DIREKTIIVID

EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV (EL) 2022/2555,

14. detsember 2022,

mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv)

(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 Keskpanga arvamust ([1]),

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust ([2]),

pärast konsulteerimist Regioonide Komiteega,

toimides seadusandliku tavamenetluse kohaselt ([3])

ning arvestades järgmist:

(1) Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 ([4]) eesmärk oli luua kogu liidus küberturvalisuse alast võimekust, leevendada ohte peamistes sektorites elutähtsate teenuste osutamiseks kasutatavatele võrgu- ja infosüsteemidele ning tagada selliste teenuste katkematu osutamine intsidentide korral, aidates seeläbi kaasa liidu julgeolekule ning majanduse ja ühiskonna tõhusale toimimisele.

(2) Alates direktiivi (EL) 2016/1148 jõustumisest on liidu kübervastupidavusvõime suurendamisel tehtud märkimisväärseid edusamme. Kõnealuse direktiivi läbivaatamine on näidanud, et see on kannustanud liidu küberturvalisust käsitleva institutsioonilise ja regulatiivse käsituse kujunemist ning sillutanud seeläbi teed mõtteviisi oluliseks muutumiseks. Kõnealuse direktiiviga on tagatud riiklike raamistike ülesehitamine, mis on hõlmanud riiklike võrgu- ja infosüsteemide turvalisuse strateegiate koostamist, riikliku võimekuse kujundamist ning regulatiivsete meetmete kohaldamist iga liikmesriigi määratud elutähtsate taristute ja üksuste suhtes. Direktiiv (EL) 2016/1148 on aidanud ka kaasa koostöö edendamisele liidu tasandil koostöörühma ja riiklike küberturbe intsidentide lahendamise üksuste võrgustiku loomise kaudu. Vaatamata nendele saavutustele on direktiivi (EL) 2016/1148 läbivaatamisel tuvastatud olemuslikke puudusi, mis takistavad praeguste ja esilekerkivate küberturvalisuse probleemide tulemuslikku lahendamist.

(3) Võrgu- ja infosüsteemidest on saanud igapäevaelu keskne osa ühes kiire digiülemineku ja ühiskonnaosaliste vastastikuse seotusega, mille hulka kuulub piiriülene suhtlus. See areng on viinud küberohtude suurenemiseni ning toonud kaasa uued väljakutsed, mis nõuavad kohandatud, koordineeritud ja uuenduslikke lahendusi kõigis liikmesriikides. Intsidentide arv, ulatus, keerukus, sagedus ja mõju suureneb ning see kujutab endast võrgu- ja infosüsteemide toimimisele suurt ohtu. Selle tulemusena võivad intsidendid tõkestada majandustegevust siseturul, põhjustada rahalist kahju, õõnestada kasutajate usaldust ning tekitada suurt kahju liidu majandusele ja ühiskonnale.

([1]) ELT C 233, 16.6.2022, lk 22.
([2]) ELT C 286, 16.7.2021, lk 170.
([3]) Euroopa Parlamendi 10. novembri 2022. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu 28. novembri 2022. aasta otsus.
([4]) 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, 19.7.2016, lk 1).

Seetõttu on küberturvalisuse alane valmisolek ja tõhusus praegu siseturu tõrgeteta toimimiseks olulisem kui kunagi varem. Lisaks on küberturvalisus paljude kriitilise tähtsusega sektorite jaoks peamine tegur, mis võimaldab digiüleminekuga edukalt toime tulla ning digitaliseerimise majanduslikke, sotsiaalseid ja kestlikkuse eeliseid täielikult ära kasutada.

(4) Direktiivi (EL) 2016/1148 õiguslik alus oli Euroopa Liidu toimimise lepingu (ELi toimimise leping) artikkel 114, mille eesmärk on siseturu rajamine ja toimimise tagamine riigisiseste normide ühtlustamise meetmete tõhustamise abil. Teenuseid osutavatele või majanduslikult olulist tegevust ellu viivatele üksustele kehtestatud küberturvalisuse nõuded erinevad liikmesriigiti märkimisväärselt nii nõuete liigi, üksikasjalikkuse kui ka järelevalvemeetodi poolest. Need erisused toovad kaasa lisakulusid ning põhjustavad raskusi piiriüleselt kaupu või teenuseid pakkuvatele üksustele. Ühe liikmesriigi kehtestatud nõuded, mis erinevad teise liikmesriigi kehtestatud nõuetest või on nendega lausa vastuolus, võivad sellist piiriülest tegevust oluliselt pärssida. Lisaks mõjutab küberturvalisuse nõuete ebatõhus kavandamine või rakendamine ühes liikmesriigis tõenäoliselt küberturvalisuse taset ka teistes liikmesriikides, kui piiriülene suhtlus on sedavõrd intensiivne. Direktiivi (EL) 2016/1148 läbivaatamise käigus selgus, et liikmesriigid kohaldavad seda väga erinevalt, muu hulgas seoses selle kohaldamisalaga, mille piiritlemine jäeti suuresti liikmesriikide otsustada. Direktiiviga (EL) 2016/1148 anti liikmesriikidele ka väga ulatuslik kaalutlusõigus direktiivis sätestatud turvalisuse tagamise ja intsidentidest teatamise kohustuse rakendamisel. Seega rakendati neid kohustusi liikmesriigi tasandil väga erinevalt. Sarnaseid lahknevusi oli ka direktiivi (EL) 2016/1148 järelevalve- ja täitmise tagamise sätete rakendamisel.

(5) Kõik need erinevused põhjustavad siseturu killustumist ja võivad kahjustada selle toimimist, mõjutades eelkõige teenuste piiriülest osutamist ja kübervastupidavusvõime taset, kuna rakendatavad meetmed on erinevad. Lõppkokkuvõttes võivad need erinevused tuua kaasa selle, et mõni liikmesriik on küberohtude vastu vähem kaitstud, millel võib olla ülekanduv mõju kogu liidus. Käesoleva direktiivi eesmärk on kõrvaldada sellised suured erinevused liikmesriikide vahel, sätestades koordineeritud reguleeriva raamistiku toimimisega seotud miinimumnormid, kehtestades liikmesriikide vastutavate asutuste tulemuslikuks koostööks vajalikud mehhanismid, ajakohastades selliste sektorite ja tegevuste loetelu, mille suhtes küberturvalisusega seotud kohustusi kohaldatakse, ning nähes ette tõhusad õiguskaitsevahendid ja täitemeetmed, mis on olulised nende kohustuste tulemusliku täitmise tagamiseks. Seega tuleks direktiiv (EL) 2016/1148 kehtetuks tunnistada ja asendada käesoleva direktiiviga.

(6) Direktiivi (EL) 2016/1148 kehtetuks tunnistamisega tuleks sektoripõhist kohaldamisala laiendada suuremale osale majandusest, et hõlmata võimalikult täielikult kõik sektorid ja teenused, mis on siseturu peamise ühiskondliku ja majandustegevuse jaoks elutähtsad. Eelkõige on käesoleva direktiivi eesmärk kõrvaldada puudused, mis on seotud elutähtsate teenuste osutajate ja digiteenuse osutajate eristamisega, mis on osutunud iganenuks, kuna ei kajasta sektorite või teenuste tähtsust siseturu ühiskondliku ja majandustegevuse jaoks.

(7) Direktiivi (EL) 2016/1148 kohaselt oli liikmesriikidel kohustus kindlaks teha üksused, mis vastavad oluliste teenuste operaatori kriteeriumidele. Et kõrvaldada sellest tulenevad liikmesriikidevahelised suured erinevused ning tagada kõigile asjaomastele üksustele küberturvalisuse riskijuhtimismeetmete ja teatamiskohustusega seoses õiguskindlus, tuleks kehtestada ühtne kriteerium, mille alusel tehakse kindlaks käesoleva direktiivi kohaldamisalasse kuuluvad üksused. See kriteerium peaks põhinema suuruse ülempiiri reegli kohaldamisel, mille kohaselt jäävad käesoleva direktiivi kohaldamisalasse kõik üksused, mida käsitatakse komisjoni soovituse 2003/361/EÜ ([5]) lisa artikli 2 kohaselt keskmise suurusega ettevõtjana või mis ületavad keskmise suurusega ettevõtja ülemmäärasid, mis on esitatud kõnealuse artikli lõikes 1, ning tegutsevad käesoleva direktiiviga hõlmatud sektorites, osutavad teenuseid

([5]) Komisjoni 6. mai 2003. aasta soovitus 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratluse kohta (ELT L 124, 20.5.2003, lk 36).

või viivad ellu tegevusi, mis kuuluvad selle kohaldamisalasse. Liikmesriigid peaksid samuti ette nägema, et käesoleva direktiivi kohaldamisalasse kuuluvad teatavad kõnealuse soovituse lisa artikli 2 lõigetes 2 ja 3 määratletud väikesed ettevõtjad ja mikroettevõtjad, mis vastavad konkreetsetele kriteeriumidele, mis näitavad ühiskonna, majanduse või konkreetsete sektorite või teenuseliikide võtmerolli.

(8) Käesoleva direktiivi kohaldamisalast tuleks välja jätta avaliku halduse üksused, kes tegutsevad peamiselt riigi julgeoleku, avaliku julgeoleku, kaitse või õiguskaitse valdkonnas, sealhulgas kuritegude ennetamine, avastamine, uurimine ja nende eest vastutusele võtmine. Käesoleva direktiivi kohaldamisalast tuleks välja jätta ka sellised avaliku halduse üksused, kelle tegevus on nende valdkondadega seotud vaid vähesel määral. Regulatiivse pädevusega üksusi ei käsitata käesoleva direktiivi kohaldamisel õiguskaitse valdkonnas tegutsevate üksustena ja seetõttu ei jäeta neid ka käesoleva direktiivi kohaldamisalast välja. Käesoleva direktiivi kohaldamisalast jäetakse välja avaliku halduse üksused, mis on vastavalt rahvusvahelisele lepingule asutatud ühiselt kolmanda riigiga. Käesolevat direktiivi ei kohaldata liikmesriikide diplomaatiliste ja konsulaaresinduste suhtes kolmandates riikides ega nende võrgu- ja infosüsteemide suhtes, kui sellised süsteemid asuvad esinduse ruumides või kui neid käitatakse kolmanda riigi kasutajate jaoks.

(9) Liikmesriikidel peaks olema võimalik võtta vajalikke meetmeid, et tagada riikliku julgeoleku oluline huvi, tagada avalik kord ja julgeolek ning võimaldada kuritegude ennetamist, uurimist, avastamist ja nende eest vastutusele võtmist. Selleks peaks liikmesriikidel olema võimalik vabastada konkreetsed üksused, kes tegutsevad riigi julgeoleku, avaliku julgeoleku, kaitse või õiguskaitse valdkonnas, sealhulgas kuritegude ennetamine, uurimine, avastamine ja nende eest vastutusele võtmine, teatavate käesolevas direktiivis sätestatud kohustuste täitmisest. Kui üksus osutab teenuseid üksnes avaliku halduse üksusele, mis on käesoleva direktiivi kohaldamisalast välja jäetud, peaks liikmesriikidel olema võimalik otsustada, et see üksus ei pea seoses nimetatud teenustega käesolevas direktiivis sätestatud kohustusi täitma. Lisaks ei tohiks liikmesriike kohustada esitama teavet, mille avalikustamine on vastuolus nende riigi julgeoleku, avaliku julgeoleku või kaitse oluliste huvidega. Kõnealuses kontekstis tuleks arvesse võtta salastatud teabe kaitset käsitlevaid riigisiseseid ja liidu norme, ametlikke ja mitteametlikke mitteavaldamise kokkuleppeid, nagu fooritulede analoogial põhinev fooriprotokoll teabe tundlikkuse märgistamiseks. Fooriprotokolli teabe tundlikkuse märgistamiseks tuleb mõista kui vahendit, millega antakse teavet teabe edasise levitamisega seotud piirangute kohta. Seda kasutatakse peaaegu kõigis küberturbe intsidentide lahendamise üksustes (CSIRTid) ning mõnes teabeanalüüsi- ja -jagamiskeskuses.

(10) Kuigi käesolevat direktiivi kohaldatakse üksuste suhtes, kes viivad ellu tegevusi elektrienergiat tootvates tuumaelektrijaamades, võivad mõned need tegevused olla seotud riikliku julgeolekuga. Kui see on nii, peaks liikmesriigil olema võimalik täita vastavalt aluslepingutele oma kohustust kaitsta seoses kõnealuse tegevusega, sealhulgas tegevusega tuumaenergia väärtusahelas, riiklikku julgeolekut.

(11) Mõned üksused tegutsevad riikliku julgeoleku, avaliku julgeoleku, kaitse või õiguskaitse valdkonnas, sealhulgas kuritegude ennetamine, uurimine, avastamine ja nende eest vastutusele võtmine, osutades samal ajal ka usaldusteenuseid. Usaldusteenuse osutajad, kes kuuluvad Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 ([6]) kohaldamisalasse, peaksid kuuluma käesoleva direktiivi kohaldamisalasse, et tagada turvanõuded ja järelevalve samal tasemel, mis oli juba eelnevalt nimetatud määruses sätestatud seoses usaldusteenuse osutajatega. Nii nagu määrust (EL) nr 910/2014 ei kohaldata teatavate konkreetsete teenuste suhtes, ei tuleks ka käesolevat direktiivi kohaldada selliste usaldusteenuste osutamise suhtes, mida kasutatakse eranditult suletud süsteemides, mis tulenevad liikmesriigi õigusest või kindlaksmääratud osalejate vahelistest kokkulepetest.

([6]) 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).

(12) Euroopa Parlamendi ja nõukogu direktiivis 97/67/EÜ ([7]) määratletud postiteenuse osutajate, sealhulgas kullerpostiteenuse osutajate suhtes tuleks kohaldada käesolevat direktiivi juhul, kui nad osutavad vähemalt ühe postiteenuseahela etapi teenust, eeskätt kogumis-, sorteerimis- või jaotamisteenust, sealhulgas järeletulemise teenused, võttes arvesse nende võrgu- ja infosüsteemidest sõltuvuse määra. Transporditeenust, mida ei osutata ühegi nimetatud etapi raames, ei peaks käsitama postiteenusena.

(13) Arvestades küberohtude intensiivistumist ja keerukamaks muutumist, peaksid liikmesriigid püüdma tagada, et käesoleva direktiivi kohaldamisalast välja jäetud üksused saavutaksid küberturvalisuse kõrge taseme, ning toetama nende üksuste tundlikku olemust kajastavate samaväärsete küberturvalisuse riskijuhtimismeetmete rakendamist.

(14) Käesoleva direktiivi alusel toimuva isikuandmete töötlemise suhtes kohaldatakse liidu andmekaitseõigust ja eraelu puutumatuse kaitset käsitlevat liidu õigust. Eelkõige ei mõjuta käesolev direktiiv Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 ([8]) ega Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ ([9]) kohaldamist. Seetõttu ei tohiks käesolev direktiiv muu hulgas mõjutada nende asutuste ülesandeid ja volitusi, kes on pädevad seirama kohaldatava liidu andmekaitseõiguse ja eraelu puutumatuse kaitset käsitleva õiguse järgimist.

(15) Küberturvalisuse riskijuhtimismeetmete järgimiseks ja teatamiskohustuse täitmiseks tuleks käesoleva direktiivi kohaldamisalasse kuuluvad üksused liigitada kahte kategooriasse – elutähtsad üksused ja olulised üksused, mis näitab, mil määral on nad kriitilise tähtsusega nende sektori või osutatavate teenuste liigi, aga ka oma suuruse seisukohast. Sellega seoses tuleks igakülgselt arvesse võtta kõiki asjakohaseid valdkondlikke riskihindamisi või pädevate asutuste suuniseid, kui see on kohaldatav. Nende kahe üksuseliigi järelevalve- ja täitmise tagamise kord peaks olema erinev, et tagada õiglane tasakaal kohaldatavate riskipõhiste nõuete ja kohustuste ning nõuete täitmise järelevalvega seotud halduskoormuse vahel.

(16) Vältimaks seda, et üksusi, millel on partnerettevõtjad või mis on sidusettevõtjad, peetaks elutähtsateks või olulisteks üksusteks, kui see oleks ebaproportsionaalne, on liikmesriikidel võimalik soovituse 2003/361/EÜ lisa artikli 6 lõike 2 kohaldamisel võtta arvesse üksuse oma partneritest või sidusettevõtjatest sõltumatuse määra. Eelkõige on liikmesriikidel võimalik võtta arvesse asjaolu, et üksus on oma partner- või sidusettevõtjatest sõltumatu teenuste osutamisel kasutatavate võrgu- ja infosüsteemide osas, ja teenuste osas, mida üksus osutab. Selle põhjal võivad liikmesriigid asjakohasel juhul leida, et nimetatud üksust ei saa käsitada 2003/361/EÜ lisa artikli 2 kohase keskmise suurusega ettevõtjana või et üksus ei ületa keskmise suurusega ettevõtja kõnealuse artikli lõikes 1 esitatud ülemmäärasid, kui pärast selle üksuse sõltumatuse määra arvestamist üksnes tema enda andmete arvesse võtmisel ei käsitataks teda keskmise suurusega ettevõtjana või neid ülemmäärasid ületavana. See ei mõjuta käesoleva direktiivi kohaldamisalasse kuuluvate partner- ja sidusettevõtjate käesolevas direktiivis sätestatud kohustusi.

(17) Liikmesriikidel peaks olema võimalik otsustada, et üksusi, mis on direktiivi (EL) 2016/1148 kohaselt identifitseeritud kui oluliste teenuste operaatorid enne käesoleva direktiivi jõustumist, käsitatakse elutähtsate üksustena.

([7]) 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).

([8]) 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).

([9]) 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).

(18) Selleks et tagada selge ülevaade käesoleva direktiivi kohaldamisalasse kuuluvatest üksustest, peaksid liikmesriigid koostama elutähtsate ja oluliste üksuste ning domeeninimede registreerimise teenuseid osutavate üksuste loetelu. Selleks peaksid liikmesriigid nõudma, et üksused esitaksid pädevatele asutustele vähemalt järgmise teabe: nimi, aadress ja ajakohastatud kontaktandmed, sealhulgas üksuse e-posti aadressid, IP-vahemikud ja telefoninumbrid ning, kui see on kohaldatav, lisades osutatud asjaomane sektor ja allsektor ning, kui see on kohaldatav, selliste liikmesriikide loetelu, kus nad käesoleva direktiivi kohaldamisalasse kuuluvaid teenuseid osutavad. Selleks peaks komisjon Euroopa Liidu Küberturvalisuse Ameti (ENISA) abiga kehtestama põhjendamatu viivituseta teabe esitamise kohustusega seotud suunised ja vormid. Elutähtsate ja oluliste üksuste ning domeeninimede registreerimise teenuseid osutavate üksuste loetelu koostamise ja ajakohastamise hõlbustamiseks peaks liikmesriikidel olema võimalik luua riiklikud mehhanismid, mis võimaldavad üksustel end ise registreerida. Kui registrid on riigi tasandil olemas, saavad liikmesriigid otsustada asjakohaste mehhanismide üle, mis võimaldavad käesoleva direktiivi kohaldamisalasse kuuluvaid üksusi kindlaks määrata.

(19) Liikmesriigid peaksid esitama komisjonile vähemalt igasse lisades osutatud sektorisse ja allsektorisse kuuluvate elutähtsate ja oluliste üksuste arvu, samuti asjakohase teabe kindlaks määratud üksuste arvu kohta ja selle kohta, millise käesoleva direktiivi sätte põhjal need üksused kindlaks määrati ning millist liiki teenust nad osutavad. Liikmesriike julgustatakse vahetama komisjoniga teavet elutähtsate ja oluliste üksuste kohta ning ulatusliku küberturbeintsidendi korral asjakohast teavet (näiteks asjaomase üksuse nimi).

(20) Komisjon peaks koostöös koostöörühmaga ja pärast konsulteerimist asjaomaste sidusrühmadega andma mikroettevõtjate ja väikeste ettevõtjate suhtes kohaldatavate kriteeriumide rakendamise suunised, et hinnata, kas nad kuuluvad käesoleva direktiivi kohaldamisalasse. Samuti peaks komisjon tagama, et asjakohaseid suuniseid antakse käesoleva direktiivi kohaldamisalasse kuuluvatele mikroettevõtjatele ja väikestele ettevõtjatele. Komisjon peaks liikmesriikide toetusel tegema sellekohase teabe mikroettevõtjatele ja väikestele ettevõtjatele kättesaadavaks.

(21) Komisjon peaks andma suunised, mille eesmärk on abistada liikmesriike kohaldamisala käsitlevate käesoleva direktiivi sätete rakendamisel ja käesoleva direktiivi kohaselt võetavate meetmete proportsionaalsuse hindamisel, eelkõige seoses üksustega, millel on keerukad ärimudelid või tegevuskeskkonnad, mille puhul võib üksus vastata korraga nii elutähtsa kui ka olulise üksuse kriteeriumidele või viia samal ajal ellu tegevusi, millest osa kuulub käesoleva direktiivi kohaldamisalasse ja osa mitte.

(22) Käesolevas direktiivis sätestatakse selle kohaldamisalasse kuuluvate sektorite küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse baastase. Selleks et vältida liidu õigusaktide küberturvalisuse sätete killustumist, kui küberturvalisuse kõrge taseme tagamiseks kogu liidus peetakse vajalikuks valdkondlikke lisasätteid, mis käsitlevad küberturvalisuse riskijuhtimismeetmeid ja teatamiskohustust, peaks komisjon hindama, kas sellised lisasätted võiks ette näha käesoleva direktiivi alla kuuluvas rakendusaktis. Kui sellised rakendusaktid ei ole selleks sobivad, võiksid liidu valdkondlikud õigusaktid aidata tagada kogu liitu hõlmava küberturvalisuse kõrge taseme, võttes ühtlasi täielikult arvesse asjaomaste sektorite eripära ja keerukust. Sel otstarbel ei välista käesolev direktiiv ka niisuguste küberturvalisuse riskijuhtimismeetmeid ja intsidentidest teatamist käsitlevate edasiste valdkondlike liidu õigusaktide vastuvõtmist, milles võetakse igakülgselt arvesse vajadust luua terviklik ja ühtne küberturvalisuse raamistik. Käesolev direktiiv ei piira komisjonile mitmes sektoris, sealhulgas transpordi- ja energeetikasektoris antud rakendamisvolitusi.

(23) Kui valdkondlikes liidu õigusaktides on sätted, millega nõutakse elutähtsatelt või olulistelt üksustelt küberturvalisuse riskijuhtimismeetmete võtmist või olulistest intsidentidest teatamist, ning kui need nõuded on vähemalt samaväärsed käesolevas direktiivis sätestatud kohustustega, tuleks neid sätteid, sealhulgas järelevalve- ja täitmise tagamise sätteid,

niisuguste üksuste suhtes kohaldada. Kui valdkondlik liidu õigusakt ei hõlma kõiki konkreetse sektori üksusi, mis kuuluvad käesoleva direktiivi kohaldamisalasse, tuleks nimetatud liidu õigusaktiga hõlmamata üksuste suhtes kohaldada jätkuvalt käesoleva direktiivi asjakohaseid sätteid.

(24) Kui valdkondliku liidu õigusakti kohaselt peavad elutähtsad või olulised üksused täitma teatamise kohustust, mille mõju on vähemalt samaväärne käesolevas direktiivis sätestatud teatamiskohustusega, tuleks tagada intsidenditeadete ühtne ja tulemuslik käsitlemine. Selleks tuleks intsidenditeateid käsitleva valdkondliku liidu õigusakti sätetega anda CSIRTidele, pädevatele asutustele või käesoleva direktiivi kohastele ühtsetele küberturvalisuse kontaktpunktidele (edaspidi „ühtsed kontaktpunktid“) vastavalt valdkondlikule liidu õigusaktile esitatud intsidenditeadetele viivitamata juurdepääs. Sellise viivitamatu juurdepääsu saab tagada eelkõige juhul, kui intsidenditeated edastatakse põhjendamatu viivituseta CSIRTile, pädevale asutusele või käesoleva direktiivi kohasele ühtsele kontaktpunktile. Kui see on asjakohane, peaksid liikmesriigid looma intsidenditeadete käsitlemiseks automaatse ja otsese teavitamise mehhanismi, mis tagab süstemaatilise ja vahetu teabevahetuse CSIRTide, pädevate asutuste või ühtse kontaktpunktiga. Teatamise lihtsustamiseks ning automaatse ja otsese teatamise mehhanismi rakendamiseks võiksid liikmesriigid kooskõlas valdkondliku liidu õigusaktiga kasutada ühtset kontaktpunkti.

(25) Valdkondlikes liidu õigusaktides, millega nähakse ette küberturvalisuse riskijuhtimismeetmed või teatamiskohustus, millel on käesolevas direktiivis sätestatuga vähemalt samaväärne mõju, võiks ette näha, et nende õigusaktide kohased pädevad asutused kasutavad selliste meetmete või kohustustega seoses oma järelevalve- ja täitmise tagamise volitusi käesoleva direktiivi kohaselt määratud pädevate asutuste abil. Asjaomased pädevad asutused võivad sel eesmärgil kehtestada koostöökorra. Sellises koostöökorras võiks muu hulgas täpsustada järelevalvetegevuse koordineerimise korra, sealhulgas liikmesriigi õiguse kohaste uurimiste ja kohapealsete kontrollide korra ning pädevate asutuste vahelise järelevalvet ja täitmise tagamist käsitleva asjakohase teabe vahetamise mehhanismi, sealhulgas juurdepääsu kübervaldkonda puudutavale teabele, mida pädevad asutused käesoleva direktiivi kohaselt taotlevad.

(26) Kui valdkondlikes liidu õigusaktides on nõue, et üksused teataksid olulistest küberohtudest või pakutakse neile selleks stiimuleid, peaksid liikmesriigid samuti julgustama oluliste küberohtude jagamist CSIRTide, pädevate asutuste või käesoleva direktiivi kohaste ühtsete kontaktpunktidega, et tagada kõnealuste organite suurem teadlikkus küberohtudest ning võimaldada neil oluliste küberohtude realiseerumise korral tulemuslikult ja aegsasti reageerida.

(27) Käesolevas direktiivis sätestatud mõisteid ning järelevalve- ja täitmise tagamise raamistikku tuleks tulevastes valdkondlikes liidu õigusaktides igakülgselt arvesse võtta.

(28) Käesoleva direktiiviga seoses tuleks Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 ([10]) käsitada finantssektori ettevõtjate suhtes valdkondliku liidu õigusaktina. Käesoleva direktiivi sätete asemel tuleks kohaldada määruse (EL) 2022/2554 sätteid, mis käsitlevad info- ja kommunikatsioonitehnoloogia (IKT) riskijuhtimist, IKT intsidentide haldamist ja eelkõige tõsistest IKT intsidentidest teavitamist, samuti digitaalse tegevuskerksuse testimist, teabevahetuse kokkuleppeid ja kolmandatest isikutest tulenevat IKT-riski. Seetõttu ei tohiks liikmesriigid käesoleva direktiivi sätteid, mis käsitlevad küberturvalisuse riskijuhtimist ja teatamiskohustust, järelevalvet ja täitmise tagamist, määruse (EL) 2022/2554 kohaldamisalasse jäävate finantssektori ettevõtjate suhtes kohaldada. Samal ajal on käesoleva direktiivi kohaselt oluline tihedate suhete ja teabevahetuse säilitamine finantssektoriga. Selleks võimaldab määrus (EL) 2022/2554 Euroopa järelevalveasutustel ja kõnealuse määruse kohastel pädevatel asutustel osaleda koostöörühma tegevuses ning vahetada teavet ja teha koostööd ühtsete kontaktpunktidega, samuti CSIRTidega ja käesoleva direktiivi kohaste pädevate asutustega. Määruse (EL) 2022/2554 kohased pädevad asutused peaksid edastama tõsiste IKT intsidentide ja asjakohasel juhul oluliste küberohtude üksikasjad ka CSIRTidele,

([10]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (vt käesoleva *Euroopa Liidu Teataja* lk 1).

pädevatele asutusele või käesoleva direktiivi kohastele ühtsetele kontaktpunktidele. See on saavutatav vahetu juurdepääsu tagamisega intsidenditeadetele ja nende otsese või intsidenditeadete ühtse kontaktpunkti edastamise kaudu. Lisaks peaksid liikmesriigid jätkuvalt kaasama finantssektori oma küberturvalisuse strateegiatesse ning CSIRTid võivad oma tegevuses hõlmata ka finantssektorit.

(29) Selleks et vältida lennundussektori üksustele kehtestatud küberturvalisuse kohustustes lünki ja kohustuste dubleerimist, peaksid Euroopa Parlamendi ja nõukogu määruste (EÜ) nr 300/2008 ([11]) ja (EL) 2018/1139 ([12]) kohased riiklikud asutused ning käesoleva direktiivi kohased pädevad asutused tegema seoses küberturvalisuse riskijuhtimismeetmete rakendamisega ja nende meetmete järgimise järelevalvega riiklikul tasandil koostööd. Kui üksus järgib määrustes (EÜ) nr 300/2008 ja (EL) 2018/1139 ning nende määruste alusel vastu võetud asjakohastes delegeeritud õigusaktides ja rakendusaktides sätestatud turvanõudeid, võivad käesoleva direktiivi kohased pädevad asutused käsitada seda käesolevas direktiivis sätestatud vastavate nõuete järgimisena.

(30) Üksuste küberturvalisuse ja füüsilise julgeoleku omavahelisi seoseid arvestades tuleks tagada Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2557 ([13]) ja käesoleva direktiivi lähenemisviiside kooskõla. Selle saavutamiseks tuleks direktiivi (EL) 2022/2557 kohaseid elutähtsa teenuse osutajaid käsitada käesoleva direktiivi kohaselt elutähtsate üksustena. Lisaks peaks iga liikmesriik tagama, et tema riikliku küberturvalisuse strateegiaga nähakse ette poliitikaraamistik, mis võimaldab kõnealuses liikmesriigis käesoleva direktiivi ja direktiivi (EL) 2022/2557 kohaste tema pädevate asutuste vahelist tõhusamat koordineerimist seoses teabevahetusega küberriskide, -ohtude ja -intsidentide ning muude kui küberriskide, -ohtude ja -intsidentide kohta ning järelevalveülesannete täitmisega. Käesoleva direktiivi ja direktiivi (EL) 2022/2022/2557 kohased pädevad asutused peaksid tegema koostööd ja vahetama põhjendamatu viivituseta teavet, eelkõige seoses sellega, mis puudutab elutähtsate üksuste, küberriskide, -ohtude ja -intsidentide tuvastamist ning elutähtsaid üksusi mõjutavaid muid kui küberriske, -ohte ja -intsidente, sealhulgas elutähtsate üksuste võetavaid küberturvalisuse ja füüsilisi meetmeid ning selliste üksustega seotud järelevalvetegevuse tulemusi.

Lisaks, et ühtlustada käesoleva direktiivi ja direktiivi (EL) 2022/2022/2557 kohaste pädevate asutuste vahelist järelevalvetegevust ja minimeerida asjaomaste üksuste halduskoormust, peaksid kõnealused pädevad asutused püüdma ühtlustada intsidenditeadete vorme ja järelevalveprotsesse. Kui see on asjakohane, peaks direktiivi (EL) 2022/2557 kohastel pädevatel asutustel olema võimalik taotleda käesoleva direktiivi kohastelt pädevatelt asutustelt, et nad kasutaksid oma järelevalve- ja täitmise tagamise volitusi seoses üksusega, mida käsitatakse direktiivi (EL) 2022/2557 kohase elutähtsa teenuse osutajana. Käesoleva direktiivi ja direktiivi (EL) 2022/2557 kohased pädevad asutused peaksid, kui see on reaalajas võimalik, sel eesmärgil koostööd tegema ja teavet vahetama.

(31) Digitaristu sektorisse kuuluvad üksused põhinevad sisuliselt võrgu- ja infosüsteemidel ning seetõttu peaksid neile üksustele käesoleva direktiivi alusel pandud kohustused nende üksuste küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse raames hõlmama terviklikult ka selliste süsteemide füüsilist turvalisust. Kuna need küsimused on hõlmatud käesoleva direktiiviga, ei kohaldata selliste üksuste suhtes direktiivi (EL) 2022/2557 III, IV ja VI peatükis sätestatud kohustusi.

([11]) 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).

([12]) 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).

([13]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2557 mis käsitleb elutähtsa teenuse osutajate toimepidevust ja millega tunnistatakse kehtetuks nõukogu direktiiv 2008/114/EÜ (vt käesoleva *Euroopa Liidu Teataja* lk 164).

(32) Usaldusväärse, vastupidava ja turvalise domeeninimede süsteemi (DNS) tagamine ja hoidmine on võtmetähtsusega, et säilitada interneti usaldusväärsus ning oluline, et tagada selle pidev ja stabiilne toimimine, millest sõltuvad digimajandus ja -ühiskond. Seepärast tuleks käesolevat direktiivi kohaldada tippdomeeninimede registrite ja domeeninimede süsteemi teenuse osutajate suhtes, mida tuleb käsitada üksustena, mis osutavad interneti lõppkasutajatele mõeldud üldkasutatavate domeeninimede rekursiivse teisendamise teenust või kolmandatele isikutele kasutamiseks mõeldud domeeninimede autoriteetse teisendamise teenust. Käesolevat direktiivi ei tuleks kohaldada juurnimeserverite suhtes.

(33) Pilvandmetöötlusteenused peaksid hõlmama digiteenuseid, mis võimaldavad jagatavate andmetöötlusressursside skaleeritava ja paindliku kogumi nõudepõhist haldamist ning ulatuslikku kaugpääsu sellele kogumile, muu hulgas juhul, kui need ressursid paiknevad hajutatult erinevates kohtades. Andmetöötlusressursid on näiteks võrgud, serverid ja muu taristu, operatsioonisüsteemid, tarkvara, talletusruum, 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 „pilvandmetöötlusteenus“ ja „korraldusmudel“ on sama tähendus nagu nimetatud mõistetel standardi ISO/IEC 17788:2014 määratluses. Pilvandmetöötlusteenuse kasutaja võimekust tagada endale ühepoolselt andmetöötlusvõimekus, nagu serveriaeg või võrgu talletusruum, ilma pilvandmetöötlusteenuse osutaja inimesepoolse sekkumiseta, võiks nimetada nõudepõhiseks haldamiseks.

Mõistega „ulatuslik kaugpääs“ peetakse silmas seda, et pilvevõimalusi pakutakse võrgu kaudu ja need on kättesaadavad mehhanismide kaudu (sealhulgas mobiiltelefonid, tahvelarvutid, sülearvutid ja tööjaamad), mis toetavad heterogeensete nn kõhnade või paksude kliendiplatvormide kasutamist. Mõiste „skaleeritav“ osutab andmetöötlusressurssidele, mis on nõudluse kõikumisega toimetulekuks pilveteenuse osutaja poolt paindlikult jaotatavad olenemata ressursside geograafilisest asukohast. Mõistet „paindlik kogum“ kasutatakse andmetöötlusressursside kirjeldamiseks, mida pakutakse ja mis tehakse kättesaadavaks vastavalt nõudlusele, et kättesaadavaid ressursse suurendada või vähendada sõltuvalt töökoormusest. Mõistet „jagatav“ kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mida pakutakse paljudele kasutajatele, kellel on ühine juurdepääs teenusele, kuid mille puhul andmete töötlemine toimub iga kasutaja jaoks eraldi, olgugi et teenust osutatakse samadest elektroonilistest seadmetest. 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.

(34) Kuna maad võtavad uuenduslikud tehnoloogiad ja ärimudelid, tulevad eeldatavasti tarbijate muutuvate vajaduste järgi siseturule uued pilvandmetöötlusteenuse ja korraldusmudelid. Sellises kontekstis võib pilvandmetöötlusteenuseid osutada väga hajusal kujul, mille puhul töötlus toimub andmete loomise või kogumise kohale veelgi lähemal; seega liikudes nn traditsiooniliselt mudelilt väga hajusale mudelile (servtöötlus).

(35) 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 seetõttu käesoleva direktiivi kohaldamisalasse kuuluma ka selliste andmekeskusteenuste pakkujad, 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- (IT) ja võrguseadmete keskseks majutamiseks, omavahel sidumiseks ja käitamiseks, võttes arvesse ka energiajaotuse ja keskkonnajuhtimisega seotud rajatisi ja taristuid. Mõiste „andmekeskusteenus“ ei tohiks hõlmata asutusesiseseid andmekeskusi, mis kuuluvad asjaomasele üksusele ja mida käitatakse üksuse enda tarbeks.

(36) Teadusuuringutel on uute toodete ja protsesside väljatöötamisel võtmeroll. Paljusid neist tegevustest viivad ellu üksused, mis jagavad, levitavad või kasutavad oma teadusuuringute tulemusi ärilistel eesmärkidel. Need üksused võivad seega olla olulised osalejad väärtusahelates, mis muudab nende võrgu- ja infosüsteemide turvalisuse siseturu üldise küberturvalisuse lahutamatuks osaks. Teadusorganisatsioone tuleks käsitada nii, et need hõlmavad üksusi, mis pühendavad olulise osa oma tegevusest rakendusuuringutele või tootearendusele Majanduskoostöö ja Arengu

Organisatsiooni 2015. aasta Frascati käsiraamatu „Guidelines for Collecting and Reporting Data on Research and Experimental Development, with a view to exploiting their results for commercial purposes, such as the manufacturing and marketing of a product, process or the provision of a service“ („Teadus- ja arendustegevuse andmete kogumise ja esitamise suunised, et kasutada nende tulemusi ärilistel eesmärkidel, näiteks toote, protsessi või teenuse tootmiseks või turustamiseks“) tähenduses.

(37) Kasvav vastastikune sõltuvus tuleneb 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 hõlma see selliseid taristuid, mida omab, haldab või käitab liit või mida hallatakse või käitatakse liidu nimel liidu kosmoseprogrammi osana). Sellised vastastikused sõltuvussuhted tähendavad seda, et mis tahes häirel – 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 ajal hoogustunud küberründed on näidanud, kui vähe kaitstud on meie üha enam üksteisest sõltuvad ühiskonnad väikese realiseerumisvõimalusega riskide esinemise korral.

(38) Arvestades liikmesriikide juhtimisstruktuuride erinevusi ning selleks, et kaitsta juba kehtivat valdkondlikku korda või liidu reguleerivaid ja järelevalveasutusi, peaks liikmesriikidel olema võimalik määrata küberturvalisuse ja käesoleva direktiivi kohaste järelevalveülesannete eest vastutavaks vähemalt ühe riikliku pädeva asutuse või see asutada.

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

(40) Ühtsed kontaktpunktid peaksid tagama tõhusa piiriülese koostöö teiste liikmesriikide asjaomaste asutustega ning asjakohasel juhul komisjoni ja ENISAga. Seepärast tuleks ühtsetele kontaktpunktidele teha ülesandeks edastada CSIRTi või pädeva asutuse taotlusel teated piiriülese mõjuga oluliste intsidentide kohta teiste mõjutatud liikmesriikide ühtsetele kontaktpunktidele. Riiklikul tasandil peaksid ühtsed kontaktpunktid võimaldama sujuvat valdkondadevahelist koostööd teiste pädevate asutustega. Ühtsed kontaktpunktid võiksid olla ka määruse (EL) 2022/2554 kohaste pädevate asutuste edastatava, finantssektori ettevõtjatega seotud intsidente käsitleva asjakohase teabe adressaadid ning, kui see on asjakohane, peaks neil olema võimalik edastada kõnealune teave CSIRTidele või käesoleva direktiivi kohastele pädevatele asutustele.

(41) Liikmesriigid peaksid olema nii tehniliselt kui ka töökorralduse mõttes piisavalt varustatud, et ennetada, vältida ja avastada intsidente ja riske ning neile reageerida ja nende mõju leevendada. Seepärast peaksid liikmesriigid käesoleva direktiivi alusel looma või määrama ühe või mitu CSIRTi ning tagama, et neil on piisavad vahendid ja tehniline võimekus. CSIRTid peaksid vastama käesolevas direktiivis sätestatud nõuetele, et tagada tulemuslik ja ühilduv võimekus tulla toime intsidentide ja riskidega ning tagada liidu tasandil tõhus koostöö. Liikmesriigid peaksid saama CSIRTideks määrata ka olemasolevaid infoturbeintsidentidega tegelevaid rühmi (CERTe). Et tugevdada üksuste ja CSIRTide vahelist usalduslikku suhet olukorras, kus CSIRT on pädeva asutuse osa, peaks liikmesriikidel olema võimalik kaaluda CSIRTide operatiivülesannete funktsionaalset eraldamist, eelkõige seoses sellega, mis puudutab teabevahetust ja üksuste toetamist ning pädevate asutuste järelevalvetegevust.

(42) CSIRTide ülesandeks on intsidentide käsitlemine. See hõlmab suure hulga mõnikord tundlike andmete töötlemist. Liikmesriigid peaksid tagama, et CSIRTidel on teabevahetuse ja töötlemise taristu, samuti hästi varustatud töötajad, mis tagab nende tegevuse konfidentsiaalsuse ja usaldusväärsuse. CSIRTid võiksid sellega seoses vastu võtta ka tegevusjuhendid.

(43) Mis puutub isikuandmetesse, siis peaks CSIRTidel olema võimalik kooskõlas määrusega (EL) 2016/679 teha elutähtsa või olulise üksuse taotlusel üksuse teenuste osutamiseks kasutatavate võrgu- ja infosüsteemide ennetavat kontrolli. Kui see on kohaldatav, peaksid liikmesriigid püüdma tagada kõikide valdkondlike CSIRTide tehnilise võimekuse võrdse taseme. Liikmesriikidel peaks olema võimalik paluda oma CSIRTide arendamisel ENISA abi.

(44) CSIRTidel peaks üksuse taotluse alusel olema võimalik elutähtsa või olulise üksuse kõiki internetiühendusega varasid pidevalt jälgida, nii siseruumides kui ka väljaspool, et tuvastada, mõista ja hallata üksuse üldisi organisatsioonilisi riske seoses hiljuti tuvastatud tarneahela kahjustuste ja kriitilisel tasemel nõrkustega. Üksust tuleks julgustada CSIRTile teatama, kas tal on privilegeeritud juhtimisliides, kuna see võib mõjutada leevendusmeetmete võtmise kiirust.

(45) Arvestades küberturvalisuse alase rahvusvahelise koostöö tähtsust, peaks CSIRTidel olema võimalik lisaks käesoleva direktiivi kohaselt loodud CSIRTide võrgustikule osaleda ka rahvusvaheliste koostöövõrgustike töös. Seepärast peaks CSIRTidel ja pädevatel asutustel olema oma ülesannete täitmiseks võimalik vahetada teavet, sealhulgas isikuandmeid, kolmandate riikide riiklike küberturbe intsidentide lahendamise üksuste või pädevate asutustega, kui on täidetud liidu andmekaitseõiguses sätestatud tingimused isikuandmete edastamiseks kolmandatele riikidele, muu hulgas määruse (EL) 2016/679 artiklis 49 sätestatud tingimused.

(46) Oluline on tagada piisavad vahendid käesoleva direktiivi eesmärkide saavutamiseks ning võimaldada pädevatel asutustel ja CSIRTidel täita selles sätestatud kohustusi. Liikmesriigid võivad riiklikul tasandil kehtestada rahastamismehhanismi, et katta käesoleva direktiivi kohaselt liikmesriigis küberturvalisuse eest vastutavate avaliku sektori asutuste ülesannete täitmisega seotud vajalikud kulud. Selline mehhanism peaks olema kooskõlas liidu õigusega, proportsionaalne ja mittediskrimineeriv ning võtma arvesse erinevaid lähenemisviise turvaliste teenuste pakkumisele.

(47) 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 poliitika kujundamisega seotud asjaomased liidu asutused ja ametid, näiteks Europoli.

(48) Küberturvalisuse kõrge taseme saavutamiseks ja säilitamiseks peaksid käesoleva direktiiviga nõutavad riiklikud küberturvalisuse strateegiad koosnema sidusatest raamistikest, milles on esitatud strateegilised eesmärgid ja prioriteedid küberturvalisuse valdkonnas ning nende saavutamiseks vajalik juhtimine. Need strateegiad võivad koosneda ühest või mitmest seadusandlikust või muust kui seadusandlikust aktist.

(49) Võrgu- ja infosüsteemide taristu, riistvara, tarkvara ja veebipõhiste rakenduste turvalisuse ning selliste ettevõtjate või lõppkasutajate andmete kaitsmiseks, millest üksused sõltuvad, luuakse alus küberhügieeni poliitikameetmetega. Küberhügieeni poliitikameetmed, mis koosnevad ühistest alustavadest, sealhulgas tarkvara ja riistvara uuendamine, salasõnade muutmine, uute paigalduste haldamine, administraatori õigustega juurdepääsukontode piiramine ja andmete varundamine, võimaldavad luua intsidentide või küberohtude puhuks valmisoleku ning üldise turvalisuse ja julgeoleku ennetava raamistiku. Liikmesriikide küberhügieeni poliitikameetmeid peaks jälgima ja analüüsima ENISA.

(50) Küberturvalisuse alane teadlikkus ja küberhügieen on liidu küberturvalisuse taseme tõstmiseks üliolulised, eelkõige seetõttu, et ühendatud seadmete arv kasvab pidevalt ja neid võetakse küberrünnete puhul üha enam sihtmärgiks. Tuleks teha pingutusi, et suurendada üldist teadlikkust selliste seadmetega seotud riskidest, samal ajal kui liidu tasandil tehtavad hindamised võiksid aidata tagada ühtse arusaama sellistest riskidest siseturul.

(51) Liikmesriigid peaksid ergutama uuendusliku tehnoloogia, sealhulgas tehisintellekti kasutamist, mis võiks parandada küberrünnete avastamist ja ennetamist ning ressursse küberrünnete vastu paremini suunata. Seepärast peaksid liikmesriigid sellise tehnoloogia kasutamise hõlbustamiseks soodustama oma riiklikes küberturvalisuse strateegiates teadus- ja arendustegevust, eelkõige seoses küberturvalisuse automatiseeritud või poolautomaatsete vahenditega, ning, kui see on kohane, jagama sellise tehnoloogia kasutajate koolitamiseks ja tehnoloogia täiustamiseks vajalikke andmeid. Uuendusliku tehnoloogia, sealhulgas tehisintellekti kasutamine peaks olema kooskõlas liidu andmekaitseõigusega, sealhulgas andmekaitsepõhimõtetega, nagu andmete täpsus, võimalikult väheste andmete kogumine, õiglus ja läbipaistvus ning andmeturve, näiteks tipptasemel krüpteerimine. Määruses (EL) 2016/679 sätestatud lõimitud ja vaikimisi andmekaitse nõuetest tuleb täielikult kinni pidada.

(52) Tänu avatud lähtekoodiga küberturbevahenditele ja -rakendustele võib tõusta avatuse tase ja need võivad mõjuda soodsalt tööstusinnovatsiooni tõhususele. Avatud standardid soodustavad turbevahendite koostalitlusvõimet, mis on kasulik tööstusvaldkonna sidusrühmade turvalisuse seisukohast. Avatud lähtekoodiga küberturbevahendid ja -rakendused võivad võimendada laiemat arendajate kogukonda, võimaldades tarnijate mitmekesistamist. Avatud lähtekoodiga võib kaasneda küberturvalisusega seotud vahendite kontrolliprotsessi suurem läbipaistvus ning kogukonna juhitav nõrkuste tuvastamise protsess. Seetõttu peaks liikmesriikidel olema võimalik edendada avatud lähtekoodiga tarkvara ja avatud standardite kasutuselevõttu, järgides poliitikat, mis on seotud avatud andmete ja avatud lähtekoodi kasutamisega läbipaistvusel põhineva turvalisuse osana. Avatud lähtekoodiga küberturbevahendite kasutuselevõttu ja kestlikku kasutamist edendavad tegevuskavad, on eriti olulised väikeste ja keskmise suurusega ettevõtjate jaoks, kellel on märkimisväärsed rakenduskulud, mida saaks vähendada, kui vajadust spetsiifiliste rakenduste või vahendite järele vähendataks.

(53) Kommunaalettevõtted on üha enam ühendatud linnade digivõrkudega, et parandada linnatranspordivõrke, ajakohastada veevarustust ja jäätmekäitlust ning suurendada valgustuse ja hoonete kütmise tõhusust. Need digitaliseeritud kommunaalettevõtted on küberrünnete vastu vähe kaitstud ja edukas küberrünne võib kodanikke nende ettevõtete omavahelise seotuse tõttu ulatuslikult kahjustada. Liikmesriigid peaksid oma riikliku küberturvalisuse strateegia raames välja töötama poliitika, milles käsitletakse selliste ühendatud või arukate linnade arendamist ja nende võimalikku mõju ühiskonnale.

(54) Viimastel aastatel on liit seisnud silmitsi lunavararünnete hüppelise kasvuga, mille puhul pahavara krüpteerib andmeid ja süsteeme ning nõuab vabastamiseks lunaraha maksmist. Lunavararünnete sagenemist ja tõsidust võivad mõjutada mitmed tegurid, nagu erinevad ründemustrid, nagu lunavara kui teenusega seotud kuritegelikud ärimudelid ja krüptoraha, lunaraha nõudmised ja tarneahela rünnete sagenemine. Liikmesriigid peaksid oma riikliku küberturvalisuse strateegia raames välja töötama poliitika, milles käsitletakse lunavararünnete sagenemist.

(55) Sobiva raamistiku kõigi sidusrühmade vahel teadmiste vahetamiseks, parimate tavade jagamiseks ja vastastikuse mõistmise ühise taseme loomiseks võib pakkuda küberturvalisuse valdkonna avaliku ja erasektori partnerlus. Liikmesriigid peaksid edendama poliitikat, millega toetatakse küberturvalisuse valdkonna avaliku ja erasektori partnerluse loomist. Niisuguses poliitikas tuleks muu hulgas täpsustada, millised on avaliku ja erasektori partnerluse ulatus ja kaasatud sidusrühmad, juhtimismudel, olemasolevad rahastamisvõimalused ja osalevate sidusrühmade koostoime. Avaliku ja erasektori partnerluse raames saab võimendavalt kasutada erasektori üksuste eksperditeadmisi, et abistada pädevaid asutusi tänapäevaste teenuste ja protsesside arendamisel, sealhulgas teabevahetus, varajane hoiatamine, küberohtude ja intsidentidega seotud õppused, kriisiohje ning vastupanuvõime kavandamine.

(56) Liikmesriigid peaksid oma riiklikes küberturvalisuse strateegiates käsitlema väikeste ja keskmise suurusega ettevõtjate küberturvalisuse vajadusi. Liidus on väikeste ja keskmise suurusega ettevõtjate osakaal tööstus- ja äriturul suur ning neil on sageli raske kohaneda uute äritavadega üha rohkem ühendatud maailmas ja digitaalses keskkonnas, kus töötajad on kodutööl ja äritegevus toimub järjest rohkem interneti kaudu. Mõnedel väikestel ja keskmise suurusega ettevõtjatel on küberturvalisusega seoses sellised probleemid nagu vähene küberteadlikkus, kaugtöösüsteemide IT-turvalisuse puudumine, küberturvalisuse tagamiseks kasutatavate lahenduste suured kulud ja kõrgem ohutase, näiteks lunavaraga seoses, mille lahendamiseks nad peaksid saama suuniseid ja tuge. Väikestest ja keskmise suurusega ettevõtjatest on üha enam saamas tarneahela rünnete sihtmärk, sest nende küberturvalisuse riskijuhtimismeetmed ja ründehaldamine ei ole nii ranged ning asjaolu tõttu, et neil on piiratud turberessursid. Sellised tarneahela ründed ei mõjuta üksnes väikeseid ja keskmise suurusega ettevõtjaid ja nende tegevust, vaid võivad avaldada astmelist mõju ka üksustele, kellele nad tarnivad, põhjustades ulatuslikuma ründe. Liikmesriigid peaksid oma riiklike küberturvalisuse strateegiate kaudu aitama väikestel ja keskmise suurusega ettevõtjatel

tarneahelates esinevaid probleeme lahendada. Liikmesriikidel peaks olema väikeste ja keskmise suurusega ettevõtjate jaoks riiklikul või piirkondlikul tasandil kontaktpunkt, mis kas annab väikestele ja keskmise suurusega ettevõtjatele suuniseid ja abi või suunab nad küberturvalisuse küsimustes suuniste ja abi saamiseks asjakohaste asutuste juurde. Liikmesriike julgustatakse osutama ka selliseid teenuseid nagu veebisaidi konfigureerimine ja logimise võimaldamine mikroettevõtjatele ja väikestele ettevõtjatele, kellel see võimekus puudub.

(57) Liikmesriigid peaksid oma riiklikes küberturvalisuse strateegiates laiema kaitsestrateegia osana võtma kasutusele aktiivse küberkaitse edendamise poliitika. Selle asemel et tegutseda reageerivalt, tähendab aktiivne küberkaitse võrguturbe rikkumise aktiivset ennetamist, avastamist, seiret, analüüsimist ja tagajärgede leevendamist, milleks kasutatakse nii ohvri võrgus kui ka sellest väljaspool olevaid võimalusi. See võiks hõlmata liikmesriike, kes pakuvad teatavatele üksustele tasuta teenuseid või vahendeid, sealhulgas iseteeninduskontrolle, avastamisvahendeid ja kõrvaldamisteenuseid. Võime ohuteavet ja -analüüse, kübertegevuse hoiatusi ja reageerimismeetmeid kiiresti ja automaatselt jagada ning mõista on üliolulise, et teha ühtseid pingutusi võrgu- ja infosüsteemide vastu suunatud rünnete tulemuslikuks ennetamiseks, avastamiseks ja vastumeetmete võtmiseks. Aktiivne küberkaitse põhineb kaitsestrateegial, millega välistatakse ründemeetmed.

(58) Kuna võrgu- ja infosüsteemide nõrkuste ärakasutamine võib põhjustada suuri häireid ja olulist kahju, on selliste nõrkuste kiire tuvastamine ja kõrvaldamine riskide vähendamise tähtis tegur. Üksused, mis võrgu- ja infosüsteeme välja töötavad või haldavad, peaksid seetõttu kehtestama asjakohase korra, mille alusel nõrkuste avastamise korral neid käsitleda. Kuna nõrkusi avastavad ja avalikustavad sageli kolmandad isikud, peaks IKT-toodete või IKT-teenuste tootja või osutaja kehtestama ka vajaliku menetluskorra kolmandatelt isikutelt nõrkusi käsitleva teabe saamiseks. Suunised nõrkuste käsitlemiseks ja nende avalikustamiseks on esitatud rahvusvahelistes standardites ISO/IEC 30111 ja ISO/IEC 29147. Selleks et soodustada nõrkuste avalikustamise vabatahtlikku raamistikku, on eriti oluline tugevdada füüsiliste ja juriidiliste isikute ning IKT-toodete või IKT-teenuste tootjate või osutajate vahelise koostöö koordineerimist. Nõrkuste koordineeritud avalikustamise all peetakse silmas struktureeritud protsessi, mille käigus teatatakse potentsiaalselt nõrkade IKT-toodete või IKT-teenuste tootjale või osutajale nõrkustest viisil, mis võimaldab neil nõrkust diagnoosida ja selle kõrvaldada enne, kui nõrkusega seotud üksikasjalik teave avalikustatakse kolmandatele isikutele või üldsusele. Nõrkuste koordineeritud avalikustamise protsess peaks hõlmama ka füüsiliste ja juriidiliste isikute ning potentsiaalselt nõrkade IKT-toodete või IKT-teenuste tootja või osutaja vahelist koordineerimist nõrkuste kõrvaldamise ja avalikustamise ajastamise asjus.

(59) Komisjon, ENISA ja liikmesriigid peaksid ka edaspidi edendama küberturvalisuse riskijuhtimise valdkonna rahvusvaheliste standardite ja tööstusvaldkonna praeguste parimate tavadega kooskõla saavutamist, näiteks tarneahela turvalisuse hindamise, teabevahetuse ja nõrkuste avalikustamise valdkonnas.

(60) Liikmesriigid peaksid võtma koostöös ENISAga meetmeid, et nõrkuste koordineeritud avalikustamist hõlbustada, kehtestades selleks asjakohase riikliku poliitika. Oma riikliku poliitika raames peaksid liikmesriigid kooskõlas oma õigusega püüdma võimalikult suures ulatuses lahendada probleeme, millega puutuvad kokku nõrkuste valdkonnas uuringuid läbi viivad isikud, sealhulgas probleeme, mis on seotud nende võimaliku kriminaalvastutusega. Võttes arvesse, et mõnes liikmesriigis võib nõrkuste valdkonnas uuringuid läbi viivate füüsiliste ja juriidiliste isikute suhtes kohaldada kriminaal- ja tsiviilvastutust, soovitatakse liikmesriikidel võtta vastu suunised, mis käsitlevad infoturbeuurijate nende tegevuse eest vastutusele võtmisest loobumist ja tsiviilvastutusest vabastamist.

(61) Liikmesriigid peaksid määrama ühe oma CSIRTidest koordinaatoriks, kes tegutseb vajaduse korral usaldatud vahendajana teavitavate üksuste ja IKT-toodete või IKT-teenuste tootjate või osutajate vahel, keda nõrkus tõenäoliselt mõjutab. Koordinaatoriks määratud CSIRTi ülesanneteks peaks eelkõige olema teha kindlaks asjaomased üksused ja võtta nendega ühendust, toetada nõrkusest teavitavaid füüsilisi ja juriidilisi isikuid, pidada

läbirääkimisi avalikustamise tähtaegade üle ning hallata mitmeid üksusi mõjutavate nõrkustega seonduvat tegevust (mitut poolt puudutavate nõrkuste koordineeritud avalikustamine). Kui teatatud nõrkus võib oluliselt mõjutada üksusi rohkem kui ühes liikmesriigis, peaksid koordinaatoriks määratud CSIRTid tegema, kui see on kohane, koostööd CSIRTide võrgustiku raames.

(62) Juurdepääs õigele ja õigeaegsele teabele IKT-tooteid ja IKT-teenuseid mõjutavate nõrkuste kohta aitab küberturvalisuse riskijuhtimist tõhustada. Nõrkuste kohta avalikult kättesaadava teabe allikad on üksuste ja nende teenuste kasutajate, aga ka riiklike pädevate asutuste ja CSIRTide jaoks oluline vahend. Sel põhjusel peaks ENISA looma Euroopa nõrkuste andmebaasi, kus üksused, olenemata sellest, kas nad kuuluvad käesoleva direktiivi kohaldamisalasse, ja nende võrgu- ja infosüsteemide tarnijad, ning pädevad asutused ja CSIRTid võivad üldtuntud nõrkusi vabatahtlikult avalikustada ning registreerida, mis võimaldab kasutajatel võtta asjakohaseid leevendusmeetmeid. Andmebaasi eesmärk on käsitleda ainulaadseid probleeme, mida riskid liidu üksustele tekitavad. Ühtlasi peaks ENISA kehtestama avaldamisprotsessiga seoses sobiva menetluse, millega anda üksustele aega võtta oma nõrkuste kõrvaldamiseks leevendusmeetmeid ning kasutada tänapäevaseid küberturvalisuse riskijuhtimismeetmeid ning võtta kasutusele masinloetavad andmekogud ja vastavad liidesed. Selleks et edendada nõrkuste avalikustamise kultuuri, ei tohiks avalikustamisel olla nõrkusest teatavale füüsilisele või juriidilisele isikule kahjulikke tagajärgi.

(63) Kuigi sarnaseid nõrkuste registreid või andmebaase on ka juba loodud, majutavad ja haldavad neid üksused, mille asukoht ei ole liidus. ENISA hallatav Euroopa nõrkuste andmebaas tagaks nõrkuste ametlikule avalikustamisele eelneva avalikustamisprotsessi suurema läbipaistvuse ning suurendaks vastupidavust sarnaste teenuste osutamist mõjutava häire või katkestuse korral. Et vältida topelttööd ja püüda saavutada võimalikult suures ulatuses vastastikune täiendavus, peaks ENISA uurima võimalust sõlmida struktureeritud koostöökokkuleppeid kolmandate riikide jurisdiktsiooni alla kuuluvate sarnaste registrite või andmebaasidega. Eelkõige peaks ENISA uurima võimalust teha tihedat koostööd ühiste nõrkuste ja riskide süsteemi operaatoritega.

(64) Koostöörühm peaks hõlbustama ja toetama strateegilist koostööd ja teabevahetust ning suurendama liikmesriikide vahelist usaldust ja kindlustunnet. Koostöörühm peaks koostama iga kahe aasta järel tööprogrammi. Tööprogramm peaks hõlmama koostöörühma poolt oma eesmärkide ja ülesannete täitmiseks võetavaid meetmeid. Käesoleva direktiivi kohase esimese tööprogrammi koostamise ajakava tuleks viia vastavusse direktiivi (EL) 2016/1148 alusel koostatud viimase tööprogrammi ajakavaga, et vältida võimalikke häireid koostöörühma töös.

(65) Juhenddokumentide väljatöötamisel peaks koostöörühm olemasolevate reeglite tõhusamaks rakendamiseks järjepidevalt kaardistama riiklikud lahendused ja kogemused, hindama koostöörühma tegevuse tulemuste mõju riiklikele lähenemisviisidele, arutama rakendamisega seotud probleeme ning sõnastama konkreetsed soovitused olemasolevate reeglite tõhusamaks rakendamiseks, eelkõige hõlbustamaks käesoleva direktiivi ühtlast ülevõtmist liikmesriikides. Koostöörühm peaks riiklikud lahendused ka kaardistama, et edendada kogu liidus igas konkreetses sektoris kasutatavate küberturvalisuse lahenduste ühilduvust. See on eriti oluline rahvusvahelise või piiriülese olemusega sektoritele.

(66) Koostöörühm peaks jääma paindlikuks foorumiks ning suutma reageerida muutuvatele ja uutele poliitilistele prioriteetidele ja probleemidele, võttes seejuures arvesse vahendite kättesaadavust. Ta võiks korraldada korrapäraseid ühiskohtumisi asjaomaste erasektori sidusrühmadega kogu liidust, et arutada koostöörühma tegevust ning koguda andmeid ja sisendit esilekerkivate poliitiliste probleemide kohta. Lisaks peaks koostöörühm korrapäraselt hindama küberohtude või intsidentide, näiteks lunavara olukorda. Et tõhustada koostööd liidu

tasandil, peaks koostöörühm kaaluma võimalust kutsuda oma töös osalema küberturvalisuse poliitika kujundamisega seotud asjaomased liidu institutsioonid, organid ja asutused, näiteks Euroopa Parlament, Europol, Euroopa Andmekaitsenõukogu, määrusega (EL) 2018/1139 loodud Euroopa Liidu Lennundusohutusamet ning Euroopa Parlamendi ja nõukogu määrusega (EL) 2021/696 ([14]) loodud Euroopa Liidu Kosmoseprogrammi Amet.

(67) Pädevatel asutustel ja CSIRTidel peaks olema võimalik liikmesriikidevahelise koostöö parandamiseks ja usalduse suurendamiseks osaleda teiste liikmesriikidega ametnike vahetamise programmis konkreetses raamistikus ja, kui see on kohaldatav, tingimusel et niisugustes vahetusprogrammides osalevad ametnikud läbivad kohustusliku julgeoleku-kontrolli. Pädevad asutused peaksid võtma vajalikud meetmed, et võimaldada teiste liikmesriikide ametnikel täita vastuvõtva pädeva asutuse või vastuvõtva CSIRTi tegevuses tulemuslikku rolli.

(68) Liikmesriigid peaksid aitama kaasa komisjoni soovituses (EL) 2017/1584 ([15]) ette nähtud küberturvalisuse kriisidele reageerimise ELi raamistiku loomisele olemasolevate koostöövõrgustike, eelkõige Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikule (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 puudutav kord, muu hulgas rollid, koostööviisid, teiste asjaomaste osalejatega suhtlemine, teabevahetuse vormid ja kommunikatsioonivahendid. Liidu tasandi kriisiohje puhul peaksid asjaomased pooled lähtuma nõukogu rakendusotsuses (EL) 2018/1993 ([16]) sätestatud kriisidele poliitilist reageerimist käsitlevast ELi integreeritud korrast (edaspidi „IPCRi kord“). Komisjon peaks selleks rakendama üldise kiirhoiatussüsteemi ARGUS kõrgetasemelise valdkondadevahelise kriisikoordineerimise menetlusprotsessi. Kui kriisil on oluline välispoliitiline või ühise julgeoleku- ja kaitsepoliitikaga seotud mõõde, tuleks käivitada Euroopa välisteenistuse kriisidele reageerimise mehhanism.

(69) Soovituse (EL) 2017/1584 lisa kohaselt tuleks ulatusliku küberturbeintsidendina mõista intsidenti, mille põhjustatud häired on niivõrd laialdased, et ühe liikmesriigi suutlikkusest nendega toimetulekuks ei piisa, või millel on märkimisväärne mõju vähemalt kahele liikmesriigile. Olenevalt nende põhjusest ja mõjust võivad ulatuslikud küberturbeintsidendid eskaleeruda ning muutuda täieulatuslikuks kriisiks, mis takistab siseturu tõrgeteta toimimist või kujutab endast mitme liikmesriigi või kogu liidu üksustele või kodanikele tõsist avaliku julgeoleku- või turvalisusriski. 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.

(70) Liidu tasandi ulatuslike küberturbeintsidentide ja kriiside puhul tuleb kiire ja tõhusa reageerimise tagamiseks võtta koordineeritud meetmeid, kuna sektorite ja liikmesriikide omavaheline sõltuvus on väga suur. Kübervastupidavus-võimeliste võrgu- ja infosüsteemide olemasolu ning andmete kättesaadavus, konfidentsiaalsus ja terviklus on väga olulised liidu julgeoleku ning liidu kodanike, ettevõtjate ja institutsioonide kaitsmiseks intsidentide ja küberohtude eest ning samuti selleks, et suurendada üksikisikute ja organisatsioonide usaldust liidu võimekuse vastu edendada ja kaitsta üleilmset, avatud, vaba, stabiilset ja turvalist küberruumi, mis põhineb inimõigustel, põhivabadustel, demokraatial ja õigusriigil.

([14]) Euroopa Parlamendi ja nõukogu 28. aprilli 2021. aasta määrus (EL) 2021/696, millega luuakse liidu kosmoseprogramm ja Euroopa Liidu Kosmoseprogrammi Amet ning tunnistatakse kehtetuks määrused (EL) nr 912/2010, (EL) nr 1285/2013 ja (EL) nr 377/2014 ning otsus nr 541/2014/EL (ELT L 170, 12.5.2021, lk 69).

([15]) 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).

([16]) Nõukogu 11. detsembri 2018. aasta rakendusotsus (EL) 2018/1993, mis käsitleb ELi integreeritud korda poliitiliseks reageerimiseks kriisidele (ELT L 320, 17.12.2018, lk 28).

(71) EU-CyCLONe peaks ulatuslike küberturbeintsidentide ja kriiside korral toimima vahendajana tehnilise ja poliitilise tasandi vahel ning tõhustama operatiivtasandi koostööd ja toetama otsuste tegemist poliitilisel tasandil. Võttes arvesse komisjoni pädevust kriisiohje valdkonnas, peaks EU-CyCLONe koostöös komisjoniga tuginema CSIRTide võrgustiku järeldustele ja kasutama oma võimekust, et koostada ulatuslike küberturbeintsidentide ja kriiside mõjuanalüüs.

(72) Küberründed on oma olemuselt piiriülesed ning oluline intsident võib häirida ja kahjustada elutähtsaid teabetaristuid, millest sõltub siseturu sujuv toimimine. Kõigi asjaomaste osalejate rolli käsitletakse soovituses (EL) 2017/1584. Lisaks vastutab komisjon Euroopa Parlamendi ja nõukogu otsusega nr 1313/2013/EL ([17]) loodud liidu elanikkonnakaitse mehhanismi raames üldiste valmisolekumeetmete eest, mis hõlmavad hädaolukordadele reageerimise koordineerimiskeskuse ning ühise hädaolukordade side- ja infosüsteemi haldamist, olukorrateadlikkuse ja analüüsivõime säilitamist ja edasiarendamist ning liikmesriigi või kolmanda riigi abitaotluse korral eksperdirühmade mobiliseerimise ja lähetamise võimekuse loomist ja haldamist. Komisjon vastutab ka rakendusotsuse (EL) 2018/1993 kohase IPCRi korra analüüsiaruannete esitamise eest, muu hulgas seoses küberturvalisuse olukorrateadlikkuse ja valmisolekuga, samuti olukorrateadlikkuse ja kriisidele reageerimisega põllumajanduse, ebasoodsate ilmastikutingimuste, konfliktide kaardistamise ja prognooside, loodusõnnetuste varajase hoiatamise süsteemide, tervisealaste hädaolukordade, nakkushaiguste seire, taimetervise, keemiliste ainetega seotud juhtumite, toidu- ja söödaohutuse, loomatervise, rände, tolli, tuumaavariide ja kiirguslike avariiolukordade ning energeetika valdkonnas.

(73) Kui see on asjakohane, võib liit kooskõlas ELi toimimise lepingu artikliga 218 sõlmida kolmandate riikide või rahvusvaheliste organisatsioonidega rahvusvahelisi lepinguid, mis võimaldab neil osaleda ja korraldada osalust mõningates koostöörühma, CSIRTide võrgustiku ning EU-CyCLONe tegevuses. Selliste lepingutega tuleks tagada liidu huvid ja piisaval tasemel andmekaitse. See ei tohiks välistada liikmesriikide õigust teha nõrkuste haldamisel ja küberturvalisuse riskijuhtimisel koostööd kolmandate riikidega, hõlbustades liidu õiguse kohast teatamist ja üldist teabevahetust.

(74) Selleks et hõlbustada käesoleva direktiivi tulemuslikku rakendamist muu hulgas sellistes valdkondades nagu nõrkuste haldamine, küberturvalisuse riskijuhtimismeetmed, teatamiskohustus ja küberturvalisuse alase teabevahetuse kokkulepped, võivad liikmesriigid teha koostööd kolmandate riikidega ja võtta meetmeid, mida peetakse sel eesmärgil asjakohaseks, sealhulgas küberohtude, intsidentide, nõrkuste, vahendite ja meetodite, taktika, võtete ja menetlustega seotud teabevahetus, küberturvalisuse kriiside ohjamisega seotud valmisolek ja õppused, koolitus, usalduse loomine ja struktureeritud teabevahetuse kokkulepped.

(75) Kasutusele tuleks võtta vastastikune hindamine, et aidata õppida ühistest kogemustest, tugevdada vastastikust usaldust ja saavutada küberturvalisuse ühtlaselt kõrge tase. Vastastikune hindamine võib anda väärtuslikke teadmisi ja viia soovitusteni, mis tugevdavad üldist küberturvalisuse võimekust, luues uue funktsionaalse tee parimate tavade jagamiseks liikmesriikide vahel ning aidates tõsta liikmesriikide küberturvalisuse taset. Lisaks peaks vastastikuses hindamises võtma arvesse sarnaste mehhanismide, näiteks CSIRTide võrgustiku vastastikuse hindamise süsteemi tulemusi, looma lisaväärtust ja vältima dubleerimist. Vastastikuse hindamise rakendamine ei tohiks piirata konfidentsiaalse ja salastatud teabe kaitset käsitlevate riiklike või liidu õigusaktide kohaldamist.

(76) Koostöörühm peaks kehtestama liikmesriikide jaoks enesehindamise metoodika, mille eesmärk on hõlmata selliseid tegureid nagu küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse rakendamise tase, pädevate asutuste võimekuse tase ja ülesannete täitmise tulemuslikkus, CSIRTide tegevusvõimekus, vastastikuse abi rakendamise tase, küberturvalisuse alase teabevahetuse korra rakendamise tase või konkreetsed piiriülese või valdkondadevahelise iseloomuga küsimused. Liikmesriike tuleks julgustada tegema korrapäraselt enesehindamisi ning esitama ja arutama oma enesehindamise tulemusi koostöörühmas.

([17]) Euroopa Parlamendi ja nõukogu 17. detsembri 2013. aasta otsus nr 1313/2013/EL liidu elanikkonnakaitse mehhanismi kohta (ELT L 347, 20.12.2013, lk 924).

(77) Vastutus võrgu- ja infosüsteemi turvalisuse tagamise eest lasub suurel määral elutähtsatel ja olulistel üksustel. Tuleks edendada ja arendada riskijuhtimiskultuuri, mis hõlmab riskihindamisi ja riskile vastavate küberturvalisuse riskijuhtimismeetmete rakendamist.

(78) Küberturvalisuse riskijuhtimismeetmetes peaks võtma arvesse, mil määral elutähtis või oluline üksus võrgu- ja infosüsteemidest sõltub, ning hõlmama meetmeid intsidendiriskide tuvastamiseks, vältimiseks, avastamiseks, neile reageerimiseks ja neist taastumiseks ning nende mõju leevendamiseks. Võrgu- ja infosüsteemide turvalisus peaks hõlmama salvestatavate, edastatavate ja töödeldavate andmete turvalisust. Küberturvalisuse riskijuhtimismeetmetega tuleks tagada süsteemne analüüs, milles võetakse arvesse inimtegurit, et saada võrgu- ja infosüsteemi turvalisusest terviklik pilt.

(79) Kuna võrgu- ja infosüsteemide turvalisust ähvardavatel ohtudel võib olla erinev põhjus, peaksid küberturvalisuse riskijuhtimismeetmed tuginema kõiki ohte hõlmavale käsitusele, mille eesmärk on kaitsta võrgu- ja infosüsteeme ja nende füüsilist keskkonda selliste olukordade eest nagu vargus, tulekahju, üleujutus, telekommunikatsiooni- või elektrikatkestus või loata füüsiline juurdepääs elutähtsa või olulise 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 küberturvalisuse riskijuhtimismeetmed käsitlema ka võrgu- ja infosüsteemide füüsilist turvalisust ja keskkonnaohutust, hõlmates selliste süsteemide kaitsmist süsteemirikete, inimliku eksimuse, pahatahtliku tegevuse või loodusnähtuste eest kooskõlas Euroopa ja rahvusvaheliselt tunnustatud standarditega, näiteks ISO/IEC 27000 seeria standarditega. Sellega seoses peaksid elutähtsad ja olulised üksused oma küberturvalisuse riskijuhtimismeetmete osana käsitlema ka personali turvalisust ja kehtestama asjakohased juurdepääsukontrolli põhimõtted. Need meetmed peaksid olema kooskõlas direktiiviga (EL) 2022/2557.

(80) Selleks et tõendada vastavust küberturvalisuse riskijuhtimismeetmetele ja kui puuduvad Euroopa Parlamendi ja nõukogu määrusele (EL) 2019/881 ([18]) vastavad asjakohased Euroopa küberturvalisuse sertifitseerimise kavad, peaksid liikmesriigid konsulteerides koostöörühma ja Euroopa küberturvalisuse sertifitseerimise rühmaga edendama asjaomaste Euroopa ja rahvusvaheliste standardite kasutamist elutähtsate ja oluliste üksuste poolt, või liikmesriigid võivad üksustelt nõuda, et nad kasutaksid sertifitseeritud IKT-tooteid, IKT-teenuseid ja IKT-protsesse.

(81) Et vältida elutähtsatele ja olulistele üksustele ebaproportsionaalse finants- ja halduskoormuse panemist, peaksid küberturvalisuse riskijuhtimismeetmed olema proportsionaalsed asjaomase võrgu- ja infosüsteemi puhul esineva riski tasemega ning lähtuma selliste meetmete tehnilisest tasemest ning, kui see on kohaldatav, Euroopa ja rahvusvahelistest standarditest ning nende rakendamise kuludest.

(82) Küberturvalisuse riskijuhtimismeetmed peaksid olema proportsionaalsed elutähtsa või olulise üksuse riskidele avatuse määraga ning intsidendi ühiskondliku ja majandusliku mõjuga. Elutähtsatele ja olulistele üksustele kohandatud küberturvalisuse riskijuhtimismeetmete kehtestamisel tuleks igakülgselt arvesse võtta elutähtsate ja oluliste üksuste erinevat avatust riskidele, näiteks üksuse kriitilisuse määra, riske, sealhulgas ühiskondlikke riske, millega ta kokku puutub, üksuse suurust, intsidentide esinemise tõenäosust ja nende tõsidust, sealhulgas nende ühiskondlikku ja majanduslikku mõju.

([18]) 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).

(83) 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 elutähtsa või olulise üksuse enda IT-töötajad või mille turvalisusega seotud teenused ostetakse sisse. Käesolevas direktiivis sätestatud küberturvalisuse riskijuhtimismeetmeid ning teatamiskohustust tuleks kohaldada asjaomaste elutähtsate ja oluliste üksuste suhtes olenemata sellest, kas kõnealused üksused hooldavad oma võrgu- ja infosüsteeme ise või tellivad selleks hooldusteenuse väljast.

(84) Võttes arvesse nende piiriülest olemust, tuleks domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate, hallatud teenuse osutajate, turbetarnijate, internetipõhise kauplemiskohtade, internetipõhiste otsingumootorite, sotsiaalvõrguteenuse platvormi pakkujate ja usaldusteenuse osutajate suhtes kohaldada liidu tasandil suuremat ühtlustamist. Seetõttu tuleks küberturvalisuse riskijuhtimismeetmete rakendamise hõlbustamiseks seoses kõnealuste üksustega võtta vastu rakendusakt.

(85) Eriti oluline on tegeleda riskidega, mis tulenevad üksuse tarneahelast ja suhetest tema tarnijatega, näiteks andmete talletamise ja töötlemise teenuse osutajate või turbeteenuse osutajate ja sisutoimetajatega, kui võtta arvesse selliste intsidentide esinemise sagedust, mille puhul üksused on langenud võrgu- ja infosüsteemi vastu suunatud küberrünnete ohvriks ning kurjategijad on suutnud kahjustada üksuse võrgu- ja infosüsteemide turvalisust, kasutades ära kolmandate isikute tooteid ja teenuseid mõjutavaid nõrkusi. Seepärast peaksid elutähtsad ja olulised üksused hindama ja arvesse võtma toodete ja teenuste üldist kvaliteeti ja vastupidavust, nendesse integreeritud küberturvalisuse riskijuhtimismeetmeid, samuti oma tarnijate ja teenuseosutajate küberturvalisuse tavasid, sealhulgas nende turvalise arenduse menetlusi. Elutähtsaid ja olulisi üksusi tuleks eelkõige julgustada lisama küberturvalisuse riskijuhtimismeetmeid oma otseste tarnijate ja teenuseosutajatega sõlmitavatesse lepingutesse. Kõnealused üksused võiksid võtta arvesse ka riske, mis tulenevad muu tasandi tarnijatest ja teenuseosutajatest.

(86) Teenuseosutajate seas on intsidentide ennetamisel, tuvastamisel, lahendamisel ja neist taastumisel üksuste jaoks eriti oluline tugiroll turbetarnijatel sellistes teenusevaldkondades nagu intsidentide lahendamine, läbistustestimine, turvaaudit ja konsultatsioonid. Turbetarnijad on aga olnud ka ise küberrünnete sihtmärgiks ja kuna nad on üksuste tegevusse tihedalt lõimitud, kaasneb nendega eriline risk. Seega peaksid elutähtsad ja olulised üksused olema turbetarnija valimisel iseäranis hoolikad.

(87) Pädevad asutused võivad oma järelevalveülesannete täitmisel kasutada ka selliseid küberturvalisuse teenuseid nagu turvaauditid, läbistustestimine või intsidentide lahendamine.

(88) Elutähtsad ja olulised üksused peaksid tähelepanu pöörama ka sellistele riskidele, mis tulenevad nende suhtlemisest ja suhetest teiste sidusrühmadega laiemas ökosüsteemis, et muu hulgas tõkestada tööstusspionaaži ja kaitsta ärisaladusi. Täpsemalt peaksid üksused võtma asjakohaseid meetmeid tagamaks, et nende koostöö akadeemiliste ja teadusasutustega toimub kooskõlas nende küberturvalisuse poliitikaga ning et selles koostöös järgitakse teabele turvalise juurdepääsu ja selle levitamisega seotud üldisi häid tavasid ja eelkõige intellektuaalomandi kaitsega seotud tavasid. Võttes arvesse andmete olulisust ja väärtust elutähtsate ja oluliste üksuste tegevuse jaoks, peaksid kõnealused üksused kolmandate isikute poolt osutatavatele andmete teisendamise ja analüüsi teenustele tuginedes võtma kõik asjakohased küberturvalisuse riskijuhtimismeetmed.

(89) Elutähtsad ja olulised üksused peaksid kasutusele võtma mitmesugused küberhügieeni põhitavad, näiteks usaldamatuse põhimõtte, tarkvarauuendused, seadme konfiguratsiooni, võrgu segmenteerimise, identiteedi ja juurdepääsu halduse ning kasutajateadlikkuse, ning pakkuma oma töötajatele koolitusi ning suurendama teadlikkust küberohtude, andmepüügi ja inimestega manipuleerimise meetodite kohta. Lisaks peaksid kõnealused üksused hindama oma küberturvalisuse võimekust ning püüdma võtta asjakohasel juhul kasutusele küberturvalisust suurendavad tehnoloogiad, näiteks tehisintellekti või masinõppesüsteemid, et suurendada oma võimekust ning võrgu- ja infosüsteemide turvalisust.

(90) Et käsitleda põhjalikumalt peamisi tarneahelariske ning aidata asjakohaselt juhtida käesoleva direktiivi kohaldamisalasse kuuluvates sektorites tegutsevatel elutähtsatel ja olulistel üksustel tarneahela ja tarnijatega seotud riske, peaks koostöörühm tegema koostöös komisjoni ja ENISAga ning asjakohasel juhul pärast asjakohaste sidusrühmadega, sealhulgas tööstusega konsulteerimist koordineeritud kriitilise tähtsusega tarneahelate turberiski hindamise (nagu tehti 5G-võrkude kohta vastavalt soovitusele (EL) 2019/534 ([19]) (5G-võrkude küberturvalisuse kohta)), eesmärgiga määrata iga sektori jaoks kindlaks kriitilise tähtsusega IKT-teenused, IKT-süsteemid või IKT-tooted, asjaomased ohud ja nõrkused. Sellise turberiski koordineeritud hindamise käigus tuleks kindlaks teha meetmed, leevenduskavad ja parimad tavad, millega võidelda kriitilise tähtsusega sõltuvuse vastu, potentsiaalsete nõrkade lülide, ohtude, nõrkuste ja muude riskide vastu, mis on seotud tarneahelaga, ning uurida, kuidas saaks elutähtsaid ja olulisi üksusi julgustada neid ulatuslikumalt kasutusele võtma. Võimalikud muud kui tehnilised riskitegurid, nagu kolmanda riigi lubamatu mõju tarnijatele ja teenuseosutajatele, eelkõige alternatiivsete juhtimismudelite puhul, hõlmavad varjatud nõrkusi või tagauksi ja võimalikke süsteemseid tarnehäireid, eriti tehnoloogilise kinnistumise või teenuseosutajast sõltuvuse korral.

(91) Kriitilise tähtsusega tarneahela turberiskide koordineeritud hindamisel tuleks asjaomase sektori omadusi silmas pidades võtta arvesse nii tehnilisi kui ka asjakohasel juhul muid kui tehnilisi tegureid, sealhulgas neid, mis on kindlaks määratud 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 turberiski koordineeritud hindamist, tuleks arvesse võtta järgmisi kriteeriume: i) kui suurel määral elutähtsad ja olulised üksused kindlaid kriitilise tähtsusega IKT-teenuseid, IKT-süsteeme või IKT-tooteid kasutavad ning nendele tuginevad; ii) kindlate kriitilise tähtsusega IKT-teenuste, IKT-süsteemide või IKT-toodete asjakohasus kriitilise tähtsusega või tundlike funktsioonide (sealhulgas isikuandmete töötlemine) täitmisel; iii) alternatiivsete IKT-teenuste, IKT-süsteemide või IKT-toodete kättesaadavus; iv) IKT-teenuste, IKT-süsteemide või IKT-toodete tarneahela kui terviku vastupidavusvõime kogu nende olelusringi jooksul häirivate sündmuste korral või v) kui tegemist on kujunemisjärgus IKT-teenuste, IKT-süsteemide või IKT-toodetega, siis nende potentsiaalne tulevane tähtsus üksuste tegevuse jaoks. Lisaks tuleks erilist tähelepanu pöörata IKT-teenustele, IKT-süsteemidele või IKT-toodetele, mille suhtes kehtivad kolmandatest riikidest tingitud erinõuded.

(92) Et ühtlustada üldkasutatavate elektroonilise side võrkude või üldkasutatavate elektroonilise side teenuste pakkujatele ja usaldusteenuse osutajatele pandud võrgu- ja infosüsteemide turvalisusega seotud kohustused ning võimaldada kõnealustel üksustel ja Euroopa Parlamendi ja nõukogu direktiivi (EL) 2018/1972 ([20]) ja määruse (EL) nr 910/2014 kohastel pädevatel asutustel saada kasu käesoleva direktiiviga kehtestatud õigusraamistikust, sealhulgas riskide ja intsidentidega seotud tegevuste eest vastutava CSIRTi määramine, pädevate asutuste ja organite osalemine koostöörühma tegevuses ja CSIRTide võrgustikus, peaksid need üksused kuuluma käesoleva direktiivi kohaldamisalasse. Seega tuleks määruse (EL) nr 910/2014 ning direktiivi (EL) 2018/1972 sätted, mis on seotud turva- ja teatamisnõude kehtestamisega kõnealust liiki üksuste suhtes, välja jätta. Käesolevas direktiivis sätestatud teatamiskohustuse reeglid ei tohiks piirata määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ kohaldamist.

(93) Käesolevas direktiivis sätestatud küberturvalisuse kohustusi tuleks käsitada täiendusena nõuetele, mis on kehtestatud usaldusteenuse osutajatele määrusega (EL) nr 910/2014. Usaldusteenuse osutajatelt tuleks nõuda, et nad võtaksid kõik asjakohased ja proportsionaalsed meetmed, et juhtida oma teenuseid ohustavaid riske, sealhulgas seoses klientide ja teenustest sõltuvate kolmandate isikutega, ning teataksid käesoleva direktiivi kohaselt intsidentidest. Sellised küberturvalisuse kohustused ja teatamiskohustus peaksid hõlmama osutatavate teenuste füüsilist kaitset. Määruse (EL) nr 910/2014 artiklis 24 kvalifitseeritud usaldusteenuse osutajate suhtes sätestatud nõudeid kohaldatakse ka edaspidi.

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

([20]) 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).

(94) Liikmesriigid võivad määrata usaldusteenuste eest vastutavaks pädevaks asutuseks määruse (EL) nr 910/2014 kohase järelevalveasutuse, et tagada praeguste tavade jätkumine ning kasutada nimetatud määruse kohaldamisel saadud teadmisi ja kogemusi. Sellisel juhul peaksid käesoleva direktiivi kohased pädevad asutused tegema tihedalt ja aegsasti koostööd kõnealuste järelevalveasutustega, vahetades asjakohast teavet, et tagada tulemuslik järelevalve ja see, et usaldusteenuse osutajad täidavad käesolevas direktiivis ja määruses (EL) nr 910/2014 sätestatud nõudeid. Kui see on kohaldatav, peaks CSIRT või käesoleva direktiivi kohane pädev asutus viivitamata teavitama määruse (EL) nr 910/2014 kohast järelevalveasutust igast teatatud olulisest küberohust või intsidendist, mis mõjutab usaldusteenuseid, ning igast käesoleva direktiivi rikkumisest usaldusteenuse osutaja poolt. Liikmesriigid võivad, kui see on kohaldatav, kasutada teatamiseks ühtset kontaktpunkti, mis on loodud selleks, et tagada ühtne ja automaatne intsidentidest teatamine nii määruse (EL) nr 910/2014 kohasele järelevalveasutusele kui ka käesoleva direktiivi kohasele CSIRTile või pädevale asutusele.

(95) Kui see on asjakohane ja et vältida tarbetuid häireid, tuleks käesoleva direktiivi ülevõtmisel arvesse võtta olemasolevaid riiklikke suuniseid, mis on võetud vastu direktiivi (EL) 2018/1972 artiklites 40 ja 41 sätestatud turvameetmetega seotud normide ülevõtmiseks, tuginedes seega teadmistele ja oskustele, mis on direktiivi (EL) 2018/1972 alusel seoses turvameetmete ja intsidenditeadetega juba omandatud. ENISA võib koostada üldkasutatavate elektroonilise side võrkude pakkujate või üldkasutatavate elektrooniliste side teenuste osutajate jaoks ka turvanõudeid ja teatamiskohustust käsitlevad suunised, et hõlbustada ühtlustamist ja üleminekut ning minimeerida häireid. Liikmesriigid võivad anda elektroonilise side eest vastutava pädeva asutuse rolli direktiivi (EL) 2018/1972 kohastele riigi reguleerivatele asutustele, et tagada praeguste tavade jätkumine ning kasutada nimetatud direktiivi rakendamisel saadud teadmisi ja kogemusi.

(96) Võttes arvesse, et direktiivis (EL) 2018/1972 määratletud numbrivaba isikutevahelise side teenuste olulisus kasvab, tuleb tagada, et ka nende teenuste kohta kehtiksid asjakohased, nende eripära ja majanduslikku tähtsust arvestavad turvanõuded. Ründepinna üha laienedes muutuvad levinud sihtmärkideks numbrivaba isikutevahelise side teenused, näiteks sõnumiteenused. Kurjategijad kasutavad platvorme suhtlemiseks ja selleks, et meelitada ohvreid avama nakatatud veebisaite, suurendades seeläbi isikuandmete ärakasutamise ja laiemalt ka infosüsteemide turvalisusega seotud intsidentide esinemise tõenäosust. Numbrivaba isikutevahelise side teenuste pakkujad peaksid tagama riskitasemele vastava võrgu- ja infosüsteemide turvalisuse taseme. Arvestades, et numbrivaba isikutevahelise side teenuste osutajatel puudub tavaliselt tegelik kontroll võrkudes signaalide edastamise üle, võib selliste teenustega seotud riske pidada mõnes mõttes väiksemaks kui riske, mis esinevad tavapäraste elektroonilise side teenuste puhul. Sama kehtib ka selliste direktiivis (EL) 2018/1972 määratletud isikutevahelise side teenuste kohta, mille puhul kasutatakse numbreid ja millel puudub tegelikult kontroll signaaliedastuse üle.

(97) 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 kõikidel üldkasutatavate elektroonilise side võrkude pakkujatel oleksid asjakohased küberturvalisuse riskijuhtimismeetmed ja et nendega seotud olulistest intsidentidest teatataks. Liikmesriigid peaksid tagama üldkasutatavate elektroonilise side võrkude turvalisuse säilimise ning oma eluliste julgeolekuhuvide kaitse sabotaaži ja spionaaži eest. Kuna rahvusvaheline ühenduvus edendab ja kiirendab liidu ja selle majanduse konkurentsipõhist digitaliseerimist, tuleks merealuseid sidekaableid mõjutavatest intsidentidest teavitada CSIRTi või, kui see on kohaldatav, pädevat asutust. Kui see on asjakohane, tuleks merealuste sidekaablite küberturvalisust riiklikus küberturvalisuse strateegias arvesse võtta ning see peaks hõlmama võimalike küberturvalisuse riskide kaardistamist ja leevendusmeetmeid, et tagada nende kaitse kõrgeimal tasemel.

(98) Üldkasutatavate elektroonilise side võrkude ja üldkasutatavate elektroonilise side teenuste turvalisuse tagamiseks tuleks edendada krüpteerimistehnoloogiate kasutamist, eelkõige otspunktkrüpteerimist ja andmekeskseid turbekontseptsioone, nagu kartograafia, segmenteerimine, märgistamine, juurdepääsupoliitika ja juurdepääsu haldamine ning automatiseeritud juurdepääsu otsused. Vajaduse korral peaks üldkasutatavate elektroonilise side võrkude pakkujatele või üldkasutatavate elektroonilise side teenuste osutajatele olema käesoleva direktiivi kohaldamisel kohustuslik kasutada krüpteerimist, eelkõige otspunktkrüpteerimist, 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 ennetamist, uurimist, avastamist ja nende eest vastutusele võtmist kooskõlas liidu õigusega. Sellega ei tohiks aga kaasneda otspunktkrüpteerimise nõrgestamine, kuna see on tõhusa andmekaitse, privaatsuse ja side turvalisuse jaoks olulise tähtsusega tehnoloogia.

(99) Üldkasutatavate elektroonilise side võrkude ja üldkasutatavate elektroonilise side teenuste turvalisuse tagamiseks ning nende kuritarvitamise ja manipuleerimise vältimiseks tuleks edendada koostalitlusvõimeliste turvaliste marsruutimisstandardite kasutamist, et tagada marsruutimisfunktsioonide terviklus ja töökindlus kogu internetiühenduse teenuse osutajate ökosüsteemis.

(100) Et kaitsta interneti funktsionaalsust ja terviklust ning edendada domeeninimede süsteemi turvalisust ja vastupanuvõimet, tuleks asjaomaseid sidusrühmi, sealhulgas liidu erasektori üksusi, üldkasutatavate elektroonilise side teenuste osutajaid, eelkõige internetiühenduse teenuse osutajaid, ja internetipõhise otsingumootori teenuse osutajaid, innustada võtma vastu domeeninimede süsteemi teisendamise mitmekesistamise strateegia. Ühtlasi peaksid liikmesriigid innustama avaliku ja turvalise Euroopa domeeninimede süsteemi teisendamise teenuse väljatöötamist ja kasutamist.

(101) Käesolevas direktiivis sätestatakse olulistest intsidentidest teatamisele mitmeetapiline lähenemisviis, et saavutada õige tasakaal kahe ülesande vahel: ühelt poolt kiire teatamine, mis aitab vähendada oluliste intsidentide võimalikku levikut ja võimaldab elutähtsatel ja olulistel 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. Sellega seoses peaks käesolev direktiiv hõlmama teatamist sellistest intsidentidest, mis asjaomase üksuse esialgse hinnangu kohaselt võivad põhjustada asjaomase üksuse teenustele tõsiseid tegevushäireid või kõnealusele üksusele rahalist kahju või mõjutada teisi füüsilisi või juriidilisi isikuid, põhjustades märkimisväärset varalist või mittevaralist kahju. Esialgses hinnangus tuleks muu hulgas arvesse võtta mõjutatud võrgu- ja infosüsteeme ning eelkõige nende tähtsust üksuse teenuste osutamisel, küberohu tõsidust ja tehnilisi omadusi ning kõiki ärakasutamist võimaldavaid nõrkusi, samuti üksuse kogemusi sarnaste intsidentidega. Sellised näitajad nagu teenuse toimimise mõjutamise ulatus, intsidendi kestus või mõjutatud teenusekasutajate arv võivad mängida olulist rolli selle kindlakstegemisel, kas teenuse tegevushäire on tõsine.

(102) Elutähtsatelt ja olulistelt üksustelt, kes saavad olulisest intsidendist teadlikuks, tuleks nõuda, et nad esitaksid varajase hoiatuse põhjendamatu viivituseta ja igal juhul 24 tunni jooksul. Sellele varajasele hoiatusele peaks järgnema intsidenditeade. Asjaomased üksused peaksid esitama intsidenditeate põhjendamatu viivituseta ja igal juhul 72 tunni jooksul pärast olulisest intsidendist teadlikuks saamist, et eelkõige ajakohastada varajase hoiatuse kaudu esitatud teavet ning anda esialgne hinnang olulisele intsidendile, muu hulgas selle tõsidusele ja mõjule ning, kui need on kättesaadavad, ka turvarikke indikaatoritele. Lõpparuanne tuleks esitada ühe kuu jooksul pärast intsidenditeadet. Varajane hoiatus peaks sisaldama üksnes teavet, mis on vajalik CSIRTi või, kui see on kohaldatav, pädeva asutuse olulisest intsidendist teavitamiseks ja võimaldama asjaomasel üksusel vajaduse korral abi otsida. Selline varajane hoiatus, kui see on kohaldatav, peaks näitama, kas on kahtlus, et olulise intsidendi põhjuseks on ebaseaduslik või pahatahtlik tegevus, ning kas sellel on tõenäoliselt piiriülene mõju. Liikmesriigid peaksid tagama, et kohustus

esitada kõnealune varajane hoiatus või sellele järgnev intsidenditeade ei suuna teavitava üksuse ressursse kõrvale intsidentide käsitlemisega seotud tegevusest, mis tuleks prioriseerida, et vältida olukorda, kus intsidentidest teatamise kohustus kas suunab vahendeid oluliste intsidentide lahendamiselt kõrvale või kahjustab muul viisil üksuse sellealaseid pingutusi. Kui intsident jätkub lõpparuande esitamise ajal, peaksid liikmesriigid tagama, et asjaomased üksused esitavad sel ajal vahearuande ja ühe kuu jooksul pärast olulise intsidendi nendepoolset käsitlemist lõpparuande.

(103) Kui see on kohaldatav, peaksid elutähtsad ja olulised üksused teavitama oma teenuste kasutajaid viivitamata meetmetest või parandusmeetmetest, mida nad saavad olulisest küberohust tulenevate riskide vähendamiseks võtta. Kui see on kohane ja eelkõige juhul, kui oluline küberoht tõenäoliselt realiseerub, peaksid kõnealused üksused teavitama ohust ka oma teenuste kasutajaid. Nõue teavitada teenuste kasutajaid olulistest küberohtudest tuleks täita nii hästi kui võimalik, kuid see ei vabasta kõnealuseid üksusi kohustusest võtta oma kulul viivitamata sobivaid meetmeid, et selliseid võimalikke ohte ennetada või need kõrvaldada ning taastada teenuse turvalisuse tavapärane tase. Selline teave oluliste küberohtude kohta tuleks edastada kasutajatele tasuta ja selle sõnastus peaks olema kergesti mõistetav.

(104) Üldkasutatavate elektroonilise side võrkude pakkujad või üldkasutatavate elektroonilise side teenuste osutajad peaksid rakendama sisseprojekteeritud ja vaiketurvet ning teavitama teenuse kasutajaid olulistest küberohtudest ning meetmetest, mida viimased saavad oma seadmete ja side turvalisuse kaitseks võtta, kasutades näiteks teatavat liiki tarkvara või krüpteerimistehnoloogiaid.

(105) Küberohte ennetav lähenemisviis on küberturvalisuse riskijuhtimise oluline osa, mis peaks võimaldama pädevatel asutustel tulemuslikult vältida küberohtude muutumist intsidentideks, mis võivad põhjustada märkimisväärset varalist või mittevaralist kahju. Seetõttu on küberohtudest teatamine esmatähtis. Seepärast julgustatakse üksusi küberohtudest vabatahtlikult teatama.

(106) Käesoleva direktiivi alusel nõutava teabe esitamise lihtsustamiseks ja üksuste halduskoormuse vähendamiseks peaksid liikmesriigid asjakohase teabe esitamiseks ette nägema tehnilised vahendid, nagu ühtne kontaktpunkt, automatiseeritud süsteemid, veebipõhised vormid, kasutajasõbralikud liidesed, teatevormid, spetsiaalsed platvormid, mida üksused saavad kasutada, olenemata sellest, kas nad kuuluvad käesoleva direktiivi kohaldamisalasse. Käesoleva direktiivi rakendamist toetavad liidu rahalised vahendid, eelkõige Euroopa Parlamendi ja nõukogu määrusega (EL) 2021/694 ([21]) loodud programmi „Digitaalne Euroopa“ raames, võiksid hõlmata toetust ühtsetele kontaktpunktidele. Üksused on sageli ka olukorras, kus konkreetsest intsidendist tuleb eri õigusaktides sätestatud teatamiskohustuse tõttu teavitada eri asutusi. Sellised olukorrad tekitavad lisakoormust ning võivad põhjustada kõnealuste teadete vormi ja menetluskorraga seoses ebakindlust. Kui luuakse ühtne kontaktpunkt, julgustatakse liikmesriike kasutama seda ühtset kontaktpunkti ka selleks, et teatada turvaintsidentidest, millest teatamist nõutakse muude liidu õigusaktide, näiteks määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ kohaselt. Sellise ühtse kontaktpunkti kasutamine turvaintsidentidest teatamiseks määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ alusel ei tohiks mõjutada määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ sätete, eelkõige nendes osutatud asutuste sõltumatust käsitlevate sätete kohaldamist. ENISA peaks koostöös koostöörühmaga töötama suunistes välja ühised teatevormid, et lihtsustada ja ühtlustada liidu õiguse alusel teabe esitamist ning vähendada teavitavate üksuste halduskoormust.

(107) Liikmesriigid peaksid liidu õigusega kooskõlas olevatest kriminaalmenetlusnormidest 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. Kui see on asjakohane, võiksid küberkuritegevuse vastase võitluse Euroopa keskus (EC3) ja ENISA hõlbustada eri liikmesriikide pädevate asutuste ja õiguskaitseasutuste vahelise koostöö koordineerimist, ilma et see mõjutaks Europoli suhtes kohaldatavaid isikuandmete kaitse reegleid.

([21]) Euroopa Parlamendi ja nõukogu 29. aprilli 2021. aasta määrus (EL) 2021/694, millega luuakse programm „Digitaalne Euroopa“ ja tunnistatakse kehtetuks otsus (EL) 2015/2240 (ELT L 166, 11.5.2021, lk 1).

(108) Intsidentidega kaasneb sageli isikuandmete kuritarvitamine. Sellega seoses peaksid pädevad asutused kõigis asjakohastes küsimustes tegema koostööd ning vahetama teavet asutustega, millele on osutatud määruses (EL) 2016/679 ja direktiivis 2002/58/EÜ.

(109) Domeeninimede registreerimisandmete (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 liidus saavutada küberturvalisuse ühtlaselt kõrge taseme. Selleks tuleks tippdomeeninimede registritelt ja domeeninimede registreerimise teenuseid osutavatelt üksustelt nõuda, et nad töötleksid teatavaid selle eesmärgi saavutamiseks vajalikke andmeid. Selline töötlemine peaks kujutama endast juriidilist kohustust määruse (EL) 2016/679 artikli 6 lõike 1 punkti c tähenduses. Nimetatud kohustus ei piira võimalust koguda domeeninimede registreerimise andmeid muudel eesmärkidel, näiteks lepingute või muude liidu või riigisiseste õigusaktidega kehtestatud õiguslike nõuete alusel. Selle kohustuse eesmärk on saavutada täielik ja täpne registreerimisandmete kogum ning see ei tohiks kaasa tuua samade andmete mitmekordset kogumist. Tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused peaksid tegema koostööd, et vältida selle ülesande dubleerimist.

(110) Domeeninimede registreerimise andmete kättesaadavus ja andmetele õigeaegse juurdepääsu võimaldamine õigustatud taotlejatele on domeeninimede süsteemi kuritarvitamise ennetamiseks ja selle vastu võitlemiseks ning intsidentide ennetamiseks, avastamiseks ja neile reageerimiseks väga oluline. Õigustatud taotlejate all mõeldakse füüsilist või juriidilist isikut, kes esitab taotluse liidu või liikmesriigi õiguse kohaselt. Nende hulka võivad kuuluda asutused, kes on pädevad käesoleva direktiivi alusel, ning asutused, kes on liidu või liikmesriigi õiguse kohaselt pädevad kuritegude ennetamise, uurimise, avastamise ja nende eest vastutusele võtmise valdkonnas, ning CERTid või CSIRTid. Tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused peaksid kooskõlas liidu ja liikmesriigi õigusega olema kohustatud võimaldama õigustatud taotlejatele õiguspärast juurdepääsu konkreetsetele domeeninimede registreerimise andmetele, mis on juurdepääsutaotluse jaoks vajalikud. Õigustatud taotlejate taotlusele tuleks lisada põhjendused, mis võimaldavad hinnata andmetele juurdepääsu vajalikkust.

(111) Et tagada domeeninimede registreerimise täpsete ja täielike andmete kättesaadavus, peaksid tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused koguma domeeninimede registreerimise andmeid ning tagama nende tervikluse ja kättesaadavuse. Eelkõige peaksid tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused kehtestama põhimõtted ja menetluskorra täpsete ja täielike domeeninimede registreerimisandmete kogumiseks ja säilitamiseks ning ebatäpsete registreerimisandmete vältimiseks ja parandamiseks kooskõlas liidu andmekaitseõigusega. Nendes põhimõtetes ja menetlustes tuleks võimalikult suures ulatuses arvesse võtta standardeid, mille on rahvusvahelisel tasandil välja töötanud mitut sidusrühma hõlmavad juhtimisstruktuurid. Tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused peaksid võtma vastu ja rakendama domeeninimede registreerimise andmete kontrollimiseks proportsionaalseid menetlusi. Need menetlused peaksid kajastama tööstusharus kasutatavaid parimaid tavasid ja nii palju kui võimalik ka e-identimise valdkonnas tehtud edusamme. Kontrollimenetlused võivad hõlmata näiteks registreerimise ajal tehtud eelkontrolle ja pärast registreerimist tehtud järelkontrolle. Tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused peaksid eelkõige kontrollima vähemalt üht registreerijaga kontakti võtmise võimalust.

(112) Tippdomeeninimede registritelt ja domeeninimede registreerimise teenuseid osutavatelt üksustelt tuleks nõuda, et nad teeksid üldsusele kättesaadavaks liidu andmekaitseõiguse kohaldamisalast välja jäävad domeeninimede registreerimise andmed, näiteks juriidiliste isikutega seotud andmed, kooskõlas määruse (EL) 2016/679 preambulis sätestatuga. Juriidiliste isikute puhul peaksid tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused tegema üldsusele kättesaadavaks vähemalt registreerija nime ja kontakttelefoni numbri. Samuti tuleks avaldada e-posti kontaktaadress, kui see ei sisalda isikuandmeid, näiteks e-posti varjunimi või ametikohajärgne konto. Tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused peaksid kooskõlas liidu andmekaitseõigusega võimaldama õigustatud taotlejatele õiguspärast juurdepääsu ka füüsiliste isikutega seotud domeeninimede registreerimise andmetele. Liikmesriigid peaksid nõudma, et tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused vastaksid põhjendamatu viivituseta õigustatud taotlejate domeeninimede registreerimisandmete avalikustamise taotlustele. Tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused peaksid kehtestama põhimõtted ja korra registreerimisandmete avaldamiseks ja avalikustamiseks, sealhulgas teenustaseme kokkulepped õigustatud taotlejate juurdepääsutaotluste käsitlemiseks. Nendes põhimõtetes ja selles korras tuleks võimalikult suures ulatuses arvesse võtta suuniseid ja standardeid, mille on rahvusvahelisel tasandil välja töötanud mitut

sidusrühma hõlmavad juhtimisstruktuurid. Juurdepääsumenetlus võib hõlmata ka liidese, portaali või muude tehniliste vahendite kasutamist, mis aitab tagada tõhusa süsteemi registreerimisandmete taotlemiseks ja nendele juurdepääsu saamiseks. Selleks et edendada ühtlustatud tavasid kogu siseturul, võib komisjon, ilma et see piiraks Euroopa Andmekaitsenõukogu pädevust, esitada selliste menetluste kohta suunised, milles võetakse võimalikult suures ulatuses arvesse standardeid, mille on välja töötanud mitmeid sidusrühmi hõlmavad rahvusvahelise tasandi juhtimisstruktuurid. Liikmesriigid peaksid tagama, et igasugune juurdepääs nii isiku- kui ka isikustamata domeeninimede registreerimise andmetele on tasuta.

(113) Käesoleva direktiivi kohaldamisalasse kuuluvad üksused tuleks lugeda selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on nende peamine tegevuskoht. Üldkasutatavate elektroonilise side võrkude pakkujad või üldkasutatavate elektroonilise side teenuste pakkujad tuleks siiski lugeda selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus nad oma teenuseid osutavad. Domeeninimede süsteemi teenuse osutajad, tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused, pilvandmetöötlusteenuse osutajad, andmekeskusteenuse osutajad, sisulevivõrgu pakkujad, hallatud teenuse osutajad ja turbetarnijad ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite ja sotsiaalvõrguteenuse platvormide pakkujad tuleks lugeda selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on nende peamine tegevuskoht liidus. Avaliku halduse üksused peaksid kuuluma selle liikmesriigi jurisdiktsiooni alla, kes nad asutas. Kui üksus osutab teenuseid või asub 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, kui see on kohane, võtma ühiseid järelevalvemeetmeid. Kui liikmesriigid teostavad jurisdiktsiooni, ei tohiks nad kooskõlas *ne bis in idem* põhimõttega kohaldada sama teo eest täitemeetmeid või määrata karistust rohkem kui üks kord.

(114) Kuna domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, domeeninimede registreerimise teenuseid osutavate üksuste, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate, hallatud teenuse osutajate ja turbetarnijate ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite ja sotsiaalvõrguteenuse platvormide pakkujate teenused ja tegevus on piiriülese iseloomuga, peaksid need üksused kuuluma vaid ühe liikmesriigi jurisdiktsiooni alla. Üksus peaks kuuluma selle liikmesriigi jurisdiktsiooni alla, kus on tema peamine tegevuskoht liidus. Käesoleva direktiivi tähenduses eeldatakse tegevuskoha-kriteeriumi puhul püsivalt korraldatud tegelikult toimuvat tegevust. Sellise korralduse õiguslik vorm (filiaal või juriidilisest isikust tütarettevõtja) ei ole antud juhul määrav tegur. Selle kriteeriumi täitmine ei tohiks sõltuda võrgu- ja infosüsteemide füüsilisest paiknemisest teatavas kohas; selliste süsteemide olemasolu ja kasutamine ei näita iseenesest peamist tegevuskohta ning seega ei ole need peamise tegevuskoha kindlakstegemisel otsustavad kriteeriumid. Peamise tegevuskohana tuleks käsitada liikmesriiki, kus liidus tehakse valdav osa otsustest küberturvalisuse riskijuhtimismeetmete kohta. Tavaliselt on see liidu asukoht, kus asub üksuse peakontor. Kui sellist liikmesriiki ei ole võimalik kindlaks määrata või kui selliseid otsuseid ei tehta liidus, tuleks peamise tegevuskohana käsitada liikmesriiki, kus toimub küberturvalisuse alane tegevus. Kui sellist liikmesriiki ei ole võimalik kindlaks määrata, 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.

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

(116) Kui domeeninimede süsteemi teenuse osutaja, tippdomeeninimede register, domeeninimede registreerimise teenuseid osutav üksus, pilvandmetöötlusteenuse osutaja, andmekeskusteenuse osutaja, sisulevivõrgu pakkuja, hallatud teenuse osutaja või turbetarnija või internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite või sotsiaalvõrguteenuse platvormi pakkuja, kes ei ole asutatud liidus, osutab teenuseid liidus, peaks ta määrama endale liidus esindaja. Otsustamaks, kas kõnealune üksus pakub teenuseid liidu piires, tuleks kindlaks teha, kas üksus kavatseb osutada teenuseid ühes või mitmes liikmesriigis asuvatele isikutele. Seda, et liidus pääseb juurde üksuse või vahendaja veebisaidile, e-posti aadressile või muudele kontaktandmetele, või seda, et kasutatakse keelt, mida kasutatakse üldiselt kolmandas riigis, kus üksus on asutatud, tuleks pidada sellise kavatsuse kindlakstegemiseks ebapiisavaks. Samal ajal võivad asjaolud, nagu ühes või mitmes liikmesriigis üldiselt kasutatava keele või vääringu kasutamine, millega kaasneb võimalus tellida teenuseid selles 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 CSIRTil peaks olema võimalik esindajaga ühendust võtta. Esindaja tuleks määrata sõnaselgelt üksuse kirjaliku volitusega täitma käesolevas direktiivis sätestatud kohustusi, sealhulgas intsidentidest teatamise kohustust.

(117) Selleks et tagada selge ülevaade domeeninimede süsteemi teenuse osutajatest, tippdomeeninimede registritest ja domeeninimede registreerimise teenuseid osutavatest üksustest, pilvandmetöötlusteenuse osutajatest, andmekeskusteenuse osutajatest, sisulevivõrgu pakkujatest, hallatud teenuse osutajatest ja turbetarnijatest ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite ja sotsiaalvõrguteenuse platvormi pakkujatest, kes osutavad kogu liidus teenuseid, mille suhtes kohaldatakse käesolevat direktiivi, peaks ENISA looma ja haldama selliste üksuste registrit, tuginedes liikmesriikidelt saadud teabele, mida saadakse, kui see on kohaldatav, riiklike mehhanismide kaudu, mis on loodud, et üksused saaksid end registreerida. Ühtsed kontaktpunktid peaksid edastama ENISA-le teabe ja kõik selle muudatused. Tagamaks, et kõnealusesse registrisse kantav teave on täpne ja täielik, võivad liikmesriigid esitada ENISA-le oma riiklikes registrites kõnealuste üksuste kohta olemasoleva teabe. ENISA ja liikmesriigid peaksid võtma meetmeid, et hõlbustada selliste registrite koostalitlusvõimet, tagades samal ajal konfidentsiaalse või salastatud teabe kaitse. ENISA peaks kehtestama asjakohased teabe klassifitseerimise ja haldamise protokollid, et tagada avalikustatud teabe turvalisus ja konfidentsiaalsus ning piirata juurdepääs sellisele teabele ning selle talletamine ja edastamine sihtkasutajatega.

(118) Kui käesoleva direktiivi alusel vahetatakse või edastatakse või jagatakse muul moel teavet, mida käsitatakse kooskõlas liikmesriigi või liidu õigusega salastatud teabena, tuleks järgida asjaomaseid salastatud teabe käitlemise erireegleid. Ühtlasi peaksid ENISA-l olema taristu, kord ja reeglid, mille abil käsitleda tundlikku ja salastatud teavet kooskõlas ELi salastatud teabe kaitseks kohaldatavate turvareeglitega.

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

(120) Liikmesriigid peaksid üksusi julgustama ja abistama, et nad kasutaksid kollektiivselt individuaalseid teadmisi ja praktilisi kogemusi strateegilisel, taktikalisel ja operatiivtasandil, et suurendada oma võimekust küberohte õigesti ennetada, avastada, neile reageerida, nendest taastuda ja nende mõju leevendada. Seega on vaja võimaldada sõlmida liidu tasandil vabatahtlikud küberturvalisuse alase teabevahetuse kokkulepped. Selleks peaksid liikmesriigid aktiivselt abistama ja julgustama üksusi, näiteks küberturvalisuse teenuseid ja teadusuuringuid pakkuvaid üksusi, ning käesoleva direktiivi kohaldamisalast välja jäävaid asjaomaseid üksusi sellistes küberturvalisuse alase teabevahetuse kokkulepetes osalema. Sellised kokkulepped tuleks sõlmida kooskõlas liidu konkurentsinormide ja liidu andmekaitseõigusega.

(121) Isikuandmete töötlemist sellises ulatuses, mis on vajalik ja proportsionaalne võrgu- ja infosüsteemide turvalisuse tagamiseks elutähtsates ja olulistes üksustes, võib pidada seaduslikuks selle alusel, et selline töötlemine on vajalik vastutava töötleja seadusjärgse kohustuse täitmiseks kooskõlas määruse (EL) 2016/679 artikli 6 lõike 1 punkti c ja artikli 6 lõike 3 nõuetega. Isikuandmete töötlemine võib olla vajalik ka elutähtsate ja oluliste üksuste ning nende üksuste nimel tegutsevate turvatehnoloogiate ja -teenuste pakkujate õigustatud huvides vastavalt määruse (EL) 2016/679 artikli 6 lõike 1 punktile f, sealhulgas juhul, kui selline töötlemine on vajalik küberturvalisuse alase teabevahetuse kokkulepete puhul või asjakohase teabe vabatahtlikuks esitamiseks kooskõlas käesoleva direktiiviga. Selliste meetmete võtmiseks, mis on seotud intsidentide ennetamise, avastamise, tuvastamise, ohjamise, analüüsimise ja lahendamisega, samuti niisuguste meetmete võtmiseks, millega suurendatakse teadlikkust konkreetsetest küberohtudest, võimaldatakse teabevahetust nõrkuste vähendamise ja nõrkuste koordineeritud avalikustamise kontekstis, samuti vabatahtlikku teabevahetust seoses kõnealuste intsidentide, küberohtude ja nõrkuste, rikkeindikaatorite, taktika, meetodite ja menetluskorra, küberturvalisuse hoiatussüsteemide ja konfiguratsioonivahenditega, võib olla vaja töödelda teatavat liiki isikuandmeid, nagu IP-aadresse, internetiaadresse (URLe), domeeninimesid, meiliaadresse, ja kui neis avalduvad isikuandmed, ajatempleid. Isikuandmete töötlemine pädevate asutuste, ühtsete kontaktpunktide ja CSIRTide poolt võib olla juriidiline kohustus või seda võib pidada vajalikuks avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks vastavalt määruse (EL) 2016/679 artikli 6 lõike 1 punktile c või e ja artikli 6 lõikele 3 või elutähtsate ja oluliste üksuste õigustatud huvi korral, nagu on osutatud kõnealuse määruse artikli 6 lõike 1 punktis f. Lisaks võiks riigisiseses õiguses sätestada reeglid, mis võimaldavad pädevatel asutustel, ühtsetel kontaktpunktidel ja CSIRTidel sellises ulatuses, mis on vajalik ja proportsionaalne elutähtsate ja oluliste üksuste võrgu- ja infosüsteemide turvalisuse tagamiseks, töödelda isikuandmete eriliike kooskõlas määruse (EL) 2016/679 artikliga 9, eelkõige nähes ette sobivad ja konkreetsed meetmed füüsiliste isikute põhiõiguste ja huvide kaitsmiseks, sealhulgas tehnilised piirangud selliste andmete taaskasutamisele ning turva- ja eraelu puutumatuse säilitamise tipptasemel meetmete kasutamine, nagu pseudonüümimine või krüpteerimine, kui anonüümimine võib taotletavat eesmärki oluliselt mõjutada.

(122) Et tugevdada järelevalvevolitusi ja -meetmeid, mis aitavad tagada nõuete tõhusat täitmist, tuleks käesoleva direktiiviga ette näha minimaalsed järelevalvemeetmed ja -vahendid, mille abil pädevad asutused saavad teha elutähtsate ja oluliste üksuste üle järelevalvet. Lisaks tuleks käesoleva direktiiviga kehtestada eraldi järelevalvekord elutähtsate ja oluliste üksuste jaoks, et tagada kõnealuste üksuste ja pädevate asutuste kohustuste vahel õiglane tasakaal. Seetõttu tuleks elutähtsate üksuste suhtes kohaldada põhjalikku eel- ja järelkontrolliga järelevalvekorda, samal ajal kui oluliste üksuste suhtes tuleks kohaldada lihtsustatud, üksnes järelkontrolliga järelevalvekorda. Olulistelt üksustelt ei peaks seega nõudma, et nad dokumenteeriksid süstemaatiliselt 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, vihjetest või teabest, millele on juhitud pädevate asutuste tähelepanu ja mille puhul pädevad asutused leiavad, et need viitavad käesoleva direktiivi võimalikele rikkumistele. 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.

(123) Järelevalveülesannete täitmine pädevate asutuste poolt ei tohiks asjaomase üksuse äritegevust tarbetult takistada. Kui pädevad asutused täidavad elutähtsate üksustega seotud järelevalveülesandeid, näiteks teevad kohapealseid kontrolle ja kaugjärelevalvet, uurivad käesoleva direktiivi rikkumisi, viivad läbi turvaauditeid või turvalisuse kontrolle, peaks nende mõju asjaomase üksuse äritegevusele olema võimalikult väike.

(124) Eelkontrolli tegemisel peaks pädevatel asutustel olema võimalik otsustada, kuidas nad prioriseerivad proportsionaalselt järelevalvemeetmete ja oma käsutuses olevate vahendite kasutamist. See tähendab, et pädevad asutused võivad sellise prioriseerimise üle otsustada lähtuvalt järelevalvemeetoditest, mis peaksid põhinema riskipõhisel lähenemisviisil. 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 liigid, 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. Avaliku halduse üksuste puhul tuleks järelevalvevolitusi teostada kooskõlas riiklike õigus- ja institutsiooniliste raamistikega.

(125) Pädevad asutused peaksid tagama, et elutähtsate ja oluliste üksustega seotud järelevalveülesandeid täidavad koolitatud spetsialistid, kellel peaksid olema nende ülesannete täitmiseks vajalikud oskused, eelkõige seoses kohapealsete kontrollide ja kaugjärelevalvega, sealhulgas andmebaaside, riistvara, tulemüüride, krüpteerimise ja võrkude nõrkuste tuvastamisega. Neid kontrolle ja järelevalvet tuleks teha objektiivselt.

(126) Piisavalt põhjendatud juhtudel, kui pädev asutus on teadlik olulisest küberohust või vahetust riskist, peaks pädeval asutusel olema võimalik teha viivitamata täiteotsuseid, et intsidenti ära hoida või see lahendada.

(127) Et täitmine tõhusalt tagada, tuleks koostada käesolevas direktiivis sätestatud küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse rikkumise korral miinimumloetelu täitmise tagamise volitustest, mida võib kasutada, ning kehtestada selliste täitmise tagamise jaoks kogu liidus selge ja ühtne raamistik. Igakülgset tähelepanu tuleks pöörata käesoleva direktiivi rikkumise laadile, tõsidusele ja kestusele, põhjustatud varalisele või mittevaralisele kahjule, sellele, kas rikkumine oli tahtlik või tingitud hooletusest, varalise või mittevaralise kahju vältimiseks või leevendamiseks võetud meetmetele, vastutuse tasemele ja varasematele asjaomastele rikkumistele, pädeva asutusega tehtava koostöö tasemele ning muule raskendavale või leevendavale tegurile. Sellised täitemeetmed, sealhulgas haldustrahvid, peaksid olema proportsionaalsed ja nende määramise suhtes tuleks kooskõlas liidu õiguse üldpõhimõtete ja Euroopa Liidu põhiõiguste hartaga (edaspidi „harta“) kohaldada asjakohaseid menetluslikke kaitsemeetmeid, sealhulgas õigust tõhusale õiguskaitsevahendile ja õiglasele kohtumenetlusele, süütuse presumptsiooni ja kaitseõigust.

(128) Käesolevas direktiivis ei nõuta, et liikmesriigid näeksid ette kriminaal- või tsiviilvastutuse füüsiliste isikute suhtes, kes vastutavad selle eest, et üksused järgiksid käesolevat direktiivi, kui selle rikkumise tagajärjel on tekitatud kahju kolmandatele isikutele.

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

(130) Kui haldustrahv määratakse elutähtsale või olulisele üksusele, kes on ettevõtja, tuleks selline ettevõtja lugeda ettevõtjaks ELi toimimise lepingu artiklite 101 ja 102 tähenduses. Kui haldustrahv määratakse isikule, kes ei ole ettevõtja, peaks pädev asutus sobiva trahvisumma määramisel arvesse võtma üldist sissetulekutaset selles liikmesriigis ja isiku majanduslikku olukorda. See, kas ja mil määral tuleks kohaldada haldustrahve 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 liikmesriigi õigusnormides.

(131) Liikmesriikidel peaks olema võimalik kehtestada kriminaalkaristusi käsitlevad normid, mida kohaldatakse käesolevat direktiivi ülevõtvate liikmesriigi õigusnormide rikkumise korral. Kriminaalkaristuste määramine selliste liikmesriigi normide rikkumise korral ja seotud halduskaristuste määramine ei tohiks aga kaasa tuua *ne bis in idem* põhimõtte rikkumist, nagu seda on tõlgendanud Euroopa Liidu Kohus.

(132) Kui käesoleva direktiiviga ei ole halduskaristusi ühtlustatud või vajaduse korral muudel juhtudel, näiteks käesoleva direktiivi olulise rikkumise korral, peaksid liikmesriigid rakendama süsteemi, mis näeb ette tõhusad, proportsionaalsed ja heidutavad karistused. Selliste karistuste laad ja see, kas tegemist on kriminaal- või halduskaristusega, tuleks kindlaks määrata liikmesriigi õigusega.

(133) Et veelgi suurendada kohaldatavate täitemeetmete tõhusust ja hoiatavust käesoleva direktiivi rikkumiste korral, peaks pädevatel asutustel olema õigus ajutiselt peatada või nõuda, et ajutiselt peataks elutähtsa üksuse osutatavate mõnede või kõigi asjakohaste teenuste või pakutavate tegevuste sertifikaat või luba, ning nõuda, et füüsilisele isikule, kes täidab juhtimisülesandeid üksuse tegevjuhi või seadusliku esindaja tasandil, kehtestataks ajutine juhtimisülesannete täitmise keeld. Võttes arvesse ajutiste peatamiste ja keeldude karmust ja mõju üksuste tegevusele ning seeläbi ka nende tarbijatele, tuleks neid kohaldada alati proportsionaalselt rikkumise raskusega ning iga juhtumi konkreetseid asjaolusid silmas pidades, sealhulgas seda, kas rikkumine oli tahtlik või tulenes ettevaatamatusest, ning seda, milliseid meetmeid varalise või mittevaralise kahju vältimiseks või vähendamiseks võeti. Selliseid ajutisi peatamisi ja keelde tuleks kohaldada üksnes viimase abinõuna, nimelt alles pärast seda, kui muud käesolevas direktiivis sätestatud asjakohased täitemeetmed on ammendatud, ja ainult seni, kuni üksus, kelle suhtes neid kohaldatakse, võtab vajalikud meetmed puuduste kõrvaldamiseks või täidab pädeva asutuse need nõuded, millega seoses niisuguseid ajutisi peatamisi ja keelde kohaldati. Selliste ajutiste peatamiste või keeldude määramise suhtes peaks kohaldama kooskõlas liidu õiguse üldpõhimõtete ja hartaga asjakohaseid menetluslikke tagatisi, sealhulgas õigust tõhusale õiguskaitsevahendile ja õiglasele kohtumenetlusele, süütuse presumptsiooni ja kaitseõigust.

(134) Selleks et tagada, et üksused täidavad käesolevast direktiivis sätestatud kohustusi, peaksid liikmesriigid seoses järelevalve- ja täitemeetmetega tegema üksteisega koostööd ja üksteist abistama, eelkõige juhul, kui üksus osutab teenuseid rohkem kui ühes liikmesriigis või kui tema võrgu- ja infosüsteemid asuvad muus liikmesriigis kui see, kus ta teenuseid osutab. Abi osutamisel peaks taotluse saanud pädev asutus võtma järelevalve- või täitemeetmeid kooskõlas riigisisese õigusega. Selleks et tagada käesoleva direktiivi kohase vastastikuse abi sujuv toimimine, peaksid pädevad asutused kasutama juhtumite ja konkreetsete abitaotluste arutamise foorumina koostöörühma.

(135) Tulemusliku järelevalve ja täitmise tagamiseks, eelkõige piiriülese mõõtmega olukorras, peaks liikmesriik, kes on saanud vastastikuse abi taotluse, võtma kõnealuse taotluse piires asjakohaseid järelevalve- ja täitemeetmeid üksuse suhtes, kelle kohta taotlus tehti ja kes osutab kõnealuse liikmesriigi territooriumil teenuseid või kellel on seal võrgu- ja infosüsteem.

(136) Käesolevas direktiivis tuleks sätestada määruse (EL) 2016/679 kohaste pädevate asutuste ja järelevalveasutuste vahelise koostöö reeglid, et käsitleda käesoleva direktiivi rikkumist, mis on seotud isikuandmetega.

(137) Käesoleva direktiivi eesmärk peaks olema tagada kõrgel tasemel vastutus küberturvalisuse riskijuhtimismeetmete rakendamise ja teatamiskohustuse täitmise eest elutähtsate ja oluliste üksuste tasandil. Seepärast peaksid elutähtsate ja oluliste üksuste juhtorganid kiitma küberturvalisuse riskijuhtimismeetmed heaks ja jälgima nende rakendamist.

(138) Selleks et tagada käesoleva direktiivi alusel küberturvalisuse ühtlaselt kõrge tase kogu liidus, peaks komisjonil olema õigus võtta kooskõlas ELi toimimise lepingu artikliga 290 vastu delegeeritud õigusakte, et täiendada käesolevat direktiivi, määrates kindlaks, millistelt elutähtsate ja oluliste üksuste kategooriatelt tuleks nõuda, et nad kasutaksid teatavaid sertifitseeritud IKT-tooteid, IKT-teenuseid ja IKT-protsesse või omandaksid sertifikaadi Euroopa küberturvalisuse sertifitseerimise kava alusel. On eriti oluline, et komisjon viiks oma ettevalmistava töö käigus läbi asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil, ja et kõnealused konsultatsioonid viidaks läbi kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes [22] sätestatud põhimõtetega. Eelkõige selleks, et tagada delegeeritud õigusaktide ettevalmistamises võrdne osalemine, saavad Euroopa Parlament ja nõukogu kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel on pidev juurdepääs komisjoni eksperdirühmade koosolekutele, millel arutatakse delegeeritud õigusaktide ettevalmistamist.

[22] ELT L 123, 12.5.2016, lk 1.

(139) Et tagada käesoleva direktiivi ühetaolised rakendamistingimused, tuleks komisjonile anda rakendamisvolitused, et kehtestada koostöörühma toimimiseks vajalik menetluskord ning küberturvalisuse riskijuhtimismeetmetega seotud tehnilised, metoodilised ja valdkondlikud nõuded, ning et täpsustada täiendavalt teabe liik, intsidentidest, küber- ja intsidendiohust teatamise ning oluliste küberohtudega seotud teabevahetuse vorm ja kord ning juhtumid, mil intsidenti tuleb käsitada olulisena. Neid volitusi tuleks teostada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011 ([23]).

(140) Komisjon peaks huvitatud isikutega konsulteerides käesoleva direktiivi sätted regulaarselt läbi vaatama, eelkõige selleks, et teha kindlaks, kas on asjakohane esitada muudatusettepanekuid seoses ühiskondlike, poliitiliste, tehnoloogiliste või turutingimuste muutumisega. Kõnealuste läbivaatamiste raames peaks komisjon hindama küberturvalisusega seoses asjaomaste üksuste suuruse asjakohasust ning käesoleva direktiivi lisades osutatud üksuse sektori, allsektori ja liigi asjakohasust majanduse ja ühiskonna toimimise seisukohast. Komisjon peaks muu hulgas hindama, kas kõiki käesoleva direktiivi kohaldamisalasse kuuluvaid pakkujaid, keda käsitatakse väga suurte digiplatvormidena Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2065 ([24]) artikli 33 tähenduses, saaks käesoleva direktiivi alusel käsitada elutähtsate üksustena.

(141) Käesoleva direktiiviga luuakse ENISA-le uued ülesanded, suurendades seeläbi tema rolli, ning sellega võib kaasneda ka olukord, kus ENISA peab täitma määruse (EL) 2019/881 kohaseid seniseid ülesandeid varasemast kõrgemal tasemel. Tagamaks, et ENISA-l on vajalikud rahalised vahendid ning inimressursid oma praeguste ja uute ülesannete täitmiseks ning, et tulenevalt oma suuremast rollist täidab ta neid ülesandeid kõrgemal tasemel, tuleks tema eelarvet sellele vastavalt suurendada. Lisaks tuleks ressursside tõhusa kasutamise tagamiseks anda ENISA-le suurem paindlikkus, nii et tal oleks võimalik ressursse ametisiseselt eraldada, et täita tulemuslikult oma ülesandeid ja vastata talle seatud ootustele.

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

(143) Käesolevas direktiivis austatakse põhiõigusi ja järgitakse hartas tunnustatud põhimõtteid, eelkõige õigust eraelu ja edastatavate sõnumite puutumatusele, isikuandmete kaitsele, ettevõtlusvabadusele, omandile, tõhusale õiguskaitsevahendile ja õiglasele kohtumenetlusele, süütuse presumptsiooni ning kaitseõigust. Õigus tõhusale õiguskaitsevahendile laieneb elutähtsate ja oluliste üksuste osutatavate teenuste kasutajatele. Käesolevat direktiivi tuleks rakendada kooskõlas nimetatud õiguste ja põhimõtetega.

(144) Euroopa Andmekaitseinspektoriga konsulteeriti kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([25]) artikli 42 lõikega 1 ning ta esitas arvamuse 11. märtsil 2021 ([26]),

([23]) 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).

([24]) Euroopa Parlamendi ja nõukogu 19. oktoobri 2022. aasta määrus (EL) 2022/2065, mis käsitleb digiteenuste ühtset turgu ja millega muudetakse direktiivi 2000/31/EÜ (digiteenuste määrus) (ELT L 277, 27.10.2022, lk 1).

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

([26]) ELT C 183, 11.5.2021, lk 3.

ON VASTU VÕTNUD KÄESOLEVA DIREKTIIVI:

I PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese

1. Käesolevas direktiivis sätestatakse meetmed, mille eesmärk on saavutada küberturvalisuse ühtlaselt kõrge tase kogu liidus, et parandada siseturu toimimist.

2. Selle eesmärgi saavutamiseks sätestatakse käesolevas direktiivis:

a) liikmesriikide kohustus võtta vastu riiklikud küberturvalisuse strateegiad ning määrata või asutada pädevad asutused, küberkriisi juhtimise asutused, küberturbe ühtsed kontaktpunktid (edaspidi „ühtsed kontaktpunktid“) ja küberturbe intsidentide lahendamise üksused (edaspidi „CSIRTid“);

b) I või II lisas osutatud üksuste ning direktiivi (EL) 2022/2557 kohaselt elutähtsana käsitatavate üksuste küberturvalisuse riskijuhtimismeetmed ja teatamiskohustus;

c) küberturvalisuse alase teabevahetusega seotud reeglid ja kohustused;

d) järelevalve ja täitmise tagamisega seotud kohustused liikmesriikidele.

Artikkel 2

Kohaldamisala

1. Käesolevat direktiivi kohaldatakse I või II lisas osutatud sellist liiki avalik-õiguslike või eraõiguslike üksuste suhtes, mis kvalifitseeruvad soovituse 2003/361/EÜ lisa artikli 2 kohaselt keskmise suurusega ettevõtjateks või ületavad kõnealuse artikli lõikes 1 sätestatud keskmise suurusega ettevõtja piirmäärasid, ning osutavad teenuseid või tegutsevad liidus.

Käesoleva direktiivi kohaldamisel ei kohaldata nimetatud soovituse lisa artikli 3 lõiget 4.

2. Käesolevat direktiivi kohaldatakse ka I või II lisas osutatud liiki üksuste suhtes olenemata nende suurusest, kui

a) teenuseid osutavad:

   i) üldkasutatavate elektroonilise side võrkude pakkujad või üldkasutatavate elektroonilise side teenuste osutajad;

   ii) usaldusteenuse osutajad;

   iii) tippdomeeninimede registrid ja domeeninimede süsteemi teenuse osutajad;

b) üksus on liikmesriigis sellise teenuse ainuosutaja, mis on kriitilise tähtsusega ühiskondliku või majandustegevuse säilitamiseks;

c) üksuse osutatava teenuse häirel võib olla oluline mõju avalikule turvalisusele, avalikule julgeolekule või rahvatervisele;

d) üksuse osutatava teenuse häire võib tuua kaasa olulise süsteemse riski, eelkõige sektorites, kus sellisel häirel võib olla piiriülene mõju;

e) üksus on kriitilise tähtsusega oma erilise olulisuse tõttu riiklikul või piirkondlikul tasandil konkreetse sektori või teenuseliigi või liikmesriigi muude üksteisest sõltuvate sektorite jaoks;

f) üksus on

i) keskvalitsuse avaliku halduse üksus, nagu see on kindlaks määratud liikmesriigi poolt kooskõlas tema õigusega, või

ii) liikmesriigi poolt tema õiguse kohaselt kindlaks määratud piirkondliku tasandi üksus, mis vastavalt riskipõhisele hindamisele osutab teenuseid, mille häirel võib olla oluline mõju kriitilise tähtsusega ühiskondlikule või majandustegevusele.

3. Käesolevat direktiivi kohaldatakse direktiivi (EL) 2022/2557 kohaselt elutähtsa teenuse osutajatena käsitatavate üksuste suhtes olenemata nende suurusest.

4. Käesolevat direktiivi kohaldatakse domeeninimede registreerimise teenuseid osutavate üksuste suhtes olenemata nende suurusest.

5. Liikmesriigid võivad ette näha, et käesolevat direktiivi kohaldatakse:

a) kohaliku tasandi avaliku halduse üksuste suhtes;

b) haridusasutuste suhtes, eelkõige juhul, kui nad teevad kriitilise tähtsusega teadusuuringuid.

6. Käesolev direktiiv ei piira liikmesriikide kohustust kaitsta riiklikku julgeolekut ega nende õigust kaitsta muid riigi põhifunktsioone, sealhulgas tagada riigi territoriaalne terviklikkus ja säilitada õiguskord.

7. Käesolevat direktiivi ei kohaldata avaliku halduse üksuste suhtes, mis tegutsevad riigi julgeoleku, avaliku julgeoleku, kaitse või õiguskaitse valdkonnas, sealhulgas kuritegude ennetamise, uurimise, avastamise ja nende eest vastutusele võtmise valdkonnas.

8. Liikmesriigid võivad vabastada konkreetsed üksused, mis tegutsevad riigi julgeoleku, avaliku julgeoleku, kaitse või õiguskaitse valdkonnas, sealhulgas kuritegude ennetamise, uurimise, avastamise ja nende eest vastutusele võtmisega seotud tegevused, või mis osutavad teenuseid üksnes käesoleva artikli lõikes 7 osutatud avaliku halduse üksustele, artiklis 21 või 23 sätestatud kohustuste täitmisest seoses nimetatud tegevuste ja teenustega. Sellistel juhtudel VII peatükis osutatud järelevalve- ja täitemeetmeid nende konkreetsete tegevuste või teenuste suhtes ei kohaldata. Kui üksused tegelevad üksnes sellist liiki tegevusega või osutavaid üksnes sellist liiki teenuseid, millele on osutatud käesolevas lõikes, võivad liikmesriigid otsustada need üksused ka artiklites 3 ja 27 sätestatud kohustuste täitmisest vabastada.

9. Lõikeid 7 ja 8 ei kohaldata, kui üksus tegutseb usaldusteenuse osutajana.

10. Käesolevat direktiivi ei kohaldata üksuste suhtes, mille liikmesriigid on kooskõlas määruse (EL) 2022/2554 artikli 2 lõikega 4 kõnealuse määruse kohaldamisalast välja jätnud.

11. Käesolevas direktiivis sätestatud kohustused ei hõlma sellise teabe esitamist, mille avalikustamine oleks vastuolus liikmesriikide riikliku julgeoleku, avaliku julgeoleku või riigikaitse oluliste huvidega.

12. Käesolev direktiiv ei piira määruse (EL) 2016/679, direktiivi 2002/58/EÜ, direktiivide 2011/93/EL ([27]) ja 2013/40/EL ([28]) ega direktiivi (EL) 2022/2557 kohaldamist.

13. Ilma et see piiraks ELi toimimise lepingu artikli 346 kohaldamist, tuleks teavet, mis on liidu või liikmesriikide õigusnormide, näiteks ärisaladust käsitlevate õigusnormide kohaselt konfidentsiaalne, vahetada käesoleva direktiivi kohaselt komisjoni ja teiste asjakohaste asutustega üksnes juhul, kui selline teabevahetus on vajalik käesoleva direktiivi kohaldamiseks. Vahetada võib ainult teavet, mis on teabevahetuse eesmärgi seisukohast oluline ja proportsionaalne. Teabevahetuse puhul tuleb säilitada asjaomase teabe konfidentsiaalsus ning kaitsta asjaomaste üksuste turvalisust ja ärihuve.

([27]) 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).

([28]) 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).

14. Üksused, pädevad asutused, ühtsed kontaktpunktid ja CSIRTid töötlevad isikuandmeid ulatuses, mis on vajalik käesoleva direktiivi kohaldamiseks, ja kooskõlas määrusega (EL) 2016/679, eelkõige tuginedes sellise töötlemise puhul kõnealuse määruse artiklile 6.

Käesoleva direktiivi kohane isikuandmete töötlemine üldkasutatavate elektroonilise side võrkude pakkujate või üldkasutatavate elektroonilise side teenuste osutajate poolt toimub kooskõlas liidu andmekaitseõiguse ja eraelu puutumatuse kaitset käsitleva õiguse, eelkõige direktiiviga 2002/58/EÜ.

Artikkel 3

Elutähtsad ja olulised üksused

1. Käesoleva direktiivi kohaldamisel käsitatakse elutähtsate üksustena järgmisi üksusi:

a) I lisas osutatud liiki üksused, mis ületavad soovituse 2003/361/EÜ lisa artikli 2 lõikes 1 esitatud keskmise suurusega ettevõtja ülemmäärasid;

b) kvalifitseeritud usaldusteenuse osutajad ja tippdomeeninimede registrid ning domeeninimede süsteemi teenuse osutajad, olenemata nende suurusest;

c) üldkasutatavate elektroonilise side võrkude või üldkasutatavate elektroonilise side teenuste pakkujad, mida käsitatakse soovituse 2003/361/EÜ lisa artikli 2 kohaselt keskmise suurusega ettevõtjana;

d) artikli 2 lõike 2 punkti f alapunktis i osutatud avaliku halduse üksused;

e) muud I ja II lisas osutatud liiki üksused, mida liikmesriik käsitab elutähtsa üksusena artikli 2 lõike 2 punktide b–e kohaselt;

f) direktiivi (EL) 2022/2557 kohaselt elutähtsa teenuse osutajatena käsitatavad üksused, millele on osutatud käesoleva direktiivi artikli 2 lõikes 3;

g) kui liikmesriigid nii ette näevad, siis üksused, mida liikmesriigid käsitasid enne 16. jaanuari 2023 oluliste teenuste operaatoritena vastavalt direktiivile (EL) 2016/1148 või liikmesriigi õigusele.

2. Käesoleva direktiivi kohaldamisel käsitatakse oluliste üksustena I või II lisas osutatud üksusi, mis ei kvalifitseeru käesoleva artikli lõike 1 kohaselt elutähtsateks üksusteks. See hõlmab üksusi, mida liikmesriigid käsitavad oluliste üksustena artikli 2 lõike 2 punktide b–e alusel.

3. Hiljemalt 17. aprilliks 2025 koostavad liikmesriigid elutähtsate ja oluliste üksuste ning domeeninime registreerimise teenuseid osutavate üksuste loetelu. Liikmesriigid vaatavad loetelu läbi ja asjakohasel juhul ajakohastavad seda korrapäraselt ning seejärel vähemalt iga kahe aasta järel.

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

a) üksuse nimi;

b) aadress ja ajakohased kontaktandmed, sealhulgas e-posti aadressid, IP-vahemikud ja telefoninumbrid;

c) kui see on kohaldatav, I või II lisas osutatud asjakohane sektor ja allsektor ning

d) kui see on kohaldatav, nende liikmesriikide loetelu, kus nad osutavad käesoleva direktiivi kohaldamisalasse kuuluvaid teenuseid.

Lõikes 3 osutatud üksused teatavad kõigist käesoleva lõike esimese lõigu kohaselt esitatud andmetes toimunud muutustest viivitamata ning igal juhul kahe nädala jooksul alates muutuse kuupäevast.

Euroopa Liidu Küberturvalisuse Ameti (ENISA) abil annab komisjon põhjendamatu viivituseta käesolevas lõikes sätestatud kohustustega seotud suunised ja näeb ette vormid.

Liikmesriigid võivad kehtestada riiklikud mehhanismid, mis võimaldavad üksustel end ise registreerida.

5. Hiljemalt 17. aprilliks 2025 ja seejärel iga kahe aasta järel teatavad pädevad asutused:

a) komisjonile ja koostöörühmale iga I või II lisas osutatud sektori ja allsektori kohta lõike 3 kohases loetelus sisalduvate üksuste arvu ning

b) komisjonile asjakohase teabe seoses artikli 2 lõike 2 punktide b–e kohaselt kindlaks määratud elutähtsate ja oluliste üksuste arvuga, I või II lisas osutatud sektori ja allsektoriga, kuhu need kuuluvad, nende osutatavate teenuste liigiga ning sellega, millise artikli 2 lõike 2 punktide b–e sätte kohaselt need kindlaks määrati.

6. Kuni 17. aprillini 2025 ja komisjoni taotlusel võivad liikmesriigid teatada komisjonile lõike 5 punktis b osutatud elutähtsate ja oluliste üksuste nimed.

Artikkel 4

Valdkondlikud liidu õigusaktid

1. Kui valdkondlikes liidu õigusaktides nõutakse elutähtsatelt või olulistelt üksustelt küberturvalisuse riskijuhtimismeetmete võtmist või olulistest intsidentidest teatamist ning kui need nõuded on vähemalt samaväärse toimega kui käesolevas direktiivis sätestatud kohustused, ei kohaldata selliste üksuste suhtes käesoleva direktiivi asjakohaseid sätteid, sealhulgas VII peatükis sätestatud järelevalve- ja täitmise tagamise sätteid. Kui valdkondlikud liidu õigusaktid ei hõlma kõiki konkreetse sektori üksusi, mis kuuluvad käesoleva direktiivi kohaldamisalasse, kohaldatakse jätkuvalt käesoleva direktiivi asjakohaseid sätteid nende valdkondlike liidu õigusaktidega hõlmamata üksuste suhtes.

2. Käesoleva artikli lõikes 1 osutatud nõudeid käsitatakse samaväärse toimega kui käesolevas direktiivis sätestatud kohustused juhul, kui:

a) küberturvalisuse riskijuhtimismeetmed on mõjult vähemalt samaväärsed artikli 21 lõigetes 1 ja 2 sätestatud meetmetega või

b) valdkondlikus liidu õigusaktis nähakse ette käesoleva direktiivi kohane CSIRTide, pädevate asutuste või ühtsete kontaktpunktide viivitamatu, asjakohasel juhul automaatne ja otsene juurdepääs käesoleva direktiivi kohastele intsidenditeadetele ning kui olulistest intsidentidest teatamise nõuded on mõjult vähemalt samaväärsed käesoleva direktiivi artikli 23 lõigetes 1–6 sätestatud nõuetega.

3. Komisjon annab hiljemalt 17. juuliks 2023 suunised, milles selgitatakse lõigete 1 ja 2 kohaldamist. Komisjon vaatab kõnealused suunised korrapäraselt läbi. Nende suuniste ettevalmistamisel võtab komisjon arvesse koostöörühma ja ENISA tähelepanekuid.

Artikkel 5

Minimaalne ühtlustamine

Käesolev direktiiv ei takista liikmesriike tarbijate kaitseks vastu võtmast või kehtima jätmast sätteid, millega tagatakse kõrgem küberturvalisuse tase, tingimusel et sellised sätted on kooskõlas liikmesriikide kohustustega, mis on sätestatud liidu õiguses.

Artikkel 6

Mõisted

Käesolevas direktiivis kasutatakse järgmisi mõisteid:

1) „võrgu- ja infosüsteem“ –

   a) direktiivi (EL) 2018/1972 artikli 2 punktis 1 määratletud elektroonilise side võrk;

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

c) digiandmed, mida salvestatakse, töödeldakse, saadakse päringutega või edastatakse punktidega a ja b hõlmatud komponente kasutades 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 kahjustada salvestatavate, edastatavate või töödeldavate andmete või võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust või konfidentsiaalsust;

3) „küberturvalisus“ – määruse (EL) 2019/881 artikli 2 punktis 1 määratletud küberturvalisus;

4) „riiklik küberturvalisuse strateegia“ – liikmesriigi ühtne raamistik, mis näeb ette küberturvalisuse valdkonna strateegilised eesmärgid ja prioriteedid ning nende saavutamiseks vajaliku juhtimise kõnealuses liikmesriigis;

5) „intsidendioht“ – sündmus, mis oleks võinud kahjustada salvestatavate, edastatavate või töödeldavate andmete või võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust ja konfidentsiaalsust, kuid mis õnnestus ära hoida või mis ei tekkinud;

6) „intsident“ – sündmus, mis kahjustab salvestatavate, edastatavate või töödeldavate andmete või võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust või konfidentsiaalsust;

7) „ulatuslik küberturbeintsident“ – intsident, mille põhjustatud häired on niivõrd laialdased, et üks liikmesriik ei suuda nendega toime tulla või millel on märkimisväärne mõju vähemalt kahele liikmesriigile;

8) „intsidendi käsitlemine“ – toimingud ja menetlused, mille eesmärk on intsidenti ennetada, tuvastada, analüüsida, ohjata või lahendada ja sellest taastuda;

9) „risk“ – intsidendist tingitud kahju või häire võimalus, mida tuleb väljendada sellise kahju või häire ulatust ja kõnealuse intsidendi esinemise tõenäosust arvesse võtva kombineeritud näitajana;

10) „küberoht“ – määruse (EL) 2019/881 artikli 2 punktis 8 määratletud küberoht;

11) „oluline küberoht“ – küberoht, mille tehniliste näitajate põhjal võib eeldada, et sellel võib olla tõsine mõju üksuse võrgu- ja infosüsteemile või üksuse süsteemide kasutajatele, tekitades märkimisväärset varalist või mittevaralist kahju;

12) „IKT-toode“ – määruse (EL) 2019/881 artikli 2 punktis 12 määratletud IKT-toode;

13) „IKT-teenus“ – määruse (EL) 2019/881 artikli 2 punktis 13 määratletud IKT-teenus;

14) „IKT-protsess“ – määruse (EL) 2019/881 artikli 2 punktis 14 määratletud IKT-protsess;

15) „nõrkus“ – IKT-toote või -teenuse nõrkus, tundlikkus või viga, mida küberohu tekitaja võib ära kasutada;

16) „standard“ – Euroopa Parlamendi ja nõukogu määruse (EL) nr 1025/2012 ([29]) artikli 2 punktis 1 määratletud standard;

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

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

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

19) „domeeninimede süsteem“ – hierarhiline ja hajus nimesüsteem, mis võimaldab tuvastada internetiteenuseid ja -ressursse, võimaldades lõppkasutaja seadmetel kasutada internetimarsruutimise ja ühenduvuse teenuseid, et jõuda nende teenuste ja ressurssideni;

20) „domeeninimede süsteemi teenuse osutaja“ – üksus, kes osutab:

a) interneti lõppkasutajatele üldsusele kättesaadavat domeeninime rekursiivse teisendamise teenust või

b) kolmandatele isikutele kasutuseks domeeninime autoriteetse teisendamise teenust, välja arvatud juurnimeserverid;

21) „tippdomeeninimede register“ – üksus, kellele on delegeeritud kindel tippdomeen ja kes vastutab selle tippdomeeni haldamise eest, sealhulgas tippdomeeni alldomeeninimede registreerimise eest ja tippdomeeni tehnilise toimimise eest, sealhulgas nimeserverite käitamise, andmebaaside hooldamise ning nimeserverite vahel tippdomeeni tsoonifailide jaotamise eest, olenemata sellest, kas mõne neist toimingutest teeb üksus ise või ostetakse need sisse, kuid välja arvatud olukorrad, kus tippdomeeninimesid kasutab register ise ainult enda tarbeks;

22) „domeeninimede registreerimise teenuseid osutav üksus“ – registripidaja või registripidaja nimel tegutsev esindaja, näiteks registreerimisega seotud privaatsusteenuse või proksiteenuse osutaja või edasimüüja;

23) „digiteenus“ – Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/1535 ([30]) artikli 1 lõike 1 punktis b määratletud teenus;

24) „usaldusteenus“ – määruse (EL) nr 910/2014 artikli 3 punktis 16 määratletud usaldusteenus;

25) „usaldusteenuse osutaja“ – määruse (EL) nr 910/2014 artikli 3 punktis 19 määratletud usaldusteenuse osutaja;

26) „kvalifitseeritud usaldusteenus“ – määruse (EL) nr 910/2014 artikli 3 punktis 17 määratletud kvalifitseeritud usaldusteenus;

27) „kvalifitseeritud usaldusteenuse osutaja“ – määruse (EL) nr 910/2014 artikli 3 punktis 20 määratletud kvalifitseeritud usaldusteenuse osutaja;

28) „internetipõhine kauplemiskoht“ – Euroopa Parlamendi ja nõukogu direktiivi 2005/29/EÜ ([31]) artikli 2 punktis n määratletud internetipõhine kauplemiskoht;

29) „internetipõhine otsingumootor“ – Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/1150 ([32]) artikli 2 punktis 5 määratletud internetipõhine otsingumootor;

30) „pilvandmetöötlusteenus“ – digiteenus, mis võimaldab jagatavate andmetöötlusressursside skaleeritava ja paindliku kogumi nõudepõhist haldamist ning ulatuslikku kaugpääsu sellele kogumile, sealhulgas juhul, kui need ressursid paiknevad hajutatult erinevates kohtades;

([30]) 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).

([31]) 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).

([32]) 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).

31) „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, sealhulgas kõiki energiajaotuse ja keskkonnakontrolliga seotud vahendeid ja taristuid;

32) „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;

33) „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;

34) „esindaja“ – füüsiline isik, kelle tegevuskoht on liidus või liidus asutatud juriidiline isik, kes on sõnaselgelt määratud tegutsema väljaspool liitu asuva domeeninimede süsteemi teenuse osutaja (DNS), tippdomeeninimede (TLD) registri, domeeninime registreerimise teenuseid osutava üksuse, pilvandmetöötlusteenuse osutaja, andmekeskusteenuse osutaja, sisulevivõrkude pakkuja, hallatud teenuse osutaja, turbetarnija, internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite või sotsiaalvõrguteenuse platvormi pakkuja nimel ja kelle poole võib liikmesriigi pädev asutus või CSIRT pöörduda seoses kõnealuse üksuse käesolevast direktiivist tulenevate kohustustega;

35) „avaliku halduse üksus“ – üksus, mida tunnustatakse avaliku halduse üksusena liikmesriigis tema õiguse kohaselt, välja arvatud kohtud, parlamendid ja keskpangad, ning mis vastab järgmistele kriteeriumidele:

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

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

   c) üksust rahastavad põhiliselt riik, piirkondlikud ametiasutused või muud avalik-õiguslikud isikud või selle juhtimine toimub kõnealuste asutuste või avalik-õiguslike isikute järelevalve all või üle poole selle haldus-, juhtimis- või järelevalveorgani liikmetest on määranud riik, piirkondlikud asutused või muud avalik-õiguslikud isikud;

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

36) „üldkasutatav elektroonilise side võrk“ – direktiivi (EL) 2018/1972 artikli 2 punktis 8 määratletud üldkasutatav elektroonilise side võrk;

37) „elektroonilise side teenus“ – direktiivi (EL) 2018/1972 artikli 2 punktis 4 määratletud elektroonilise side teenus;

38) „üksus“ – füüsiline isik või juriidiline isik, kes on asutatud ja keda tunnustatakse tema tegevuskohajärgse riigisisese õiguse kohaselt, kes võib enda nimel omada õigusi ja kanda kohustusi;

39) „hallatud teenuse osutaja“ – üksus, mis osutab teenuseid, mis on seotud IKT-toodete, võrkude, taristu, rakenduste või muude võrgu- ja infosüsteemide paigaldamise, haldamise, käitamise või hooldamisega toe või aktiivse haldamise kaudu kas klientide ruumides või kaugteel;

40) „turbetarnija“ – hallatud teenuste osutaja, kes viib ellu küberturvalisuse riskijuhtimisega seotud tegevust või pakub selleks tuge;

41) „teadusasutus“ – üksus, mille peamine eesmärk on viia ellu rakendusuuringuid või tootearendust eesmärgiga kasutada selliste teadusuuringute tulemusi ärilistel eesmärkidel, kuid mis ei hõlma haridusasutusi.

II PEATÜKK

KOORDINEERITUD KÜBERTURVALISUSE RAAMISTIKUD

Artikkel 7

Riiklik küberturvalisuse strateegia

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

a) liikmesriigi küberturvalisuse strateegia eesmärgid ja prioriteedid, mis hõlmavad eelkõige I ja II lisas osutatud sektoreid;

b) juhtimisraamistik käesoleva lõike punktis a osutatud eesmärkide ja prioriteetide saavutamiseks, sealhulgas lõikes 2 osutatud poliitikameetmed;

c) juhtimisraamistik, milles selgitatakse asjaomaste sidusrühmade rolli ja kohustusi riiklikul tasandil, mis toetavad käesoleva direktiivi kohaste pädevate asutuste, ühtsete kontaktpunktide ja CSIRTide vahelist koostööd ja koordineerimist riiklikul tasandil, samuti nende organite ja valdkondlike liidu õigusaktide kohaste pädevate asutuste vahelist koordineerimist ja koostööd;

d) mehhanism asjakohaste varade kindlaks tegemiseks ja kõnealuse liikmesriigi riskide hinnang;

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

f) riikliku küberturvalisuse strateegia rakendamisse kaasatavate asutuste ja sidusrühmade loetelu;

g) poliitikaraamistik käesoleva direktiivi ning direktiivi (EL) 2022/2557 kohaste pädevate asutuste vahelise tegevuse tõhusaks koordineerimiseks küberriskide, -ohtude ja -intsidentide ning asjakohasel juhul muude kui küberriskide, -ohtude ja -intsidentide alase teabe jagamise ning järelevalveülesannete täitmise eesmärgil;

h) kava, sealhulgas vajalikud meetmed kodanike küberturvalisuse alase teadlikkuse üldise taseme suurendamiseks.

2. Riikliku küberturvalisuse strateegia osana võtavad liikmesriigid vastu eelkõige poliitikameetmed,

a) mis käsitlevad üksuste teenuste osutamiseks kasutatavate IKT-toodete ja IKT-teenuste tarneahela küberturvalisust;

b) mis käsitlevad IKT-toodete ja IKT-teenuste küberturvalisusega seotud nõuete ja vastavate spetsifikatsioonide lisamist riigihankemenetlusse, sealhulgas seoses küberturvalisuse sertifitseerimise, krüpteerimisnõuete ning avatud lähtekoodiga küberturvalisuse toodete kasutamisega;

c) nõrkuste haldamiseks, mis hõlmab kohase nõrkuste koordineeritud avalikustamise edendamist ja hõlbustamist artikli 12 lõikele 1 kohaselt;

d) mis on seotud avatud interneti avaliku tuuma üldise kättesaadavuse, usaldusväärsuse ja konfidentsiaalsuse säilitamisega, sealhulgas vajaduse korral merealuste sidekaablite küberturvalisusega;

e) mis edendavad selliste asjakohaste kõrgetasemeliste tehnoloogiate väljatöötamist ja integreerimist, mille eesmärk on rakendada tipptasemel küberturvalisuse riskijuhtimismeetmeid;

f) mille abil edendatakse ja arendatakse küberturvalisuse alast haridust ja koolitust, küberturvalisuse alaseid oskusi, teadlikkust, teadus- ja arendusalgatusi ning suuniseid heade küberhügieenitavade ja -kontrolli kohta kodanikele, sidusrühmadele ja üksustele;

g) millega toetatakse akadeemilisi ja teadusasutusi küberturvalisuse vahendite ja turvalise võrgutaristu väljatöötamisel, täiustamisel ja kasutuselevõtmise edendamisel;

h) sealhulgas asjakohane menetluskord ja sobivad teabevahetuslahendused, millega toetatakse vabatahtlikku küberturvalisuse alase teabe vahetamist üksuste vahel kooskõlas liidu õigusega;

i) mis tugevdavad väikeste ja keskmise suurusega ettevõtjate, eelkõige nende, kes on käesoleva direktiivi kohaldamisalast välja jäetud, kübervastupidavusvõimet ja küberhügieeni lähtetaset, pakkudes nende erivajaduste rahuldamiseks kergesti kättesaadavaid suuniseid ja tuge;

j) mis edendavad aktiivset küberkaitset.

3. Liikmesriigid teavitavad komisjoni oma riiklikust küberturvalisuse strateegiast kolme kuu jooksul pärast selle vastuvõtmist. Liikmesriigid võivad jätta sellistest teadetest välja teabe, mis on seotud nende riikliku julgeolekuga.

4. Liikmesriigid hindavad oma riiklikke küberturvalisuse strateegiaid peamiste tulemusnäitajate põhjal korrapäraselt ja vähemalt iga viie aasta järel ja vajaduse korral ajakohastavad neid. Riikliku küberturvalisuse strateegia ja selle hindamiseks vajalike peamiste tulemusnäitajate väljatöötamisel või ajakohastamisel, et viia strateegia käesolevas direktiivis sätestatud nõuete ja kohustustega kooskõlla, abistab liikmesriike nende taotluse korral ENISA.

Artikkel 8

Pädevad asutused ja ühtsed kontaktpunktid

1. Iga liikmesriik määrab või asutab vähemalt ühe pädeva asutuse, kes vastutab küberturvalisuse ja käesoleva direktiivi VII peatükis osutatud järelevalveülesannete täitmise eest (edaspidi „pädevad asutused“).

2. Lõikes 1 osutatud pädevad asutused jälgivad käesoleva direktiivi rakendamist liikmesriigi tasandil.

3. Iga liikmesriik määrab või asutab ühe kontaktpunkti. Kui liikmesriik määrab või asutab vastavalt lõikele 1 ainult ühe pädeva asutuse, 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 asjakohasel juhul komisjoni ja ENISAga ning ka valdkondadevaheline koostöö oma liikmesriigi teiste pädevate asutustega.

5. Liikmesriigid tagavad, et nende pädevatel asutustel ja ühtsetel kontaktpunktidel on piisavad ressursid, et täita oma ülesandeid tulemuslikult ja tõhusalt ning saavutada seeläbi käesoleva direktiivi eesmärgid.

6. Iga liikmesriik teatab komisjonile põhjendamatu viivituseta lõikes 1 osutatud pädeva asutuse ja lõikes 3 osutatud ühtse kontaktpunkti andmed, nende asutuste ülesanded ning nendega seotud hilisemad muudatused. Iga liikmesriik avalikustab kõnealuse pädeva asutuse andmed. Komisjon avalikustab ühtsete kontaktpunktide loetelu.

Artikkel 9

Riiklikud küberkriiside ohjamise raamistikud

1. Iga liikmesriik määrab või asutab vähemalt ühe ulatuslike küberturbeintsidentide ja kriiside ohjamise eest vastutava pädeva asutuse (edaspidi „küberkriisi ohjamise asutused“). Liikmesriigid tagavad, et nendel asutustel on nendele pandud ülesannete tulemuslikuks ja tõhusaks täitmiseks piisavad ressursid. Liikmesriigid tagavad sidususe oma olemasolevate üldiste kriisiohjeraamistikega.

2. Kui liikmesriik määrab või asutab lõike 1 kohaselt rohkem kui ühe küberkriisi ohjamise asutuse, märgib ta selgelt, milline neist asutustest tegutseb ulatuslike küberturbeintsidentide ja kriiside ohjamisel koordinaatorina.

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

4. Iga liikmesriik võtab vastu riikliku ulatuslike küberturbeintsidentide ja kriiside lahendamise kava, milles kirjeldatakse ulatuslike küberturbeintsidentide ja kriiside ohjamise eesmärke ja korda. Nimetatud kavaga nähakse täpsemalt ette järgmine:

a) riiklike valmisolekumeetmete ja nendega seotud tegevuse eesmärgid;

b) küberkriisi ohjamise asutuste kohustused ja ülesanded;

c) küberkriisi ohjamise menetlused, sealhulgas nende lõimimine üldisesse riiklikku kriisiohjeraamistikku ja teabevahetuskanalitesse;

d) riiklikud valmisolekumeetmed, sealhulgas õppuste ja koolitusega seotud tegevus;

e) asjakohased avaliku ja erasektori sidusrühmad ning seotud taristud;

f) liikmesriigi menetlused ja kord asjaomaste riiklike asutuste ja organite vahelise koostöö korraldamiseks, et tagada liikmesriigi tulemuslik osalemine ulatuslike küberturbeintsidentide ja kriiside koordineeritud ohjamisel liidu tasandil ja selle ohjamise toetamine.

5. Liikmesriigid teatavad komisjonile kolme kuu jooksul lõikes 1 osutatud küberkriisi ohjamise asutuste määramisest või asutamisest, nende andmed ja kõik hilisemad muudatused nendes. Liikmesriigid esitavad komisjonile ja Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikule (EU-CyCLONe) asjakohase teabe, mis on seotud lõikes 4 sätestatud nõuetega nende riiklike ulatuslike küberturbeintsidentide ja kriiside lahendamise kavade kohta kolme kuu jooksul pärast kõnealuste kavade vastuvõtmist. Liikmesriigid võivad jätta teatava osa teabest esitamata, kui ja millises ulatuses see on vajalik riikliku julgeoleku tagamiseks.

Artikkel 10

Küberturbe intsidentide lahendamise üksused (CSIRTid)

1. Iga liikmesriik määrab või asutab vähemalt ühe CSIRTi. CSIRTi võib määrata või asutada pädevas asutuses. CSIRTid peavad vastama artikli 11 lõikes 1 sätestatud nõuetele, hõlmama vähemalt I ja II lisas osutatud sektoreid, allsektoreid või üksuste liike ning vastutama intsidentide käsitlemise eest kindla menetluse kohaselt.

2. Liikmesriigid tagavad, et igal CSIRTil on artikli 11 lõikes 3 sätestatud ülesannete tulemuslikuks täitmiseks piisavad vahendid.

3. Liikmesriigid tagavad, et iga CSIRTi käsutuses on asjakohane, turvaline ja vastupidav side- ja teabetaristu, mille abil vahetada teavet elutähtsate ja oluliste üksuste ning muude asjaomaste sidusrühmadega. Selleks tagavad liikmesriigid, et iga CSIRT aitab kaasa turvaliste teabejagamisvahendite kasutuselevõtule.

4. CSIRTid teevad koostööd ning, kui see on kohane, vahetavad kooskõlas artikliga 29 asjakohast teavet elutähtsate ja oluliste üksuste sektoripõhiste või -vaheliste kogukondadega.

5. CSIRTid osalevad artikli 19 kohaselt korraldatud vastastikuses hindamises.

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

7. CSIRTid võivad luua koostöösuhteid kolmandate riikide riiklike küberturbe intsidentide lahendamise üksustega. Selliste koostöösuhete osana hõlbustavad liikmesriigid tõhusat, tulemuslikku ja turvalist teabevahetust nende kolmandate riikide riiklike küberturbeintsidentide lahendamise üksustega, kasutades asjakohaseid teabevahetuse protokolle, sealhulgas fooriprotokolli. CSIRTid võivad vahetada kolmandate riikide riiklike küberturbeintsidentide lahendamise üksustega asjakohast teavet, sealhulgas isikuandmeid kooskõlas liidu andmekaitseõigusega.

8. CSIRTid võivad teha kolmandate riikide riiklike küberturbeintsidentide lahendamise üksustega või samaväärsete kolmandate riikide asutustega koostööd, eelkõige selleks, et anda neile küberturvalisuse alast abi.

9. Iga liikmesriik teatab komisjonile põhjendamatu viivituseta käesoleva artikli lõikes 1 osutatud CSIRTi ja artikli 12 lõike 1 kohaselt koordinaatoriks määratud CSIRTi andmed, nende asjaomased ülesanded seoses elutähtsate ja oluliste üksustega ning nendega seotud hilisemad muudatused.

10. Liikmesriigid võivad oma CSIRTide moodustamisel paluda ENISA abi.

Artikkel 11

CSIRTidele esitatavad nõuded, nende tehniline võimekus ja ülesanded

1. CSIRTid peavad vastama järgmistele nõuetele:

a) CSIRTid peavad tagama oma sidekanalite laialdase kättesaadavuse, vältides nõrku lülisid, ning kasutama mitmesuguseid vahendeid, mis võimaldavad neil teistega ja teistel nendega igal ajal ühendust võtta; CSIRTid määravad selgelt kindlaks sidekanalid ning teevad need oma sihtrühmadele ja koostööpartneritele teatavaks;

b) CSIRTide ametiruumid ja nende tööd toetavad infosüsteemid peavad asuma turvalises kohas;

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

d) CSIRTid peavad tagama oma tegevuse konfidentsiaalsuse ja usaldusväärsuse;

e) CSIRTidel peab olema piisavalt töötajaid, et tagada nende teenuste alaline kättesaadavus, ja nad peavad tagama oma töötajatele asjakohase väljaõppe;

f) CSIRTidel peavad olema varusüsteemid ja varutööruumid, et tagada oma teenuste toimepidevus.

CSIRTid võivad osaleda rahvusvahelistes koostöövõrgustikes.

2. Liikmesriigid tagavad, et nende CSIRTidel on ühiselt artiklis 3 osutatud ülesannete täitmiseks vajalik tehniline võimekus. Liikmesriigid tagavad, et nende CSIRTidele eraldatakse piisavalt vahendeid, et tagada selline töötajate arv, mis võimaldab CSIRTidel arendada oma tehnilist võimekust.

3. CSIRTidel on järgmised ülesanded:

a) korraldada küberohtude, nõrkuste ja intsidentide seiret ja analüüsi riiklikul tasandil, ning taotluse korral osutada abi asjaomastele elutähtsatele ja olulistele üksustele seoses nende võrgu- ja infosüsteemide reaalajas või reaalajalähedase seirega;

b) tagada küberohtude, nõrkuste ja intsidentide kohta varajaste hoiatuste, hoiatuste ja teadete edastamine ning teabe levitamine asjaomastele elutähtsatele ja olulistele üksustele ning pädevatele asutustele ning muudele asjaomastele sidusrühmadele, võimaluse korral reaalajalähedaselt;

c) lahendada intsidente ning, kui see on kohaldatav, abistada asjaomaseid elutähtsaid ja olulisi üksusi;

d) koguda ja analüüsida kohtuekspertiisiandmeid ning analüüsida järjepidevalt riske ja intsidente ning tagada küberturvalisuse alane olukorrateadlikkus;

e) kontrollida elutähtsa või olulise üksuse taotlusel ennetavalt selle üksuse võrgu- ja infosüsteeme, et teha kindlaks potentsiaalselt olulise mõjuga nõrkused;

f) osaleda CSIRTide võrgustikus ning osutada teistele võrgustiku liikmetele nende taotluse korral oma võimekusele ja pädevusele vastavat vastastikust abi;

g) kui see on kohaldatav, tegutseda artikli 12 lõikes 1 osutatud nõrkuste koordineeritud avalikustamise protsessi koordinaatorina;

h) panustada artikli 10 lõike 3 kohaste turvaliste teabejagamisvahendite kasutuselevõtmisse.

CSIRTid võivad elutähtsate ja oluliste üksuste üldkasutatavaid võrgu- ja infosüsteeme ennetavalt väliselt kontrollida. Selline kontrollimine toimub nõrkade või ebaturvaliselt konfigureeritud võrgu- ja infosüsteemide tuvastamiseks ning asjaomaste üksuste teavitamiseks. Sellisel kontrollimisel ei tohi olla negatiivset mõju üksuste teenuste toimimisele.

Esimeses lõigus osutatud ülesannete täitmisel võivad CSIRTid riskipõhise lähenemisviisi alusel teatavaid ülesandeid prioriseerida.

4. CSIRTid loovad koostöösuhteid erasektori asjaomaste sidusrühmadega, et saavutada käesoleva direktiivi eesmärgid.

5. Lõikes 4 osutatud koostöö hõlbustamiseks toetavad CSIRTid ühtsete või standardsete tavade, liigitamissüsteemide ja taksonoomiate kasutuselevõttu seoses järgmisega:

a) intsidentide käsitlemise menetlused;

b) kriisiohje ning

c) artikli 12 lõike 1 kohane nõrkuste koordineeritud avalikustamine.

Artikkel 12

Nõrkuste koordineeritud avalikustamine ja Euroopa nõrkuste andmebaas

1. Iga liikmesriik määrab ühe oma CSIRTidest nõrkuste koordineeritud avalikustamise koordinaatoriks. Koordinaatoriks määratud CSIRT tegutseb usaldusväärse vahendajana, hõlbustades vajaduse korral suhtlust nõrkusest teavitava füüsilise või juriidilise isiku ning potentsiaalse nõrkusega IKT-toodete tootja või IKT-teenuste osutaja vahel, tegutsedes ükskõik kumma poole taotlusel. Koordinaatoriks määratud CSIRTi ülesandeks on

a) teha kindlaks asjaomased üksused ja võtta nendega ühendust;

b) abistada nõrkusest teavitavaid füüsilisi ja juriidilisi isikuid ning

c) pidada läbirääkimisi avalikustamise tähtaegade üle ning hallata mitut üksust mõjutavaid nõrkusi.

Liikmesriigid tagavad, et füüsilised või juriidilised isikud saavad koordinaatoriks määratud CSIRTi nõrkusest teavitada taotluse korral anonüümselt. Koordinaatoriks määratud CSIRT tagab, et teatatud nõrkusega seoses võetakse hoolikaid järelmeetmeid, ning tagab nõrkusest teatava füüsilise või juriidilise isiku anonüümsuse. Kui teates osutatud nõrkus võib oluliselt mõjutada üksusi rohkem kui ühes liikmesriigis, teeb iga asjaomase liikmesriigi poolt koordinaatoriks määratud CSIRT asjakohasel juhul teiste koordinaatoriks määratud CSIRTidega CSIRTide võrgustikus koostööd.

2. ENISA töötab pärast koostöörühmaga konsulteerimist välja Euroopa nõrkuste andmebaasi ja haldab seda. Selleks loob ENISA asjakohased infosüsteemid, põhimõtted ja menetlused ning haldab neid ning võtab Euroopa nõrkuste andmebaasi turvalisuse ja tervikluse tagamiseks vajalikud tehnilised ja korralduslikud meetmed eelkõige selleks, et võimaldada üksustel, olenemata sellest, kas nad kuuluvad käesoleva direktiivi kohaldamisalasse, ning nende võrgu- ja infosüsteemide tarnijatel vabatahtlikult avalikustada ja registreerida IKT-toodete või IKT-teenuste üldtuntud nõrkusi. Juurdepääs Euroopa nõrkuste andmebaasis sisalduvale nõrkusi käsitlevale teabele antakse kõigile sidusrühmadele. Andmebaas sisaldab teavet:

a) nõrkuse olemuse kohta;

b) mõjutatud IKT-toodete või IKT-teenuste ning nõrkuse tõsiduse kohta, pidades silmas selle võimaliku ärakasutamise olukordi;

c) seotud paikade kättesaadavuse kohta ning paikade puudumisel nõrkustega IKT-toodete ja IKT-teenuste kasutajatele suunatud, pädevate asutuste või CSIRTide poolt antud suunised selle kohta, kuidas avalikustatud nõrkustest tulenevaid riske vähendada.

Artikkel 13

Koostöö liikmesriigi tasandil

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

2. Liikmesriigid tagavad, et nende CSIRTid või, kui see on kohaldatav, nende pädevad asutused saavad artikli 23 kohaselt esitatud teateid oluliste intsidentide ning artikli 30 kohaselt esitatud teateid intsidentide, küber- ja intsidendiohtude kohta.

3. Liikmesriigid tagavad, et nende CSIRTid või, kui see on kohaldatav, nende pädevad asutused teavitavad intsidentide, küber- ja intsidendiohtude kohta käesoleva direktiivi kohaselt esitatud teadetest oma riigi ühtset kontaktpunkti.

4. Selleks et tagada pädevate asutuste, ühtsete kontaktpunktide ja CSIRTide ülesannete ja kohustuste tulemuslik täitmine, tagavad liikmesriigid nii suures ulatuses kui võimalik asjakohase koostöö nende kõnealuse liikmesriigi organite ning õiguskaitseasutuste, andmekaitseasutuste, määruste (EÜ) nr 300/2008 ja (EL) 2018/1139 kohaste riiklike asutuste, määruse (EL) nr 910/2014 kohaste järelevalveasutuste, määruse (EL) 2022/2554 kohaste pädevate asutuste, direktiivi (EL) 2018/1972 kohaste riigi reguleerivate asutuste, direktiivi (EL) 2022/2557 kohaste pädevate asutuste ning muude valdkondlike liidu õigusaktide kohaste pädevate asutuste vahel.

5. Liikmesriigid tagavad, et nende käesoleva direktiivi kohased pädevad asutused ja direktiivi (EL) 2022/2557 kohased pädevad asutused teevad koostööd ja vahetavad korrapäraselt teavet elutähtsa teenuse osutajateks määramise, küberriskide, -ohtude ja -intsidentide kohta ning direktiivi (EL) 2022/2557 alusel elutähtsa teenuse osutajatena käsitatavaid elutähtsaid üksusi mõjutavate muude kui küberriskide, -ohtude ja -intsidentide kohta ning selliste riskide, ohtude ja intsidentide lahendamiseks võetud meetmete kohta. Samuti tagavad liikmesriigid, et nende käesoleva direktiivi kohased pädevad asutused ning määruste (EL) nr 910/2014, (EL) 2022/2554 ja direktiivi (EL) 2018/1972 kohased pädevad asutused vahetavad korrapäraselt asjakohast teavet, sealhulgas asjaomaste intsidentide ja küberohtude kohta.

6. Liikmesriigid lihtsustavad artiklites 23 ja 30 osutatud teatamist tehniliste vahendite abil.

III PEATÜKK

KOOSTÖÖ LIIDU JA RAHVUSVAHELISEL TASANDIL

Artikkel 14

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 7.

3. Koostöörühma moodustavad liikmesriikide, komisjoni ja ENISA esindajad. Euroopa välisteenistus osaleb koostöörühma tegevuses vaatlejana. Euroopa järelevalveasutused ja määruse (EL) 2022/2554 kohased pädevad asutused võivad osaleda koostöörühma tegevuses kooskõlas kõnealuse määruse artikli 47 lõikega 1.

Kui see on asjakohane, võib koostöörühm kutsuda oma töös osalema Euroopa Parlamendi ja asjakohaste sidusrühmade esindajad.

Sekretariaaditeenuseid osutab komisjon.

4. Koostöörühmal on järgmised ülesanded:

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

b) anda pädevatele asutustele suuniseid artikli 7 lõike 2 punktis c osutatud nõrkuste koordineeritud avalikustamise poliitika väljatöötamise ja rakendamise kohta;

c) vahetada parimaid tavasid ja teavet seoses käesoleva direktiivi rakendamisega, sealhulgas seoses küberohtude, intsidentide, nõrkuste, intsidendiohtude, teadlikkuse suurendamise algatuste, koolituse, õppuste ja oskuste, võimekuse suurendamise, standardite ja tehniliste spetsifikatsioonide ning elutähtsate ja oluliste üksuste kindlaksmääramisega artikli 2 lõike 2 punktide b–e kohaselt;

d) vahetada nõuandeid ja teha koostööd komisjoniga seoses uute küberturvalisuse poliitika algatustega ning valdkondlike küberturvalisuse nõuete üldise järjepidevusega;

e) vahetada nõuandeid ja teha koostööd komisjoniga seoses käesoleva direktiivi kohaselt vastu võetavate delegeeritud õigusaktide või rakendusaktide eelnõudega;

f) vahetada parimaid tavasid ja teavet asjaomaste liidu institutsioonide, organite ja asutustega;

g) vahetada arvamusi küberturvalisust käsitlevaid sätteid sisaldavate valdkondlike liidu õigusaktide rakendamise üle;

h) arutada artikli 19 lõikes 9 osutatud vastastikuse hindamise aruandeid, kui see on asjakohane, ning koostada järeldusi ja soovitusi;

i) teha kriitilise tähtsusega tarneahelate turberiski koordineeritud hindamisi kooskõlas artikli 22 lõikega 1;

j) arutada vastastikuse abi juhtumeid, sealhulgas artiklis 37 osutatud piiriüleste ühiste järelevalvemeetmete rakendamisest saadud kogemusi ja tulemusi;

k) arutada ühe või mitme asjaomase liikmesriigi taotlusel artiklis 37 osutatud konkreetseid vastastikuse abi taotlusi;

l) anda CSIRTide võrgustikule ja EU-CyCLONe-le strateegilisi suuniseid spetsiifilistes esilekerkivates küsimustes;

m) vahetada CSIRTide võrgustikust ja EU-CyCLONe-st saadud kogemuste põhjal arvamusi ulatuslike küberturbeintsidentide ja kriisijärgsete järelmeetmete poliitika üle;

n) aidata tagada küberturvalisuse alane võimekus liidus, hõlbustades riigiametnike vahetust suutlikkuse suurendamise programmi kaudu, millesse kaasatakse pädevate asutuste või CSIRTide töötajad;

o) korraldada korrapäraseid ühiskoosolekuid erasektori asjaomaste sidusrühmadega kogu liidust, et arutada koostöörühma tegevust ja koguda teavet esilekerkivate poliitikaprobleemide kohta;

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

q) panna komisjoni ja ENISA abiga paika artikli 19 lõikes 1 osutatud vastastikuste hindamiste metoodika ja korralduslikud aspektid, kehtestada artikli 19 lõike 5 kohane liikmesriikide enesehindamise metoodika ning töötada vastavalt artikli 19 lõikele 6 koostöös komisjoni ja ENISAga välja tegevusjuhendid, millele toetuvad määratud küberturvalisuse ekspertide töömeetodid;

r) koostada artiklis 40 osutatud läbivaatamise eesmärgil aruandeid strateegilisel tasandil ja vastastikuste hindamiste käigus omandatud kogemuste kohta;

s) arutada ja korrapäraselt hinnata küberohtude või intsidentide, näiteks lunavara olukorda.

Koostöörühm esitab esimese lõigu punktis r osutatud aruanded komisjonile, Euroopa Parlamendile ja nõukogule.

5. Liikmesriigid tagavad oma esindajate tõhusa, tulemusliku ja turvalise koostöö koostöörühmas.

6. Koostöörühm võib tellida CSIRTide võrgustikult valitud teemasid käsitlevaid tehnilisi aruandeid.

7. Koostöörühm koostab 1. veebruariks 2024 ja seejärel iga kahe aasta järel tööprogrammi oma eesmärkide ja ülesannete täitmiseks võetavate meetmete kohta.

8. Komisjon võib võtta vastu rakendusaktid, millega kehtestatakse koostöörühma toimimiseks vajalik menetluskord.

Kõnealused rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

Komisjon peab koostöörühmaga nõu ja teeb temaga lõike 4 punkti e kohaselt käesoleva lõike esimeses lõigus osutatud rakendusaktide eelnõude osas koostööd.

9. Koostöörühm kohtub korrapäraselt ning vähemalt kord aastas direktiivi (EL) 2022/2557 alusel loodud elutähtsa teenuse osutajate toimepidevuse töörühmaga, et edendada ja hõlbustada strateegilist koostööd ja teabevahetust.

Artikkel 15

CSIRTide võrgustik

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

2. CSIRTide võrgustik luuakse artikli 10 kohaselt määratud või asutatud CSIRTide ning liidu institutsioonide ja ametite infoturbeintsidentidega tegeleva rühma (CERT-EU) esindajatest. Komisjon osaleb CSIRTide võrgustiku tegevuses vaatlejana. ENISA tagab sekretariaaditeenused ja toetab aktiivselt CSIRTide-vahelist koostööd.

3. CSIRTide võrgustikul on järgmised ülesanded:

a) vahetada CSIRTide võimekust puudutavat teavet;

b) hõlbustada tehnoloogia ja asjaomaste meetmete, poliitika, vahendite, protsesside, parimate tavade ja raamistike jagamist, ülekandmist ja vahetamist CSIRTide vahel;

c) vahetada asjakohast teavet intsidentide, intsidendiohtude, küberohtude, riskide ja nõrkuste kohta;

d) vahetada teavet seoses küberturvalisust käsitlevate väljaannete ja soovitustega;

e) tagada koostalitlusvõime teabevahetuse spetsifikatsioonide ja protokollide osas;

f) vahetada ja arutada intsidendist potentsiaalselt mõjutatud CSIRTide võrgustiku liikme taotlusel teavet intsidendi ning sellega seotud küberohtude, riskide ja nõrkuste kohta;

g) arutada CSIRTide võrgustiku liikme taotlusel kõnealuse liikmesriigi jurisdiktsioonis tuvastatud intsidendi koordineeritud lahendamist ning võimaluse korral lahendada intsident koordineeritult;

h) abistada liikmesriike piiriüleste intsidentide käesoleva direktiivi kohasel käsitlemisel;

i) teha koostööd, vahetada parimaid tavasid ning abistada artikli 12 lõike 1 kohaselt koordinaatoriteks määratud CSIRT-e selliste nõrkuste koordineeritud avalikustamise haldamisel, millel võib olla märkimisväärne mõju rohkem kui ühe liikmesriigi üksustele;

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

   i) küberohtude ja intsidentide liigid;

   ii) varajased hoiatused;

   iii) vastastikune abi;

   iv) piiriüleste riskide ja intsidentide koordineeritud lahendamise põhimõtted ja kord;

   v) osalemine liikmesriigi taotlusel artikli 9 lõikes 4 osutatud riikliku ulatuslike küberturbeintsidentide ja kriiside lahendamise kava koostamises;

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

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

m) arutada CSIRTi taotlusel kõnealuse CSIRTi võimekust ja valmisolekut;

n) teha koostööd ning vahetada teavet piirkondlike ja liidu tasandi turbekeskustega, et parandada ühist olukorrateadlikkust intsidentide ja küberohtude vallas kogu liidus;

o) asjakohasel juhul arutada artikli 19 lõikes 9 osutatud vastastikuse hindamise aruandeid;

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

4. Hiljemalt 17. jaanuariks 2025 ning seejärel iga kahe aasta tagant hindab CSIRTide võrgustik artiklis 40 osutatud läbivaatamise eesmärgil operatiivkoostöös tehtud edusamme ja võtab vastu sellekohase aruande. Aruanne sisaldab eelkõige järeldusi ja soovitusi, mis põhinevad riiklike CSIRTide artiklis 19 osutatud vastastikuste hindamiste tulemustel. See aruanne esitatakse koostöörühmale.

5. CSIRTide võrgustik võtab vastu oma töökorra.

6. CSIRTide võrgustik ja EU-CyCLONe lepivad kokku menetluskorra ja teevad selle alusel koostööd.

Artikkel 16

Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik (EU-CyCLONe)

1. EU-CyCLONe luuakse selleks, et toetada ulatuslike küberturbeintsidentide ja kriiside koordineeritud ohjamist operatiivtasandil ning tagada asjakohase teabe korrapärane vahetamine liikmesriikide ning liidu institutsioonide, organite ja asutuste vahel.

2. EU-CyCLONe-sse kuuluvad liikmesriikide küberkriisi ohjamise asutuste esindajad ning juhul, kui võimalikul või jätkuval ulatuslikul küberturbeintsidendil on või tõenäoliselt on oluline mõju käesoleva direktiivi kohaldamisalasse kuuluvatele teenustele ja tegevustele, komisjoni esindajad. Muudel juhtudel osaleb komisjon EU-CyCLONe tegevuses vaatlejana.

ENISA tagab EU-CyCLONe jaoks sekretariaaditeenused ja toetab turvalist teabevahetust ning pakub vajalikke vahendeid liikmesriikide vahelise koostöö toetamiseks, tagades turvalise teabevahetuse.

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

3. EU-CyCLONe ülesanded on järgmised:

a) tõsta valmisoleku taset ulatuslike küberturbeintsidentide ja kriiside ohjamiseks;

b) arendada ühist olukorrateadlikkust ulatuslike küberturbeintsidentide ja kriiside korral;

c) hinnata ulatuslike küberturbeintsidentide ja kriiside tagajärgi ja mõju ning pakkuda välja võimalikke leevendusmeetmeid;

d) koordineerida ulatuslike küberturbeintsidentide ja kriiside ohjamist ning toetada selliste intsidentide ja kriisidega seotud otsuste tegemist poliitilisel tasandil;

e) arutada asjaomase liikmesriigi taotlusel artikli 9 lõikes 4 osutatud riiklikke ulatuslike küberturbeintsidentide ja kriiside lahendamise kavasid.

4. EU-CyCLONe võtab vastu oma töökorra.

5. EU-CyCLONe esitab koostöörühmale korrapäraselt ulatuslike küberturbeintsidentide ja kriiside ohjamist ning suundumusi käsitleva aruande, keskendudes eelkõige mõjule, mida need avaldavad elutähtsatele ja olulistele üksustele.

6. EU-CyCLONe teeb CSIRTide võrgustikuga koostööd artikli 15 lõikes 6 sätestatud kokkulepitud menetluskorra alusel.

7. Hiljemalt 17. juuliks 2024 ning seejärel iga 18 kuu järel esitab EU-CyCLONe Euroopa Parlamendile ja nõukogule oma tööd hindava aruande.

Artikkel 17

Rahvusvaheline koostöö

Kui see on kohane, võib liit kooskõlas ELi toimimise lepingu artikliga 218 sõlmida kolmandate riikide või rahvusvaheliste organisatsioonidega rahvusvahelisi lepinguid, mis võimaldavad neil osaleda ja korraldada osalust mõningates koostöörühma, CSIRTide võrgustiku ning EU-CyCLONe tegevustes. Sellised lepingud peavad olema kooskõlas liidu andmekaitseõigusega.

Artikkel 18

Aruanne küberturvalisuse olukorra kohta liidus

1. ENISA võtab koostöös komisjoni ja koostöörühmaga iga kahe aasta järel vastu aruande, mis käsitleb küberturvalisuse olukorda liidus, ning esitab selle ja tutvustab seda Euroopa Parlamendile. Aruanne tehakse muu hulgas kättesaadavaks masinloetavate andmetega ning sisaldab järgmist:

a) liidu tasandi küberturvalisuse riskihindamine, mille puhul võetakse arvesse küberohtude kaardistamist;

b) hinnang küberturvalisuse alase võimekuse kohta kogu liidu avalikus ja erasektoris;

c) hinnang kodanike ja üksuste, sealhulgas väikeste ja keskmise suurusega ettevõtjate küberturvalisuse alase teadlikkuse ja küberhügieeni üldise taseme kohta;

d) koondhinnang artiklis 19 osutatud vastastikuse hindamise tulemuste kohta;

e) koondhinnang küberturvalisuse alase võimekuse ja ressursside küpsuse taseme kohta kogu liidus, sealhulgas sektori tasandil, ning selle kohta, mil määral on liikmesriikide riiklikud küberturvalisuse strateegiad omavahel kooskõlas.

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

3. ENISA töötab koostöös komisjoni, koostöörühma ja CSIRTide võrgustikuga välja metoodika, mis hõlmab lõike 1 punktis e osutatud koondhinnangu asjaomaseid muutujaid, nagu kvantitatiivsed ja kvalitatiivsed näitajad.

Artikkel 19

Vastastikune hindamine

1. Koostöörühm töötab 17. jaanuariks 2025 komisjoni ja ENISA ning, kui see on asjakohane, CSIRTide võrgustiku abiga välja vastastikuse hindamise metoodika ja korralduslikud aspektid, et õppida jagatud kogemustest, tugevdada vastastikust usaldust, saavutada küberturvalisuse ühtlaselt kõrge tase ning suurendada liikmesriikide küberturvalisuse alast võimekust ja poliitikat, mis on vajalik käesoleva direktiivi rakendamiseks. Vastastikuses hindamises osalemine on vabatahtlik. Vastastikuse hindamise viivad läbi küberturvalisuse valdkonna eksperdid. Küberturvalisuse eksperdid määravad vähemalt kaks liikmesriiki, mis on muud liikmesriigid kui see, mida hinnatakse.

Vastastikuse hindamise raames hinnatakse vähemalt ühte järgmistest aspektidest:

a) artiklites 21 ja 23 sätestatud küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse rakendamise tase;

b) võimekuse tase, sealhulgas olemasolevad rahalised, tehnilised ja inimressursid, ning pädevate asutuste ülesannete täitmise tõhusus;

c) CSIRTide tegevusvõimekus;

d) artiklis 37 osutatud vastastikuse abi rakendamise tase;

e) artiklis 29 osutatud küberturvalisuse alase teabevahetuse kokkulepete rakendamise tase;

f) piiriülese või valdkonnaülese iseloomuga eriküsimused.

2. Lõikes 1 osutatud metoodika sisaldab objektiivseid, mittediskrimineerivaid, õiglasi ja läbipaistvaid kriteeriume, mille alusel liikmesriigid määravad vastastikuse hindamise läbiviimiseks sobivad küberturvalisuse valdkonna eksperdid. ENISA ja komisjon osalevad vastastikuses hindamises vaatlejatena.

3. Liikmesriigid võivad määrata kindlaks lõike 1 punktis f osutatud eriküsimused vastastikuseks hindamiseks.

4. Enne lõikes 1 osutatud vastastikuse hindamise alustamist teatavad liikmesriigid osalevatele liikmesriikidele selle ulatuse, sealhulgas lõike 3 kohaselt kindlaks määratud eriküsimused.

5. Enne vastastikuse hindamise algust võib liikmesriik teha vaatlusaluste aspektide enesehindamise ja esitada selle määratud küberturvalisuse ekspertidele. Liikmesriikide enesehindamise metoodika kehtestab komisjoni ja ENISA abiga koostöörühm.

6. Vastastikune hindamine hõlmab kohapealseid või virtuaalseid külastusi ja teabevahetust väljaspool tegevuskohta. Kooskõlas hea koostöö põhimõttega esitab liikmesriik, keda vastastikku hinnatakse, määratud küberturvalisuse 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. Koostöörühm töötab koostöös komisjoni ja ENISAga välja asjakohased tegevusjuhendid, millele määratud küberturvalisuse ekspertide töömeetodid toetuvad. Vastastikuses hindamises saadavat teavet kasutatakse üksnes hindamise eesmärgil. Vastastikuses hindamises osalevad küberturvalisuse valdkonna eksperdid ei avalda vastastikuse hindamise käigus saadud tundlikku või konfidentsiaalset teavet kolmandatele isikutele.

7. Liikmesriigis juba vastastikku hinnatud aspektid ei kuulu kõnealuses liikmesriigis enam vastastikusele hindamisele kahe aasta jooksul pärast vastastikuse hindamise lõppemist, välja arvatud juhul, kui seda taotleb liikmesriik või nii lepitakse kokku pärast koostöörühma ettepanekut.

8. Liikmesriigid tagavad, et määratud küberturvalisuse ekspertidega seotud huvide konflikti oht tehakse enne vastastikuse hindamise algust teatavaks teistele liikmesriikidele, koostöörühmale, komisjonile ja ENISA-le. Liikmesriik, keda vastastikku hinnatakse, võib esitada vastuväiteid konkreetsete küberturvalisuse ekspertide määramisele piisavalt põhjendatud juhtudel, millest on teatatud määravale liikmesriigile.

9. Vastastikuses hindamises osalevad küberturvalisuse eksperdid koostavad aruanded vastastikuse hindamise tulemuste ja järelduste kohta. Liikmesriigid, keda vastastikku hinnatakse, võivad esitada märkusi neid käsitlevate aruannete kavandite kohta ning sellised märkused lisatakse aruannetele. Aruanded sisaldavad soovitusi vastastikuse hindamisega hõlmatud aspektide parandamiseks. Aruanded esitatakse koostöörühmale ja CSIRTide võrgustikule, kui see on asjakohane. Liikmesriik, keda vastastikku hinnatakse, võib otsustada teha oma aruande või selle toimetatud versiooni üldsusele kättesaadavaks.

IV PEATÜKK

KÜBERTURVALISUSEGA SEOTUD RISKIJUHTIMISMEETMED JA TEATAMISKOHUSTUS

Artikkel 20

Juhtimine

1. Liikmesriigid tagavad, et elutähtsate ja oluliste üksuste juhtorganid kiidavad heaks küberturvalisuse riskijuhtimismeetmed, mida nimetatud üksused on võtnud artikli 21 järgimiseks, jälgivad nende rakendamist ning neid üksusi võib võtta vastutusele kõnealuse artikli rikkumise eest.

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 elutähtsate ja oluliste üksuste juhtorganite liikmed on kohustatud läbima korrapäraselt erikoolitusi, ning ergutavad elutähtsaid ja olulisi üksusi pakkuma sarnaseid koolitusi korrapäraselt oma töötajatele, et nad saaksid omandada piisavad teadmised ja oskused, et mõista ja hinnata küberturvalisuse riske ja nende juhtimise tavasid ning nendest tulenevat mõju üksuse osutatavatele teenustele.

Artikkel 21

Küberturvalisuse riskijuhtimismeetmed

1. Liikmesriigid tagavad, et elutähtsad ja olulised üksused võtavad asjakohased ja proportsionaalsed tehnilised, tegevuslikud ja korralduslikud meetmed, et juhtida riske, mis ohustavad nende üksuste tegevuses või teenuste osutamisel kasutatavate võrgu- ja infosüsteemide turvalisust, ning et ennetada või minimeerida intsidentide mõju nende teenuste saajatele ja muudele teenustele.

Võttes arvesse kaasaegseid ning, kui see on kohaldatav, asjakohaseid Euroopa ja rahvusvahelisi standardeid ja rakendamiskulusid tagatakse esimeses lõigus osutatud meetmetega ähvardavale ohule vastav võrgu- ja infosüsteemide turvalisuse tase. Nende meetmete proportsionaalsuse hindamisel võetakse igakülgselt arvesse üksuse riskidele avatuse määra, üksuse suurust ning intsidentide esinemise tõenäosust ja nende tõsidust, sealhulgas nende ühiskondlikku ja majanduslikku mõju.

2. Lõikes 1 osutatud meetmed põhinevad kõiki ohte hõlmaval lähenemisviisil, mille eesmärk on kaitsta võrgu- ja infosüsteeme ning nende süsteemide füüsilist keskkonda intsidentide eest, ning hõlmavad vähemalt järgmist:

a) riskianalüüsi ja infosüsteemide turbe põhimõtteid;

b) intsidentide käsitlemist;

c) talitluspidevust, näiteks varundushaldus ja avariitaaste, ning kriisiohjet;

d) tarneahela turvalisust, sealhulgas sellised turvalisusesse puutuvad aspektid, mis on seotud iga üksuse ja tema otseste tarnijate või teenuseosutajate vaheliste suhetega;

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

f) tööpõhimõtteid ja menetluskorda küberturvalisuse riskijuhtimismeetmete tõhususe hindamiseks;

g) küberhügieeni põhitavasid ja küberturvalisuse koolitust;

h) krüptograafia ja, kui see on kohane, krüpteerimise kasutamise põhimõtteid ja menetlusi;

i) personali turvalisust, juurdepääsukontrolli põhimõtteid ja varade haldust;

j) kui see on kohane, mitmikautentimise või pidevautentimise lahenduste, turvalise hääl-, video- ja tekstiside ning turvaliste hädaolukorra sidesüsteemide kasutamist üksuses.

3. Liikmesriigid tagavad, et käesoleva artikli lõike 2 punktis d osutatud meetmete asjakohasust kaaludes võtavad üksused arvesse 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 nimetatud punktis osutatud meetmete asjakohasust kaaludes võtavad üksused arvesse artikli 22 lõike 1 kohaselt korraldatud kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamiste tulemusi.

4. Liikmesriigid tagavad, et üksus, kes leiab, et ta ei järgi lõikes 2 sätestatud meetmeid, võtab põhjendamatu viivituseta kõik vajalikud, asjakohased ja proportsionaalsed parandusmeetmed.

5. Hiljemalt 17. oktoobriks 2024 võtab komisjon vastu rakendusaktid, milles sätestatakse lõikes 2 osutatud meetmete tehnilised ja metoodilised nõuded seoses domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate, hallatud teenuse osutajate, turbetarnijate, internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite ning sotsiaalvõrguteenuse platvormide ja usaldusteenuse pakkujatega.

Komisjon võib võtta vastu rakendusakte, milles sätestatakse lõikes 2 osutatud meetmete tehnilised ja metoodilised ning vajaduse korral valdkondlikud nõuded seoses muude kui käesoleva lõike esimeses lõigus osutatud elutähtsate ja oluliste üksustega.

Käesoleva lõike esimeses ja teises lõigus osutatud rakendusaktide ettevalmistamisel järgib komisjon võimalikult suures ulatuses Euroopa ja rahvusvahelisi standardeid ning asjakohaseid tehnilisi spetsifikatsioone. Komisjon peab kooskõlas artikli 14 lõike 4 punktiga e rakendusaktide eelnõude osas koostöörühma ja ENISAga nõu ning teeb nendega koostööd.

Kõnealused rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 22

Liidu tasandi kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamised

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

2. Komisjon määrab pärast koostöörühma ja ENISAga ning vajaduse korral asjaomaste sidusrühmadega konsulteerimist kindlaks konkreetsed kriitilise tähtsusega IKT-teenused, IKT-süsteemid või IKT-tooted, mille suhtes võib kohaldada lõikes 1 osutatud turberiski koordineeritud hindamist.

Artikkel 23

Teatamiskohustus

1. Liikmesriigid tagavad, et elutähtsad ja olulised üksused teavitavad põhjendamatu viivituseta oma CSIRTi või, kui see on kohaldatav, oma pädevat asutust vastavalt lõikele 4 kõikidest intsidentidest, mis nende teenuste osutamist märkimisväärselt mõjutavad, nagu on osutatud lõikes 3 (edaspidi „oluline intsident“). Kui see on asjakohane, teavitavad asjaomased üksused põhjendamatu viivituseta oma teenuste kasutajaid olulistest intsidentidest, mis tõenäoliselt kahjustavad kõnealuse teenuse osutamist. Liikmesriigid tagavad, et need üksused esitavad muu hulgas teabe, mis võimaldab CSIRTil või, kui see on kohaldatav, pädeval asutusel teha kindlaks intsidendi piiriülese mõju. Pelgalt teatamisega teavitava üksuse vastutus ei suurene.

Kui asjaomased üksused teavitavad pädevat asutust olulisest intsidendist esimese lõigu alusel, tagab liikmesriik, et kõnealune pädev asutus edastab teate selle kättesaamisel CSIRTile.

Piiriülese või sektoriülese olulise intsidendi korral tagavad liikmesriigid, et nende ühtsetele kontaktpunktidele antakse aegsasti asjakohast teavet kooskõlas lõikega 4.

2. Kui see on kohaldatav, tagavad liikmesriigid, et elutähtsad ja olulised üksused teavitavad 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 teenuse saajaid ka olulisest küberohust endast.

3. Intsidenti käsitatakse olulisena, kui:

a) see on põhjustanud või võib põhjustada asjaomase üksuse teenuste osutamisel tõsiseid tegevushäireid või rahalist kahju;

b) see 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 CSIRTile või, kui see on kohaldatav, pädevale asutusele järgmise:

a) põhjendamatu viivituseta ning igal juhul hiljemalt 24 tunni jooksul pärast olulisest intsidendist teada saamist varajase hoiatuse, milles märgitakse (kui see kohaldatav), kas olulise intsidendi põhjuseks on eeldatavasti ebaseaduslik või pahatahtlik tegevus või kas sellel võib olla piiriülene mõju;

b) põhjendamatu viivituseta ja igal juhul 72 tunni jooksul pärast olulisest intsidendist teadlikuks saamist intsidenditeate, millega, kui see on kohaldatav, ajakohastatakse punktis a osutatud teavet ning antakse esialgne hinnang olulisele intsidendile, sealhulgas selle tõsidusele ja mõjule ning võimaluse korral ka rikkeindikaatoritele;

c) CSIRTi või, kui see on kohaldatav, pädeva asutuse taotlusel vahearuande vaatlusaluste asjade seisu kohta;

d) ühe kuu jooksul pärast punktis b osutatud intsidenditeate esitamist lõpparuande, mis sisaldab järgmist:

   i) intsidendi, sealhulgas selle tõsiduse ja mõju üksikasjalik kirjeldus;

   ii) ohu liik või lähtepõhjus, mis intsidendi tõenäoliselt põhjustas;

   iii) juba kohaldatud ja kohaldamisel olevad leevendusmeetmed;

   iv) kui see on kohaldatav, intsidendi piiriülene mõju;

e) kui intsident punktis d osutatud lõpparuande esitamise ajal jätkub, peavad liikmesriigid tagama, et asjaomased üksused esitavad sel ajal vahearuande ja ühe kuu jooksul pärast intsidendi nendepoolset käsitlemist lõpparuande.

Erandina esimese lõigu punktist b teavitab usaldusteenuse osutaja oma usaldusteenuste osutamist mõjutavatest olulistest intsidentidest CSIRTi või, kui see on kohaldatav, pädevat asutust põhjendamatu viivituseta ja igal juhul 24 tunni jooksul pärast olulisest intsidendist teada saamist.

5. CSIRT või pädev asutus annab põhjendamatu viivituseta ja võimaluse korral 24 tunni jooksul pärast lõike 4 punktis a osutatud varajase hoiatuse saamist teavitavale üksusele vastuse, mis sisaldab esialgset tagasisidet olulise intsidendi kohta ja üksuse taotluse korral võimalike leevendusmeetmete rakendamise suuniseid või nõu, kuidas toimida. Kui CSIRT ei ole lõikes 1 osutatud teate algne saaja, annab mainitud suunised pädev asutus koostöös CSIRTiga. CSIRT pakub täiendavat tehnilist tuge, kui asjaomane üksus seda taotleb. Kui kahtlustatakse, et oluline intsident on kuritegelik, annab CSIRT või pädev asutus ka juhiseid olulisest intsidendist õiguskaitseasutuste teavitamiseks.

6. Kui see on asjakohane ja eelkõige juhul, kui oluline intsident puudutab kahte või enamat liikmesriiki, peab CSIRT, pädev asutus või ühtne kontaktpunkt teavitama olulisest intsidendist põhjendamatu viivituseta teisi mõjutatud liikmesriike ja ENISAt. Teavitus peab sisaldama sellist liiki teavet, mis on saadud lõike 4 kohaselt. Seda tehes kaitsevad CSIRT, pädev asutus või ühtne kontaktpunkt kooskõlas liidu või liikmesriigi õigusega üksuse turvalisust ja ärihuve ning esitatud teabe konfidentsiaalsust.

7. Kui üldsuse teadlikkus või intsidendi avalikustamine on vajalik olulise intsidendi ärahoidmiseks või olulise intsidendi lahendamiseks või muul moel üldsuse huvides, võivad liikmesriigi CSIRT või, kui see on kohaldatav, pädev asutus ning, kui see on kohane, ka teiste asjaomaste liikmesriikide CSIRTid või pädevad asutused teavitada pärast asjaomase üksusega konsulteerimist olulisest intsidendist üldsust või nõuda, et seda teeks asjaomane üksus.

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

9. Ühtne kontaktpunkt esitab ENISA-le iga kolme kuu tagant koondaruande, mis sisaldab anonüümseid koondandmeid käesoleva artikli lõike 1 ning artikli 30 kohaselt teatatud oluliste intsidentide, intsidentide, küber- ja intsidendiohtude kohta. Teabe võrreldavuse tagamiseks võib ENISA võtta kokkuvõtvas aruandes esitatava teabe parameetrite kohta vastu tehnilisi suuniseid. ENISA teavitab koostöörühma ja CSIRTide võrgustikku oma järeldustest saadud teadete kohta iga kuue kuu järel.

10. CSIRTid või, kui see on kohaldatav, pädevad asutused esitavad direktiivi (EL) 2022/2557 kohastele pädevatele asutustele teabe oluliste intsidentide, intsidentide, küber- ja intsidendiohtude kohta, millest on käesoleva artikli lõike 1 ja artikli 30 kohaselt teatanud üksused, mida käsitatakse direktiivi (EL) 2022/2557 alusel elutähtsa teenuse osutajatena.

11. Komisjon võib võtta vastu rakendusakte, milles täpsustatakse käesoleva artikli lõike 1 ja artikli 30 kohaselt esitatava teate ning käesoleva artikli lõike 2 kohase teavituse teabeliik, -vorming ning esitamise kord.

Hiljemalt 17. oktoobriks 2024 võtab komisjon seoses domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, pilvandmetöötlusteenuste osutajate, andmekeskusteenuste osutajate, sisulevivõrgu pakkujate, hallatud teenuse osutajate, turbetarnijate ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite ja sotsiaalvõrguteenuse platvormide pakkujatega vastu rakendusaktid, millega täpsustatakse, millisel juhul käsitatakse intsidenti olulisena, nagu on osutatud lõikes 3. Komisjon võib selliseid rakendusakte vastu võtta ka seoses muude elutähtsate ja oluliste üksustega.

Komisjon peab kooskõlas artikli 14 lõike 4 punktiga e käesoleva lõike esimeses ja teises lõigus osutatud rakendusaktide eelnõude osas koostöörühmaga nõu ja teeb temaga koostööd.

Kõnealused rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 24

Euroopa küberturvalisuse sertifitseerimise kavade kasutamine

1. Liikmesriigid võivad nõuda elutähtsatelt ja olulistelt üksustelt artikli 21 teatavatele nõuetele vastavuse tõenduseks teatavate IKT-toodete, IKT-teenuste ja IKT-protsesside kasutamist, mille on välja töötanud elutähtis või oluline üksus või mis on hangitud kolmandatelt isikutelt ning mis on sertifitseeritud määruse (EL) 2019/881 artikli 49 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavade alusel. Lisaks ergutavad liikmesriigid elutähtsaid ja olulisi üksusi kasutama kvalifitseeritud usaldusteenuseid.

2. Komisjonil on õigus võtta kooskõlas artikliga 38 vastu delegeeritud õigusakte, et täiendada käesolevat direktiivi, määrates kindlaks, mis liiki elutähtsatelt ja olulistelt üksustelt nõutakse teatavate IKT-toodete, IKT-teenuste ja IKT-protsesside kasutamist või sertifikaadi omandamist määruse (EL) 2019/881 artikli 49 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava alusel. Need delegeeritud õigusaktid võetakse vastu juhul, kui on kindlaks tehtud, et küberturvalisuse tase ei ole piisav, ja nendega nähakse ette rakendusperiood.

Enne selliste delegeeritud õigusaktide vastuvõtmist teeb komisjon mõjuhinnangu ja korraldab konsultatsioone kooskõlas määruse (EL) 2019/881 artikliga 56.

3. Kui asjakohast Euroopa küberturvalisuse sertifitseerimise kava käesoleva artikli lõike 2 kohaldamiseks ei ole, võib komisjon pärast koostöörühma ja Euroopa küberturvalisuse sertifitseerimise rühmaga konsulteerimist taotleda määruse (EL) 2019/881 artikli 48 lõike 2 kohaselt ENISA-lt ettevalmistava kava koostamist.

Artikkel 25

Standardimine

1. Artikli 21 lõigete 1 ja 2 ühtse kohaldamise edendamiseks toetavad liikmesriigid võrgu- ja infosüsteemide turvalisust käsitlevate Euroopa ja rahvusvaheliste standardite ja tehniliste spetsifikatsioonide rakendamist, ilma et nad seejuures nõuaksid või diskrimineerivalt soosiksid konkreetset tüüpi tehnoloogia kasutamist.

2. ENISA koostab koostöös liikmesriikidega ja, kui see on kohane, pärast konsulteerimist asjaomaste sidusrühmadega nõuanded ja suunised seoses tehniliste valdkondadega, mida tuleb lõike 1 puhul arvesse võtta, ning seoses olemasolevate, sealhulgas riiklike standarditega, mis võimaldaksid neid valdkondi hõlmata.

V PEATÜKK

JURISDIKTSIOON JA REGISTREERIMINE

Artikkel 26

Jurisdiktsioon ja territoriaalsus

1. Käesoleva direktiivi kohaldamisalasse kuuluvaid üksusi loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on nende tegevuskoht või kus nad on asutatud, välja arvatud järgmistel juhtudel:

a) üldkasutatavate elektroonilise side võrkude pakkujaid või üldkasutatavate elektroonilise side teenuste osutajaid loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus nad oma teenuseid osutavad;

b) domeeninimede süsteemi teenuse osutajaid, tippdomeeninimede registreid, domeeninimede registreerimise teenuseid osutavaid üksusi, pilvandmetöötlusteenuse osutajaid, andmekeskusteenuse osutajaid, sisulevivõrgu pakkujaid, hallatud teenuse osutajaid, turbetarnijaid ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite ja sotsiaalvõrguteenuse platvormide pakkujaid loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on nende lõike 2 kohane peamine tegevuskoht liidus;

c) avaliku halduse üksusi loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kes nad asutas.

2. Käesoleva direktiivi kohaldamisel käsitatakse lõike 1 punktis b osutatud üksuse peamise tegevuskohana seda liidu liikmesriiki, kus küberturvalisuse riskijuhtimismeetmeid käsitlevad otsused valdavalt tehakse. Kui sellist liikmesriiki ei ole võimalik kindlaks määrata või kui selliseid otsuseid ei tehta liidus, käsitatakse peamise tegevuskohana seda liikmesriiki, kus toimub küberturvalisuse alane tegevus. Kui sellist liikmesriiki ei ole võimalik kindlaks määrata, käsitatakse peamise tegevuskohana seda liikmesriiki, mille territooriumil on asjaomasel üksusel tegevuskoht liidus kõige suurema arvu töötajatega.

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

4. Esindaja määramine lõike 1 punktis b osutatud üksuse poolt ei piira õiguslike meetmete võtmist üksuse enda vastu.

5. Liikmesriik, kes on saanud seoses lõike 1 punktis b osutatud üksusega vastastikuse abi taotluse, võib võtta kõnealuse üksuse suhtes, mis osutab selle riigi territooriumil teenuseid või millel on seal võrgu- ja infosüsteem, taotluse ulatuses asjakohaseid järelevalve- ja täitemeetmeid.

Artikkel 27

Üksuste register

1. ENISA loob ühtsetelt kontaktpunktidelt lõike 4 kohaselt saadud teabe põhjal domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, domeeninimede registreerimise teenuseid osutavate üksuste, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate, hallatud teenuse osutajate ja turbetarnijate ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite ja sotsiaalvõrguteenuse platvormide pakkujate registri ning haldab seda. Taotluse korral võimaldab ENISA pädevatele asutustele kõnealusele registrile juurdepääsu, tagades samal ajal teabe konfidentsiaalsuse kaitses, kui see on kohaldatav.

2. Liikmesriigid nõuavad lõikes 1 osutatud üksustelt hiljemalt 17. jaanuariks 2025 järgmise teabe esitamist pädevatele asutustele:

a) üksuse nimi;

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

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

d) üksuse ja, kui see on kohaldatav, tema artikli 26 lõike 3 kohaselt määratud esindaja ajakohased kontaktandmed, sealhulgas e-posti aadressid ja telefoninumbrid;

e) liikmesriigid, kus üksus teenust osutab, ning

f) üksuse IP-vahemikud.

3. Liikmesriigid tagavad, et lõikes 1 osutatud üksused teavitavad pädevat asutust viivitamata lõike 2 kohaselt esitatud teabe muutumisest, tehes seda igal juhul hiljemalt kolme kuu jooksul alates muudatuse kuupäevast.

4. Lõigetes 2 ja 3 osutatud teabe, välja arvatud lõike 2 punktis f osutatud teave, kättesaamisel edastab asjaomase liikmesriigi ühtne kontaktpunkt selle põhjendamatu viivituseta ENISA-le.

5. Kui see on kohaldatav, esitatakse käesoleva artikli lõigetes 2 ja 3 osutatud teave artikli 3 lõike 4 neljandas lõigus osutatud riikliku mehhanismi kaudu.

Artikkel 28

Domeeninimede registreerimisandmete andmebaas

1. Et aidata suurendada domeeninimede süsteemi turvalisust, stabiilsust ja vastupanuvõimet, nõuavad liikmesriigid, et tippdomeeninimede registrid ja tippdomeenide domeeninimede registreerimise teenuseid osutavad üksused koguksid ja säilitaksid täpseid ja täielikke domeeninimede registreerimise andmeid spetsiaalses andmebaasis, kohaldades isikuandmetena käsitatavate andmetega seoses hoolsust kooskõlas liidu andmekaitseõigusega.

2. Lõike 1 kohaldamiseks nõuavad liikmesriigid, et domeeninimede registreerimisandmete andmebaas sisaldaks vajalikku teavet, mis võimaldab tuvastada domeeninimede omanikud ja tippdomeenide alldomeeninimesid haldavad kontaktpunktid ning nendega ühendust võtta. Selline teave sisaldab järgmist:

a) domeeninimi;

b) registreerimise kuupäev;

c) registreerija nimi, e-posti aadress ja telefoninumber;

d) domeeninime haldava kontaktpunkti e-posti aadress ja telefoninumber, kui see erineb registreerija omast.

3. Liikmesriigid nõuavad, et tippdomeeninimede registritel ja tippdomeenide domeeninimede registreerimise teenuseid osutavatel üksustel oleksid töö põhimõtted ja menetluskord, sealhulgas kontrollimenetlused, millega tagatakse, et lõikes 1 osutatud andmebaasid sisaldavad täpset ja täielikku teavet. Liikmesriigid nõuavad, et sellised põhimõtted ja menetluskord tehtaks üldsusele kättesaadavaks.

4. Liikmesriigid nõuavad, et tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused teeksid põhjendamatu viivituseta pärast domeeninime registreerimist üldsusele kättesaadavaks need domeeninimede registreerimisandmed, mis ei ole isikuandmed.

5. Liikmesriigid nõuavad, et tippdomeeninimede registrid ja domeeninimede registreerimise teenuseid osutavad üksused võimaldaksid õigustatud taotlejatele õiguspärast ja piisavalt põhjendatud juurdepääsu domeeninimede registreerimisandmetele kooskõlas liidu andmekaitseõigusega. Liikmesriigid nõuavad, et tippdomeeninimede registrid ja domeeninime registreerimise teenuseid osutavad üksused vastaksid juurdepääsutaotlustele põhjendamatu viivituseta ja igal juhul 72 tunni jooksul pärast juurdepääsutaotluse saamist. Liikmesriigid nõuavad, et selliste andmete avalikustamise põhimõtted ja kord tehtaks üldsusele kättesaadavaks.

6. Lõigetes 1–5 sätestatud kohustuste täitmine ei tohi kaasa tuua domeeninimede registreerimisandmete topeltkogumist. Selleks nõuavad liikmesriigid, et tippdomeeninimede registrid ja domeeninime registreerimise teenuseid osutavad üksused teeksid omavahel koostööd.

VI PEATÜKK

TEABEVAHETUS

Artikkel 29

Küberturvalisuse alase teabevahetuse kokkulepped

1. Liikmesriigid tagavad, et käesoleva direktiivi kohaldamisalasse kuuluvad üksused ning, kui see on asjakohane, muud üksused, mis ei kuulu käesoleva direktiivi kohaldamisalasse, saavad omavahel vabatahtlikult vahetada asjakohast küberturvalisuse alast teavet, sealhulgas teavet, mis on seotud küberohtude, intsidendiohtude, nõrkuste, meetodite ja menetluste, rikkeindikaatorite, kahjulike taktikate, ohusubjekti spetsiifilise teabe, küberturvalisuse hoiatuste ning soovitustega küberturvalisuse vahendite konfiguratsiooni kohta küberrünnete tuvastamiseks, kui selline teabevahetus:

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, ohjamise ja ennetamise meetodeid, leevendusstrateegiaid, lahendamis- ja taastamisetappe ning avaliku ja erasektori üksuste koostöös toimuvat küberohtude uurimist.

2. Liikmesriigid tagavad, et teabevahetus toimub elutähtsate ja oluliste üksuste ning asjakohasel juhul nende tarnijate või teenuseosutajate kogukondades. Kõnealune teabevahetus toimub küberturvalisuse alase teabevahetuse kokkulepete alusel, pidades silmas jagatud teabe potentsiaalselt tundlikku laadi.

3. Liikmesriigid hõlbustavad käesoleva artikli lõikes 2 osutatud küberturvalisuse alase teabevahetuse kokkulepete sõlmimist. Sellistes kokkulepetes võidakse täpsustada teabevahetuse korraldusega seotud tegevusaspekte (sealhulgas sihtotstarbeliste IKT-platvormide ja automatiseerimisvahendite kasutamine), sisu ja tingimusi. Liikmesriigid võivad nende üksikasjade sätestamisel, mis puudutavad avaliku sektori asutuste osalemist sellistes kokkulepetes, kehtestada pädevate asutuste või CSIRTide poolt kättesaadavaks tehtud teabele tingimusi. Liikmesriigid toetavad selliste kokkulepete rakendamist lähtuvalt artikli 7 lõike 2 punktis h osutatud poliitikameetmetest.

4. Liikmesriigid tagavad, et elutähtsad ja olulised üksused teavitavad pädevaid asutusi oma osalemisest lõikes 2 osutatud küberturvalisuse alase teabevahetuse kokkulepetes, kui nad on selliste kokkulepetega ühinenud, või, kui see on asjakohane, kokkulepetest taganemisest pärast taganemise jõustumist.

5. ENISA toetab lõikes 2 osutatud küberturvalisuse alase teabevahetuse alaste kokkulepete sõlmimist, vahetades parimaid tavasid ja andes suuniseid.

Artikkel 30

Vabatahtlik teavitamine asjakohasest teabest

1. Liikmesriigid tagavad, et lisaks artiklis 23 sätestatud teatamiskohustusele võivad CSIRTidele või, kui see on kohaldatav, pädevatele asutustele vabatahtlikult teatada:

a) elutähtsad ja olulised üksused intsidentidest, küber- ja intsidendiohtudest;

b) muud kui punktis a osutatud üksused olenemata sellest, kas nad kuuluvad käesoleva direktiivi kohaldamisalasse, olulistest intsidentidest, küber- ja intsidendiohtudest.

2. Lõikes 1 osutatud teadete läbivaatamisel järgivad liikmesriigid artiklis 23 sätestatud menetluskorda. Liikmesriigid võivad seada kohustuslike teadete menetlemise vabatahtlike teadete menetlemisest tähtsamale kohale.

Vajaduse korral annavad CSIRTid ja, kui see on kohaldatav, pädevad asutused ühtsetele kontaktpunktidele teavet käesoleva artikli kohaselt saadud teadete kohta, tagades seejuures teavitava üksuse esitatud teabe konfidentsiaalsuse ja asjakohase kaitse. Ilma et see piiraks kuritegude ennetamist, uurimist, avastamist ja nende eest vastutusele võtmist, ei kaasne vabatahtliku teavitamisega teavitava üksuse jaoks mingeid täiendavaid kohustusi, mida tal ei oleks olnud, kui ta ei oleks teadet esitanud.

VII PEATÜKK

JÄRELEVALVE JA TÄITMISE TAGAMINE

Artikkel 31

Järelevalve ja täitmise tagamise üldised aspektid

1. Liikmesriigid tagavad, et nende pädevad asutused teevad käesoleva direktiivi täitmise tagamiseks tõhusat järelevalvet ning võtavad selleks vajalikke meetmeid.

2. Liikmesriigid võivad lubada oma pädevatel asutustel järelevalveülesandeid prioriseerida. Selline prioriseerimine põhineb riskipõhisel lähenemisviisil. Selleks võivad pädevad asutused kehtestada artiklites 32 ja 33 sätestatud järelevalveülesannete täitmisel järelevalvemeetodid, mis võimaldavad ülesandeid riskipõhise lähenemisviisi alusel prioriseerida.

3. Kui intsidendiga kaasneb isikuandmetega seotud rikkumine, teevad pädevad asutused selle lahendamisel tihedat koostööd määruse (EL) 2016/679 kohaste järelevalveasutustega, ilma et see piiraks kõnealuse määruse kohast järelevalveasutuste pädevust ja ülesandeid.

4. Ilma et see piiraks riigisiseste õigus- ja institutsiooniliste raamistike kohaldamist, tagavad liikmesriigid, et järelevalve tegemisel selle üle, kas avaliku halduse üksused täidavad käesoleva direktiivi nõudeid, ning võimalike täitemeetmete kohaldamisel seoses käesoleva direktiivi rikkumistega, on pädevatel asutustel asjakohased volitused selliste ülesannete täitmiseks ja nende tegevus on järelevalve alla kuuluvatest avaliku halduse üksustest sõltumatu. Liikmesriigid võivad otsustada, et kõnealuste üksuste suhtes kehtestatakse asjakohased, proportsionaalsed ja mõjusad järelevalve- ja täitemeetmed kooskõlas riigisiseste õigus- ja institutsiooniliste raamistikega.

Artikkel 32

Järelevalve- ja täitemeetmed seoses elutähtsate üksustega

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

2. Liikmesriigid tagavad, et pädevatel asutustel on elutähtsate üksustega seotud järelevalveülesannete täitmisel nende üksuste suhtes vähemalt järgmised õigused:

a) teha kohapealset kontrolli ja kaugjärelevalvet, sealhulgas pistelisi kontrolle, mida teevad eriväljaõppe saanud spetsialistid;

b) teha korrapäraseid ja sihipäraseid turvaauditeid, mida teeb sõltumatu organ või pädev asutus;

c) teha *ad hoc* auditeid, sealhulgas juhul, kui see on põhjendatud olulise intsidendi või käesoleva direktiivi rikkumisega elutähtsa üksuse poolt;

d) teha vajaduse korral koostöös asjaomase üksusega objektiivsetel, mittediskrimineerivatel, õiglastel ja läbipaistvatel riskihindamise kriteeriumidel põhinevaid turvalisuse kontrolle;

e) esitada teabenõudeid, mis on vajalikud üksuse võetud küberturvalisuse riskijuhtimismeetmete, sealhulgas tema dokumenteeritud küberturvalisuse põhimõtete hindamiseks ning samuti artikli 27 kohase pädevatele asutustele teabe edastamise kohustuse täitmise hindamiseks;

f) taotleda juurdepääsu andmetele, dokumentidele ja teabele, mis on vajalik järelevalveülesannete täitmiseks;

g) nõuda küberturvalisuse poliitika rakendamise tõendamist, näiteks kvalifitseeritud audiitori tehtud turvaauditite tulemusi ja nende aluseks olevaid tõendavaid dokumente.

Esimese lõigu punktis b osutatud sihipärased turvaauditid põhinevad pädeva asutuse või auditeeritava üksuse tehtud riskihindamisel või muul kättesaadaval riskialasel teabel.

Sihipärase turvaauditi tulemused tehakse kättesaadavaks pädevale asutusele. Sõltumatu organi poolt läbi viidava sihipärase turvaauditi kulud tasub auditeeritud üksus, välja arvatud igakülgselt põhjendatud juhtudel, kui pädev asutus otsustab teisiti.

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

4. Liikmesriigid tagavad, et nende pädevatel asutustel on elutähtsate üksustega seotud täitmise tagamise volituste rakendamisel vähemalt järgmised õigused:

a) teha hoiatusi käesoleva direktiivi rikkumiste kohta asjaomaste üksuste poolt;

b) võtta vastu siduvaid juhiseid, sealhulgas meetmete kohta, mis on vajalikud intsidendi ennetamiseks või heastamiseks, nende meetmete rakendamise tähtaegade ja rakendamisest aruandmise kohta, või korraldusi, millega nõutakse, et asjaomased üksused kõrvaldaksid tuvastatud puudused või heastaksid käesoleva direktiivi rikkumised;

c) anda asjaomastele üksustele korraldus lõpetada tegevus, mis rikub käesolevat direktiivi, ja hoiduda sellist tegevust kordamast;

d) kohustada asjaomaseid üksusi tagama, et nende riskijuhtimismeetmed vastavad artiklis 21 sätestatud nõuetele ning et nad täidavad artiklis 23 sätestatud teatamiskohustust kindlaksmääratud viisil ja kindlaksmääratud ajavahemiku jooksul;

e) kohustada asjaomaseid üksusi teavitama füüsilisi või juriidilisi isikuid, kellele nad osutavad teenuseid või pakuvad tegevusi, mida võib mõjutada oluline küberoht, ohu laadist ning võimalikest kaitse- või parandusmeetmetest, mida need füüsilised või juriidilised isikud võivad vastavale ohule reageerimiseks võtta;

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

g) määrata kindlaks ajavahemikuks seireametniku, kelle ülesanded on täpselt kindlaks määratud ning kes jälgib, kas asjaomased üksused täidavad artiklite 21 ja 23 nõudeid;

h) kohustada asjaomaseid üksusi avalikustama kindlaksmääratud viisil käesoleva direktiivi rikkumiste aspektid;

i) määrata või taotleda, et asjaomased organid või kohtud määraksid vastavalt liikmesriigi õigusele lisaks käesoleva lõike punktides a–h osutatud meetmele artikli 34 kohase haldustrahvi.

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

a) ajutiselt peatada, või nõuda, et sertifikaate või lube väljastav organ või kohus peataks kooskõlas liikmesriigi õigusega ajutiselt elutähtsa üksuse kõigi või mõnede osutatavate asjaomaste teenuste või läviviidavate tegevuste sertifikaadi või loa;

b) taotleda, et asjaomased organid või kohtud keelaksid kooskõlas liikmesriigi õigusega füüsilisel isikul, kes täidab selles elutähtsas üksuses tegevjuhina või seadusliku esindajana juhtimisülesandeid, selles üksuses ajutiselt juhtimisülesannete täitmise.

Vastavalt käesolevale lõikele kehtestatud ajutist peatamist või keeldu kohaldatakse ainult seni, kuni asjaomane üksus võtab vajalikud meetmed puuduste kõrvaldamiseks või pädeva asutuse nõuete täitmiseks, mille tõttu selliseid täitemeetmeid kohaldati. Sellise ajutise peatamise või keelu kehtestamise suhtes kohaldatakse kooskõlas liidu õiguse üldpõhimõtete ja hartaga asjakohaseid menetluslikke tagatisi, sealhulgas õigust tõhusale õiguskaitsevahendile ja õiglasele kohtumenetlusele, süütuse presumptsiooni ja kaitseõigust.

Käesolevas lõikes sätestatud täitemeetmeid ei kohaldata nende avaliku halduse üksuste suhtes, kelle suhtes kohaldatakse käesolevat direktiivi.

6. Liikmesriigid tagavad, et elutähtsa üksuse eest vastutaval või seda seaduslikult esindaval füüsilisel isikul, keda on volitatud üksust esindama, üksuse nimel otsuseid tegema või üksuse tegevust kontrollima, on pädevus tagada käesoleva direktiivi täitmine. Liikmesriigid tagavad, et selliseid füüsilisi isikuid on võimalik käesoleva direktiivi täitmata jätmise eest vastutusele võtta.

Avaliku halduse üksuste puhul ei piira käesolev lõige liikmesriigi õiguse kohaldamist seoses avalike teenistujate ning valitud ja ametisse nimetatud ametnike vastutusega.

7. Lõikes 4 või 5 osutatud täitemeetmete võtmisekorral järgivad pädevad asutused kaitseõigust ning arvestavad iga üksikjuhtumi asjaolusid, võttes nõuetekohaselt arvesse vähemalt järgmist:

a) rikkumise raskus ja rikutud sätete olulisus; raske rikkumisena käsitatakse muu hulgas alati järgmist:

   i) korduv rikkumine;

   ii) olulistest intsidentidest teatamata jätmine või parandusmeetmete võtmata jätmine;

   iii) pädevatelt asutustelt saadud siduvate juhiste järgi puuduste kõrvaldamata jätmine;

   iv) rikkumise tuvastamise järel pädevate asutuste tellitud auditite või järelevalvetegevuse takistamine;

   v) valeandmete või lubamatult ebatäpsete andmete esitamine seoses artiklites 21 ja 23 sätestatud küberturvalisuse riskijuhtimismeetmete või teatamiskohustusega;

b) rikkumise kestus;

c) asjaomase üksuse varasemad asjassepuutuvad rikkumised;

d) põhjustatud varaline või mittevaraline kahju, sealhulgas rahaline või majanduslik kahju, mõju teistele teenustele ja mõjutatud kasutajate arv;

e) rikkumise toimepanija tahtlus või hooletus;

f) meetmed, mida üksus on võtnud varalise või mittevaralise kahju ennetamiseks või vähendamiseks;

g) kinnitatud tegevusjuhendite järgimine või kinnitatud sertifitseerimismehhanismide rakendamine;

h) vastutavate füüsiliste või juriidiliste isikute ja pädevate asutuste koostöö tase.

8. Pädevad asutused esitavad oma täitemeetmete üksikasjaliku põhjenduse. Enne selliste meetmete võtmist teavitavad pädevad asutused asjaomaseid üksusi oma esialgsetest järeldustest. Samuti jätavad nad kõnealustele üksustele mõistliku aja märkuste esitamiseks, välja arvatud igakülgselt põhjendatud juhtudel, kui see takistaks intsidentide ennetamiseks või lahendamiseks vajalikku vahetut tegevust.

9. Liikmesriigid tagavad, et nende käesoleva direktiivi kohased pädevad asutused teavitavad oma liikmesriigi direktiivi (EL) 2022/2557 kohaseid asjaomaseid pädevaid asutusi, kui nad kasutavad oma järelevalve- ja täitmise tagamise volitusi, et tagada direktiivi (EL) 2022/2557 kohaselt elutähtsa teenuse osutajana käsitatava üksuse vastavus käesolevale direktiivile. Kui see on asjakohane, võivad direktiivi (EL) 2022/2557 kohased pädevad asutused taotleda käesoleva direktiivi kohastelt pädevatelt asutustelt, et nad kasutaksid oma järelevalve- ja täitmise tagamise volitusi üksuse suhtes, mida käsitatakse direktiivi (EL) 2022/2557 kohaselt elutähtsa teenuse osutajana.

10. Liikmesriigid tagavad, et nende käesoleva direktiivi kohased pädevad asutused teevad asjaomase liikmesriigi määruse (EL) 2022/2554 kohaste pädevate asutustega koostööd. Eelkõige tagavad liikmesriigid, et nende käesoleva direktiivi kohased pädevad asutused teavitavad määruse (EL) 2022/2554 artikli 32 lõike 1 kohaselt järelevaatamise foorumit, kui nad kasutavad oma järelevalve- ja täitmise tagamise volitusi, et tagada määruse (EL) 2022/2554 artikli 31 kohaselt kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajana käsitatava ja käesoleva direktiivi kohaldamisalasse kuuluva elutähtsa üksuse vastavus käesolevale direktiivile.

Artikkel 33

Järelevalve- ja täitemeetmed seoses oluliste üksustega

1. Liikmesriigid tagavad, et pädevad asutused võtavad meetmeid, vajaduse korral järelkontrollimeetmeid, kui neile esitatakse tõendeid, vihjeid või teavet selle kohta, et oluline üksus väidetavalt ei järgi käesolevat direktiivi, eelkõige selle artikleid 21 ja 23. Liikmesriigid tagavad, et need meetmed on tõhusad, proportsionaalsed ja heidutavad, võttes arvesse iga üksikjuhtumi asjaolusid.

2. Liikmesriigid tagavad, et pädevatel asutustel on oluliste üksustega seotud järelevalveülesannete täitmisel kõnealuste üksuste suhtes vähemalt järgmised õigused:

a) teha kohapealseid kontrolle ja kaugjärelevalve korras järelkontrolli, mida teevad eriväljaõppe saanud spetsialistid;

b) teha sihipäraseid turvaauditeid, mida teeb sõltumatu organ või pädev asutus;

c) teha vajaduse korral koostöös asjaomase üksusega objektiivsetel, mittediskrimineerivatel, õiglastel ja läbipaistvatel riskihindamise kriteeriumidel põhinevaid turvalisuse kontrolle;

d) esitada teabenõudeid, mis on vajalikud üksuse võetud küberturvalisuse riskijuhtimismeetmete, sealhulgas tema dokumenteeritud küberturvalisuse poliitika järelhindamiseks ning samuti artikli 27 kohase pädevate asutuste teabe esitamise kohustuse täitmise järelhindamiseks;

e) taotleda juurdepääsu andmetele, dokumentidele ja teabele, mis on vajalik nende järelevalveülesannete täitmiseks;

f) nõuda küberturvalisuse poliitika rakendamise tõendamist, näiteks kvalifitseeritud audiitori tehtud turvaauditite tulemusi ja nende aluseks olevaid tõendavaid dokumente.

Esimese lõigu punktis b osutatud sihipärased turvaauditid põhinevad pädeva asutuse või auditeeritava üksuse tehtud riskihindamisel või muul kättesaadaval riskialasel teabel.

Sihipärase turvaauditi tulemused tehakse pädevale asutusele kättesaadavaks. Sõltumatu organi poolt läbi viidava sihipärase turvaauditi kulud tasub auditeeritav üksus, välja arvatud igakülgselt põhjendatud juhtudel, kui pädev asutus otsustab teisiti.

3. Lõike 2 punktis d, e või f kohaste volituste kasutamisel märgivad pädevad asutused ära taotluse eesmärgi ja täpsustavad, millist teavet nõutakse.

4. Liikmesriigid tagavad, et pädevatel asutustel on oluliste üksustega seotud täitmise tagamise volituste kasutamisel vähemalt järgmised õigused:

a) teha hoiatusi asjaomaste üksuste käesoleva direktiivi rikkumiste kohta;

b) võtta vastu siduvaid juhiseid või korraldusi, millega nõutakse, et asjaomased üksused kõrvaldaksid tuvastatud puudused või heastaksid käesoleva direktiivi rikkumise;

c) anda asjaomastele üksustele korraldus lõpetada tegu, mis rikub käesolevat direktiivi, ja hoiduda sellist tegu kordamast;

d) kohustada asjaomaseid üksusi tagama, et nende riskijuhtimismeetmed vastavad artiklis 21 sätestatud nõuetele ning et nad täidavad artiklis 23 sätestatud teatamiskohustust kindlaksmääratud viisil ja kindlaksmääratud ajavahemiku jooksul;

e) kohustada asjaomaseid üksusi teavitama füüsilisi või juriidilisi isikuid, kellele osutatakse teenuseid või pakutakse tegevusi, mida võib mõjutada oluline küberoht, ohu laadist ning võimalikest kaitse- või parandusmeetmetest, mida need füüsilised või juriidilised isikud võivad vastavale ohule reageerimiseks võtta;

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

g) kohustada asjaomaseid üksusi avalikustama kindlaksmääratud viisil käesoleva direktiivi rikkumistega seotud aspektid;

h) määrata või taotleda, et asjaomased organid või kohtud määraksid vastavalt liikmesriigi õigusele lisaks käesoleva lõike punktides a–g osutatud meetmele artikli 34 kohase haldustrahvi.

5. Artikli 32 lõikeid 6, 7 ja 8 kohaldatakse *mutatis mutandis* käesolevas artiklis sätestatud järelevalve- ja täitemeetmete puhul, mida kohaldatakse oluliste üksuste suhtes.

6. Liikmesriigid tagavad, et nende käesoleva direktiivi kohased pädevad asutused teevad asjaomase liikmesriigi määruse (EL) 2022/2554 kohaste pädevate asutustega koostööd. Eelkõige tagavad liikmesriigid, et nende käesoleva direktiivi kohased pädevad asutused teavitavad määruse (EL) 2022/2554 artikli 32 lõike 1 kohaselt järelevaatamise foorumit, kui nad kasutavad oma järelevalve- ja täitmise tagamise volitusi, et tagada määruse (EL) 2022/2554 artikli 31 kohaselt kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajana käsitatava ja käesoleva direktiivi kohaldamisalasse kuuluva olulise üksuse vastavus käesolevale direktiivile.

Artikkel 34

Elutähtsatele ja olulistele üksustele haldustrahvide määramise üldtingimused

1. Liikmesriigid tagavad, et haldustrahvid, mis määratakse käesoleva artikli kohaselt elutähtsatele ja olulistele üksustele käesoleva direktiivi rikkumise korral, on mõjusad, proportsionaalsed ja heidutavad ning et nende puhul võetakse arvesse iga üksikjuhtumi asjaolusid.

2. Haldustrahvid määratakse lisaks artikli 32 lõike 4 punktides a–h, artikli 32 lõikes 5 ja artikli 33 lõike 4 punktides a–g osutatud meetmetele.

3. Haldustrahvi määramise ja selle suuruse üle otsustamisel võetakse iga üksikjuhtumi puhul nõuetekohaselt arvesse vähemalt artikli 32 lõikes 7 sätestatud asjaolusid.

4. Liikmesriigid tagavad, et kui elutähtsad üksused rikuvad artiklit 21 või 23, määratakse kooskõlas käesoleva artikli lõigetega 2 ja 3 elutähtsatele üksustele haldustrahv, mille maksimummäär on vähemalt 10 000 000 eurot või kuni 2 % selle ettevõtja ülemaailmsest aastasest kogukäibest eelneval majandusaastal (olenevalt sellest, kumb summa on suurem), kellele elutähtis üksus kuulub.

5. Liikmesriigid tagavad, et artikli 21 või 23 rikkumise korral määratakse kooskõlas käesoleva artikli lõigetega 2 ja 3 olulistele üksustele haldustrahv, mille maksimummäär on vähemalt 7 000 000 eurot või kuni 1,4 % selle ettevõtja ülemaailmsest aastasest kogukäibest eelneval majandusaastal (olenevalt sellest, kumb summa on suurem), kellele oluline üksus kuulub.

6. Liikmesriigid võivad näha ette õiguse määrata sunniraha, mille eesmärk on sundida elutähtsat või olulist üksust käesoleva direktiivi rikkumist lõpetama, kooskõlas pädeva asutuse eelneva otsusega.

7. Ilma et see piiraks pädevate asutuste artiklite 32 ja 33 kohaseid volitusi, võib iga liikmesriik kehtestada õigusnormid selle kohta, kas ja millises ulatuses võib haldustrahve määrata avalik-õiguslikele asutustele.

8. Kui liikmesriigi õigussüsteemis ei ole haldustrahve ette nähtud, tagab see liikmesriik, et käesolevat artiklit kohaldatakse viisil, et trahvi algatab pädev asutus ning selle määravad liikmesriigi pädevad kohtud, tagades seejuures, et need õiguskaitsevahendid on tõhusad ja pädevate asutuste poolt määratud haldustrahvidega samaväärse mõjuga. Igal juhul peavad määratavad trahvid olema mõjusad, proportsionaalsed ja heidutavad. Liikmesriik teavitab komisjoni käesoleva lõike alusel vastuvõetavatest õigusnormidest hiljemalt 17. oktoobriks 2024 ning teavitab teda viivitamata kõigist hilisematest neid õigusnorme mõjutavatest muutmisaktidest või muudatustest.

Artikkel 35

Isikuandmete väärkasutamisega seotud rikkumised

1. Kui pädevad asutused on järelevalve või täitmise tagamise käigus saanud teadlikuks sellest, et käesoleva direktiivi artiklites 21 ja 23 sätestatud kohustuste rikkumisega elutähtsa või olulise üksuse poolt võib kaasneda isikuandmetega seotud rikkumine, nagu on määratletud määruse (EL) 2016/679 artikli 4 punktis 12 ja millest tuleb teavitada kõnealuse määruse artikli 33 kohaselt, teatavad nad sellest põhjendamatu viivituseta kõnealuse määruse artikli 55 või 56 kohastele järelevalveasutustele.

2. Kui määruse (EL) 2016/679 artiklis 55 või 56 osutatud järelevalveasutused määravad kõnealuse määruse artikli 58 lõike 2 punkti i alusel haldustrahvi, ei määra pädevad asutused käesoleva direktiivi artikli 34 alusel haldustrahvi käesoleva artikli lõikes 1 osutatud rikkumise korral, mis tuleneb samast teost, mille eest määrati määruse (EL) 2016/679 artikli 58 lõike 2 punkti i kohane haldustrahv. Pädevad asutused võivad siiski kohaldada täitemeetmeid käesoleva direktiivi artikli 32 lõike 4 punktide a–h, artikli 32 lõike 5 ja artikli 33 lõike 4 punktide a–g alusel.

3. Kui määruse (EL) 2016/679 kohane pädev järelevalveasutus on asutatud muus liikmesriigis kui pädev asutus, teavitab pädev asutus oma liikmesriigis asutatud järelevalveasutust lõikes 1 osutatud võimalikust isikuandmetega seotud rikkumisest.

Artikkel 36

Karistused

Liikmesriigid kehtestavad karistusnormid, mida kohaldatakse käesoleva direktiivi alusel vastu võetud liikmesriigi meetmete rikkumise korral, ning võtavad kõik vajalikud meetmed, et tagada kõnealuste normide rakendamine. Kehtestatud karistused peavad olema mõjusad, proportsionaalsed ja heidutavad. Liikmesriigid teavitavad komisjoni hiljemalt 17. jaanuariks 2025 kõnealustest õigusnormidest ja meetmetest ning teavitavad teda viivitamata ka nende hilisematest muudatustest.

Artikkel 37

Vastastikune abi

1. Kui 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.

Esimese lõigu punktis c osutatud vastastikune abi võib hõlmata teabenõudeid ja järelevalvemeetmeid, sealhulgas taotlusi teha kohapealseid kontrolle või kaugjärelevalvet või sihipäraseid turvaauditeid. Abitaotluse saanud pädev asutus ei või taotlust tagasi lükata, välja arvatud juhul, kui leitakse, et asutus ei ole pädev taotletud abi andma või et taotletav abi ei ole pädeva asutuse järelevalveülesannete suhtes proportsionaalne või kui taotlus puudutab teavet või sisaldab tegevust, mis avalikustamise või elluviimise korral oleksid asjaomase vastuolus liikmesriigi riikliku julgeoleku, avaliku julgeoleku või riigikaitse oluliste huvidega. Enne sellise taotluse rahuldamata jätmist konsulteerib pädev asutus teiste asjaomaste pädevate asutustega ning ühe asjaomase liikmesriigi taotluse korral ka komisjoni ja ENISAga.

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

VIII PEATÜKK

DELEGEERITUD ÕIGUSAKTID JA RAKENDUSAKTID

Artikkel 38

Delegeeritud volituste rakendamine

1. Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.

2. Artikli 24 lõikes 2 osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile viieks aastaks alates 16. jaanuarist 2023.

3. Euroopa Parlament ja nõukogu võivad artikli 24 lõikes 2 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.

4. Enne delegeeritud õigusakti vastuvõtmist konsulteerib komisjon vastavalt 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetele iga liikmesriigi määratud ekspertidega.

5. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle samal ajal teatavaks Euroopa Parlamendile ja nõukogule.

6. Artikli 24 lõike 2 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kahe kuu jooksul pärast õigusakti teatavakstegemist Euroopa Parlamendile ja nõukogule esitanud selle suhtes vastuväidet või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväidet. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kahe kuu võrra.

Artikkel 39

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 ilma tulemust saavutamata, kui arvamuse esitamiseks ettenähtud tähtaja jooksul komitee eesistuja nii otsustab või komitee liige seda taotleb.

IX PEATÜKK

LÕPPSÄTTED

Artikkel 40

Läbivaatamine

Hiljemalt 17. oktoobriks 2027 ja seejärel iga 36 kuu järel vaatab komisjon käesoleva direktiivi toimimise läbi ning esitab sellekohase aruande Euroopa Parlamendile ja nõukogule. Aruandes hinnatakse eelkõige asjaomaste üksuste suuruse asjakohasust ning I ja II lisas osutatud üksuse sektorite, allsektorite ning liigi asjakohasust majanduse ja ühiskonna toimimise aspektist seoses küberturvalisusega. Sel eesmärgil ning strateegilise ja operatiivkoostöö täiendavaks edendamiseks võtab komisjon arvesse koostöörühma ja CSIRTide võrgustiku aruandeid strateegilisel ja operatiivtasandil saadud kogemuste kohta. Vajaduse korral lisatakse aruandele seadusandlik ettepanek.

Artikkel 41

Ülevõtmine

1. Liikmesriigid võtavad käesoleva direktiivi järgimiseks vajalikud meetmed vastu ja avaldavad need hiljemalt 17. oktoobriks 2024. Liikmesriigid teatavad nendest viivitamata komisjonile.

Nad kohaldavad kõnealuseid meetmeid alates 18. oktoobrist 2024.

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

Artikkel 42

Määruse (EL) nr 910/2014 muutmine

Määruse (EL) nr 910/2014 artikkel 19 jäetakse välja alates 18. oktoobrist 2024.

Artikkel 43

Direktiivi (EL) 2018/1972 muutmine

Direktiivi (EL) 2018/1972 artiklid 40 ja 41 jäetakse välja alates 18. oktoobrist 2024.

Artikkel 44

Kehtetuks tunnistamine

Direktiiv (EL) 2016/1148 tunnistatakse kehtetuks alates 18. oktoobrist 2024.

Viiteid kehtetuks tunnistatud direktiivile käsitatakse viidetena käesolevale direktiivile ja loetakse vastavalt III lisas esitatud vastavustabelile.

Artikkel 45

Jõustumine

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

Artikkel 46

Adressaadid

Käesolev direktiiv on adresseeritud liikmesriikidele.

Strasbourg, 14. detsember 2022

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*
R. METSOLA	M. BEK

I LISA

KRIITILISE TÄHTSUSEGA SEKTORID

Sektor	Allsektor	Üksuse liik
1. Energeetika	a) Elekter	— Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/944 ([1]) artikli 2 punktis 57 määratletud elektriettevõtjad, kes täidavad nimetatud direktiivi artikli 2 punktis 12 määratletud tarnimise ülesannet
		— Direktiivi (EL) 2019/944 artikli 2 punktis 29 määratletud jaotusvõrguettevõtjad
		— Direktiivi (EL) 2019/944 artikli 2 punktis 35 määratletud põhivõrguettevõtjad
		— Direktiivi (EL) 2019/944 artikli 2 punktis 38 määratletud tootjad
		— Euroopa Parlamendi ja nõukogu määruse (EL) 2019/943 ([2]) artikli 2 punktis 8 määratletud määratud elektriturukorraldajad — Määruse (EL) 2019/943 artikli 2 punktis 25 määratletud turuosalised, kes osutavad direktiivi (EL) 2019/944 artikli 2 punktides 18, 20 ja 59 määratletud agregeerimis-, tarbimiskaja- või energia salvestamise teenuseid — laadimispunkti käitajad, kes vastutavad sellise laadimispunkti haldamise ja käitamise eest, mis osutab lõppkasutajatele laadimisteenust, sealhulgas liikuvusteenuse osutaja nimel ja eest
	b) Kaugküte ja-jahutus	— Euroopa Parlamendi ja nõukogu direktiivi (EL) 2018/2001 ([3]) artikli 2 punktis 19 määratletud kaugkütte ja kaugjahutuse pakkujad
	c) Nafta	— Naftajuhtmete operaatorid
		— Nafta tootmise, rafineerimise ja töötlemise rajatiste ning hoiustamise ja ülekandmisega tegelevad operaatorid
		— Nõukogu direktiivi 2009/119/EÜ ([4]) artikli 2 punktis f määratletud varude säilitamise kesküksused
	d) Gaas	— Euroopa Parlamendi ja nõukogu direktiivi 2009/73/EÜ ([5]) artikli 2 punktis 8 määratletud tarneettevõtjad
		— Direktiivi 2009/73/EÜ artikli 2 punktis 6 määratletud jaotussüsteemi haldurid
		— Direktiivi 2009/73/EÜ artikli 2 punktis 4 määratletud ülekandesüsteemi haldurid
		— Direktiivi 2009/73/EÜ artikli 2 punktis 10 määratletud hoidlatevõrgu haldurid
		— Direktiivi 2009/73/EÜ artikli 2 punktis 12 määratletud 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

Sektor	Allsektor	Üksuse liik
2. Transport	a) Lennutransport	— Kommertsvaldkonnas tegutsevad määruse (EÜ) nr 300/2008 artikli 3 punktis 4 määratletud lennuettevõtjad
		— Euroopa Parlamendi ja nõukogu direktiivi 2009/12/EÜ ([6]) artikli 2 punktis 2 määratletud lennujaama juhtorganid, nimetatud direktiivi artikli 2 punktis 1 määratletud lennujaamad, sealhulgas Euroopa Parlamendi ja nõukogu määruse (EL) nr 1315/2013 ([7]) II lisa 2. jaos loetletud põhivõrgu lennujaamad ning lennujaamades olevaid abirajatisi käitavad üksused
		— Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 549/2004 ([8]) artikli 2 punktis 1 määratletud lennujuhtimise teenust osutavad liikluskorraldusettevõtjad
	b) Raudteetransport	— Euroopa Parlamendi ja nõukogu direktiivi 2012/34/EL ([9]) artikli 3 punktis 2 määratletud raudteeinfrastruktuuri-ettevõtjad
		— Direktiivi 2012/34/EL artikli 3 punktis 3 määratletud raudteeveo-ettevõtjad, sealhulgas nimetatud direktiivi artikli 3 punktis 12 määratletud teenindusrajatiste käitajad
	c) Veetransport	— Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 725/2004 ([10]) I lisas meretranspordi puhul määratletud reisijate ja kauba vedamisega sisevetes, merel ja rannavetes tegelevad ettevõtjad, välja arvatud kõnealuste ettevõtjate käidatud üksikud laevad
		— Euroopa Parlamendi ja nõukogu direktiivi 2005/65/EÜ ([11]) artikli 3 punktis 1 määratletud sadamate valdajad, sealhulgas nende määruse (EÜ) nr 725/2004 artikli 2 punktis 11 määratletud sadamarajatised ning sadamates tööde ja varustuse haldamisega tegelevad üksused
		— Euroopa Parlamendi ja nõukogu direktiivi 2002/59/EÜ ([12]) artikli 3 punktis o määratletud laevaliikluse juhtimise keskuste (VTS) operaatorid
	d) Maanteetransport	— Komisjoni delegeeritud määruse (EL) 2015/962 ([13]) artikli 2 punktis 12 määratletud maanteeametid, kes vastutavad liikluskorralduse eest, välja arvatud avaliku sektori üksused, kelle jaoks liikluskorraldus või intelligentsete transpordisüsteemide käitamine moodustab üksnes väheolulise osa nende tegevusest
		— Euroopa Parlamendi ja nõukogu direktiivi 2010/40/EL ([14]) artikli 4 punktis 1 määratletud intelligentsete transpordisüsteemide operaatorid
3. Pangandus		Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 ([15]) artikli 4 punktis 1 määratletud krediidiasutused
4. Finantsturutaristud		— Euroopa Parlamendi ja nõukogu direktiivi 2014/65/EL ([16]) artikli 4 punktis 24 määratletud kauplemiskohtade korraldajad
		— Euroopa Parlamendi ja nõukogu määruse (EL) nr 648/2012 ([17]) artikli 2 punktis 1 määratletud kesksed vastaspooled

Sektor	Allsektor	Üksuse liik
5. Tervishoid		— Euroopa Parlamendi ja nõukogu direktiivi 2011/24/EL ([18]) artikli 3 punktis g määratletud tervishoiuteenuse osutajad
		— Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2371 ([19]) artiklis 15 määratletud ELi referentlaborid
		— Üksused, mis tegelevad Euroopa Parlamendi ja nõukogu direktiivi 2001/83/EÜ ([20]) artikli 1 punktis 2 määratletud ravimite uurimise ja arendamisega — NACE Rev. 2 C jao jaotises 21 osutatud põhifarmaatsiatooteid ja ravimpreparaate tootvad üksused — Üksused, mis toodavad rahvatervise hädaolukorras kriitilise tähtsusega meditsiiniseadmeid (rahvatervise hädaolukorra esmatähtsate meditsiiniseadmete loetelu) Euroopa Parlamendi ja nõukogu määruse (EL) 2022/123 ([21]) artikli 22 tähenduses
6. Joogivesi		Euroopa Parlamendi ja nõukogu direktiivi (EL) 2020/2184 ([22]) artikli 2 punkti 1 alapunktis a määratletud olmeveega varustajad ja olmevee jaotajad, välja arvatud jaotajad, kelle puhul olmevee jaotamine on väheoluline osa nende üldisest muude tarbekaupade ja kaupade tarnimistegevusest
7. Reovesi		Ettevõtjad, kes tegelevad nõukogu direktiivi 91/271/EMÜ ([23]) artikli 2 punktides 1, 2 ja 3 määratletud asulareovee, olmereovee või tööstusreovee kogumise, ärajuhtimise või puhastamisega, välja arvatud ettevõtjad, kelle puhul asulareovee, olmereovee või tööstusreovee kogumine, ärajuhtimine või puhastamine on väheoluline osa nende üldisest tegevusest
8. Digitaristu		— Interneti vahetuspunkti teenuse osutajad
		— Domeeninimesüsteemide süsteemi teenuse osutajad, välja arvatud juurnimeserverite operaatorid
		— Tippdomeeninimede registrite pidajad
		— Pilvandmetöötlusteenuse osutajad
		— Andmekeskusteenuse osutajad
		— Sisulevivõrguteenuse osutajad
		— Usaldusteenuse osutajad
		— Üldkasutatavale elektroonilise side võrkude pakkujad
		— Üldkasutatavate elektroonilise side teenuste osutajad
9. IKT-teenuste haldamine (ettevõtetevaheline)		— Hallatud teenuse osutajad — Turbetarnijad

Sektor	Allsektor	Üksuse liik
10. Avaliku halduse üksused		— Keskvalitsuste avaliku halduse üksused, nagu need on kindlaks määranud liikmesriik vastavalt oma õigusele
		— Piirkondade avaliku halduse üksused, nagu need on kindlaks määranud liikmesriik vastavalt oma õigusele
11. Kosmos		Liikmesriigi või eraõiguslike isikute omandis olevate, hallatavate või käitatavate maapealsete taristute operaatorid, kes toetavad kosmosepõhiste teenuste osutamist, välja arvatud elektroonilise side võrkude pakkujad

(1) 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).
(2) Euroopa Parlamendi ja nõukogu 5. juuni 2019. aasta määrus (EL) 2019/943, milles käsitletakse elektrienergia siseturgu (ELT L 158, 14.6.2019, lk 54).
(3) 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).
(4) 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).
(5) 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).
(6) Euroopa Parlamendi ja nõukogu 11. märtsi 2009. aasta direktiiv 2009/12/EÜ lennujaamatasude kohta (ELT L 70, 14.3.2009, lk 11).
(7) 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).
(8) 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).
(9) 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).
(10) 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).
(11) Euroopa Parlamendi ja nõukogu 26. oktoobri 2005. aasta direktiiv 2005/65/EÜ sadamate turvalisuse tugevdamise kohta (ELT L 310, 25.11.2005, lk 28).
(12) 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).
(13) 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).
(14) 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).
(15) Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta määrus (EL) nr 575/2013, mis käsitleb krediidiasutuste suhtes kohaldatavaid usaldatavusnõudeid ja millega muudetakse määrust (EL) nr 648/2012 (ELT L 176, 27.6.2013, lk 1).
(16) 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).
(17) 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).
(18) 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).

([19]) Euroopa Parlamendi ja nõukogu 23. novembri 2022. aasta määrus (EL) 2022/2371, milles käsitletakse tõsiseid piiriüleseid terviseohtusid ja millega tunnistatakse kehtetuks otsus nr 1082/2013/EL (ELT L 314, 6.12.2022, lk 26).

([20]) 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).

([21]) Euroopa Parlamendi ja nõukogu 25. jaanuari 2022. aasta määrus (EL) 2022/123, mis käsitleb Euroopa Ravimiameti suuremat rolli ravimite ja meditsiiniseadmete alases kriisivalmiduses ja -ohjes (ELT L 20, 31.1.2022, lk 1).

([22]) Euroopa Parlamendi ja nõukogu 16. detsembri 2020. aasta direktiiv (EL) 2020/2184 olmevee kvaliteedi kohta (ELT L 435, 23.12.2020, lk 1).

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

II LISA

MUUD KRIITILISE TÄHTSUSEGA SEKTORID

Sektor	Allsektor	Üksuse liik
1. Posti- ja kulleriteenused		Direktiivi 97/67/EÜ artikli 2 punktis 1a määratletud postiteenuste osutajad, sealhulgas kulleriteenuste osutajad
2. Jäätmekäitlus		Ettevõtjad, kes tegelevad Euroopa Parlamendi ja nõukogu direktiivi 2008/98/EÜ ([1]) artikli 3 punktis 9 määratletud jäätmekäitlusega, välja arvatud ettevõtjad, kelle põhitegevus ei ole jäätmekäitlus
3. Kemikaalide valmistamine, tootmine ja levitamine		Ettevõtjad, kes tegelevad Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 1907/2006 ([2]) artikli 3 punktides 9 ja 14 osutatud ainete valmistamisega ning ainete või segude levitamisega, ning ettevõtjad, kes toodavad ainetest või segudest kõnealuse määruse artikli 3 punktis 3 määratletud tooteid
4. Toiduainete tootmine, töötlemine ja turustamine		Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 178/2002 ([3]) artikli 3 punktis 2 määratletud toidukäitlemisettevõtjad, kes tegelevad hulgimüügi ning tööstusliku tootmise ja töötlemisega
5. Töötlev tööstus	a) Meditsiiniseadmete ja *in vitro* diagnostikameditsiiniseadmete tootmine	Euroopa Parlamendi ja nõukogu määruse (EL) 2017/745 ([4]) artikli 2 punktis 1 määratletud meditsiiniseadmeid tootvad üksused ning Euroopa Parlamendi ja nõukogu määruse (EL) 2017/746 ([5]) artikli 2 punktis 2 määratletud *in vitro* diagnostikameditsiiniseadmeid tootvad üksused, välja arvatud käesoleva direktiivi I lisa punkti 5 viiendas taandes osutatud 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

Sektor	Allsektor	Üksuse liik
6. Digiteenuste osutajad		— Internetipõhiste kauplemiskohtade pakkujad
		— Internetipõhiste otsingumootorite pakkujad
		— Sotsiaalvõrguteenuse platvormide pakkujad
7. Teadustegevus		Teadusasutused

([1]) 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).

([2]) Euroopa Parlamendi ja nõukogu 18. detsembri 2006. aasta määrus (EÜ) nr 1907/2006, mis käsitleb kemikaalide registreerimist, hindamist, autoriseerimist ja piiramist (REACH) ning millega asutatakse Euroopa Kemikaaliamet ning muudetakse direktiivi 1999/45/EÜ ja tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 793/93 ja 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).

([3]) 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).

([4]) 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).

([5]) 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).

III LISA

VASTAVUSTABEL

Direktiiv (EL) 2016/1148	Käesolev direktiiv
Artikli 1 lõige 1	Artikli 1 lõige 1
Artikli 1 lõige 2	Artikli 1 lõige 2
Artikli 1 lõige 3	–
Artikli 1 lõige 4	Artikli 2 lõige 12
Artikli 1 lõige 5	Artikli 2 lõige 13
Artikli 1 lõige 6	Artikli 2 lõiked 6 ja 11
Artikli 1 lõige 7	Artikkel 4
Artikkel 2	Artikli 2 lõige 14
Artikkel 3	Artikkel 5
Artikkel 4	Artikkel 6
Artikkel 5	–
Artikkel 6	–
Artikli 7 lõige 1	Artikli 7 lõiked 1 ja 2
Artikli 7 lõige 2	Artikli 7 lõige 4
Artikli 7 lõige 3	Artikli 7 lõige 3
Artikli 8 lõiked 1–5	Artikli 8 lõiked 1–5
Artikli 8 lõige 6	Artikli 13 lõige 4
Artikli 8 lõige 7	Artikli 8 lõige 6
Artikli 9 lõiked 1, 2 ja 3	Artikli 10 lõiked 1, 2 ja 3
Artikli 9 lõige 4	Artikli 10 lõige 9
Artikli 9 lõige 5	Artikli 10 lõige 10
Artikli 10 lõiked 1, 2 ja lõike 3 esimene lõik	Artikli 13 lõiked 1, 2 ja 3
Artikli 10 lõike 3 teine lõik	Artikli 23 lõige 9
Artikli 11 lõige 1	Artikli 14 lõiked 1 ja 2
Artikli 11 lõige 2	Artikli 14 lõige 3
Artikli 11 lõige 3	Artikli 14 lõike 4 esimese lõigu punktid a–q ja s ning lõige 7
Artikli 11 lõige 4	Artikli 14 lõike 4 esimese lõigu punkt r ja teine lõik
Artikli 11 lõige 5	Artikli 14 lõige 8
Artikli 12 lõiked 1–5	Artikli 15 lõiked 1–5
Artikkel 13	Artikkel 17
Artikli 14 lõiked 1 ja 2	Artikli 21 lõiked 1–4
Artikli 14 lõige 3	Artikli 23 lõige 1
Artikli 14 lõige 4	Artikli 23 lõige 3
Artikli 14 lõige 5	Artikli 23 lõiked 5, 6 ja 8

Direktiiv (EL) 2016/1148	Käesolev direktiiv
Artikli 14 lõige 6	Artikli 23 lõige 7
Artikli 14 lõige 7	Artikli 23 lõige 11
Artikli 15 lõige 1	Artikli 31 lõige 1
Artikli 15 lõike 2 esimese lõigu punkt a	Artikli 32 lõike 2 punkt e
Artikli 15 lõike 2 esimese lõigu punkt b	Artikli 32 lõike 2 punkt g
Artikli 15 lõike 2 teine lõik	Artikli 32 lõige 3
Artikli 15 lõige 3	Artikli 32 lõike 4 punkt b
Artikli 15 lõige 4	Artikli 31 lõige 3
Artikli 16 lõiked 1 ja 2	Artikli 21 lõiked 1–4
Artikli 16 lõige 3	Artikli 23 lõige 1
Artikli 16 lõige 4	Artikli 23 lõige 3
Artikli 16 lõige 5	–
Artikli 16 lõige 6	Artikli 23 lõige 6
Artikli 16 lõige 7	Artikli 23 lõige 7
Artikli 16 lõiked 8 ja 9	Artikli 21 lõige 5 ja artikli 23 lõige 11
Artikli 16 lõige 10	–
Artikli 16 lõige 11	Artikli 2 lõiked 1, 2 ja 3
Artikli 17 lõige 1	Artikli 33 lõige 1
Artikli 17 lõike 2 punkt a	Artikli 32 lõike 2 punkt e
Artikli 17 lõike 2 punkt b	Artikli 32 lõike 4 punkt b
Artikli 17 lõige 3	Artikli 37 lõike 1 punktid a ja b
Artikli 18 lõige 1	Artikli 26 lõike 1 punkt b ja lõige 2
Artikli 18 lõige 2	Artikli 26 lõige 3
Artikli 18 lõige 3	Artikli 26 lõige 4
Artikkel 19	Artikkel 25
Artikkel 20	Artikkel 30
Artikkel 21	Artikkel 36
Artikli 22	Artikkel 39
Artikkel 23	Artikkel 40
Artikkel 24	–
Artikkel 25	Artikkel 41
Artikkel 26	Artikkel 45
Artikkel 27	Artikkel 46
I lisa punkt 1	Artikli 11 lõige 1
I lisa punkti 2 alapunkti a alapunktid i–iv	Artikli 11 lõike 2 punktid a–d

Direktiiv (EL) 2016/1148	Käesolev direktiiv
I lisa punkti 2 alapunkti a alapunkt v	Artikli 11 lõike 2 punkt f
I lisa punkti 2 alapunkt b	Artikli 11 lõige 4
I lisa punkti 2 alapunkti c alapunktid i ja ii	Artikli 11 lõike 5 punkt a
II lisa	I lisa
III lisa punktid 1 ja 2	II lisa punkt 6
III lisa punkt 3	I lisa punkt 8