste üle järelevalvet. Lisaks tuleks käesoleva direktiiviga kehtestada eraldi järelevalvekord elutähtsate ja oluliste üksuste jaoks, et tagada kohustuste õiglane tasakaal nii üksuste kui ka pädevate asutuste suhtes. Seega tuleks elutähtsate üksuste suhtes kohaldada täiemahulist järelevalvekorda, mis hõlmab nii eelkontrolli (*ex-ante*-kontroll) kui ka järelkontrolli (*ex-post*-kontroll), ja oluliste üksuste suhtes lihtsustatud järelevalvekorda, mis hõlmab üksnes järelkontrolli. Viimasel juhul ei peaks üksused **olema kohustatud** süstemaatiliselt dokumenteerima küberturvalisuse riskijuhtimise nõuete täitmist. Pädevad asutused peaksid rakendama järelevalve tegemisel tagantjärele reageerimisel põhinevat lähenemisviisi ja seega ei peaks neil olema üldist kohustust nende üksuste üle järelevalvet teha. **Oluliste üksuste järelkontrolli võib algatada lähtuvalt tõenditest või mis tahes vihjetest või teabest, millele pädevate asutuste tähelepanu juhitakse ja mille puhul pädevad asutused leiavad, et need viitavad käesolevas direktiivis sätestatud kohustuste võimalikule täitmata jätmisele. Selliseid tõendeid, vihjeid või teavet võivad pädevatele asutustele esitada näiteks muud asutused, üksused, kodanikud, meedia või muud allikad, see võib olla avalikult kättesaadav teave või tuleneda muust pädevate asutuste tegevusest oma ülesannete täitmisel.**

(70bis) Eelkontrolli teostamisel peaks pädevatel asutustel olema võimalik otsustada proportsionaalselt, kuidas nad prioriseerivad järelevalvemeetmete ja nende käsutuses olevate vahendite kasutamist. See tähendab, et pädevad asutused võivad sellise prioriseerimise üle otsustada lähtuvalt järelevalvemeetoditest, mis peaksid järgima riskipõhist lähenemisviisi. Täpsemalt võiksid sellised meetodid sisaldada kriteeriume või võrdlusaluseid oluliste üksuste liigitamiseks riskikategooriatesse ning vastavaid järelevalvemeetmeid ja -vahendeid, mida soovitatakse iga riskikategooria kohta, nagu kohapealsete kontrollide või sihipäraste turvaauditite või turvalisuse kontrollide kasutamine, sagedus või liik, taotletava teabe liik ja selle teabe üksikasjalikkuse aste. Selliste järelevalvemeetoditega võivad kaasneda ka tööprogrammid ning neid võidakse korrapäraselt hinnata ja läbi vaadata, sealhulgas seoses vahendite jaotamise ja vajadustega.

(70bisa) Avaliku halduse üksuste puhul tuleks järelevalvevolitusi teostada kooskõlas riiklike raamistike ja õiguskorraga. Liikmesriikidel peaks olema võimalus otsustada kehtestada nende üksuste suhtes asjakohaseid, proportsionaalseid ja tõhusaid järelevalve- ja täitemeetmeid.

(70bisaa) Teatavate küberturvalisuse riskijuhtimismeetmete järgimise tõendamiseks võivad liikmesriigid nõuda elutähtsatelt ja olulistelt üksustelt määruse (EL) nr 910/2014 kohaste kvalifitseeritud usaldusteenuste või teavitatud e-identimise süsteemide kasutamist.

(71) Et tagada jõustamise tõhusus, tuleks koostada käesolevas direktiivis sätestatud küberturvalisuse riskijuhtimis- ja aruandluskohustuste rikkumise eest kohaldatavate halduskaristuste miinimumloetelu ning kehtestada selliste karistuste jaoks kogu liidus selge ja ühtne raamistik. Nõuetekohast tähelepanu tuleks pöörata rikkumise laadile, raskusastmele ja kestusele, tegelikult põhjustatud kahjule või võimalikule kahjule (mis oleks võinud kaasneda), rikkumise tahtlikkuse või hooletuse aspektile, kahju vältimiseks või leevendamiseks võetud meetmetele, vastutuse tasemele või varasematele asjaomastele rikkumistele, pädeva asutusega tehtava koostöö tasemele ning muule raskendavale või leevendavale tegurile. Karistuste, sealhulgas trahvide määramise suhtes tuleks kooskõlas liidu õiguse üldpõhimõtete ja Euroopa Liidu põhiõiguste hartaga kohaldada asjakohaseid menetluslikke kaitsemeetmeid, sealhulgas tõhusat õiguskaitset ja nõuetekohast menetluskorda.

(71bis) Sätted, mis käsitlevad üksuses teatavaid kohustusi täitva füüsilise isiku vastutust, juhul kui ta rikub oma kohustust tagada käesolevas direktiivis sätestatud kohustuste täitmine, ei nõua, et liikmesriigid peaksid tagama sellise rikkumisega kolmandatele isikutele tekitatud kahju eest kriminaal- või tsiviilvastutuse.

(72) Et tagada käesolevas direktiivis sätestatud kohustuste tõhus täitmine, peaks igal pädeval asutusel olema õigus määrata haldustrahve või taotleda nende määramist.

(73) Kui haldustrahvid määratakse ettevõtjale, tuleks ettevõtja määratlemisel lähtuda ELi toimimise lepingu artiklites 101 ja 102 toodud määratlusest. Kui trahvid määratakse isikule, kes ei ole ettevõtja, peaks järelevalveasutus sobiva trahvisumma määramisel arvesse võtma üldist sissetulekutaset selles liikmesriigis ja isiku majanduslikku olukorda. See, kas ja mil määral tuleks kohaldada trahve avaliku sektori asutustele, peaks olema liikmesriikide otsustada. Haldustrahvi määramine ei mõjuta pädevate asutuste muude volituste rakendamist ega muude karistuste kohaldamist, mis on sätestatud käesolevat direktiivi ülevõtvates siseriiklikes õigusnormides.

(74) **Liikmesriigid** [...] **võivad** kehtestada kriminaalkaristuste normid, mida kohaldatakse käesolevat direktiivi ülevõtvate siseriiklike õigusnormide rikkumise korral. Kriminaalkaristuste määramine selliste liikmesriigi normide rikkumise eest ja seotud halduskaristuste määramine ei tohiks aga põhjustada põhimõtte *ne bis in idem* (Euroopa Kohtu tõlgenduses) rikkumist.

(75) Kui käesoleva määrusega ei ole halduskaristusi ühtlustatud või vajaduse korral muudel juhtudel, näiteks käesolevas direktiivis sätestatud kohustuste raske rikkumise korral, peaksid liikmesriigid rakendama süsteemi, mis näeb ette tõhusad, proportsionaalsed ja heidutavad karistused. Selliste karistuste laad (kriminaal- või halduskaristus) tuleks määrata liikmesriigi õigusega.

(76) Et täiendavalt suurendada käesoleva direktiiviga kehtestatud kohustuste rikkumise korral kohaldatavate karistuste tõhusust ja heidutavat mõju, peaks pädevatel asutustel olema õigus kohaldada karistusi, millega peatatakse elutähtsa üksuse osutatavate mõnede või kõigi teenuste sertifikaat või luba ning keelatakse füüsilisel isikul ajutiselt juhtimisülesannete täitmine. Selliseid karistusi tuleks kohaldada alati proportsionaalselt rikkumise raskusastmega ning iga juhtumi konkreetseid asjaolusid (sh seda, kas rikkumine oli tahtlik või tulenes ettevaatamatusest, ning seda, milliseid meetmeid kahju vältimiseks või vähendamiseks võeti) silmas pidades, võttes arvesse karistuste raskusastet ja mõju üksuste tegevusele ning seeläbi ka nende tarbijatele. Selliseid karistusi tuleks kohaldada üksnes *ultima ratio* põhimõttel, st alles pärast seda, kui muud käesolevas direktiivis sätestatud asjakohased täitemeetmed on ammendatud, ja ainult seni, kuni üksused, kelle suhtes neid kohaldatakse, võtavad vajalikud meetmed puuduste kõrvaldamiseks või täidavad pädeva asutuse need nõuded, millega seoses karistusi kohaldati. Selliste karistuste määramise suhtes tuleks kooskõlas liidu õiguse üldpõhimõtete ja Euroopa Liidu põhiõiguste hartaga kohaldada asjakohaseid menetluslikke kaitsemeetmeid, sealhulgas tõhusat õiguskaitset ja nõuetekohast menetluskorda.

(76bis) Tõhusa järelevalve ja jõustamise tagamiseks, eelkõige piiriülese mõõtmega juhtudel, peaksid liikmesriigid, kes on saanud vastastikuse abi taotluse, võtma taotluse ulatuses asjakohaseid järelevalve- ja täitemeetmeid asjaomase üksuse suhtes, kes osutab teenuseid või kellel on võrgu- ja infosüsteem nende territooriumil.

(77) Käesoleva direktiiviga tuleks kehtestada kooskõlas määrusega (EL) 2016/679 pädevate asutuste ja järelevalveasutuste vahelise koostöö eeskirjad isikuandmetega seotud rikkumiste käsitlemiseks.

(78) Käesoleva direktiivi eesmärk peaks olema tagada kõrgel tasemel vastutus küberturvalisuse riskijuhtimismeetmete rakendamise ja teatamiskohustuse täitmise eest organisatsioonide tasandil. Seega peaksid käesoleva direktiivi kohaldamisalasse kuuluvate üksuste juhtorganid küberturvalisuse riskijuhtimismeetmed kinnitama ja tegema järelevalvet nende rakendamise üle.

(79) Kehtestada tuleks vastastikuse [...] **õppe süsteem**, **et aidata tugevdada vastastikust usaldust ning õppida headest tavadest ja kogemustest**, mis võimaldaks liikmesriikide määratud [...] **ekspertidel vahetada** küberturvalisuse alaste eeskirjade [...] **rakendamisega seotud kogemusi** [...]. **Vastastikuse õppe süsteemi rakendamisel tuleks erilist tähelepanu pöörata sellele, et see ei tekitaks asjaomaste liikmesriikide asutustele tarbetut ja ebaproportsionaalset koormust. Komisjon peaks uurima kõiki võimalusi, et tagada asjakohasel juhul vastastikuse õppe raames toimuvate lähetuste korraldamisega kaasnevate võimalike kulude katmine. Lisaks peaks vastastikuse õppe süsteem võtma arvesse sarnaste mehhanismide, näiteks CSIRTide võrgustiku vastastikuse hindamise süsteemi tulemusi, looma lisaväärtust ja vältima dubleerimist. Vastastikuse õppe süsteemi rakendamine ei tohiks piirata konfidentsiaalse ja salastatud teabe kaitset käsitlevate riiklike või liidu õigusaktide kohaldamist. Enne vastastikuse õppe voorude algust võivad liikmesriigid korraldada asjakohaste aspektide puhul enesehindamise. Koostöörühma taotlusel võib ENISA anda vajaduse korral suuniseid enesehindamise ja asjakohaste vormide kohta. Liikmesriigid võivad otsustada teha oma aruanded üldsusele kättesaadavaks.**

(80) [...]

(81) Et tagada ühetaolised tingimused käesoleva direktiivi selliste asjaomaste sätete rakendamiseks, mis käsitlevad koostöörühma toimimiseks vajalikku menetluskorda, riskijuhtimismeetmete tehnilisi aspekte või intsidentidest teatamise andmeid, vormi ja korda, **niisuguste üksuste liike, mis peavad kasutama kindlaid sertifitseeritud IKT-tooteid, -teenuseid ja -protsesse**, tuleks komisjonile anda rakendamisvolitused. Neid volitusi tuleks teostada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011[26].

(82) Komisjon peaks huvitatud isikutega konsulteerides käesoleva direktiivi sätted regulaarselt läbi vaatama, eelkõige selleks, et teha kindlaks, kas neid on vaja muuta seoses ühiskondlike, poliitiliste, tehnoloogiliste ja turutingimuste muutumisega.

[26] Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrus (EL) nr 182/2011, millega kehtestatakse eeskirjad ja üldpõhimõtted, mis käsitlevad liikmesriikide läbiviidava kontrolli mehhanisme, mida kohaldatakse komisjoni rakendamisvolituste teostamise suhtes (ELT L 55, 28.2.2011, lk 13).

(83) Kuna käesoleva direktiivi eesmärki – tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus – ei suuda liikmesriigid eraldi tegutsedes täielikult saavutada ning kuna seda on võimalik meetme toimet arvestades paremini saavutada liidu tasandil tegutsedes, 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.

(84) Käesolevas direktiivis järgitakse Euroopa Liidu põhiõiguste hartas tunnustatud põhiõigusi ja põhimõtteid, eelkõige õigust eraelu ja edastatavate sõnumite puutumatusele, isikuandmete kaitset, ettevõtlusvabadust, õigust omandile ning õigust tõhusale õiguskaitsevahendile kohtus ja õiglasele kohtulikule arutamisele. Käesolevat direktiivi tuleks rakendada kooskõlas nimetatud õiguste ja põhimõtetega,

ON VASTU VÕTNUD KÄESOLEVA DIREKTIIVI:

I PEATÜKK

Üldsätted

Artikkel 1

Reguleerimisese

1. Käesolevas direktiivis sätestatakse meetmed, mille eesmärk on tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, **et parandada siseturu toimimis**t.

2. Selle eesmärgi saavutamiseks tehakse käesoleva direktiiviga järgmist:

   a) pannakse liikmesriikidele kohustus võtta vastu riiklikud küberturvalisuse strateegiad, määrata pädevad riiklikud asutused, ühtsed kontaktpunktid ja küberturbe intsidentide lahendamise üksused (CSIRTid);

   b) pannakse **I** [...] **ja II lisas** osutatud [...] liiki üksustele küberturvalisuse alased riskijuhtimis- ja teatamiskohustused;

   c) kehtestatakse küberturvalisuse alase teabevahetusega seotud **normid ja** kohustused.

Artikkel 2

Kohaldamisala

1. Käesolevat direktiivi kohaldatakse sellist liiki avaliku ja erasektori üksuste suhtes, mis on [...] **loetletud I ja II lisas ning mis vastavad keskmise suurusega ettevõtjaks** liigitamise ülemmääradele komisjoni soovituse 2003/361/EÜ[27] tähenduses või ületavad neid. **Käesoleva direktiivi kohaldamisel ei kohaldata kõnealuse soovituse lisa artikli 3 lõiget 4 ja artikli 6 lõike 2 teist ja kolmandat lõiku.**

2. [...] **Olenemata lõikes 1 osutatud üksuste suurusest kohaldatakse käesolevat direktiivi siiski ka juhul, kui**: [...]

   a) teenuseid osutab mõni järgmistest üksustest:

      i) I lisa punktis 8 osutatud üldkasutatavate elektroonilise side võrkude pakkuja või üldkasutatavate elektroonilise side teenuste pakkuja**;**

      ii) I lisa punktis XX osutatud kvalifitseeritud usaldusteenuse osutaja;

      iii) I lisa punktis XX osutatud kvalifitseerimata usaldusteenuse osutaja;

      iv) I lisa punktis 8 osutatud tippdomeeninimede register [...];

   b) [...]

[27] 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).

c) üksus, kes [...] **osutab üksi liikmesriigis teatavat teenust, mis on oluline elutähtsa ühiskondliku või majandustegevuse säilitamise seisukohast**;

d) üksus, kelle osutatava teenuse võimalik katkemine avaldaks [...] **olulist** mõju avalikule ohutusele, avalikule julgeolekule või rahvatervisele;

e) üksus, kelle osutatava teenuse võimalik katkemine võib tekitada [...] **olulisi** süsteemseid riske, eriti kui see puudutab sektoreid, kus sellisel katkemisel võib olla piiriülene mõju;

f) [...];

g) üksus on määratletud kriitilise tähtsusega üksusena vastavalt Euroopa Parlamendi ja nõukogu direktiivile (EL) XXXX/XXXX[28] [kriitilise tähtsusega üksuste vastupanuvõime direktiiv] **[**või kriitilise tähtsusega üksusega samaväärse üksusena vastavalt kõnealuse direktiivi artiklile 7**]**.

2a. **Olenemata nende suurusest, kohaldatakse käesolevat direktiivi ka keskvalitsuse avaliku halduse üksuste suhtes, mida tunnustatakse liikmesriigis siseriikliku õiguse kohaselt ja millele on osutatud I lisa punktis 9. Liikmesriigid võivad sätestada, et käesolevat direktiivi kohaldatakse ka piirkondlikul ja kohalikul tasandi avaliku halduse üksuste suhtes.**

[28] [lisada täielik pealkiri ja ELTs avaldamise viide, kui see on teada]

3. [...]

Käesolev direktiiv ei piira liikmesriikide kohustusi kaitsta riiklikku julgeolekut ega nende õigust kaitsta muid riigi põhifunktsioone, sealhulgas riigi territoriaalse terviklikkuse tagamist ja avaliku korra säilitamist.

3a. 1) Käesolevat direktiivi ei kohaldata:

a) üksuste suhtes, mis ei kuulu liidu õiguse kohaldamisalasse, ja igal juhul kõikide üksuste suhtes, kes tegutsevad peamiselt kaitse, riikliku julgeoleku, avaliku julgeoleku või õiguskaitse valdkonnas, olenemata sellest, milline üksus neid tegevusi teostab ning kas tegemist on avaliku sektori või erasektori üksusega, ilma et see piiraks punkti 2 kohaldamist;

b) üksuste suhtes, kes tegutsevad kohtute, parlamentide või keskpankade valdkonnas.[...]

2) kui avaliku halduse üksuste tegevus nendes valdkondades on ainult üks osa nende üldisest tegevusest, jäetakse nad käesoleva direktiivi kohaldamisalast täielikult välja.

3aa. Käesolevat direktiivi ei kohaldata:

i) liidu õiguse kohaldamisalast välja jäävate üksuste tegevuse suhtes ning igal juhul igasuguse riikliku julgeoleku või riigikaitsega seotud tegevuse suhtes, olenemata sellest, milline üksus neid tegevusi teostab ja kas tegemist on avaliku sektori või erasektori üksusega;

ii) kohtute, parlamentide, keskpankade ja avaliku julgeoleku valdkonnas tegutsevate üksuste, sealhulgas avaliku halduse üksuste tegevuse suhtes, kes tegelevad õiguskaitsega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil.

3aaa. Käesolevas direktiivis sätestatud kohustused ei hõlma sellise teabe edastamist, mille avalikustamine on vastuolus liikmesriikide oluliste riikliku julgeoleku, avaliku julgeoleku või riigikaitse huvidega.

3aaaa. Käesolev direktiiv ei piira isikuandmete kaitset käsitleva liigu õiguse, eelkõige määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ kohaldamist.

3b. Käesolevat direktiivi ei kohaldata üksuste suhtes, kes ei kuulu Euroopa Parlamendi ja nõukogu määruse (EL) XXXX/XXXX [DORA määrus] kohaldamisalasse vastavalt selle määruse artikli 2 lõikele 4.

4. Käesolev direktiiv ei piira [...][29] Euroopa Parlamendi ja nõukogu direktiivide 2011/93/EL[30] ja 2013/40/EL[31] kohaldamist.

5. Ilma et see piiraks ELi toimimise lepingu artikli 346 kohaldamist, tuleks teavet, mis on liidu ja siseriiklike õigusnormide, näiteks ärisaladust käsitlevate õigusnormide kohaselt konfidentsiaalne, **vahetada käesoleva direktiivi kohaselt** komisjoni ja teiste asjakohaste asutustega ainult siis, kui selline teabevahetus on vajalik käesoleva direktiivi kohaldamiseks. Vahetada võib ainult teavet, mis on teabevahetuse eesmärki arvestades oluline ja proportsionaalne. Teavet vahetades peab tagama asjaomase teabe konfidentsiaalsuse ning elutähtsate ja oluliste üksuste turvalisuse ja ärihuvide kaitse.

---

29 [...]

30 Euroopa Parlamendi ja nõukogu 13. detsembri 2011. aasta direktiiv 2011/93/EL, mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning lasteporno vastast võitlust ja mis asendab nõukogu raamotsuse 2004/68/JSK (ELT L 335, 17.12.2011, lk 1).

31 Euroopa Parlamendi ja nõukogu 12. augusti 2013. aasta direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK (ELT L 218, 14.8.2013, lk 8).

Artikkel 2bis

Elutähtsad ja olulised üksused

1. Üksustest, mille suhtes käesolevat direktiivi kohaldatakse, loetakse esmatähtsateks üksusteks järgmisi:

i) käesoleva direktiivi I lisa punktides 1–8a ja 10 sätestatud liiki üksused, mis ületavad komisjoni soovituses 2003/361/EÜ määratletud keskmise suurusega ettevõtjateks liigitamise ülemmäära;

ii) artikli 2 lõike 2 punkti a alapunktis i osutatud keskmise suurusega üksused;

iii) käesoleva direktiivi artikli 2 lõike 2 punkti a alapunktides ii ja iv osutatud üksused, olenemata nende suurusest;

iv) käesoleva direktiivi artikli 2 lõike 2 punktis g ja artikli 2 lõikes 2a osutatud üksused, olenemata nende suurusest;

v) üksused, mille liikmesriigid on enne käesoleva direktiivi jõustumist määratlenud oluliste teenuste operaatoritena vastavalt direktiivile (EL) 2016/1148 või siseriiklikule õigusele, kui nende üksuste asutajaks on liikmesriigid;

vi) komisjoni soovituses 2003/361/EÜ määratletud keskmise suurusega ettevõtjaks liigitamise ülemmäära ületavad II lisas sätestatud liiki üksused, mida liikmesriigid peavad esmatähtsateks vastavalt artikli 2 lõike 2 punktides c–e osutatud kriteeriumidele;

vii) keskmise suurusega üksused komisjoni soovituse 2003/361/EÜ tähenduses, mida liikmesriigid peavad esmatähtsateks vastavalt artikli 2 lõike 2 punktides c–e osutatud kriteeriumidele;

viii) mikro- või väikeüksused komisjoni soovituse 2003/361/EÜ tähenduses, mis on sätestatud lõike 2 punkti a alapunktis i või mis on kindlaks määratud vastavalt käesoleva artikli lõike 2 punktidele c–e ning mida liikmesriigid määratlevad esmatähtsatena riiklike riskihindamiste põhjal.

2. Üksustest, mille suhtes käesolevat direktiivi kohaldatakse, loetakse olulisteks üksusteks järgmisi:

i) käesoleva direktiivi I lisas sätestatud üksused, mis liigitatakse keskmise suurusega ettevõtjateks komisjoni soovituse 2003/361/EÜ tähenduses, ja II lisas sätestatud üksused, mis vastavad keskmise suurusega ettevõtjaks liigitamise ülemmääradele komisjoni soovituse 2003/361/EÜ[32] tähenduses või ületavad neid;

ii) käesoleva direktiivi artikli 2 lõike 2 punktis iii osutatud üksused, olenemata nende suurusest;

iii) artikli 2 lõike 2 punkti a alapunktis i osutatud väike- ja mikroüksused;

iv) väike- ja mikroüksused, mida liikmesriigid määratlevad vastavalt artikli 2 lõike 2 punktidele c–e oluliste üksustena.

---

32 **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)**.

Artikkel 2a

Teavitusmehhanismid

1. **Liikmesriigid võivad kehtestada riikliku enesest teavitamise mehhanismi, millega nõutakse, et kõik käesoleva direktiivi kohaldamisalasse kuuluvad üksused teataksid käesoleva direktiivi kohastele pädevatele asutustele või liikmesriikide poolt selleks määratud asutustele vähemalt oma nime, aadressi, kontaktandmed ning sektori, milles nad tegutsevad, või osutatava teenuse liigi ning vajaduse korral loetelu liikmesriikidest, kus nad osutavad käesoleva direktiivi kohaldamisalasse kuuluvaid teenuseid.**

2. **Liikmesriigid esitavad komisjonile seoses artikli 2 lõike 2 punktide b-e kohaselt kindlaks määratud üksustega vähemalt asjakohase teabe, mis käsitleb kindlaks määratud üksuste arvu, sektorit, millesse need üksused kuuluvad, või nende üksuste poolt osutatavate teenuste liiki, nagu on sätestatud lisades, ning artikli 2 lõike 2 erisätet (erisätteid), mille alusel need üksused kindlaks määrati [12 kuud pärast käesoleva direktiivi ülevõtmise tähtaega]**. Liikmesriigid vaatavad [...] **selle teabe** läbi [...] korrapäraselt vähemalt iga kahe aasta järel ning vajaduse korral ajakohastavad loetelu.

Artikkel 2b

Valdkondlikud liidu õigusaktid

1. Kui valdkondlikes liidu **õigusaktides** [...] nõutakse elutähtsatelt või olulistelt üksustelt küberturvalisuse riskijuhtimismeetmete võtmist või [...] **olulistest** intsidentidest või [...] küberohtudest teatamist ning kui need nõuded on vähemalt samaväärsed käesolevas direktiivis sätestatud vastavate kohustustega, **ei kohaldata niisuguste üksuste suhtes** käesoleva direktiivi asjakohaseid sätted, **sealhulgas VI peatükis sätestatud järelevalve- ja täitmise tagamise sätteid**. **Kui valdkondlikud liidu õigusaktid ei hõlma kõiki konkreetse sektori üksusi, mis kuuluvad käesoleva direktiivi kohaldamisalasse, kohaldatakse nende valdkondlike sätetega hõlmamata üksuste suhtes jätkuvalt käesoleva direktiivi asjakohaseid sätteid.**

2. Käesoleva artikli lõikes 1 osutatud nõudeid loetakse mõjult samaväärseks käesolevas direktiivis sätestatud kohustustega, kui vastava valdkondliku liidu õigusaktiga on ette nähtud viivitamatu ning vajaduse korral automaatne ja otsene juurdepääs käesoleva direktiivi kohaste pädevate asutuste või kindlaks määratud CSIRTide teadetele intsidentide kohta, ning juhul, kui:

a) küberturvalisuse riskijuhtimismeetmed on mõjult vähemalt samaväärsed käesoleva direktiivi artikli 18 lõigetes 1 ja 2 sätestatud meetmetega; või

b) olulistest intsidentidest teatamise nõuded on mõjult vähemalt samaväärsed artikli 20 lõigetes 1–6 sätestatud nõuetega.

3. Komisjon vaatab korrapäraselt läbi, kuidas kohaldatakse käesoleva artikli lõigetes 1 ja 2 sätestatud, liidu õigusaktide valdkondlike sätetega seotud samaväärse mõju nõuet. Komisjon konsulteerib nende korrapäraste läbivaatamiste ettevalmistamisel koostöörühma ja ENISAga.

Artikkel 3

Minimaalne ühtlustamine

Ilma et see piiraks liikmesriikide muid liidu õigusest tulenevaid kohustusi, võivad liikmesriigid [...] **käesoleva direktiiviga hõlmatud valdkondades** võtta vastu või säilitada sätted, millega tagatakse kõrgem küberturvalisuse tase.

Artikkel 4

Mõisted

Käesolevas direktiivis kasutatakse järgmisi mõisteid:

1) „võrgu- ja infosüsteem“ –

a) elektroonilise side võrk direktiivi (EÜ) 2018/1972 artikli 2 punktis 1 sätestatud tähenduses;

b) seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub mõne programmi kohaselt digiandmete automaatne töötlemine;

c) digitaalsed andmed, mida salvestatakse, töödeldakse, saadakse päringutega või edastatakse punktidega a ja b hõlmatud komponentide poolt nende töö, kasutamise, kaitsmise või hooldamise jaoks;

2) „võrgu- ja infosüsteemide turvalisus“ – võrgu- ja infosüsteemi võime panna teatava kindlusega vastu mis tahes [...] **sündmusele**, mis **võib seada** ohtu salvestatavate, edastatavate või töödeldavate andmete või [...] võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse;

2a) „elektroonilise side teenused“ – elektroonilise side [...] teenused direktiivi (EÜ) 2018/1972 artikli 2 punktis 4 sätestatud tähenduses;

3) „küberturvalisus“ – küberturvalisus Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881[33] artikli 2 punktis 1 sätestatud tähenduses;

4) „riiklik **küberturvalisuse** strateegia“ – liikmesriigi ühtne raamistik, [...] **millega nähakse ette suunised strateegiliste eesmärkide ja prioriteetide saavutamiseks küberturvalisuse valdkonnas** kõnealuses liikmesriigis;

5) „intsident“ – mis tahes sündmus, mis ohustab või kahjustab salvestatavate, edastatavate või töödeldavate andmete või [...] võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust ja konfidentsiaalsust;

5a) „ulatuslik küberturvalisuse intsident“ – intsident, millel on märkimisväärne mõju vähemalt kahele liikmesriigile või millega kaasnev häire ületab liikmesriigi võime sellele reageerida.

---

[33] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

6) „intsidendi käsitlemine“ – kõik toimingud ja menetlused, mis toetavad intsidendi tuvastamist, analüüsimist, ohjeldamist ja lahendamist;

6a) „risk“ – intsidendist tingitud kahju või häire võimalus, mida väljendatakse sellise kahju või häire ulatust ja kõnealuse intsidendi esinemise tõenäosust kajastava kombineeritud näitajana;

7) „küberoht“ – küberoht määruse (EL) 2019/881 artikli 2 punktis 8 sätestatud tähenduses;

7a) **„oluline küberoht“ – küberoht, mille tehniliste näitajate põhjal võib eeldada, et see võib oluliselt kahjustada üksuse või selle kasutajate võrgu- ja infosüsteeme, tekitades märkimisväärset materiaalset või mittemateriaalset kahju;**

8) „nõrkus“ – [...] IKT-vara või -süsteemi nõrkus, tundlikkus või viga, mida küberohu tekitaja võib ära kasutada;

8a) „ohuolukord“ – sündmus, mis oleks võinud kahjustada üksuse või selle kasutajate võrgu- ja infosüsteeme, kuid mille täielik realiseerumine suudeti edukalt ära hoida;

9) „esindaja“ – liidus asuv füüsiline või juriidiline isik, kes on sõnaselgelt määratud tegutsema väljaspool liitu asuva i) I lisa punktis 8 osutatud domeeninimede süsteemi teenuse osutaja (DNS), tippdomeeninimede (TLD) registri, pilvandmetöötlusteenuse osutaja, andmekeskusteenuse osutaja või sisulevivõrgu pakkuja või ii) II lisa punktis [...] **6** osutatud üksuse nimel ja kelle poole võib liikmesriigi pädev asutus või CSIRT pöörduda seoses kõnealuse üksuse käesolevast direktiivist tulenevate kohustustega;

10) „standard“ – standard Euroopa Parlamendi ja nõukogu määruse (EÜ) 1025/2012[34] artikli 2 punktis 1 sätestatud tähenduses;

11) „tehniline spetsifikatsioon“ – tehniline spetsifikatsioon määruse (EL) nr 1025/2012 artikli 2 punktis 4 sätestatud tähenduses;

12) „interneti vahetuspunkt (IXP)“ – võrguvahend, mis võimaldab rohkem kui kahe sõltumatu võrgu (autonoomse süsteemi) omavahelist ühendamist, eelkõige selleks, et hõlbustada internetiliikluse vahetamist; IXP võimaldab üksnes autonoomsete süsteemide omavahelist ühendamist; IXP ei nõua ühegi kahe osaleva autonoomse süsteemi vahel kulgeva internetiliikluse kulgemist mõne kolmanda autonoomse süsteemi kaudu, ei muuda sellist liiklust ega sekku sellesse mingil muul viisil;

13) „domeeninimede süsteem“ – hierarhiline ja hajus nimesüsteem, mis võimaldab lõppkasutajatel jõuda internetis teenuste ja ressurssideni;

14) „domeeninimede süsteemi teenuse osutaja“ – üksus, kes osutab [...] domeeninime rekursiivse või autoriteetse lahendamise teenust **kasutamiseks kolmandatele isikutele, välja arvatud juurnimeserveritele** [...] ;

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

15) „tippdomeeninimede register“ – üksus, kellele on delegeeritud kindel tippdomeen ja kes vastutab selle tippdomeeni haldamise eest, sealhulgas tippdomeeni all domeeninimede registreerimise eest ja tippdomeeni tehnilise toimimise eest, sealhulgas nimeserverite käitamise, andmebaaside hooldamise ning nimeserverite vahel tippdomeeni tsoonifailide jaotamise eest, **välistades võimaluse, et registrid kasutaksid tippdomeenimesid üksnes oma tarbeks;**

15a) „tippdomeeni domeeninimede registreerimise teenuseid osutavad üksused“ – tippdomeeninimede registrid, tippdomeenide registripidajad ja registripidajate esindajad, näiteks edasimüüjad ja proksiteenuste osutajad;

16) „digiteenus“ – teenus Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/1535[35] artikli 1 lõike 1 punktis b sätestatud tähenduses;

16a) „usaldusteenused“ – usaldusteenused määruse (EL) nr 910/2014 artikli 3 punktis 16 sätestatud tähenduses;

[35] Euroopa Parlamendi ja nõukogu 9. septembri 2015. aasta direktiiv (EL) 2015/1535, millega nähakse ette tehnilistest eeskirjadest ning infoühiskonna teenuste eeskirjadest teatamise kord (ELT L 241, 17.9.2015, lk 1).

16b) „kvalifitseeritud usaldusteenuse osutaja“ – kvalifitseeritud usaldusteenuse osutaja määruse (EL) nr 910/2014 artikli 3 punktis 20 sätestatud tähenduses;

17) „internetipõhine kauplemiskoht“ – digiteenus Euroopa Parlamendi ja nõukogu direktiivi 2005/29/EÜ[36] artikli 2 punktis n sätestatud tähenduses;

18) „veebipõhine otsingumootor“ – digiteenus Euroopa Parlamendi ja nõukogu määruse (EL) 2019/1150[37] artikli 2 punktis 5 sätestatud tähenduses;

19) „pilvandmetöötlusteenus“ – digiteenus, mis võimaldab jagatavate [...] andmetöötlusressursside skaleeritava ja paindliku kogumi nõudepõhist haldamist ning ulatuslikku kaugpääsu sellele kogumile, **kaasa arvatud juhul, kui need ressursid paiknevad erinevates kohtades**;

20) „andmekeskusteenus“ – teenus, mis hõlmab struktuure või struktuuride rühmi, mis on ette nähtud andmete talletamiseks, töötlemiseks ja edastamiseks kasutatavate infotehnoloogia- ja võrguseadmete keskseks majutamiseks, omavahel sidumiseks ja käitamiseks, sh kõiki energiajaotuse ja keskkonnakontrolliga seotud vahendeid ja taristuid;

---

36 Euroopa Parlamendi ja nõukogu 11. mai 2005. aasta direktiiv 2005/29/EÜ, mis käsitleb ettevõtja ja tarbija vaheliste tehingutega seotud ebaausaid kaubandustavasid siseturul ning millega muudetakse nõukogu direktiivi 84/450/EMÜ, Euroopa Parlamendi ja nõukogu direktiive 97/7/EÜ, 98/27/EÜ ja 2002/65/EÜ ning Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 2006/2004 (ebaausate kaubandustavade direktiiv) (ELT L 149, 11.6.2005, lk 22).

37 Euroopa Parlamendi ja nõukogu 20. juuni 2019. aasta määrus (EL) 2019/1150, mis käsitleb õigluse ja läbipaistvuse edendamist veebipõhiste vahendusteenuste ärikasutajate jaoks (ELT L 186, 11.7.2019, lk 57).

21) „sisulevivõrk“ – geograafiliselt hajutatud serverite võrk, mille eesmärk on tagada digisisu ja digiteenuste laialdane kättesaadavus, neile juurdepääsetavus või nende kiire edastamine internetikasutajatele sisu- ja teenusepakkujate nimel;

22) „sotsiaalvõrguteenuse platvorm“ – platvorm, mis võimaldab lõppkasutajatel vastastikku ühendust pidada, sisu jagada, teavet otsida ja suhelda mitme seadme kaudu, eelkõige vestluste, postituste, videote ja soovituste vormis;

23) „avaliku halduse üksus“ – [...] üksus, **mida tunnustatakse liikmesriigis siseriikliku õiguse kohaselt ning** mis vastab järgmistele kriteeriumidele:

a) üksus on asutatud konkreetse eesmärgiga täita üldhuvivajadusi ja see ei tegele tööstuse ega kaubandusega;

b) üksus on juriidiline isik **või tal on seaduse kohaselt õigus tegutseda teise juriidilise isiku staatusega üksuse nimel;**

c) üksust rahastavad peamiselt riik, piirkondlikud ametiasutused või muud avalik-õiguslikud asutused; üksuse juhtimine toimub mainitud asutuste järelevalve all; üksuse haldus-, juhtimis- või järelevalveorgani liikmetest üle poole on määranud riik, piirkondlikud asutused või muud avalik-õiguslikud asutused;

d) üksusel on voli teha füüsilisi või juriidilisi isikuid puudutavaid halduslikke või reguleerivaid otsuseid, mis mõjutavad nende isikute õigusi seoses isikute, kaupade, teenuste või kapitali piiriülese liikumisega;

24) „üksus“ – mis tahes füüsiline isik või asukohajärgse liikmesriigi õiguse kohaselt asutatud ja vastavalt tunnustatud juriidiline isik, kes võib enda nimel kasutada teatavaid õigusi ja täita teatavaid kohustusi;

25) „elutähtis üksus“ – iga selline üksus, [...] **mis on sätestatud I lisas ja mis on määratletud „elutähtsana“ vastavalt artikli 2*bis* punktile 1**;

26) „oluline üksus“ – iga selline üksus, [...] **mis on sätestatud I ja II lisas ja mis on määratletud „olulisena“ vastavalt artikli 2*bis* punktile 2**;

26a) „IKT-toode“ – IKT-toode määruse (EL) nr 2019/881 artikli 2 punktis 12 sätestatud tähenduses;

26aa) „IKT-teenus“ – IKT-teenus määruse (EL) nr 2019/881 artikli 2 punktis 13 sätestatud tähenduses;

26ab) „IKT-protsess“ – IKT-protsess määruse (EL) 2019/881 artikli 2 punktis 14 sätestatud tähenduses;

26ac) „hallatud teenuste osutaja“ – üksus, mis osutab teenuseid, näiteks võrgu-, rakendus-, taristu- ja turvateenuseid pideva ja korrapärase juhtimis-, tugi- ja aktiivse haldustöö kaudu klientide ruumides, oma hallatud teenuse osutaja andmekeskuses (majutus) või kolmanda isiku andmekeskuses.

(26ad) „turbetarnija“ – üksus, kes teostab turvaseadmete ja -süsteemide järelevalvet ja haldamist allhanke korras. Tavapärased teenused hõlmavad tulemüüri haldamist, sissetungide tuvastamist, virtuaalset privaatvõrku, nõrkuseotsingut ja viirusetõrjeteenuseid.

Samuti hõlmab see kõrgkäideldavate turbekeskuste (nii oma keskuste kui muude andmekeskuste) kasutamist, et pakkuda ööpäevaringselt teenuseid, mille eesmärk on vähendada selliste turbetöötajate arvu, keda ettevõte peab tööle võtma, koolitama ja tööl hoidma, et säilitada vastuvõetav turvaolek.

II PEATÜKK

Koordineeritud küberturvalisuse õigusraamistikud

Artikkel 5

Riiklik küberturvalisuse strateegia

1. Iga liikmesriik võtab vastu riikliku küberturvalisuse strateegia, milles määratakse kindlaks strateegilised eesmärgid ning asjakohased poliitilised ja regulatiivsed meetmed, et saavutada ja säilitada kõrgel tasemel küberturvalisus. Riiklik küberturvalisuse strateegia peab eelkõige sisaldama järgmist:

   a) selle liikmesriigi küberturvalisuse strateegia eesmärgid ja prioriteedid [...];

   b) juhtimisraamistik nende eesmärkide ja prioriteetide saavutamiseks, sh lõikes 2 osutatud poliitilised meetmed [...] ja strateegia rakendamises osalevate erinevate asutuste ning osalejate rollid ja ülesanded;

   c) [...] **suunised** asjakohaste varade [...] kindlaks tegemiseks ja küberturvalisusega seotud riskide **hindamiseks** kõnealuses liikmesriigis;

   d) intsidentideks valmisoleku ja neile reageerimise meetmete ning seotud taastemeetmete, sh avaliku ja erasektori koostöö kirjeldus;

   e) [...]

f) poliitikaraamistik käesoleva direktiivi ning Euroopa Parlamendi ja nõukogu direktiivi (EL) XXXX/XXXX[38] [kriitilise tähtsusega üksuste vastupanuvõime direktiiv] kohaste pädevate asutuste vahelise tegevuse paremaks koordineerimiseks **küberturvalisuse riskide**, [...] küberohtude **ja -intsidentide ning kübervaldkonnaväliste riskide, ohtude ja intsidentide** alase teabe jagamise ning järelevalveülesannete täitmise eesmärgil, **kui see on asjakohane**;

fa) poliitikaraamistik käesoleva direktiivi kohaste pädevate asutuste ja valdkondlike õigusaktide alusel määratud pädevate asutuste vaheliseks tegevuse koordineerimiseks ja koostööks.

2. Riikliku küberturvalisuse strateegia osana võtavad liikmesriigid vastu eelkõige järgmised poliitikameetmed:

a) poliitikameetmed, mis käsitlevad [...] üksuste teenuste osutamiseks kasutatavate IKT-toodete ja -teenuste tarneahela küberturvalisust;

b) **poliitikameetmed** [...] IKT-toodete ja -teenuste küberturvalisusega seotud nõuete ja vastavate spetsifikatsioonide hõlmamiseks riigihankemenetlusse, **sealhulgas küberturvalisuse sertifitseerimine**;

c) poliitikameetmed, [...] **mis käsitlevad nõrkuste haldamist ja mis hõlmavad vabatahtliku** nõrkuste koordineeritud avalikustamise **edendamist ja hõlbustamist** artikli 6 **lõike 1** tähenduses;

d) poliitikameetmed, mis on seotud avatud interneti avaliku tuuma üldise kättesaadavuse, [...] **tervikluse ja konfidentsiaalsuse** säilitamisega;

e) poliitikameetmed, mille abil edendatakse ja arendatakse **haridust ja koolitust**, oskusi, suurendatakse teadlikkust ning toetatakse teadus- ja arendusalgatusi küberturvalisuse vallas;

---

38 *[lisada täielik pealkiri ja ELTs avaldamise viide, kui see on teada]*

f) poliitikameetmed, millega toetatakse akadeemilisi ja teadusasutusi küberturvalisuse vahendite ja turvalise võrgutaristu väljatöötamisel;

g) poliitikameetmed, asjakohane menetluskord ja sobivad teabevahetuslahendused, millega toetatakse vabatahtlikku küberturvalisuse alase teabe vahetamist ettevõtjate vahel kooskõlas liidu õigusega;

h) poliitikameetmed, mis käsitlevad VKEde, eelkõige käesoleva direktiivi kohaldamisalast välja jäetud VKEde erivajadusi seoses suuniste ja toega, mis parandaks VKEde vastupidavusvõimet küber[...]ohtude suhtes.

3. Liikmesriigid teavitavad komisjoni oma riiklikust küberturvalisuse strateegiast kolme kuu jooksul pärast selle vastuvõtmist. **Seda tehes** võivad liikmesriigid jätta [...] **edastamata riiklikku julgeolekut puudutavad strateegia elemendid**.

4. Liikmesriigid hindavad oma riiklikke küberturvalisuse strateegiaid peamiste tulemusnäitajate põhjal korrapäraselt ja vähemalt iga [...] **viie** aasta järel ja teevad neis vajaduse korral muudatusi. Euroopa Liidu Küberturvalisuse Amet (ENISA) abistab liikmesriike **nende** taotluse korral riikliku strateegia ja selle hindamiseks vajalike peamiste tulemusnäitajate väljatöötamisel.

Artikkel 6

Nõrkuste koordineeritud avalikustamine ja Euroopa nõrkuste register

1. Iga liikmesriik määrab ühe oma artiklis 9 osutatud CSIRTidest nõrkuste koordineeritud avalikustamise koordineerijaks. Määratud CSIRT tegutseb usaldusväärse vahendajana, hõlbustades vajaduse korral suhtlust teavitava üksuse, **võimaliku nõrkuse omaja** ning IKT-toodete või -teenuste tootja või pakkuja vahel. **Iga füüsiline või juriidiline isik võib teatada määratud CSIRTile vajaduse korral anonüümselt artikli 4 lõikes 8 osutatud nõrkusest. Määratud CSIRT tagab, et teate suhtes võetakse põhjalikud järelmeetmed ja nõrkusest teatanud isiku identiteet jääb konfidentsiaalseks.** Kui teates osutatud nõrkus [...] **võib oluliselt mõjutada üksusi rohkem kui ühes liikmesriigis**, teeb iga asjaomase liikmesriigi määratud CSIRT **asjakohasel juhul** koostööd **teiste määratud CSIRTidega** CSIRTi võrgustikus.

2. ENISA **koostab koostöörühmaga konsulteerides** Euroopa nõrkuste registri ja haldab seda. Selleks võtab ENISA kasutusele asjakohased infosüsteemid, põhimõtted ja menetlused eelkõige selleks, et võimaldada elutähtsatel ja olulistel üksustel ning nende võrgu- ja infosüsteemide tarnijatel avalikustada ja registreerida **vabatahtlikult avalikkusele teadaolevaid** IKT-toodete või -teenuste nõrkusi ning anda kõigile huvitatud isikutele juurdepääs registris sisalduvale nõrkusi käsitlevale teabele. Täpsemalt sisaldab register teavet nõrkuse olemuse, mõjutatud IKT-toodete või -teenuste ning nõrkuse raskusastme kohta, pidades silmas selle võimaliku ärakasutamise olukordi, samuti seotud paikade kättesaadavuse kohta ning paikade puudumisel haavatavate toodete ja teenuste kasutajatele suunatud **riiklike pädevate asutuste või CSIRTide poolt antud** suuniseid selle kohta, kuidas avalikustatud nõrkustest tulenevaid riske vähendada. **ENISA tagab, et Euroopa nõrkuste register kasutab turvalist ja vastupidavat side- ja infotaristut.**

Artikkel 7

Riiklikud küberturvalisuse alased kriisiohjeraamistikud

1. Iga liikmesriik määrab vähemalt ühe ulatuslike **küberturvalisuse** intsidentide ja kriiside ohjamise eest vastutava pädeva asutuse. Liikmesriigid tagavad, et pädevatel asutustel on piisavad ressursid nendele pandud ülesannete tulemuslikuks ja tõhusaks täitmiseks. **Liikmesriigid tagavad sidususe olemasolevate üldise kriisiohje raamistikega.**

2. Iga liikmesriik määrab kindlaks oma suutlikkuse, vahendid ja menetlused, mida saab rakendada kriisiolukorras käesoleva direktiivi kohaldamisel.

3. Iga liikmesriik võtab vastu riikliku küberturvalisuse intsidentide ja kriiside lahendamise kava, milles kirjeldatakse ulatuslike küberturvalisuse intsidentide ja kriiside ohjamise eesmärke ja korda. Kavaga nähakse täpsemalt ette järgmine:

   a) riiklike valmisolekumeetmete ja nendega seotud tegevuste eesmärgid;

   b) riiklike pädevate ametiasutuste kohustused ja ülesanded;

   c) küberturvalisuse kriisiohjamise menetlused, **sealhulgas nende integreerimine üldisesse riiklikku kriisiohjeraamistikku** ja teabevahetuskanalitesse;

   d) valmisolekumeetmed, sealhulgas korrapärased õppuste ja koolitusega seotud tegevused;

   e) asjakohased avaliku ja erasektori [...] isikud ning seotud taristud;

   f) riigis kehtivad menetlused ja kord asjaomaste riiklike asutuste ja organite vahelise koostöö korraldamiseks, et tagada liikmesriigi tõhus osalemine ulatuslike küberturvalisuse intsidentide ja kriiside koordineeritud ohjamisel liidu tasandil ja selle ohjamise toetamine.

4. Liikmesriigid teavitavad komisjoni lõikes 1 osutatud pädevate asutuste määramisest ning esitavad **käesoleva artikli lõikes 3 sätestatud nõuetega seotud teabe** riiklike küberturvalisuse intsidentide ja kriiside lahendamise kavade kohta kolme kuu jooksul pärast kõnealuste asutuste määramist ja kõnealuste kavade vastuvõtmist. Liikmesriigid võivad jätta teatava [...] teabe edastamata, kui ja kuivõrd see on [...] põhjendatud riikliku julgeoleku, **avaliku julgeoleku või riigikaitse** tagamise vajadusega.

Artikkel 8

Riiklikud pädevad asutused ja ühtsed kontaktpunktid

1. Iga liikmesriik määrab vähemalt ühe pädeva asutuse, kes vastutab küberturvalisuse ja käesoleva direktiivi VI peatükis osutatud järelevalveülesannete täitmise eest. Liikmesriigid võivad selleks määrata juba tegutseva asutuse või tegutsevad asutused.

2. Lõikes 1 osutatud pädevad asutused jälgivad käesoleva direktiivi kohaldamist siseriiklikul tasandil.

3. Iga liikmesriik määrab küberturvalisuse valdkonna jaoks ühtse riikliku kontaktpunkti („ühtne kontaktpunkt“). Kui liikmesriik määrab ainult ühe pädeva asutuse, siis on see pädev asutus ka selle liikmesriigi ühtne kontaktpunkt.

4. Iga ühtne kontaktpunkt täidab sidepidamisfunktsiooni, et tagada oma liikmesriigi ametiasutuste piiriülene koostöö teiste liikmesriikide asjaomaste asutustega ning ka valdkondadevaheline koostöö oma liikmesriigi teiste pädevate asutustega.

5. Liikmesriigid tagavad, et lõikes 1 osutatud pädevatel asutustel ja ühtsetel kontaktpunktidel on piisavad ressursid, et neile pandud ülesandeid tulemuslikult ja tõhusalt täita ning seeläbi saavutada käesoleva direktiivi eesmärgid. Liikmesriigid tagavad määratud esindajate tõhusa, tulemusliku ja turvalise koostöö artiklis 12 osutatud koostöörühmas.

6. Iga liikmesriik teavitab komisjoni põhjendamatu viivituseta lõikes 1 osutatud pädeva asutuse ja lõikes 3 osutatud ühtse kontaktpunkti määramisest, nende ülesannetest ning nendega seotud hilisematest muudatustest. Iga liikmesriik avalikustab teabe määramiste kohta. Komisjon avaldab määratud ühtsete kontaktpunktide loetelu.

Artikkel 9

Küberturbe intsidentide lahendamise üksused (CSIRTid)

1. Iga liikmesriik määrab vähemalt ühe artikli 10 lõikes 1 sätestatud nõuetele vastava CSIRTi, kes hõlmaks vähemalt I ja II lisas osutatud sektoreid, allsektoreid või üksusi ning kes vastutaks intsidentide käsitlemise eest kindla menetluse kohaselt. CSIRTi võib luua artiklis 8 osutatud pädeva asutuse osana.

2. Liikmesriigid tagavad, et igal CSIRTil on artikli 10 lõikes 2 sätestatud ülesannete tulemuslikuks täitmiseks piisavad vahendid. **Nende ülesannete täitmisel võivad CSIRTid prioriseerida konkreetsete teenuste osutamist üksustele, tuginedes riskipõhisele lähenemisviisile.**

3. Liikmesriigid tagavad, et iga CSIRTi käsutuses on asjakohane, turvaline ja vastupidav side- ja infotaristu, vahetamaks teavet elutähtsate ja oluliste üksuste ning muude asjaomaste huvitatud isikutega. Selleks tagavad liikmesriigid, et CSIRTid aitavad kaasa turvaliste teabejagamisvahendite kasutuselevõtule.

4. CSIRTid teevad koostööd ning (kus asjakohane) vahetavad kooskõlas artikliga 26 asjakohast teavet elutähtsate ja oluliste üksuste usaldusväärsete sektoripõhiste või -vaheliste kogukondadega.

5. CSIRTid osalevad artikli 16 kohaselt korraldatud vastastikuses [...] **õppes**.

6. Liikmesriigid tagavad oma CSIRTide tõhusa, tulemusliku ja turvalise koostöö artiklis 13 osutatud CSIRTide võrgustikus.

7. Liikmesriigid teavitavad komisjoni põhjendamatu viivituseta lõike 1 kohaselt määratud CSIRTidest, artikli 6 lõike 1 kohaselt määratud CSIRTi koordinaatorist ning nende vastavatest ülesannetest seoses I ja II lisas osutatud üksustega.

8. Liikmesriigid võivad paluda ENISA abi riiklike CSIRTide moodustamisel.

Artikkel 10

CSIRTidele esitatavad nõuded ja nende ülesanded

1. CSIRTid peavad vastama järgmistele nõuetele:

   a) CSIRT peab tagama oma side[...]**kanalite** laialdase kättesaadavuse, vältides nõrku lülisid, ning kasutama mitmesuguseid vahendeid, mis võimaldavad neil teistega ja teistel nendega igal ajal ühendust võtta. CSIRTid määratlevad selgelt suhtluskanalid ning teevad need oma sihtrühmadele ja koostööpartneritele teatavaks;

   b) CSIRTi ametiruumid ja tema tööd toetavad infosüsteemid peavad asuma turvalises kohas;

c) CSIRTil peab olema päringute haldamiseks ja suunamiseks sobiv süsteem, ennekõike selleks, et tõhustada üleandmisi;

d) CSIRTil peab olema piisavalt töötajaid, et tagada tema teenuste alaline kättesaadavus;

e) CSIRTidel peavad olema varusüsteemid ja varutööruumid, mis võimaldaks tagada nende teenuste toimepidevuse;

f) CSIRTidel peab olema võimalus osaleda rahvusvaheliste koostöövõrgustike töös.

2. CSIRTidel on järgmised ülesanded:

a) korraldada küberohtude, nõrkuste ja intsidentide seiret riiklikul tasandil;

b) tagada küberohtude, nõrkuste ja intsidentide kohta eelhoiatuste, hoiatuste ja teadete edastamine ning teabe levitamine elutähtsatele ja olulistele üksustele, **pädevatele asutustele** ning muudele asjaomastele huvitatud isikutele;

c) intsidentidele reageerimine;

d) kohtuekspertiisiandmete kogumine ja analüüsimine ning järjepidev riskide ja intsidentide analüüsimine ning küberturvalisuse alase olukorrateadlikkuse tagamine;

e) võrgu- ja infosüsteemide **[...]** ennetava kontrolli teostamine, **[...]** e**t tuvastada nõrkusi, millel võib olla oluline mõju, kuid juhul, kui puudub asjaomase üksuse nõusolek, siis tema võrgu- ja infosüsteemidesse sisse ei tungita ning nende toimimist ei kahjustata;**

f) CSIRTide võrgustikus osalemine ja teistele võrgustiku liikmetele **vastavalt oma suutlikkusele ja pädevusele** nende taotluse korral vastastikuse abi osutamine.

fa) asjakohasel juhul nõrkuste koordineeritud avalikustamise koordinaatori ülesannete täitmine vastavalt artikli 6 lõikele 1, mis hõlmab eelkõige teavitavate üksuste, võimaliku nõrkuse omaja ja IKT-toodete või -teenuste tootja või pakkuja vahelise suhtluse hõlbustamist, juhul kui see on vajalik, asjaomaste üksuste kindlakstegemist ja nendega ühenduse võtmist, teavitavate üksuste toetamist, avalikustamise tähtaegade üle läbirääkimiste pidamist ja mitut organisatsiooni mõjutavate nõrkuste haldamist (mitmepoolne nõrkuste koordineeritud avalikustamine).

3. CSIRTid loovad koostöösuhteid erasektori asjaomaste osalejatega, et paremini saavutada käesoleva direktiivi eesmärke.

3a. CSIRTid võivad luua koostöösuhteid kolmandate riikide CSIRTidega. Selle koostöö raames võivad nad vahetada asjakohast teavet, sealhulgas isikuandmeid kooskõlas andmekaitset käsitlevate liidu õigusaktidega.

4. Koostöö hõlbustamiseks toetavad CSIRTid ühtsete või standardsete tavade, liigitamissüsteemide ja taksonoomiate kasutuselevõttu seoses järgmisega:

a) intsidentide käsitlemise menetlused;

b) küberturvalisusega seotud kriisiohje;

c) nõrkuste koordineeritud avalikustamine.

Artikkel 11

Koostöö liikmesriigi tasandil

1. Kui ühe liikmesriigi artiklis 8 osutatud pädevad asutused, ühtne kontaktpunkt ja CSIRTid on eraldiseisvad asutused, teevad nad käesolevas direktiivis sätestatud kohustuste täitmisel koostööd.

2. Liikmesriigid tagavad, et nende pädevad asutused või CSIRTid saavad käesoleva direktiivi kohaselt esitatud teateid intsidentide, oluliste küberohtude ja realiseerumata jäänud ohuolukordade kohta. Kui liikmesriik otsustab, et tema CSIRTid kõnealuseid teateid ei saa, tuleb CSIRTidele anda nende ülesannete täitmiseks vajalikus ulatuses juurdepääs andmetele nende intsidentide kohta, millest elutähtsad või olulised üksused on teatanud artikli 20 kohaselt.

3. Iga liikmesriik tagab, et tema pädevad asutused või CSIRTid teavitavad oma riigi ühtset kontaktpunkti intsidentide, oluliste küberohtude ja realiseerumata jäänud ohuolukordade kohta käesoleva direktiivi kohaselt esitatud teadetest.

4. Liikmesriigid tagavad käesolevas direktiivis sätestatud ülesannete ja kohustuste tõhusaks täitmiseks vajalikus ulatuses kõnealuses liikmesriigis asjakohase koostöö kõnealuse liikmesriigi pädevate asutuste, **CSIRTide**, ühtsete kontaktpunktide ja õiguskaitseasutuste, andmekaitseasutuste ja direktiivi (EL) XXXX/XXXX [kriitilise tähtsusega üksuste vastupanuvõime direktiiv] kohaselt **[...] määratud pädevate** asutuste vahel, **komisjoni rakendusmääruse 2019/1583 kohaste pädevate asutuste, direktiiviga (EL) 2018/1972 määratud riiklike reguleerivate asutuste, määruse (EL) nr 910/2014 artikli 17 kohaselt määratud riiklike asutuste,** [...] Euroopa Parlamendi ja nõukogu määruse (EL) XXXX/XXXX [DORA määrus] kohaselt määratud riiklike finantsasutuste ning **muude valdkondlike liidu õigusaktidega määratud pädevate asutuste vahel**.

5. Liikmesriigid tagavad, et nende **käesoleva direktiivi kohased pädevad asutused ning direktiivi (EL) XXXX/XXXX [kriitilise tähtsusega üksuste vastupidavusvõime direktiiv] kohaselt määratud pädevad asutused vahetavad** korrapäraselt [...] teavet [...] **kriitilise tähtsusega üksuste kindlaks määramise**, küberturvalisusega seotud riskide, küberohtude ja intsidentide **ning kübervaldkonnaväliste riskide, ohtude ja intsidentide kohta**, mis mõjutavad direktiivi (EL) XXXX/XXXX [kriitilise tähtsusega üksuste vastupidavusvõime direktiiv] alusel kriitilise tähtsusega üksustena käsitatavaid elutähtsaid üksusi **[**või kriitilise tähtsusega üksustega samaväärseid üksusi**]**, ning meetmete kohta, mida [...] on kõnealuste riskide ja intsidentidega seoses võetud. **Liikmesriigid tagavad samuti, et käesoleva direktiivi kohased pädevad asutused ning määruse XXXX/XXXX [DORA määrus], direktiivi 2018/1972 ja määruse (EL) 910/2014 kohaselt määratud pädevad asutused vahetavad korrapäraselt asjakohast teavet.**

Usaldusteenuse osutajate puhul ning [...] eelkõige juhul, kui käesoleva direktiivi kohane järelevalveroll antakse mõnele muule asutusele kui määruse (EL) 910/2014 kohaselt määratud järelevalveasutused, teevad käesoleva direktiivi kohased riiklikud pädevad asutused aegsasti tihedat koostööd, vahetades asjakohast teavet, et tagada tõhus järelevalve ja usaldusteenuse osutajate vastavus käesolevas direktiivis ja määruses [XXXX/XXXX] sätestatud nõuetele, **ning kui see on asjakohane, teavitab käesoleva direktiivi kohane riiklik pädev asutus põhjendamatu viivituseta eIDASe järelevalveasutust igast teatatud olulisest küberohust või intsidendist, mis mõjutab usaldusteenuseid**.

5a. Selleks, et intsidentidest teatamist lihtsustada, võivad liikmesriigid luua vajaduse korral ühtse kontaktpunkti kõigi käesoleva direktiivi ja määruse (EL) 2016/679 ning direktiivi 2002/58/EÜ alusel nõutavate teadete edastamise tarbeks. Liikmesriigid võivad kasutada seda ühtset kontaktpunkti, et esitada muude valdkondlike liidu õigusaktide kohaselt nõutud teateid. See ühtne kontaktpunkt ei mõjuta määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ sätete, eelkõige sõltumatuid järelevalveasutusi käsitlevate sätete kohaldamist.

III PEATÜKK

***ELi** koostöö*

Artikkel 12

Koostöörühm

1. Et toetada ja hõlbustada strateegilist koostööd ja teabevahetust liikmesriikide vahel **ning** [...] **suurendada usaldust ja kindlustunnet** [...], luuakse koostöörühm.

2. Koostöörühm täidab oma ülesandeid kaheaastaste tööprogrammide alusel, nagu on osutatud lõikes 6.

3. Koostöörühma moodustavad liikmesriikide, komisjoni ja ENISA esindajad. Euroopa välisteenistus osaleb koostöörühma tegevuses vaatlejana. Euroopa järelevalveasutused (ESAd) ja **määruse (EL) XXXX/XXXX [DORA määrus] alusel määratud pädevad asutused** [...] võivad osaleda koostöörühma tegevuses **kooskõlas määruse (EL) XXXX/XXXX [DORA määrus] artikli 42 lõikega 1**.

   Kui see on vajalik, võib koostöörühm kutsuda oma töös osalema asjakohaste sidusrühmade esindajad.

   Komisjon tagab sekretariaaditeenused.

4. Koostöörühmal on järgmised ülesanded:

   a) anda pädevatele asutustele suuniseid käesoleva direktiivi ülevõtmise ja kohaldamise kohta**;**

   aa) anda suuniseid artikli 5 lõike 2 punktis c ja artikli 6 lõikes 1 osutatud nõrkuste koordineeritud avalikustamise poliitika väljatöötamiseks ja rakendamiseks;

b) vahetada parimaid tavasid ja teavet seoses käesoleva direktiivi kohaldamisega, sealhulgas seoses küberohtude, intsidentide, nõrkuste, realiseerumata jäänud ohuolukordade, teadlikkuse suurendamise algatuste, koolituste, õppuste ja oskuste, suutlikkuse suurendamise ning samuti standardite ja tehniliste spetsifikatsioonidega;

c) vahetada nõuandeid ja teha koostööd komisjoniga seoses uute küberturvalisuse poliitika algatustega;

d) vahetada nõuandeid ja teha koostööd komisjoniga seoses käesoleva direktiivi kohaselt vastu võetavate komisjoni rakendusaktide [...] eelnõudega;

e) vahetada parimaid tavasid asjaomaste liidu institutsioonide, ametite ja asutustega;

ea) vahetada seisukohti küberturvalisuse aspekte hõlmavate valdkondlike õigusaktide rakendamise kohta;

f) arutada artikli 16 lõikes 7 osutatud vastastikuse [...] **õppe** aruandeid;

g) arutada artiklis 34 osutatud piiriüleste juhtumite ühise järelevalvetegevuse **kogemusi**[...];

h) anda CSIRTide võrgustikule ja **EU–CyCLONe-le** strateegilisi suuniseid spetsiifilistes esilekerkivates küsimustes;

ha) vahetada seisukohti seoses ulatuslike küberturvalisuse intsidentide poliitiliste järelmeetmetega, lähtudes CSIRTide võrgustiku ja EU–CyCLONe raames saadud kogemustest;

i) aidata tagada küberturvalisuse alane suutlikkus liidus, hõlbustades riigiametnike vahetust suutlikkuse suurendamise programmi kaudu, millesse hõlmatakse liikmesriikide pädevate asutuste või CSIRTide töötajad;

j) korraldada korrapäraseid ühiskoosolekuid erasektori asjaomaste huvitatud pooltega kogu liidust, et arutada rühma tegevust ja koguda teavet esilekerkivate poliitikaprobleemide kohta;

k) arutada küberturvalisuse alaste õppustega seoses tehtud tööd, sealhulgas ENISA tehtud tööd**;**

ka) luua vastastikuse õppe mehhanism kooskõlas käesoleva direktiivi artikliga 16.

5. Koostöörühm võib tellida CSIRTi**de** võrgustikult valitud teemasid käsitleva tehnilise aruande.

6. Koostöörühm koostab hiljemalt … [24 kuud pärast käesoleva direktiivi jõustumiskuupäeva] ja seejärel iga kahe aasta tagant tööprogrammi meetmete kohta, mida võetakse rühma eesmärkide ja ülesannete täitmiseks. Käesoleva direktiivi alusel vastu võetava esimese programmi ajakava viiakse kooskõlla direktiivi (EL) 2016/1148 alusel vastu võetud viimase programmi ajakavaga.

7. Komisjon võib võtta vastu rakendusaktid, millega kehtestatakse koostöörühma toimimiseks vajalik menetluskord. Kõnealused rakendusaktid võetakse vastu kooskõlas artikli 37 lõikes 2 osutatud kontrollimenetlusega.

8. Koostöörühm kohtub korrapäraselt ja vähemalt kord aastas direktiivi (EL) XXXX/XXXX [kriitilise tähtsusega üksuste vastupidavusvõime direktiiv] alusel loodud kriitilise tähtsusega üksuste vastupidavusvõime töörühmaga, et edendada strateegilist koostööd ja **hõlbustada** teabevahetust.

Artikkel 13

CSIRTide võrgustik

1. Et kasvatada usaldust ja kindlustunnet ning edendada kiiret ja tõhusat operatiivkoostööd liikmesriikide vahel, luuakse riiklike CSIRTide võrgustik.

2. CSIRTide võrgustik koosneb **artikli 9 kohaselt määratud** liikmesriikide CSIRTide esindajatest ja CERT-EU esindajatest. Komisjon osaleb CSIRTide võrgustikus vaatlejana. ENISA tagab sekretariaaditeenused ja toetab aktiivselt CSIRTide-vahelist koostööd.

3. CSIRTide võrgustikul on järgmised ülesanded:

   a) vahetada CSIRTide suutlikkust puudutavat teavet;

   b) vahetada asjakohast teavet intsidentide, ohuolukordade, küberohtude, riskide ja nõrkuste kohta;

ba) vahetada teavet seoses küberturvalisust käsitlevate väljaannete ja soovitustega;

bb) tehnilist intsidendikäsitlust hõlbustavate tehniliste lahenduste jagamine;

bc) CSIRTide ülesannetega seotud parimate tavade, vahendite ja menetluste vahetamine;

c) vahetada ja arutada intsidendist potentsiaalselt mõjutatud CSIRTi**de** võrgustiku [...] **liikme** taotlusel teavet, mis käsitleb kõnealust intsidenti ning sellega seotud küberohte, riske ja nõrkusi;

d) arutada CSIRTi**de** võrgustiku [...] **liikme** taotlusel kõnealuse liikmesriigi jurisdiktsioonis tuvastatud intsidendi koordineeritud lahendamist ning võimaluse korral lahendada intsident koordineeritult;

e) toetada liikmesriike piiriüleste intsidentide käesoleva direktiivi kohasel käsitlemisel;

f) teha koostööd **ja vahetada parimaid tavasid** artiklis 6 osutatud määratud CSIRTidega ning osutada neile abi seoses eri liikmesriikides tegutsevate IKT-toodete, -teenuste ja -protsesside tootjate või pakkujate nõrkuste [...] koordineeritud avalikustamise haldamisega;

g) arutada ja teha kindlaks täiendavaid operatiivkoostöövorme, sealhulgas seoses järgmisega:

   i) küberohtude ja intsidentide liigid;

   ii) varajased hoiatused;

   iii) vastastikune abi;

iv) piiriülestele riskidele ja intsidentidele koordineeritud reageerimise põhimõtted ja kord;

v) osalemine **liikmesriigi taotlusel** artikli 7 lõikes 3 osutatud riikliku küberturvalisuse intsidentide ja kriiside lahendamise kava koostamises;

h) teavitada koostöörühma oma tegevusest ja punkti g kohaselt arutatud täiendavatest operatiivkoostöö vormidest **ning** vajaduse korral taotleda sellega seotud suuniseid;

i) analüüsida küberturvalisuse alaseid õppusi, sealhulgas ENISA korraldatud õppusi;

j) arutada üksiku CSIRT taotlusel kõnealuse CSIRT suutlikkust ja valmisolekut;

k) teha koostööd ning vahetada teavet piirkondlike ja liidu tasandi turbekeskustega, et parandada ühist olukorrateadlikkust seoses intsidentide ja ohtudega kogu liidus;

l) arutada artikli 16 lõikes 7 osutatud vastastikuse **õppe** aruandeid;

m) anda suuniseid, et hõlbustada operatiivsete tavade lähendamist seoses käesoleva artikli operatiivkoostööd käsitlevate sätete kohaldamisega.

4. Artiklis 35 osutatud läbivaatamise eesmärgil ja hiljemalt [24 kuud pärast käesoleva direktiivi jõustumise kuupäeva] ning seejärel iga kahe aasta tagant hindab CSIRTide võrgustik operatiivkoostöös tehtud edusamme ja koostab sellekohase aruande. Aruandes tehakse eelkõige järeldused riiklikke CSIRTe käsitleva artiklis 16 osutatud vastastikuse **õppe** [...] tulemuste kohta, sealhulgas järeldused ja soovitused, mille tegemine lähtub käesolevast artiklist. See aruanne esitatakse ka koostöörühmale.

5. CSIRTide võrgustik võtab vastu oma töökorra.

6. CSIRTide võrgustik teeb EU-CyCLONe-ga koostööd kokkulepitud menetluskorra alusel.

Artikkel 14

Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik (EU-CyCLONe)

1. Et toetada ulatuslike küberturvalisuse intsidentide ja kriiside koordineeritud ohjamist operatiivsel tasandil ning tagada korrapärane teabevahetus liikmesriikide ja ELi institutsioonide, ametite ja asutuste vahel, luuakse Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik (EU-CyCLONe).

2. EU-CyCLONe moodustatakse liikmesriikide artikli 7 kohaselt määratud **küber**kriiside ohjamise asutuste [...] esindajatest. **Komisjon osaleb võrgustiku tegevuses vaatlejana.** ENISA tagab võrgustiku jaoks sekretariaaditeenused ja toetab turvalist teabevahetust **ning pakub vajalikke vahendeid liikmesriikide vahelise koostöö toetamiseks, tagades turvalise teabevahetuse.**

   Kui see on vajalik, võib EU-CyCLONe kutsuda oma töös osalema asjakohaste sidusrühmade esindajad.

3. EU-CyCLONe ülesanded on järgmised:

a) tõsta ulatuslike [...]küb**erturvalisuse** intsidentide ja kriiside ohjamiseks valmisoleku taset;

b) arendada ühist olukorrateadlikkust [...] ulatuslike kübe**r**turvalisuse intsidentide ja kriiside kohta;

ba) hinnata asjaomaste ulatuslike küberturvalisuse intsidentide tagajärgi ja mõju ning pakkuda välja võimalikke leevendusmeetmeid;

c) koordineerida ulatuslike küberturvalisuse intsidentide ja kriiside **ohjamist** [...] ning toetada selliste intsidentide ja kriisidega seotud otsuste tegemist poliitilisel tasandil;

d) **liikmesriigi taotlusel** arutada riiklikke küberturvalisuse intsidentide ja **kriiside** lahendamise kavasid, millele on osutatud artikli 7 lõikes **3** [...]**;**[...]

4. EU-CyCLONe võtab vastu oma töökorra.

5. EU-CyCLONe esitab koostöörühmale korrapäraselt **ulatuslike küberturvalisuse intsidentide ohjamist ja kriisiohjet** käsitleva aruande [...], keskendudes eelkõige mõjule, mida need avaldavad elutähtsatele ja olulistele üksustele.

6. EU-CyCLONe teeb CSIRTide võrgustikuga koostööd kokkulepitud menetluskorra alusel.

7. EU-CyCLONe esitab Euroopa Parlamendile ja nõukogule oma tööd hindava aruande hiljemalt [24 kuud pärast käesoleva direktiivi jõustumise kuupäeva].

Artikkel 14a

Rahvusvaheline koostöö

Liit võib kooskõlas ELi toimimise lepingu artikliga 218 sõlmida vajaduse korral kolmandate riikide või rahvusvaheliste organisatsioonidega rahvusvahelisi lepinguid, mis võimaldavad neil osaleda ja korraldada osalust mõningates koostöörühma, CSIRTide võrgustiku ja EU-CyCLONe tegevustes kooskõlas andmekaitset käsitlevate liidu õigusaktidega.

Artikkel 15

Aruanne küberturvalisuse olukorra kohta liidus

1. ENISA esitab koostöös komisjoni **ja koostöörühmaga** iga kahe aasta tagant aruande, mis käsitleb küberturvalisuse olukorda liidus. **Eelkõige**[...] sisaldab [...] aruanne [...] järgmist:

   aa) liidu tasandi küberturvalisuse riskihindamine, mille puhul võetakse arvesse ohtude kaardistamist;

   a) [...] **hinnang, mis käsitleb** küberturvalisuse alast suutlikkust kogu liidu avalikus ja erasektoris;

   b) [...]

   c) küberturvalisuse [...] **kvantitatiivsetel ja kvalitatiivsetel näitajatel põhinev koondhinnang**, mis annab [...] **ülevaate** küberturvalisuse alase suutlikkuse, **sealhulgas valdkondliku suutlikkuse** küpsustasemest.

2. Aruanne sisaldab konkreetseid poliitikasoovitusi küberturvalisuse taseme tõstmiseks kogu liidus ning ENISA poolt kooskõlas määruse (EL) 2019/881 artikli 7 lõikega 6 avaldatud ELi küberturvalisuse tehnilise olukorra aruannete tulemuste kokkuvõtet kindla perioodi kohta.

Artikkel 16

Vastastikune õpe

1. **Selleks, et tugevdada vastastikust usaldust, saavutada küberturvalisuse ühtlaselt kõrge tase ning tugevdada liikmesriikide küberturvalisuse alast suutlikkust ja poliitikat, mis on vajalik käesoleva direktiivi tulemuslikuks rakendamiseks,** [...] kehtestab [...] **koostöörühm komisjoni toel ja** pärast ENISAga [...] **ning, kui see on asjakohane, CSIRTide võrgustikuga** konsulteerimist, ja hiljemalt **24 [...]** kuud pärast käesoleva direktiivi jõustumist, **objektiivse, mittediskrimineeriva ja õiglase** vastastikuse [...] **õppe** süsteemi metoodika [...] **seoses käesoleva direktiivi rakendamisega** [...] liikmesriikide poolt. **Vastastikuses õppes osalemine on vabatahtlik. Süsteem koosneb hindamisvoorudest,**[...] mille korraldavad küberturvalisuse valdkonna [...] eksperdid liikmesriikidest [...] ning mis hõlmab [...] **üht või mitut** järgmistest aspektidest:

   i) artiklites 18 ja 20 osutatud küberturvalisuse riskijuhtimisnõuete ja teatamiskohustuse rakendamine [...];

   ii) suutlikkus, [...]sealhulgas olemasolevad [...] ressursid ning **artiklis 8 osutatud** riiklike pädevate asutuste ja **artiklis 9 osutatud CSIRTide** ülesannete [...] täitmine;

[...]

i**ii**[...]) artiklis 34 osutatud vastastikuse abi [...] **kohaldamine**;

iv) artiklis 26 [...] osutatud teabevahetusraamistiku [...] **kohaldamine**.

2. **Kriteeriumid, mille põhjal liikmesriigid määravad eksperdid, kes võivad osaleda vastastikuse õppe voorudes, peavad olema** [...] objektiivsed, mittediskrimineerivad, õiglased ja läbipaistvad [...] **ning need peavad sisalduma lõikes 1 osutatud metoodikas**. ENISA ja komisjon [...] **võivad** määrata eksperdid, kes osalevad [...] **vastastikuse õppe voorudes** vaatlejatena. [...]

3. [...] .

3a. Enne vastastikuse õppe voorude algust võivad liikmesriigid teha konkreetse vastastikuse õppe vooruga hõlmatavaid aspekte käsitleva enesehindamise ning edastada selle enesehindamise tulemused lõikes 2 osutatud määratud ekspertidele.

4. Vastastikune [...] **õpe** [...] **võib** hõlmata [...] **füüsilisi** või virtuaalseid külastusi ja väljaspool konkreetset asukohta toimuvat teabevahetust. Pidades silmas hea koostöö põhimõtet, esitavad [...] **vastastikuses õppes osalevad** liikmesriigid määratud ekspertidele [...] hindamiseks vajaliku teabe [...]**, ilma et see piiraks konfidentsiaalse või salastatud teabe kaitset või riigi põhifunktsioonide, näiteks riigi julgeoleku kaitset käsitleva liikmesriikide või liidu õiguse kohaldamist.** Vastastikuse [...] **õppe** protsessi kaudu saadavat teavet kasutatakse üksnes asjaomasel eesmärgil. Vastastikuses [...] **õppes** osalevad eksperdid ei avalda [...] **asjaomases kontekstis** saadud tundlikku või konfidentsiaalset teavet kolmandatele isikutele. **Vastastikuses õppes osalev liikmesriik võib esitada vastuväiteid konkreetsete ekspertide määramise kohta nõuetekohaselt põhjendatud juhtudel, millest on teatatud koostöörühmale.**

5. **Vastastikuse õppe voorus juba käsitletud** [...] aspekte ei käsitleta **osalevate** liikmesriikide puhul täiendavates vastastikuse [...] **õppe voorudes** [...] **nelja** aasta jooksul pärast **kõnealuse** vastastikuse [...] **õppe vooru** lõppu, **välja arvatud juhul, kui asjaomane liikmesriik seda taotleb või** [...] **koostöörühma vastava ettepanekuga nõustub**.

6. [...]

7. Vastastikuse [...] **õppe voorudes** osalevad eksperdid koostavad aruanded [...] **hindamiste** tulemuste ja järelduste kohta. **Liikmesriikidel lubatakse esitada oma aruannete projektide kohta märkusi, mis lisatakse aruandele. Lõpp**aruanded esitatakse [...] koostöörühmale;[...] **liikmesriigid võivad otsustada teha oma aruanded üldsusele kättesaadavaks.**

IV PEATÜKK

Küberturvalisuse riskijuhtimis- ja teatamiskohustused

I JAGU

Küberturvalisuse riskijuhtimine ja teatamine

Artikkel 17

Juhtimine

1. Liikmesriigid tagavad, et elutähtsate ja oluliste üksuste juhtorganid kinnitavad asjaomaste üksuste võetavad küberturvalisuse riskijuhtimise meetmed, et tagada kooskõla artikliga 18, [...] **teevad järelevalvet** selle rakendamise üle ning neid saab **vastutusele võtta** selle eest, kui üksused ei täida kõnealusest artiklist tulenevaid kohustusi.

   Käesoleva lõike kohaldamine ei piira liikmesriigi õigusaktide kohaldamist seoses avaliku sektori asutuste vastutust käsitlevate normidega ja avalike teenistujate ning valitud ja ametisse nimetatud ametnike vastutusega.

2. Liikmesriigid tagavad, et **juhtorgani liikmetelt** [...] **nõutakse** korrapäraselt osalemist [...] koolitustel, mis võimaldavad omandada piisavad teadmised ja oskused, et mõista ja hinnata küberturvalisuse riske ja nende juhtimise tavasid ning nendest tulenevat mõju üksuse tegevusele.

Artikkel 18

Küberturvalisuse riskijuhtimismeetmed

1**a.** **Käesoleva direktiiviga kohaldatakse kõiki ohte hõlmavat lähenemisviisi, mis hõlmab võrgu- ja infosüsteemide ning nende füüsilise keskkonna kaitset mis tahes sündmuse eest, mis võib ohustada salvestatavate, edastatavate või töödeldavate andmete või võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust või konfidentsiaalsust.**

1. Liikmesriigid tagavad, et elutähtsad ja olulised üksused [...] võtavad asjakohased ja proportsionaalsed tehnilised ja korralduslikud meetmed, et juhtida riske, mis ohustavad nende üksuste teenuste osutamisel kasutatavate võrgu- ja [...] infosüsteemide turvalisust. Tehnika taset **ja rakendamise kulusid** arvesse võttes tagatakse nende meetmete rakendamisega ähvardavale ohule vastav võrgu- ja infosüsteemide turvalisuse tase. **Kõnealuste meetmete proportsionaalsuse hindamisel võetakse nõuetekohaselt arvesse üksuse avatust riskile, selle suurust, intsidentide esinemise tõenäosust ja nende tõsidust. Võttes arvesse elutähtsaid või olulisi üksusi mõjutavate intsidentide korral ühiskonnale tuleneva riski taset ja liiki, võivad oluliste üksuste suhtes kehtestatud küberturvalisuse riskijuhtimismeetmed olla leebemad kui elutähtsate üksuste suhtes kehtestatud meetmed.**

2. Lõikes 1 osutatud meetmed hõlmavad vähemalt järgmist:

a) riskianalüüsid ja infosüsteemide turbe põhimõtted;

b) intsidentide käsitlemine (intsidentide ennetamine, tuvastamine, [...] lahendamine **ja nendest taastumine**);

c) talitluspidevus ja kriisiohje;

d) tarneahela turvalisus, sealhulgas sellised turvalisusesse puutuvad aspektid, mis on seotud iga üksuse ja tema **otseste** tarnijate või teenuseosutajate, näiteks andmesalvestuse ja -töötluse teenuste või turbetarnijate vaheliste suhetega;

e) võrgu- ja infosüsteemide hankimise, arendamise ja hooldamise turvalisus, sealhulgas nõrkuste käsitlemine ja avalikustamine;

f) tööpõhimõtted ja menetluskord [...] küberturvalisuse riskijuhtimismeetmete tõhususe hindamiseks;

g) krüptograafia ja krüpteerimise kasutamist **käsitlevad põhimõtted**;

ga) personali turvalisus, juurdepääsukontrolli põhimõtted ja varade haldus.

3. Liikmesriigid tagavad, et lõike 2 punktis d osutatud asjakohaseid meetmeid kaaludes [...] **peavad** üksused arvesse võtma igale **otsesele** tarnijale ja teenuseosutajale eriomaseid nõrkusi ning nende tarnijate ja teenuseosutajate toodete üldist kvaliteeti ja küberturvalisuse tavasid, sealhulgas nende turvalise arenduse korda. **Liikmesriigid tagavad samuti, et lõike 2 punktis d osutatud asjakohaseid meetmeid kaaludes peavad üksused arvesse võtma artikli 19 lõike 1 kohaselt korraldatud koordineeritud riskihindamiste tulemusi.**

4. Liikmesriigid tagavad, et üksus, kes leiab, et tema teenused või ülesanded ei vasta lõikes 2 sätestatud nõuetele, võtab põhjendamatu viivituseta kõik vajalikud parandusmeetmed asjaomase teenuse nõuetega vastavusse viimiseks.

5. Komisjon võib vastu võtta rakendusakte, millega kehtestatakse **käesoleva artikli** lõikes 2 osutatud elementide tehnilised ja metoodilised spetsifikatsioonid **ning vajaduse korral ka valdkondlikud eripärad**. **Komisjon võtab hiljemalt [18 kuud pärast käesoleva direktiivi jõustumise kuupäeva] vastu rakendusaktid, millega kehtestatakse tehnilised ja metoodilised spetsifikatsioonid artikli 24 lõikes 1 osutatud üksuste jaoks ja I lisa punktis 8 osutatud usaldusteenuse osutajate jaoks. Need rakendusaktid võetakse vastu kooskõlas artikli 37 lõikes 2 osutatud kontrollimenetlusega. Selliseid rakendusakte** [...] ette valmistades ja rakendades [...] **järgib** komisjon võimalikult suures ulatuses rahvusvahelisi ja Euroopa standardeid ning asjakohaseid tehnilisi spetsifikatsioone **ja vahetab artikli 12 lõike 4 punkti d kohaselt koostöörühma ning ENISAga nõuandeid rakendusakti eelnõu kohta.**

6. [...]

Artikkel 19

Kriitilise tähtsusega tarneahelate ELi koordineeritud riskihindamised

1. Koostöörühm võib koostöös komisjoni ja ENISAga teha kindlate kriitilise tähtsusega IKT-teenuste, -süsteemide või -toodete tarneahelate turvalisusega seotud riskide koordineeritud hindamisi, võttes arvesse tehnilisi ja asjakohasel juhul ka muid kui tehnilisi riskitegureid.

2. Komisjon määrab pärast koostöörühma ja ENISAga konsulteerimist kindlaks konkreetsed kriitilise tähtsusega IKT-teenused, -süsteemid või -tooted, mille suhtes võib kohaldada lõikes 1 osutatud koordineeritud riskihindamist.

Artikkel 20

Teatamiskohustus

1. Liikmesriigid tagavad, et elutähtsad ja olulised üksused teavitavad põhjendamatu viivituseta pädevaid asutusi või CSIRTi vastavalt lõigetele 3 ja 4 kõikidest intsidentidest, mis nende teenuste osutamist märkimisväärselt mõjutavad. Kui see on asjakohane, teavitavad kõnealused üksused põhjendamatu viivituseta oma teenuste kasutajaid **sellistest** intsidentidest, mis tõenäoliselt kahjustavad kõnealuse teenuse osutamist. Liikmesriigid tagavad, et kõnealused üksused esitavad muu hulgas teabe, mis võimaldab pädevatel asutustel või CSIRTil teha kindlaks intsidendi piiriülese mõju. **Teatamine kui selline ei suurenda teavitava üksuse vastutust.**

2. [...]

   Kui see on asjakohane, teavitavad [...] **elutähtsad ja olulised** üksused põhjendamatu viivituseta oma teenuste kasutajaid, keda oluline küberoht võib mõjutada, meetmetest või parandusmeetmetest, mida teenuste kasutajad saavad ohule reageerimiseks võtta. Kui see on asjakohane, teavitavad üksused teenuste kasutajaid ka ohust endast. Teatamine **kui selline** ei suurenda teavitava üksuse vastutust.

3. Intsidenti käsitatakse olulisena, kui:

a) intsident on põhjustanud või võib põhjustada asjaomase üksuse **teenusega seotud** [...] tegevuse **olulisi** katkestusi või asjaomasele üksusele rahalist kahju;

b) intsident on mõjutanud või võib mõjutada teisi füüsilisi või juriidilisi isikuid, põhjustades märkimisväärset materiaalset või mittemateriaalset kahju.

4. Liikmesriigid tagavad, et lõike 1 kohase teavitamise eesmärgil esitavad asjaomased üksused pädevatele asutustele või CSIRTile järgmise:

a) põhjendamatu viivituseta ning igal juhul hiljemalt 24 tunni jooksul pärast intsidendist teada saamist **varajase hoiatusena** esialgse teate, milles vajaduse korral märgitakse, kas intsidendi põhjuseks on eeldatavasti ebaseaduslik või pahatahtlik tegevus;

b) pädeva asutuse või CSIRTi taotlusel vahearuande vaatlusaluste asjade seisu kohta;

c) hiljemalt üks kuu pärast punktis a osutatud [...]**esialgse teate** esitamist **lõpp**aruande, mis sisaldab vähemalt järgmist:

i) intsidendi, selle raskuse ja mõju üksikasjalik kirjeldus;

ii) intsidendi tõenäoliselt põhjustanud ohu liik või algpõhjus;

iii) juba kohaldatud ja kohaldamisel olevad leevendusmeetmed.

Liikmesriigid näevad ette, et nõuetekohaselt põhjendatud juhtudel ning kokkuleppel pädevate asutuste või CSIRTiga võib asjaomane üksus punktides a ja c sätestatud tähtaegadest kõrvale kalduda. **Eelkõige võib punktis c osutatud tähtajast kõrvalekaldumine olla põhjendatud juhtudel, kui intsident veel jätkub.**

5. Pädevad riiklikud asutused või CSIRT annavad [...] **põhjendamatu viivituseta** pärast lõike 4 punktis a osutatud esialgse teate saamist teavitavale üksusele vastuse, mis sisaldab esialgset tagasisidet intsidendi kohta ja üksuse vastava taotluse korral võimalike leevendusmeetmete rakendamise suuniseid. Kui CSIRT ei ole lõikes 1 osutatud teadet saanud, annab kõnealused suunised pädev asutus koostöös CSIRTiga. CSIRT pakub täiendavat tehnilist tuge, kui asjaomane üksus seda taotleb. Kui kahtlustatakse, et intsident on seotud kuritegevusega, annavad pädevad riiklikud asutused või CSIRT juhised ka selle kohta, kuidas teavitada intsidendist õiguskaitseasutusi.

6. Kui see on asjakohane ja eelkõige juhul, kui lõikes 1 osutatud intsident puudutab kahte või enamat liikmesriiki, peab pädev asutus, CSIRT või **ühtne kontaktpunkt** teavitama intsidendist teisi mõjutatud liikmesriike ja ENISAt. **Kõnealune teave peab sisaldama vähemalt käesoleva artikli lõikes 4 ette nähtud elemente.** Seda tehes kaitsevad pädevad asutused, CSIRTid ja ühtsed kontaktpunktid kooskõlas liidu õigusega või liidu õigusele vastavate siseriiklike õigusaktidega üksuse turvalisust ja ärihuve ning esitatud teabe konfidentsiaalsust.

7. Kui üldsuse teadlikkus või intsidendi avalikustamine on vajalik intsidendi ärahoidmiseks või käimasoleva intsidendi lahendamiseks või see on muul moel üldsuse huvides, võib pädev asutus või CSIRT või, kui see on asjakohane, ka teiste asjaomaste liikmesriikide asutused või CSIRTid, teavitada üldsust intsidendist või nõuda, et asjaomane üksus seda teeks, olles eelnevalt konsulteerinud asjaomase üksusega.

8. Pädeva asutuse või CSIRTi taotlusel edastab ühtne kontaktpunkt lõike[...] 1 [...]kohaselt saadud teated teiste mõjutatud liikmesriikide ühtsetele kontaktpunktidele.

9. Ühtne kontaktpunkt esitab ENISA-le [...] **iga kuue kuu tagant** koondaruande, mis sisaldab anonüümseid koondandmeid lõike[...] 1 [...] ning artikli 27 kohaselt teatatud intsidentide, oluliste küberohtude ja ohuolukordade kohta. Võrreldava teabe esitamise soodustamiseks võib ENISA anda kokkuvõtvas aruandes esitatava teabe parameetrite kohta tehnilisi suuniseid. **ENISA teavitab iga kuue kuu järel koostöörühma ja CSIRTide võrgustikku oma järeldustest saadud teadete kohta.**

10. Pädevad asutused esitavad direktiivi (EL) XXXX/XXXX [kriitilise tähtsusega üksuste vastupidavusvõime direktiiv] kohaselt määratud pädevatele asutustele teavet intsidentide ja küberohtude kohta, millest on lõigete 1 ja 2 kohaselt teatanud üksused, mida käsitatakse kriitilise tähtsusega üksustena **[**või kriitilise tähtsusega üksustega samaväärsete üksustena**]** direktiivi (EL) XXXX/XXXX [kriitilise tähtsusega üksuste vastupidavusvõime direktiiv] alusel.

11. Komisjon võib võtta vastu rakendusakte, milles täpsustatakse lõigete 1 ja 2 kohaselt esitatava teate teabe liik, vorming ning esitamise kord. Komisjon võib ka võtta vastu rakendusakte, millega täpsustatakse, millisel juhul käsitatakse intsidenti olulisena, nagu on osutatud lõikes 3. Kõnealused rakendusaktid võetakse vastu kooskõlas artikli 37 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 21

Euroopa küberturvalisuse sertifitseerimise kavade kasutamine

1. Et tõendada vastavust artikli 18 teatavatele nõuetele, **võivad liikmesriigid nõuda üksustelt selliste teatavate IKT-toodete, -teenuste ja**[...] **-protsesside** kasutamist, mis on **sertifitseeritud** määruse (EL) 2019/881 artikli 49 kohaselt vastu võetud konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade alusel. Sertifitseerimisele kuuluvad **IKT-**tooted, -teenused ja -protsessid võib välja töötada elutähtis või oluline üksus või need võidakse tellida kolmandatelt isikutelt.

2. Komisjon võib [...] võtta vastu [...] **rakendus**akte, milles täpsustatakse, millist liiki elutähtsatelt **või olulistelt** üksustelt nõutakse t**eatavate sertifitseeritud IKT-toodete, -teenuste ja -protsesside kasutamist või** millisel **määruse (EL) 2019/881 artikli 49 kohaselt vastu võetud** Euroopa küberturvalisuse sertifitseerimise kaval [...] põhineva [...] sertifikaadi omandamist.[...] **Need rakendusaktid võetakse vastu kooskõlas artikli 37 lõikes 2 osutatud kontrollimenetlusega. Kõnealuste rakendusaktide koostamisel teeb komisjon määruse (EL) 2019/881 artikli 56 kohaselt järgmist:**

   i) võtab arvesse mõju, mida avaldavad meetmed selliste IKT-toodete, -teenuste või -protsesside tootjatele või pakkujatele ja kasutajatele nende meetmete kulude seisukohast, ning sotsiaalset ja majanduslikku kasu, mis tuleneb asjaomaste IKT-toodete, -teenuste või -protsesside turvalisuse taseme eeldatavast paranemisest, samuti nende alternatiivide kättesaadavusest turul;

   ii) konsulteerib kõigi asjaomaste sidusrühmade ja liikmesriikidega avatud, läbipaistval ja kaasaval viisil;

iii) võtab arvesse rakendamise tähtpäevi, üleminekumeetmeid ja -tähtaegu, eelkõige seoses meetmete võimaliku mõjuga IKT-toodete, -teenuste või -protsesside tootjatele, pakkujatele või kasutajatele, eelkõige VKEdele;

iv) võtab arvesse asjaomase liikmesriikide õiguse olemasolu ja rakendamist.

3. Kui asjakohast Euroopa küberturvalisuse sertifitseerimise kava **käesoleva artikli** lõike 2 kohaldamiseks ei ole, võib komisjon määruse (EL) 2019/881 artikli 48 lõike 2 kohaselt taotleda ENISA-lt ettevalmistava kava koostamist **või olemasoleva Euroopa küberturvalisuse sertifitseerimise kava läbivaatamist**.

Artikkel 22

Standardimine

1. Et edendada artikli 18 lõigete 1 ja 2 ühtset kohaldamist, toetavad liikmesriigid võrgu- ja infosüsteemide turvalisust käsitlevate Euroopa või rahvusvaheliselt heaks kiidetud standardite ja spetsifikatsioonide rakendamist, ilma et nad seejuures nõuaksid või soosiksid konkreetset tüüpi tehnoloogia kasutamist.

2. ENISA koostab koostöös liikmesriikidega nõuanded ja suunised seoses tehniliste valdkondadega, mida tuleks lõike 1 puhul arvesse võtta, ning seoses olemasolevate, sealhulgas liikmesriikide standarditega, mis võimaldaksid neid valdkondi hõlmata.

Artikkel 23

Domeeninimede ja registreerimisandmete andmebaasid

1. Et aidata suurendada domeeninimesüsteemi turvalisust, stabiilsust ja vastupanuvõimet, tagavad liikmesriigid, et tippdomeeni**nimede** registrid ja tippdomeenide domeeninimede registreerimise teenuseid osutavad üksused koguvad ja säilitavad täpseid**, [...]** ja täielikke domeeninimede registreerimise andmeid spetsiaalses andmebaasis, kohaldades isikuandmetena käsitatavate andmetega seoses hoolsust **vastavalt** [...] liidu andmekaitsealastele õigusaktidele.

2. Liikmesriigid tagavad, et lõikes 1 osutatud domeeninimede registreerimise andmete andmebaasid sisaldavad asjakohast teavet, mis võimaldab kindlaks teha domeeninimede omanikud ja tippdomeenide all domeeninimesid haldavad kontaktpunktid ning nendega ühendust võtta**, sealhulgas vähemalt järgmisi andmeid:**

   a) domeeninimi;

   b) registreerimise kuupäev;

   c) registreerija andmed, sealhulgas:

      i) üksikisikute puhul ees- ja perekonnanimi ning e-posti aadress;

      ii) juriidiliste isikute puhul nimi ja e-posti aadress.

3. Liikmesriigid tagavad, et tippdomeeni**nimede** registrid ja tippdomeenide domeeninimede registreerimise teenuseid osutavad üksused kehtestavad töö põhimõtted ja menetluskorra, millega tagatakse, et andmebaasid sisaldavad täpset ja täielikku teavet. Liikmesriigid tagavad, et osutatud põhimõtted ja menetluskord tehakse üldsusele kättesaadavaks.

4. Liikmesriigid tagavad, et tippdomeeni**nimede** registrid ja tippdomeenide domeeninimede registreerimise teenuseid osutavad üksused avaldavad põhjendamatu viivituseta pärast domeeninime registreerimist need domeeni registreerimise andmed, mis ei ole isikuandmed.

5. Liikmesriigid tagavad, et tippdomeeni**nimede** registrid ja tippdomeenide jaoks domeeninimede registreerimise teenuseid osutavad üksused võimaldavad õigustatud taotlejatele õiguspärast ja nõuetekohaselt põhjendatud juurdepääsu domeeninimede registreerimise andmetele kooskõlas liidu andmekaitseõigusega. Liikmesriigid tagavad, et tippdomeeni**nimede** registrid ja tippdomeenide domeeninimede registreerimise teenuseid osutavad üksused vastavad põhjendamatu viivituseta **ja igal juhul 72 tunni jooksul** kõigile juurdepääsutaotlustele. Liikmesriigid tagavad, et selliste andmete avalikustamise põhimõtted ja kord tehakse üldsusele kättesaadavaks.

II jaotis

Jurisdiktsioon ja registreerimine

Artikkel 24

Jurisdiktsioon ja territoriaalsus

1a. Käesoleva direktiivi kohaselt käsitatakse üksusi selle liikmesriigi jurisdiktsiooni alla kuuluvana, kus nad oma teenuseid osutavad. I lisa punktides 1–7 ja 10 osutatud üksusi, I lisa punktis 8 osutatud usaldusteenuse osutajaid ja interneti vahetuspunkti teenuse osutajaid ning II lisa punktides 1–5 osutatud üksusi käsitatakse selle liikmesriigi jurisdiktsiooni alla kuuluvana, kus on nende tegevuskoht.

1. Domeeninimesüsteemi teenuse osutajad, tippdomeeninimede registrid[...] ja **tippdomeenide domeeninimede registreerimise teenuseid osutavad üksused**, pilvandmetöötlusteenuse osutajad, andmekeskusteenuse osutajad, [...] sisulevivõrgu pakkujad**, hallatud teenuste osutajad ja turbetarnijad** kellele on osutatud I lisa punktides 8 **ja 8a**, ning digiteenuse osutajad, kellele on osutatud II lisa punktis 6, loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on nende peamine tegevuskoht liidus.

2. Käesoleva direktiivi kohaldamisel käsitatakse lõikes 1 osutatud üksuste peamise tegevuskohana seda liidu liikmesriiki, kus küberturvalisuse riskijuhtimismeetmeid käsitlevad otsused **valdavalt** tehakse. Kui **kohta, kus selliseid otsuseid valdavalt tehakse, ei ole võimalik kindlaks teha või** kui kõnealuseid otsuseid ei tehta liidus asuvas üksuses, siis tuleks peamise tegevuskohana käsitada seda liikmesriiki, kus asuvas tegevuskohas on üksusel liidus kõige rohkem töötajaid. **Kui teenuseid osutab kontsern, tuleks peamise tegevuskohana käsitada kontserni peamist tegevuskohta.**

3. Kui lõikes 1 osutatud üksus ei asu liidus, kuid pakub liidus oma teenuseid, määrab ta endale liidus esindaja. Esindaja asukohaks on üks nendest liikmesriikidest, kus teenuseid osutatakse. Kõnealust üksust käsitatakse selle liikmesriigi jurisdiktsiooni alla kuuluvana, kus on esindaja tegevuskoht. Kui käesoleva artikli kohaselt esindajat määratud ei ole, võib käesolevast direktiivist tulenevaid kohustusi mittetäitva üksuse vastu õiguslikke meetmeid võtta iga liikmesriik, kus üksus teenuseid osutab.

4. Lõikes 1 osutatud üksuse poolt esindaja määramine ei piira üksuse enda vastu õiguslike meetmete võtmist.

4a. Liikmesriigid, kes on saanud vastastikuse abi taotluse seoses lõikes 1 osutatud üksustega, võivad võtta taotluse ulatuses asjakohaseid järelevalve- ja täitemeetmeid asjaomase üksuse suhtes, kes osutab teenuseid või kellel on nende riikide territooriumil võrgu- ja infosüsteem.

Artikkel 25

Teatavate digitaristu üksuste ja digiteenuse osutajate register

1. [...] **Liikmesriigid tagavad, et artikli 24 lõikes 1 osutatud** üksused, **kelle peamine tegevuskoht on nende territooriumil, või kui neil liidus tegevuskohta ei ole, siis üksused, kelle määratud esindajal liidus on tegevuskoht nende territooriumil, peavad** [...] esitama **pädevatele asutustele** järgmise teabe [...] hiljemalt [12 kuud pärast käesoleva direktiivi jõustumist]:

a) üksuse nimi;

aa) üksuse liik vastavalt käesoleva direktiivi I ja II lisale;

b) tema peamise tegevuskoha ja liidu muude ametlike tegevuskohtade aadress või kui tal liidus tegevuskohta ei ole, siis tema artikli 24 lõike 3 kohaselt määratud esindaja aadress;

c) ajakohased kontaktandmed, sealhulgas üksuste **ning nende esindajate** e-posti aadressid ja telefoninumbrid**;**

d) liikmesriigid, kus üksus teenust osutab.

Kui see on asjakohane, esitatakse see teave artiklis 2a osutatud riikliku enesest teavitamise mehhanismi kaudu.

2. **Liikmesriigid tagavad, et** [...]lõikes 1 osutatud üksused [...] **teatavad samuti** viivitamata lõike 1 kohaselt esitatud üksikasjade muutumisest, tehes seda igal juhul hiljemalt kolme kuu jooksul alates muudatuse jõustumise kuupäevast.

3. [...] **Liikmesriikide ühtsed kontaktpunktid** edastavad **lõigetes 1 ja 2 osutatud teabe** [...] **ENISA-le**. [...]

3a. Käesoleva artikli lõike 3 kohaselt saadud teabe põhjal loob ENISA lõikes 1 osutatud üksuste registri ja haldab seda. Liikmesriikide taotluse korral võimaldab ENISA asjaomastele pädevatele asutustele juurdepääsu registrile, tagades samal ajal vajalikud tagatised teabe konfidentsiaalsuse kaitsmiseks, kui see on asjakohane.

4. [...]

V PEATÜKK

Teabevahetus

Artikkel 26

Küberturvalisuse alase teabevahetuse kord

1. [...] Liikmesriigid tagavad, et elutähtsad ja olulised üksused saavad omavahel **vabatahtlikult** vahetada asjakohast küberturvalisuse teavet, sealhulgas teavet, mis on seotud küberohtude, **ohuolukordade,** nõrkuste, rikkeindikaatorite, taktikate, meetodite ja menetluste, küberturvalisuse hoiatussüsteemide ja konfiguratsioonivahenditega, kui selline teabe jagamine:

   a) toimub intsidentide ennetamise, tuvastamise, lahendamise või nende tagajärgede leevendamise eesmärgil;

b) aitab tõsta küberturvalisuse taset, eelkõige küberohtude alase teadlikkuse suurendamise ning kõnealuste ohtude leviku piiramise või takistamise kaudu ning toetades mitmesuguseid kaitsevõimalusi, nõrkuste vähendamist ja avalikustamist, ohu tuvastamise meetodeid, leevendusstrateegiaid või lahendamis- ja taastamisetappe.

2. Liikmesriigid tagavad, et teabevahetus toimub elutähtsate ja oluliste üksuste [...] kogukondades. Kõnealune teabevahetus toimub kokkulepitud teabevahetuse korra alusel, mis arvestab jagatud teabe võimalikku tundlikku laadi [...].

3. Liikmesriigid [...] **võivad** kehtestada eeskirjad, millega täpsustatakse lõikes 2 osutatud teabevahetuse korraldusega seotud menetluskord, tegevusaspektid (sealhulgas sihtotstarbeliste IKT-platvormide kasutamine), sisu ja tingimused. Selliste eeskirjadega [...] **võidakse** sätestada ka üksikasjad, mis puudutavad avaliku sektori asutuste kaasamist kõnealuse korraldusega seotud lepetesse, samuti tegevusaspektid, sealhulgas sihtotstarbeliste IT-platvormide kasutamine. Liikmesriigid toetavad kõnealuste korralduslepete rakendamist lähtuvalt artikli 5 lõike 2 punktis g osutatud poliitikameetmetest.

4. Elutähtsad ja olulised üksused teatavad pädevatele asutustele oma osalemisest lõikes 2 osutatud teabevahetuse korralduse lepetes, kui nad on selliste lepetega ühinenud, ning (kui on asjakohane) lepetest taganemisest pärast taganemise jõustumist.

5. [...] ENISA toetab lõikes 2 osutatud küberturvalisuse alase teabevahetuse korra väljatöötamist, pakkudes parimate tavade teavet ja suuniseid.

Artikkel 27

Asjakohase teabe vabatahtlik edastamine

1. **Ilma et see piiraks artikli 20 kohaldamist, tagavad liikmesriigid, et elutähtsad ja olulised üksused võivad vabatahtlikult teatada pädevatele asutustele või CSIRTile asjakohastest intsidentidest, küberohtudest või ohuolukordadest.**

2. Ilma et see piiraks artikli 3 kohaldamist, tagavad liikmesriigid, et käesoleva direktiivi kohaldamisalast välja jäävatel üksustel on võimalik vabatahtlikult teatada olulistest intsidentidest, küberohtudest või ohuolukordadest. Teadete läbivaatamisel järgivad liikmesriigid artiklis 20 sätestatud menetluskorda. Liikmesriigid võivad vaadata kohustuslikud teated läbi enne vabatahtlikke teateid. **Ilma, et see piiraks süütegude uurimist, avastamist ja nende eest vastutusele võtmist,** [...]ei kaasne vabatahtliku teatamisega teavitava üksuse jaoks mingeid täiendavaid kohustusi, mida tal ei oleks olnud, kui ta ei oleks teadet edastanud.

3. **Vabatahtlikud teated vaadatakse läbi üksnes juhul, kui selline läbivaatamine ei ole asjaomase liikmesriigi jaoks ebaproportsionaalselt ega liigselt koormav.**

VI PEATÜKK

Järelevalve ja täitmise tagamine

Artikkel 28

Järelevalve ja täitmise tagamise üldised aspektid

1. Liikmesriigid tagavad, et pädevad asutused teevad tõhusat järelevalvet ning võtavad vajalikke meetmeid käesoleva direktiivi,[...] eelkõige selle artiklites 18**,** [...] 20 **ja 23** sätestatud kohustuste täitmise tagamiseks. **Liikmesriigid võivad lubada pädevatel asutustel seada prioriteediks järelevalve, mis põhineb riskipõhisel lähenemisviisil.**

2. Pädevad asutused teevad küberturvalisuse intsidentide lahendamisel tihedat koostööd andmekaitseasutuste, **direktiivi (EL) XXXX/XXXX [kriitilise tähtsusega üksuste vastupidavusvõime direktiiv] kohaselt määratud pädevate asutuste, määruse (EL) nr 910/2014 kohaselt määratud järelevalveasutuste ning muude valdkondlike liidu õigusaktide kohaselt määratud pädevate asutustega**. [...]

3. Ilma et see piiraks riiklike õigus- ja institutsiooniliste raamistike kohaldamist, tagavad liikmesriigid, et järelevalve teostamisel selle üle, kas avaliku halduse üksused täidavad käesoleva direktiivi nõudeid, ning võimalike karistuste rakendamisel nõuete täitmata jätmise eest, on pädevatel asutustel asjakohased volitused selliste ülesannete täitmiseks ja nende tegevus on järelevalve alla kuuluvatest üksustest sõltumatu. Liikmesriigid võivad otsustada, et kõnealuste üksuste suhtes kehtestatakse asjakohased, proportsionaalsed ja tõhusad järelevalve ja täitmise tagamise meetmed kooskõlas riiklike raamistike ja õiguskorraga.

Artikkel 29

Järelevalve ja täitmise tagamine elutähtsate üksuste puhul

1. Liikmesriigid tagavad, et käesolevas direktiivis sätestatud kohustustega seoses elutähtsate üksuste suhtes kohaldatavad järelevalve- või täitemeetmed on tõhusad, proportsionaalsed ja heidutavad ning et nende puhul võetakse arvesse iga üksikjuhtumi asjaolusid.

2. Liikmesriigid tagavad, et pädevad asutused **järgivad** elutähtsate üksustega seotud järelevalveülesannete täitmisel **riskipõhist lähenemisviisi ning et neil on** õigus kohaldada kõnealuste üksuste suhtes **vähemalt** järgmisi meetmeid:

   a) teha kohapealset kontrolli ja kaugjärelevalvet, sh pistelisi kontrolle;

   b) teha korrapäraseid **turva**auditeid;

   c) teha sihipäraseid turvaauditeid, mis põhinevad riskihindamisel või kättesaadaval riskidega seotud teabel;

   d) teha **koostöös asjaomase üksusega** objektiivsetel, mittediskrimineerivatel, õiglastel ja läbipaistvatel riskihindamiskriteeriumidel põhinevaid turvalisuse kontrolle**, kui see on tehnilistel põhjustel vajalik**;

   e) esitada teabenõudeid, mis on vajalikud üksuse võetud küberturvalisuse meetmete, sealhulgas tema dokumenteeritud küberturvalisuspoliitika hindamiseks[...];

   f) nõuda juurdepääsu andmetele, dokumentidele või mis tahes teabele, mis on vajalik järelevalveülesannete täitmiseks;

   g) nõuda küberturvalisuspoliitika rakendamise tõendamist, näiteks kvalifitseeritud audiitori tehtud turvaauditite tulemusi ja nende aluseks olevaid tõendeid.

2a. Käesoleva artikli lõikes 2 sätestatud järelevalveülesannete täitmisel võivad pädevad asutused kehtestada järelevalvemeetodid, mis võimaldavad selliseid ülesandeid riskipõhise lähenemisviisi alusel prioriseerida.

3. Lõike 2 punktides e–g sätestatud volituste rakendamisel märgivad pädevad asutused ära taotluse eesmärgi ja täpsustavad, millist teavet nõutakse.

4. Liikmesriigid tagavad, et pädevatel asutustel on elutähtsate üksustega seotud täitmise tagamise volituste rakendamisel õigus teha **vähemalt** järgmist:

a) teha hoiatusi selle kohta, et üksused ei täida käesolevas direktiivis sätestatud kohustusi;

b) anda siduvaid juhiseid või korraldusi, millega nõutakse, et kõnealused üksused kõrvaldaksid tuvastatud puudused või heastaksid käesolevas direktiivis sätestatud kohustuste rikkumise;

c) anda kõnealustele üksustele korraldus lõpetada tegevus, mis ei ole kooskõlas käesolevas direktiivis sätestatud nõuetega, ja hoiduda sellist tegevust kordamast;

d) kohustada kõnealuseid üksuseid viima kindlaksmääratud viisil ja kindlaksmääratud ajavahemiku jooksul oma riskijuhtimis- ja/või teatamiskohustuse täitmise meetmed vastavusse artiklites 18 ja 20 sätestatud nõuetega;

e) kohustada kõnealuseid üksuseid teavitama füüsilisi või juriidilisi isikuid, kellele osutatakse teenuseid või kellega seoses toimub tegevus, mida võib mõjutada oluline küberoht, **ohu laadist ning** võimalikest kaitse- või parandusmeetmetest, mida asjaomased füüsilised või juriidilised isikud võivad vastavale ohule reageerimiseks võtta;

f) kohustada kõnealuseid üksusi rakendama mõistliku aja jooksul turvaauditi tulemuste alusel tehtud soovitusi;

g) [...]

h) kohustada kõnealuseid üksuseid avalikustama kindlaksmääratud viisil käesolevas direktiivis sätestatud kohustuste täitmata jätmisega seotud aspektid**, kui sellisel avalikustamisel ei ole asjaomasele üksusele kahjulikku toimet**;

i) [...]

j) määrata või taotleda, et asjaomased asutused või kohtud määraksid vastavalt siseriiklikele õigusaktidele haldustrahvi kooskõlas artikliga 31 lisaks käesoleva lõike punktides a–i osutatud meetmetele või nende asemel, olenevalt konkreetse juhtumi asjaoludest.

5. Kui lõike 4 punktide a–d ja f kohaselt võetud täitmismeetmed ei anna tulemust, tagavad liikmesriigid, et pädevatel asutustel on õigus kehtestada tähtaeg, mille jooksul peab elutähtis üksus võtma vajalikud meetmed puuduste kõrvaldamiseks või kõnealuste asutuste esitatud nõuete täitmise tagamiseks. Liikmesriigid tagavad, et kui nõutavat meedet ettenähtud tähtaja jooksul ei võeta, on pädevatel asutustel õigus:

a) peatada või taotleda, et sertifikaate või lube väljastav asutus **või kohus** peataks **vastavalt siseriiklikele õigusaktidele** elutähtsa üksuse kõigi või mõnede osutatavate teenuste või tegevuste sertifikaadi või loa;

b) keelata või taotleda, et asjaomased asutused või kohtud keelaksid siseriikliku õiguse kohaselt isikul, kes täidab selles elutähtsas üksuses tegevjuhina või seadusliku esindajana juhtimisülesandeid, või rikkumise eest vastutaval muul füüsilisel isikul selles elutähtsas üksuses ajutiselt juhtimisülesannete täitmise.

Neid karistusi kohaldatakse ainult seni, kuni üksus võtab vajalikud meetmed nende puuduste kõrvaldamiseks või pädeva asutuse nende nõuete täitmiseks, mille tõttu karistusi kohaldati.

Käesolevas lõikes sätestatud karistusi ei kohaldata selliste avaliku halduse üksuste suhtes, kelle suhtes kohaldatakse käesolevat direktiivi.

6. Liikmesriigid tagavad, et elutähtsa üksuse eest vastutaval või seda esindaval isikul, keda on volitatud üksust esindama, üksuse nimel otsuseid tegema või üksuse tegevust kontrollima, on pädevus tagada käesolevas direktiivis sätestatud kohustuste täitmine. Liikmesriigid tagavad, et neid füüsilisi isikuid saab käesolevas direktiivis sätestatud kohustuste täitmata jätmise eest vastutusele võtta. **Avaliku halduse üksuste puhul ei piira käesolev säte liikmesriikide õigusaktide kohaldamist seoses avalike teenistujate ning valitud ja ametisse nimetatud ametnike vastutusega.**

7. Täitemeetmete võtmise või lõigete 4 ja 5 kohaste karistuste kohaldamise korral arvestavad pädevad asutused kaitseõigust ning iga üksikjuhtumi asjaolusid, võttes nõuetekohaselt arvesse vähemalt järgmist:

   a) rikkumise raskusaste ja rikutud sätete tähtsus. Raskete rikkumistena tuleks käsitleda muu hulgas järgmist: korduvad rikkumised, olulise häiriva mõjuga intsidentidest teatamata jätmine või parandusmeetmete võtmata jätmine, pädevatelt asutustelt saadud siduvate juhiste järgi puuduste kõrvaldamata jätmine, rikkumiste tuvastamise järel pädevate asutuste tellitud auditite või järelevalvetegevuse takistamine, valeandmete või lubamatult ebatäpsete andmete esitamine artiklites 18 ja 20 sätestatud riskijuhtimisnõuete või teatamiskohustustega seoses;

b) rikkumise kestus ja rikkumiste korduvus;

c) tegelikult põhjustatud kahju või potentsiaalne kahju, mis oleks võinud kaasneda, kuivõrd seda on võimalik kindlaks määrata. Selle aspekti hindamisel võetakse muu hulgas arvesse tegelikku või potentsiaalset rahalist või majanduslikku kahju, mõju teistele teenustele ja mõjutatud või potentsiaalselt mõjutatud kasutajate arvu;

d) asjaolu, kas rikkumine oli tahtlik või tulenes hooletusest;

e) meetmed, mida üksus on võtnud kahju ennetamiseks või vähendamiseks;

f) kinnitatud tegevusjuhendite järgimine või kinnitatud sertifitseerimismehhanismide rakendamine;

g) vastutava(te) füüsilis(t)e või juriidilis(t)e isiku(te) ja pädeva asutuse koostöö tase.

8. Pädevad asutused esitavad oma täitmisotsuste üksikasjaliku põhjenduse. Enne selliste otsuste tegemist teavitavad pädevad asutused asjaomaseid üksusi oma esialgsetest järeldustest ja jätavad neile mõistliku aja märkuste esitamiseks**, välja arvatud vahetu ohu korral**.

9. Liikmesriigid tagavad, et nende **käesoleva direktiivi kohased** pädevad asutused teavitavad direktiivi (EL) XXXX/XXXX [kriitilise tähtsusega üksuste vastupidavusvõime direktiiv] kohaselt määratud pädevaid asutusi **samas** [...] liikmesriigis [...], kui nad rakendavad käesoleva direktiiviga sätestatud kohustuste täitmise tagamise eesmärgil direktiivi (EL) XXXX/XXXX [kriitilise tähtsusega üksuste vastupidavusvõime direktiiv] kohaselt kriitilise tähtsusega üksusena **[**või sellega võrdväärse üksusena**]** käsitatava üksuse suhtes oma järelevalve- ja täitmise tagamise volitusi. **Kui see on asjakohane,** [...] **võivad** direktiivi (EL) XXXX/XXXX [kriitilise tähtsusega üksuste vastupidavusvõime direktiiv] kohased pädevad asutused **taotleda käesoleva direktiivi kohastelt** pädevatelt asutustelt[...], **et** viimased rakendaksid oma järelevalve- ja täitmise tagamise **volitusi seoses** käesoleva direktiivi kohaldamisalasse kuuluva elutähtsa üksuse suhtes, keda käsitatakse samuti **direktiivi (EL) XXXX/XXXX [kriitilise tähtsusega üksuste vastupidavusvõime direktiiv] kohaselt** kriitilise tähtsusega üksusena **[**või sellega võrdväärse üksusena**].**

10. Liikmesriigid tagavad, et nende käesoleva direktiivi kohased pädevad asutused teavitavad määruse (EL) XXXX/XXXX [DORA] artikli 29 lõike 1 kohast järelevalvefoorumit, kui nad rakendavad oma järelevalve- ja täitmise tagamise volitusi, et tagada käesolevast direktiivist tulenevate kohustuste täitmine elutähtsa üksuse puhul, keda käsitatakse määruse (EL) XXXX/XXXX [DORA] artikli 28 kohaselt kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajana.

10a. Liikmesriigid tagavad, et nende käesoleva direktiivi kohased pädevad asutused teavitavad asjaomaseid määruse (EL) nr 910/2014 kohaselt määratud pädevaid asutusi, kui nad rakendavad oma järelevalve- ja täitmise tagamise volitusi, et tagada käesolevast direktiivist tulenevate kohustuste täitmine üksuse puhul, keda käsitatakse määruse (EL) nr 910/2014 kohaselt usaldusteenuse osutajana.

Artikkel 30

Järelevalve ja täitmise tagamine oluliste üksuste puhul

1. Liikmesriigid tagavad, et pädevad asutused võtavad vajaduse korral järelevalve järelkontrollimeetmeid (*ex-post*-järelevalve), kui neile esitatakse tõendeid, vihjeid **või teavet** selle kohta, et oluline üksus **väidetavalt** ei täida käesolevas direktiivis, eriti selle artiklites 18 ja 20 sätestatud kohustusi.

2. Liikmesriigid tagavad, et pädevad asutused **järgivad** oluliste üksustega seotud järelevalveülesannete täitmisel **riskipõhist lähenemisviisi ning** et neil on õigus kohaldada kõnealuste üksuste suhtes **vähemalt** järgmisi meetmeid:

   a) teha kohapealseid kontrolle ja kaugjärelevalve korras järelkontrolli (*ex-post*-järelevalvet);

   b) teha sihipäraseid turvaauditeid, mis põhinevad riskihindamisel või kättesaadaval riskidega seotud teabel;

   c) teha **koostöös asjaomase üksusega** objektiivsetel, **mittediskrimineerivatel,** õiglastel ja läbipaistvatel riskihindamiskriteeriumidel põhinevaid turvalisuse kontrolle**, kui see on tehnilistel põhjustel vajalik;**

   d) nõuda teavet, mis on vajalik küberturvalisuse meetmete järelhindamiseks[...];

   e) taotleda juurdepääsu andmetele, dokumentidele ja/või mis tahes teabele, mis on vajalik järelevalveülesannete täitmiseks;

   ea) nõuda küberturvalisuse poliitika rakendamise tõendamist, näiteks kvalifitseeritud audiitori tehtud turvaauditite tulemusi ja nende aluseks olevaid tõendeid.

2a. Käesoleva artikli lõikes 2 sätestatud järelevalveülesannete täitmisel võivad pädevad asutused kehtestada järelevalvemeetodid, mis võimaldavad selliseid ülesandeid riskipõhise lähenemisviisi alusel prioriseerida.

3. Lõike 2 punktides d**–ea** sätestatud volituste rakendamisel märgivad pädevad asutused ära taotluse eesmärgi ja täpsustavad, millist teavet nõutakse.

4. Liikmesriigid tagavad, et pädevatel asutustel on oluliste üksustega seotud täitmise tagamise volituste rakendamisel õigus teha **vähemalt** järgmist:

a) teha hoiatusi selle kohta, et üksused ei täida käesolevas direktiivis sätestatud kohustusi;

b) anda siduvaid juhiseid või korraldusi, millega nõutakse, et kõnealused üksused kõrvaldaksid tuvastatud puudused või heastaksid käesolevas direktiivis sätestatud kohustuse rikkumise;

c) anda kõnealustele üksustele korraldus lõpetada tegevus, mis ei ole kooskõlas käesolevas direktiivis sätestatud nõuetega, ja hoiduda sellist tegevust kordamast;

d) kohustada kõnealuseid üksuseid viima kindlaksmääratud viisil ja kindlaksmääratud ajavahemiku jooksul oma riskijuhtimismeetmed või teatamiskohustused vastavusse artiklites 18 ja 20 sätestatud nõuetega;

e) kohustada kõnealuseid üksuseid teavitama füüsilisi või juriidilisi isikuid, kellele osutatakse teenuseid või kellega seoses toimub tegevus, mida võib mõjutada märkimisväärne küberoht, **ohu laadist ning** võimalikest kaitse- või parandusmeetmetest, mida asjaomased füüsilised või juriidilised isikud võivad vastavale ohule reageerimiseks võtta;

f) kohustada kõnealuseid üksusi rakendama mõistliku aja jooksul turvaauditi tulemuste alusel tehtud soovitusi;

g) kohustada kõnealuseid üksuseid avalikustama kindlaksmääratud viisil käesolevas direktiivis nende jaoks sätestatud kohustuste täitmata jätmisega seotud aspektid**, kui sellisel avalikustamisel ei ole asjaomasele üksusele kahjulikku toimet**;

h) [...]

i) määrata või taotleda, et asjaomased asutused või kohtud määraksid vastavalt siseriiklikele õigusaktidele haldustrahvi kooskõlas artikliga 31 lisaks käesoleva lõike punktides a–h osutatud meetmetele või nende asemel, olenevalt iga konkreetse juhtumi asjaoludest.

5. Artikli 29 lõikeid 6–8 kohaldatakse ka käesolevas artiklis sätestatud järelevalve- ja täitemeetmete puhul, mida kohaldatakse [...] oluliste üksuste suhtes.

Artikkel 31

Elutähtsatele ja olulistele üksustele haldustrahvide määramise üldtingimused

1. Liikmesriigid tagavad, et haldustrahvid, mis määratakse käesolevas direktiivis sätestatud kohustuste rikkumise eest elutähtsatele ja olulistele üksustele käesoleva artikli kohaselt, on alati (iga juhtumi asjaoludest lähtuvalt) tõhusad, proportsionaalsed ja heidutavad.

2. Haldustrahve kohaldatakse konkreetse juhtumi asjaoludest sõltuvalt kas lisaks artikli 29 lõike 4 punktides a–i, artikli 29 lõikes 5 ja artikli 30 lõike 4 punktides a–h osutatud meetmetele või nende asemel.

3. Haldustrahvi määramise ja selle suuruse üle otsustamisel võetakse iga üksiku juhtumi puhul nõuetekohaselt arvesse vähemalt artikli 29 lõikes 7 sätestatud asjaolusid.

4. Liikmesriigid tagavad, et artiklis 18 või 20 sätestatud kohustuste rikkumise eest **elutähtsate üksuste poolt** määratakse kooskõlas käesoleva artikli lõigetega 2 ja 3 haldustrahv, mille maksimummäär on vähemalt **4**[...] 000 000 eurot või **juriidilise isiku puhul** [...] 2 % selle ettevõtja ülemaailmsest aastasest kogukäibest (olenevalt sellest, kumb summa on suurem), kellele elutähtis [...] üksus eelneval majandusaastal kuulub.

4a. Liikmesriigid tagavad, et artiklis 18 või 20 sätestatud kohustuste rikkumise eest olulistele üksuste poolt määratakse kooskõlas käesoleva artikli lõigetega 2 ja 3 haldustrahv, mille maksimummäär on vähemalt 2 000 000 eurot või juriidilise isiku puhul kuni 1 % selle ettevõtja ülemaailmsest aastasest kogukäibest (olenevalt sellest, kumb summa on suurem), kellele oluline üksus eelneval majandusaastal kuulub.

5. Liikmesriigid võivad näha ette õiguse määrata perioodilisi karistusmakseid, mille eesmärk on sundida elutähtsat või olulist üksust (kompetentse asutuse eelneva otsuse alusel) rikkumist lõpetama.

6. Ilma et see piiraks artiklites 29 ja 30 osutatud pädevate asutuste volitusi, võib iga liikmesriik kehtestada eeskirjad selle kohta, kas ja millises ulatuses võib haldustrahve määrata artikli 4 lõikes 23 osutatud avalik-õiguslikele asutustele, kelle suhtes kehtivad käesolevas direktiivis sätestatud kohustused.

6a. Kui liikmesriigi õigussüsteemis ei ole haldustrahve ette nähtud, siis tagavad liikmesriigid, et käesolevat artiklit võib kohaldada sellisel viisil, et trahvi algatab pädev asutus ning selle määravad pädevad riiklikud kohtud, tagades seejuures, et need õiguskaitsevahendid on tõhusad ja pädevate asutuste poolt määratud haldustrahvidega samaväärse mõjuga. Igal juhul peavad määratavad trahvid olema tõhusad, proportsionaalsed ja heidutavad. Need liikmesriigid teavitavad komisjoni oma käesoleva lõike kohaselt vastuvõetavatest õigusnormidest hiljemalt […] ning viivitamata kõigist hilisematest neid õigusnorme mõjutavatest muutvatest õigusaktidest või muudatustest.

Artikkel 32

Isikuandmete väärkasutamisega seotud rikkumised

1. Kui pädevad asutused on **järelevalve või täitmise tagamise käigus** [...] **saanud teadlikuks** sellest, et **käesoleva direktiivi** artiklites 18 ja 20 sätestatud kohustuste rikkumisega elutähtsa või olulise üksuse poolt [...] kaasneb isikuandmetega seotud rikkumine, nagu on määratletud määruse (EL) 2016/679 artikli 4 lõikes 12 ja millest tuleb teavitada kõnealuse määruse artikli 33 kohaselt, teatavad nad sellest **põhjendamatu viivituseta** [...] kõnealuse määruse artiklite 55 ja 56 kohastele kompetentsetele järelevalveasutustele.

2. Kui määruse (EL) 2016/679 artiklite 55 ja 56 kohased pädevad järelevalveasutused otsustavad kasutada oma volitusi ja määrata kõnealuse määruse artikli 58 **lõike 2** punkti i alusel haldustrahvi, ei määra **käesoleva direktiivi artiklis 8 osutatud** pädevad asutused **sama teoga toime pandud**[...] rikkumise eest haldustrahvi käesoleva direktiivi artikli 31 alusel. Pädevad asutused võivad siiski kohaldada täitemeetmeid või kasutada oma volitusi määrata karistusi käesoleva direktiivi artikli 29 lõike 4 punktide a–i, artikli 29 lõike 5 ja artikli 30 lõike 4 punktide a–h alusel.

3. Kui määruse (EL) 2016/679 kohane pädev järelevalveasutus asub muus liikmesriigis kui pädev asutus, võib pädev asutus teavitada samas liikmesriigis asutatud järelevalveasutust.

Artikkel 33

Karistused

1. Liikmesriigid kehtestavad karistusnormid, mida kohaldatakse käesoleva direktiivi alusel vastu võetud liikmesriigi sätete rikkumise korral, ning võtavad kõik vajalikud meetmed, et tagada kõnealuste normide rakendamine. Kehtestatud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad.

2. Liikmesriigid teavitavad hiljemalt [kahe] aasta jooksul pärast käesoleva direktiivi jõustumist komisjoni kõnealustest õigusnormidest ja meetmetest, samuti teavitavad nad komisjoni viivitamata kõigist nende normide ja meetmete hilisematest muudatustest.

Artikkel 34

Vastastikune abi

1. Kui elutähtis või oluline üksus osutab teenuseid mitmes liikmesriigis või [...] kui ta **osutab teenuseid ühes või mitmes liikmesriigis**, kuid tema võrgu- ja infosüsteemid asuvad ühes või mitmes muus liikmesriigis, teevad **asjaomaste liikmesriikide pädevad asutused** [...] koostööd ning vajaduse korral abistavad üksteist. Kõnealune koostöö hõlmab vähemalt järgmist:

a) liikmesriigis järelevalve- või täitemeetmeid kohaldavad pädevad asutused teavitavad ühtse kontaktpunkti kaudu teiste asjaomaste liikmesriikide pädevaid asutusi [...] võetud järelevalve- ja täitemeetmetest [...] ning konsulteerivad nendega;

b) pädev asutus võib teiselt pädevalt asutuselt taotleda [...] järelevalve- või täitemeetmete võtmist;

c) pädev asutus osutab teise pädeva asutuse põhjendatud taotluse korral teisele pädevale asutusele **enda käsutuses olevate ressurssidega proportsionaalset** abi, et [...] järelevalve- või täitemeetmeid saaks rakendada tulemuslikult, tõhusalt ja järjepidevalt. Selline vastastikune abi võib hõlmata teabenõudeid ja järelevalvemeetmeid, sealhulgas taotlusi teha kohapealseid kontrolle või kohapealset järelevalvet või sihipäraseid turvaauditeid. Abitaotluse saanud pädev asutus ei või taotlust tagasi lükata, välja arvatud juhul, kui pärast muude asjaomaste [...] asutustega konsulteerimist leitakse, et [...] asutus ei ole pädev taotletud abi andma või **et tal ei ole selleks piisavaid ressursse või** et taotletav abi ei ole pädeva asutuse [...] täidetavate järelevalveülesannete suhtes proportsionaalne **või et taotlus käsitleb teavet või hõlmab tegevust, mis on vastuolus kõnealuse liikmesriigi riikliku julgeoleku või avaliku julgeoleku või kaitsega**.

2. Kui see on asjakohane, võivad eri liikmesriikide pädevad asutused omavahelisel kokkuleppel võtta [...] järelevalvemeetmeid ühiselt.

VII PEATÜKK

Ülemineku- ja lõppsätted

Artikkel 35

Läbivaatamine

Komisjon vaatab käesoleva direktiivi selle toimivuse hindamiseks korrapäraselt läbi ning esitab sellekohase aruande Euroopa Parlamendile ja nõukogule. Aruandes hinnatakse eelkõige I ja II lisas osutatud sektorite, allsektorite ning üksuste suuruse ja liigi asjakohasust majanduse ja ühiskonna toimimise aspektist küberturvalisusega seoses. **Läbivaatamise** [...] eesmärgil [...] võtab komisjon arvesse [...] CSIRTide võrgustiku aruandeid [...] operatiivtasandil saadud kogemuste kohta. Esimene aruanne esitatakse ... [54 kuud pärast käesoleva direktiivi jõustumise kuupäeva].

Artikkel 36

[...]

[...]

[...]

Artikkel 37

Komiteemenetlus

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

2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 5.

3. Kui komitee arvamus saadakse kirjaliku menetlusega, lõpetatakse nimetatud menetlus tulemust saavutamata, kui arvamuse esitamiseks ettenähtud tähtaja jooksul komitee eesistuja nii otsustab või komitee liige seda taotleb.

Artikkel 38

Ülevõtmine

1. Liikmesriigid võtavad vastu ja avaldavad käesoleva direktiivi järgimiseks vajalikud õigus- ja haldusnormid **hiljemalt** ... [[...]**24** kuud pärast käesoleva direktiivi jõustumist**]**. Liikmesriigid teatavad nendest viivitamata komisjonile. Nad kohaldavad kõnealuseid meetmeid alates ... [esimeses lõigus osutatud kuupäevale järgnevast päevast].

2. Kui liikmesriigid need normid vastu võtavad, lisavad nad nende ametlikul avaldamisel nendesse või nende juurde viite käesolevale direktiivile. Sellise viitamise viisi näevad ette liikmesriigid.

Artikkel 39

Määruse (EL) nr 910/2014 muutmine

Määruse (EL) nr 910/2014 artikkel 19 [...] jäetakse välja **alates ... [käesoleva direktiivi ülevõtmise tähtaeg].**

Artikkel 40

Direktiivi (EL) 2018/1972 muutmine

Direktiivi (EL) 2018/1972 artiklid 40 ja 41 [...] jäetakse välja **alates ... [käesoleva direktiivi ülevõtmise tähtaeg].**

Artikkel 41

Kehtetuks tunnistamine

Direktiiv (EL) 2016/1148 tunnistatakse kehtetuks alates ... [käesoleva direktiivi ülevõtmise tähtaeg].

Viiteid direktiivile (EL) 2016/1148 tõlgendatakse viidetena käesolevale direktiivile ja neid loetakse II[...] lisas esitatud vastavustabeli kohaselt.

Artikkel 42

Jõustumine

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

Artikkel 43

Adressaadid

Käesolev direktiiv on adresseeritud liikmesriikidele.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

I LISA

SEKTORID, ALLSEKTORID JA ÜKSUSTE LIIGID

Sektor	Allsektor	Üksuse liik
1. Energeetika	a) Elekter	- Direktiivi (EL) 2019/944 ([39]) artikli 2 punktis 57 osutatud elektriettevõtjad, kes tegelevad sama direktiivi artikli 2 punktis 12 osutatud tarnimisega
		- Direktiivi (EL) 2019/944 artikli 2 punktis 29 osutatud jaotusvõrguettevõtjad
		- Direktiivi (EL) 2019/944 artikli 2 punktis 35 osutatud põhivõrguettevõtjad
		- Direktiivi (EL) 2019/944 artikli 2 punktis 38 osutatud tootjad
		— Määruse (EL) 2019/943 ([40]) artikli 2 punktis 8 osutatud määratud elektriturukorraldajad
		- Määruse (EL) 2019/943 artikli 2 punktis 25 osutatud elektrituru osalised, kes osutavad direktiivi (EL) 2019/944 artikli 2 punktides 18, 20 ja 59 osutatud agregeerimis-, tarbimiskaja- või energia salvestamise teenuseid

[39] Euroopa Parlamendi ja nõukogu 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).

[40] Euroopa Parlamendi ja nõukogu määrus (EL) 2019/943, milles käsitletakse elektrienergia siseturgu (ELT L 158, 14.6.2019, lk 54).

	b) Kaugküte ja -jahutus	- Direktiivi (EL) 2018/2001 ([41]) (taastuvatest energiaallikatest toodetud energia kasutamise edendamise kohta) artikli 2 punktis 19 osutatud kaugküte ja kaugjahutus
	c) Nafta	- Naftajuhtmete operaatorid
		- Nafta tootmise, rafineerimise ja töötlemise rajatiste ning hoiustamise ja ülekandmisega tegelevad operaatorid
		— Nõukogu direktiivi 2009/119/EÜ ([42]) artikli 2 punktis f osutatud naftavarude säilitamise kesküksused
	d) Gaas	- Direktiivi (EÜ) 2009/73/EÜ ([43]) artikli 2 punktis 8 osutatud tarneettevõtjad
		- Direktiivi 2009/73/EÜ artikli 2 punktis 6 osutatud jaotussüsteemi haldurid
		- Direktiivi 2009/73/EÜ artikli 2 punktis 4 osutatud ülekandesüsteemi haldurid
		- Direktiivi 2009/73/EÜ artikli 2 punktis 10 osutatud hoidlatevõrgu haldurid

41 Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/2001 taastuvatest energiaallikatest toodetud energia kasutamise edendamise kohta (ELT L 328, 21.12.2018, lk 82).

42 Nõukogu 14. septembri 2009. aasta direktiiv 2009/119/EÜ, millega kohustatakse liikmesriike säilitama toornafta ja/või naftatoodete miinimumvarusid (ELT L 265, 9.10.2009, lk 9).

43 Euroopa Parlamendi ja nõukogu 13. juuli 2009. aasta direktiiv 2009/73/EÜ, mis käsitleb maagaasi siseturu ühiseeskirju ning millega tunnistatakse kehtetuks direktiiv 2003/55/EÜ (ELT L 211, 14.8.2009, lk 94).

		- Direktiivi 2009/73/EÜ artikli 2 punktis 12 osutatud maagaasi veeldusjaamade haldurid
		- Direktiivi 2009/73/EÜ artikli 2 punktis 1 määratletud maagaasiettevõtjad
		- Maagaasi rafineerimise ja töötlemise rajatiste haldurid
	e) Vesinik	Vesiniku tootmise, hoiustamise ja ülekandmisega tegelevad operaatorid
2. Transport	a) Lennutransport	- **Kommertsvaldkonnas tegutsevad** määruse (EÜ) nr 300/2008 ([44]) artikli 3 punktis 4 osutatud lennuettevõtjad
		- Direktiivi 2009/12/EÜ ([45]) artikli 2 punktis 2 osutatud lennujaama juhtorganid, sama direktiivi artikli 2 punktis 1 osutatud lennujaamad, sealhulgas määruse (EL) nr 1315/2013 ([46]) II lisa 2. punktis loetletud põhivõrgu lennujaamad ning lennujaamades olevaid abirajatisi käitavad üksused
		- Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 549/2004 ([47]) artikli 2 punktis 1 osutatud

[44] Euroopa Parlamendi ja nõukogu 11. märtsi 2008. aasta määrus (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002 (ELT L 97, 9.4.2008, lk 72).

[45] Euroopa Parlamendi ja nõukogu 11. märtsi 2009. aasta direktiiv 2009/12/EÜ lennujaamatasude kohta (ELT L 70, 14.3.2009, lk 11).

[46] Euroopa Parlamendi ja nõukogu 11. detsembri 2013. aasta määrus (EL) nr 1315/2013 üleeuroopalise transpordivõrgu arendamist käsitlevate liidu suuniste kohta ja millega tunnistatakse kehtetuks otsus nr 661/2010/EL (ELT L 348, 20.12.2013, lk 1).

[47] Euroopa Parlamendi ja nõukogu 10. märtsi 2004. aasta määrus (EÜ) nr 549/2004, millega sätestatakse raamistik ühtse Euroopa taeva loomiseks (raammäärus) (ELT L 96, 31.3.2004, lk 1).

		lennujuhtimise teenust osutavad liikluskorraldusettevõtjad
	b) Raudteetransport	- Direktiivi 2012/34/EL ([48]) artikli 3 punktis 2 osutatud raudteeinfrastruktuuri-ettevõtjad
		- Direktiivi 2012/34/EL artikli 3 punktis 1 osutatud raudteeveo-ettevõtjad, sealhulgas sama direktiivi artikli 3 punktis 12 osutatud teenindusrajatiste käitajad
	c) Veetransport	- Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 725/2004 ([49]) I lisas osutatud ettevõtjad, kes tegelevad reisijate ja kauba vedamisega sisevetel, merel ja rannavetes (ei kohaldata kõnealuste ettevõtjate käitatavate üksikute laevade suhtes)
		- Euroopa Parlamendi ja nõukogu direktiivi 2005/65/EÜ ([50]) artikli 3 punktis 1 osutatud sadamate valdajad, sealhulgas nende määruse (EÜ) nr 725/2004 artikli 2 punktis 11 osutatud sadamarajatised ning sadamates tööde ja varustuse haldamisega tegelevad üksused

[48] Euroopa Parlamendi ja nõukogu 21. novembri 2012. aasta direktiiv 2012/34/EL, millega luuakse ühtne Euroopa raudteepiirkond (ELT L 343, 14.12.2012, lk 32).

[49] Euroopa Parlamendi ja nõukogu 31. märtsi 2004. aasta määrus (EÜ) nr 725/2004 laevade ja sadamarajatiste turvalisuse tugevdamise kohta (ELT L 129, 29.4.2004, lk 6).

[50] Euroopa Parlamendi ja nõukogu 26. oktoobri 2005. aasta direktiiv 2005/65/EÜ sadamate turvalisuse tugevdamise kohta (ELT L 310, 25.11.2005, lk 28).

		- Direktiivi 2002/59/EÜ ([51]) artikli 3 punktis o osutatud laevaliikluse juhtimise keskuste operaatorid
	d) Maanteetransport	- Komisjoni delegeeritud määruse (EL) 2015/962 ([52]) artikli 2 punktis 12 osutatud maanteeametid, kes vastutavad liikluskorralduse eest**, välja arvatud avaliku sektori üksused, kelle jaoks liikluskorraldus või intelligentsete transpordisüsteemide operaatorid moodustavad üksnes väheolulise osa nende tegevusest**
		- Direktiivi 2010/40/EL ([53]) artikli 4 punktis 1 osutatud intelligentsete transpordisüsteemide operaatorid
3. Pangandus		— Määruse (EL) nr 575/2013 ([54]) artikli 4 punktis 1 osutatud krediidiasutused**, [välja arvatud direktiivi 2013/36/EL artikli 2 lõike 5 punktis 8 osutatud krediidiasutused, mis on vabastatud vastavalt määruse XX [DORA] artikli 2 lõikele 4]**

[51] Euroopa Parlamendi ja nõukogu 27. juuni 2002. aasta direktiiv 2002/59/EÜ, millega luuakse ühenduse laevaliikluse seire- ja teabesüsteem ning tunnistatakse kehtetuks nõukogu direktiiv 93/75/EMÜ (EÜT L 208, 5.8.2002, lk 10).

[52] Komisjoni 18. detsembri 2014. aasta delegeeritud määrus (EL) 2015/962, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi 2010/40/EL kogu ELis reaalajas saadava liiklusteabe teenuste pakkumise osas (ELT L 157, 23.6.2015, lk 21).

[53] Euroopa Parlamendi ja nõukogu 7. juuli 2010. aasta direktiiv 2010/40/EL, mis käsitleb raamistikku intelligentsete transpordisüsteemide kasutuselevõtmiseks maanteetranspordis ja liideste jaoks teiste transpordiliikidega (ELT L 207, 6.8.2010, lk 1).

[54] Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta määrus (EL) nr 575/2013 krediidiasutuste ja investeerimisühingute suhtes kohaldatavate usaldatavusnõuete kohta ja määruse (EL) nr 648/2012 muutmise kohta (ELT L 176, 27.6.2013, lk 1).

4. Finantsturu taristu		- Direktiivi 2014/65/EL ([55]) artikli 4 punktis 24 osutatud kauplemiskohtade korraldajad
		- Määruse (EL) nr 648/2012 ([56]) artikli 2 punktis 1 osutatud kesksed vastaspooled
5. Tervis		— Direktiivi 2011/24/EL ([57]) artikli 3 punktis g osutatud tervishoiuteenuse osutajad
		— Määruse XXXX/XXXX (milles käsitletakse tõsiseid piiriüleseid terviseohte)[58] artiklis 15 osutatud ELi referentlaborid
		— Üksused, mis tegelevad direktiivi 2001/83/EÜ ([59]) artikli 1 punktis 2 osutatud ravimite uurimise ja arendamisega — NACE Rev. 2 C jao jaotises 21 osutatud põhifarmaatsiatooteid ja ravimpreparaate tootvad üksused — Üksused, kes toodavad rahvatervise hädaolukorras kriitilise tähtsusega meditsiiniseadmeid (rahvatervise hädaolukorra kriitilise tähtsusega

[55] Euroopa Parlamendi ja nõukogu 15. mai 2014. aasta direktiiv 2014/65/EL finantsinstrumentide turgude kohta ning millega muudetakse direktiive 2002/92/EÜ ja 2011/61/EL (ELT L 173, 12.6.2014, lk 349).

[56] Euroopa Parlamendi ja nõukogu 4. juuli 2012. aasta määrus (EL) nr 648/2012 börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta (ELT L 201, 27.7.2012, lk 1).

[57] Euroopa Parlamendi ja nõukogu 9. märtsi 2011. aasta direktiiv 2011/24/EL patsiendiõiguste kohaldamise kohta piiriüleses tervishoius (ELT L 88, 4.4.2011, lk 45).

[58] [Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse tõsiseid piiriüleseid terviseohte ja millega tunnistatakse kehtetuks otsus nr 1082/2013/EL; viide ajakohastatakse pärast ettepaneku COM (2020)727 final vastuvõtmist]

[59] Euroopa Parlamendi ja nõukogu 6. novembri 2001. aasta direktiiv 2001/83/EÜ inimtervishoius kasutatavaid ravimeid käsitlevate ühenduse eeskirjade kohta (EÜT L 311, 28.11.2001, lk 67).

		meditsiiniseadmete loetelu), millele on osutatud määruse XXXX[60] artiklis 20
6. Joogivesi		Nõukogu direktiivi 98/83/EÜ ([61]) artikli 2 punkti 1 alapunktis a osutatud olmeveega varustajad ja olmevee jaotajad, kuid välja arvatud jaotajad, kelle puhul olmevee jaotamine on vaid üks **väheoluline** osa nende jaotustegevusest, mis hõlmab muude tarbekaupade ja kaupade tarnimist [...]
7. Reovesi		Ettevõtjad, kes tegelevad nõukogu direktiivi 91/271/EMÜ ([62]) artikli 2 punktides 1–3 osutatud asula-, olme- ja tööstusreovee kogumise, ärajuhtimise või puhastamisega**, kuid välja arvatud ettevõtjad, kelle jaoks asula-, olme- ja tööstusreovee kogumine, ärajuhtimine või puhastamine moodustab üksnes väheolulise osa nende tegevusest** [...]
8. Digitaristu		**-** Interneti vahetuspunkti teenuse osutajad
		- Domeeninimesüsteemi teenuse osutajad**, välja arvatud juurnimeserverite operaatorid**
		- Tippdomeeninimede registrid
		- Pilvandmetöötlusteenuse osutajad

60 [Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse Euroopa Ravimiameti suuremat rolli kriisiks valmisolekus ja kriisiohjamises ravimite ja meditsiiniseadmete valdkonnas; viide ajakohastatakse pärast ettepaneku COM(2020)725 final vastuvõtmist]

61 Nõukogu 3. novembri 1998. aasta direktiiv 98/83/EÜ olmevee kvaliteedi kohta (EÜT L 330, 5.12.1998, lk 32).

62 Nõukogu 21. mai 1991. aasta direktiiv 91/271/EMÜ asulareovee puhastamise kohta (EÜT L 135, 30.5.1991, lk 40).

		- Andmekeskusteenuse osutajad
		- Sisulevivõrgu pakkujad
		- Määruse (EL) nr 910/2014 ([63]) artikli 3 punktis 19 osutatud usaldusteenuse osutajad
		- Direktiivi (EL) 2018/1972 ([64]) artikli 2 punktis 8 osutatud üldkasutatavate elektroonilise side võrkude pakkujad või direktiivi (EL) 2018/1972 artikli 2 punktis 4 osutatud elektroonilise side teenuste osutajad, kui nende teenused on üldkasutatavad
8.a IKT-teenuste haldamine **(B2B)**		**— Hallatud teenuste osutajad** **— Turbetarnijad**

[63] 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).

[64] Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (ELT L 321, 17.12.2018, lk 36).

9. Avaliku halduse **üksused**		— Keskvalitsuste avaliku halduse üksused**, nagu need on kindlaks määranud liikmesriik vastavalt siseriiklikule õigusele** — [...][65] — [...]
10. Kosmos		— Liikmesriigi või eraõiguslike isikute omandis olevate, hallatavate või käitatavate maapealsete taristute operaatorid, kes toetavad kosmosepõhiste teenuste osutamist, välja arvatud direktiivi (EL) 2018/1972 artikli 2 punktis 8 osutatud elektroonilise side võrkude pakkujad

[65] [...]

II LISA

SEKTORID, ALLSEKTORID JA ÜKSUSTE LIIGID

Sektor	Allsektor	Üksuse liik
1. Posti- ja kulleriteenused		Direktiivi 97/67/EÜ ([66]) artikli 2 punktis 1[...] osutatud postiteenuste osutajad, **sealhulgas** [...] kulleriteenuste osutajad
2. Jäätmekäitlus		Ettevõtjad, kes tegelevad direktiivi 2008/98/EÜ ([67]) artikli 3 punktis 9 osutatud jäätmekäitlusega, välja arvatud ettevõtjad, kelle põhitegevus ei ole jäätmekäitlus

[66] Euroopa Parlamendi ja nõukogu 15. detsembri 1997. aasta direktiiv 97/67/EÜ ühenduse postiteenuste siseturu arengut ja teenuse kvaliteedi parandamist käsitlevate ühiseeskirjade kohta (EÜT L 15, 21.1.1998, lk 14)**; direktiivi on muudetud Euroopa Parlamendi ja nõukogu 20. veebruari 2008. aasta direktiiviga 2008/6/EÜ, millega muudetakse direktiivi 97/67/EÜ seoses ühenduse postiteenuste siseturu rajamise lõpuleviimisega (ELT L 52, 27.2.2008, lk 3)**.

[67] Euroopa Parlamendi ja nõukogu 19. novembri 2008. aasta direktiiv 2008/98/EÜ, mis käsitleb jäätmeid ja millega tunnistatakse kehtetuks teatud direktiivid (ELT L 312, 22.11.2008, lk 3).

3. Kemikaalide valmistamine, tootmine ja levitamine		Ettevõtjad, kes on tegelevad ainete ja [...] **segude** valmistamise, tootmise ja levitamisega, millele on osutatud määruse (EÜ) nr 1907/2006 ([68]) artikli 3 punktides [...] 9 ja 14 **ning ettevõtjad, kes tegelevad kõnealuse määruse artikli 3 punktis 3 osutatud toodete ainetest või segudest tootmisega**
4. Toiduainete tootmine, töötlemine ja turustamine		Määruse (EÜ) nr 178/2002 ([69]) artikli 3 punktis 2 osutatud toidukäitlemisettevõtjad**, kes tegelevad hulgimüügi ning tööstusliku tootmise ja töötlemisega**
5. Töötlev tööstus	a) Meditsiiniseadmete ja *in vitro* diagnostikameditsiiniseadmete tootmine	Määruse (EL) 2017/745 ([70]) artikli 2 punktis 1 osutatud meditsiiniseadmeid tootvad üksused ning määruse (EL) 2017/746 ([71]) artikli 2 punktis 2 osutatud *in vitro* diagnostikameditsiiniseadmeid tootvad üksused, välja arvatud 1. lisa punktis 5

68 Euroopa Parlamendi ja nõukogu 18. detsembri 2006. aasta määrus (EÜ) nr 1907/2006, mis käsitleb kemikaalide registreerimist, hindamist, autoriseerimist ja piiramist (REACH) ja millega asutatakse Euroopa Kemikaalide Agentuur ning muudetakse direktiivi 1999/45/EÜ ja tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 793/93, komisjoni määrus (EÜ) nr 1488/94 ning samuti nõukogu direktiiv 76/769/EMÜ ja komisjoni direktiivid 91/155/EMÜ, 93/67/EMÜ, 93/105/EÜ ja 2000/21/EÜ (ELT L 396, 30.12.2006, lk 1).

69 Euroopa Parlamendi ja nõukogu 28. jaanuari 2002. aasta määrus (EÜ) nr 178/2002, millega sätestatakse toidualaste õigusnormide üldised põhimõtted ja nõuded, asutatakse Euroopa Toiduohutusamet ja kehtestatakse toidu ohutusega seotud menetlused (EÜT L 31, 1.2.2002, lk 1).

70 Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/745, milles käsitletakse meditsiiniseadmeid, millega muudetakse direktiivi 2001/83/EÜ, määrust (EÜ) nr 178/2002 ja määrust (EÜ) nr 1223/2009 ning millega tunnistatakse kehtetuks nõukogu direktiivid 90/385/EMÜ ja 93/42/EMÜ (ELT L 117, 5.5.2017, lk 1).

71 Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/746 *in vitro* diagnostikameditsiiniseadmete kohta ning millega tunnistatakse kehtetuks direktiiv 98/79/EÜ ja komisjoni otsus 2010/227/EL (ELT L 117, 5.5.2017, lk 176).

		nimetatud meditsiiniseadmeid tootvad üksused.
	b) Arvutite, elektroonika- ja optikaseadmete tootmine	Ettevõtjad, kes tegelevad NACE Rev. 2 C jao jaotises 26 osutatud majandustegevusega
	c) Elektriseadmete tootmine	Ettevõtjad, kes tegelevad NACE Rev. 2 C jao jaotises 27 osutatud majandustegevusega
	d) Mujal liigitamata masinate ja seadmete tootmine	Ettevõtjad, kes tegelevad NACE Rev. 2 C jao jaotises 28 osutatud majandustegevusega
	e) Mootorsõidukite, haagiste ja poolhaagiste tootmine	Ettevõtjad, kes tegelevad NACE Rev. 2 C jao jaotises 29 osutatud majandustegevusega
	f) Muude transpordivahendite tootmine	Ettevõtjad, kes tegelevad NACE Rev. 2 C jao jaotises 30 osutatud majandustegevusega
6. Digiteenuste osutajad		- Internetipõhise kauplemiskoha teenuse osutajad
		- Internetipõhise otsingumootori teenuse osutajad
		- Sotsiaalvõrguteenuse platvormi pakkujad