P7_TA(2014)0244

Võrgu- ja infoturbe ühtlaselt kõrge tase ***I

Euroopa Parlamendi 13. märtsi 2014. aasta seadusandlik resolutsioon ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu direktiiv meetmete kohta, millega tagada võrgu- ja infoturbe ühtlaselt kõrge tase kogu Euroopa Liidus (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

(Seadusandlik tavamenetlus: esimene lugemine)

Euroopa Parlament,

– võttes arvesse komisjoni ettepanekut Euroopa Parlamendile ja nõukogule (COM(2013)0048),

– võttes arvesse Euroopa Liidu toimimise lepingu artikli 294 lõiget 2 ja artiklit 114, mille alusel komisjon esitas ettepaneku Euroopa Parlamendile (C7-0035/2013),

– võttes arvesse Euroopa Liidu toimimise lepingu artikli 294 lõiget 3,

– võttes arvesse Rootsi parlamendi poolt subsidiaarsuse ja proportsionaalsuse põhimõtete kohaldamist käsitleva protokolli nr 2 alusel esitatud põhjendatud arvamusi, mille kohaselt seadusandliku akti eelnõu ei vasta subsidiaarsuse põhimõttele,

– võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee 22. mai 2013. aasta arvamust[1],

– võttes arvesse Euroopa Parlamendi 12. septembri 2013. aasta resolutsiooni Euroopa Liidu küberjulgeoleku strateegia kohta: avatud, ohutu ja turvaline küberruum[2],

– võttes arvesse kodukorra artiklit 55,

– võttes arvesse siseturu- ja tarbijakaitsekomisjoni raportit ning tööstuse, teadusuuringute ja energeetikakomisjoni, kodanikuvabaduste, justiits- ja siseasjade komisjoni ning väliskomisjoni arvamusi (A7-0103/2014),

1. võtab vastu allpool toodud esimese lugemise seisukoha;

2. palub komisjonil ettepaneku uuesti Euroopa Parlamendile saata, kui komisjon kavatseb seda oluliselt muuta või selle muu tekstiga asendada;

3. teeb presidendile ülesandeks edastada Euroopa Parlamendi seisukoht nõukogule, komisjonile ja liikmesriikide parlamentidele.

---

1 ELT C 271, 19.9.2013, lk 133.

2 Vastuvõetud tekstid, P7_TA(2013)0376.

P7_TC1-COD(2013)0027

Euroopa Parlamendi seisukoht, vastu võetud esimesel lugemisel 13. märtsil 2014. aastal eesmärgiga võtta vastu Euroopa Parlamendi ja nõukogu direktiiv 2014/.../EL meetmete kohta, millega tagada võrgu- ja infoturbe ühtlaselt kõrge tase kogu Euroopa Liidus

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 riikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust[1],

toimides seadusandliku tavamenetluse kohaselt[2]

---

1 ELT C 271, 19.9.2013, lk 133.

2 Euroopa Parlamendi 13. märtsi 2014. aasta seisukoht.

ning arvestades järgmist:

(1) Võrgul ja infosüsteemidel ning -teenustel on ühiskonnas eluliselt tähtis koht. Nende usaldusväärsus ja turvalisus on ***ELi kodanike vabaduse ja üldise julgeoleku,*** majandustegevuse ja sotsiaalse heaolu ning ennekõike siseturu toimimise jaoks hädavajalik. **[ME 1]**

(2) ~~Tahtlike ja juhuslike~~ Turvaintsidentide ulatus***,*** sagedus ja ***mõju*** suurenevad ning see kujutab endast suurt ohtu võrkude ja infosüsteemide toimimisele. ***Need süsteemid võivad saada ka hõlpsaks sihtmärgiks tahtlikule kahjustamisele süsteemide töö häirimise või peatamise eesmärgil.*** Sellised intsidendid võivad takistada majandustegevust, põhjustada olulist finantskahju, vähendada kasutajate ***ja investorite*** usaldust ja tekitada ELi majandusele suurt kahju ***ning lõpptulemusena ohustada ELi kodanike heaolu ja ELi liikmesriikide suutlikkust end kaitsta ja tagada elutähtsate infrastruktuuride turvalisus***. **[ME 2]**

(3) Piire ületava sidevahendina on digitaalsetel infosüsteemidel ja eriti internetil oluline roll kaupade, teenuste ja inimeste piiriülese liikumise hõlbustamisel. Sellisest riikidevahelisusest tulenevalt võib nende süsteemide töö katkestus ühes liikmesriigis mõjutada ka teisi liikmesriike ja ELi tervikuna. Seepärast on võrgu ja infosüsteemide vastupidavus ja stabiilsus siseturu sujuvaks toimimiseks hädavajalikud.

(3a) Kuna süsteemirikete põhjused on enamasti tahtmatud, nagu looduslikud protsessid või inimlik eksimus, peaks infrastruktuur olema vastupidav nii tahtlikele kui ka juhuslikele häiretele ja elutähtsate infrastruktuuride operaatorid peaksid töötama välja vastupanuvõimelisi süsteeme. **[ME 3]**

(4) ELi tasandil tuleks luua koostöömehhanism, mis võimaldaks vahetada võrgu- ja infoturbe alast teavet ning tegeleda selles vallas koordineeritud ***ennetuse,*** avastamise ja reageerimisega. Et selline mehhanism oleks tõhus ja kaasav, on oluline, et kõigil liikmesriikidel oleks miinimumsuutlikkus ja strateegia võrgu- ja infoturbe kõrge taseme tagamiseks oma territooriumil. Minimaalseid turvanõudeid tuleks kohaldada ka ~~haldusasutuste ja elutähtsa~~ ***vähemalt teatavate*** infotaristu operaatorite suhtes, et edendada riskihalduse kultuuri ja tagada, et kõige raskematest intsidentidest teatatakse. ***Börsil noteeritud äriühinguid tuleks julgustada andma intsidentidest oma finantsaruannetes vabatahtlikkuse alusel teada. Õigusraamistik peaks põhinema vajadusel kaitsta kodanike eraelu puutumatust ja isikupuutumatust. Käesoleva direktiiviga hõlmatud operaatoritele tuleks laiendada elutähtsate infrastruktuuridega seotud teabe vahetuse infosüsteemi.*** **[ME 4]**

(4a) ***Samal ajal kui haldusasutused peaksid oma avalike ülesannete tõttu näitama oma võrgu ja infosüsteemide juhtimisel ja kaitsmisel üles vajalikku hoolsust, tuleks käesoleva direktiiviga keskenduda energeetika, transpordi-, pangandus-, finantsturu taristu ja tervishoiuvaldkonnas esmatähtsa majandusliku ja ühiskondliku tegevuse säilitamiseks vajalikule elutähtsale infrastruktuurile. Tarkvaraarendajad ja riistvaratootjad tuleks jätta direktiivi reguleerimisalast välja.*** **[ME 5]**

(4b) ***Tuleks tagada asjaomaste liidu ametiasutuste koostöö ja tegevuse kooskõlastamine ühise välis- ja julgeolekupoliitika ja ühise julgeoleku- ja kaitsepoliitika eest vastutava liidu välisasjade ja julgeolekupoliitika kõrge esindaja ja komisjoni asepresidendiga, ning ELi terrorismivastase võitluse koordinaatoriga kõigi suurt mõju omavate intsidentide puhul, mille puhul võib eeldada väliste ja terrorismiga seotud riskide esinemist.*** **[ME 6]**

(5) Et hõlmatud oleks kõik asjakohased intsidendid ja riskid, tuleks käesolevat direktiivi kohaldada kõigi võrgu- ja infosüsteemide suhtes. Haldusasutuste ja operaatorite suhtes kehtestatud kohustusi ei tuleks siiski kohaldada ettevõtjate suhtes, kes pakuvad üldkasutatavaid sidevõrke või üldkasutatavaid elektroonilisi sideteenuseid Euroopa Parlamendi ja nõukogu direktiivi 2002/21/EÜ[1] tähenduses ja kelle suhtes kehtivad konkreetsed turva- ja terviklusnõuded, mis on sätestatud nimetatud direktiivi artiklis 13a, ning neid ei tuleks kohaldada ka usaldusteenuse pakkujate suhtes.

[1] Euroopa Parlamendi ja nõukogu 7. märtsi 2002. aasta direktiiv 2002/21/EÜ elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta (raamdirektiiv) (EÜT L 108, 24.4.2002, lk 33).

(6) Praegune suutlikkus ei ole ELis võrgu ja infoturbe kõrge taseme tagamiseks piisav. Liikmesriikide valmisoleku tase on väga erinev ning see põhjustab ELi lõikes lähenemisviiside killustatuse. See omakorda toob kaasa tarbijate ja ettevõtjate kaitstuse ebaühtluse ja vähendab võrgu- ja infoturbe üldist taset ELis. Kui ~~haldusasutuste ja~~ operaatorite suhtes ei kohaldata ühised miinimumnõuded, ei ole ELi tasemel võimalik luua üldist tõhusat koostöömehhanismi. ***Ülikoolidel ja teaduskeskustel on tähtis roll teadusuuringute, arendustegevuse ja innovatsiooni edendamises kõnealustes valdkondades ja seetõttu tuleks neile tagada piisav rahastamine.*** **[ME 7]**

(7) Tulemuslik reageerimine võrgu ja infosüsteemide turvalisusega seotud probleemidele eeldab seega ELi tasandil üldist lähenemist, mis hõlmaks ühise miinimumsuutlikkuse loomist ja kavandamisnõudeid, ***piisavate küberjulgeoleku alaste oskuste arendamist,*** teabevahetust ja tegevuse koordineerimist ning turvalisuse ühiseid miinimumnõudeid ~~kõigile asjaomastele operaatoritele ja haldusasutustele~~. ***Küberjulgeoleku koordineerimise rühmade (Cyber Security Co-Ordination Groups – CSGCd) asjakohaste soovituste kohaselt tuleks kohaldada ühiseid miinimumstandardeid.*** **[ME 8]**

(8) Käesoleva direktiivi sätted ei tohiks piidata liikmesriikide võimalust võtta vajalikke meetmeid, et tagada oma oluliste turvalisusega seotud huvide kaitse, tagada avalik kord ja julgeolek ning võimaldada kriminaalkuritegude uurimist, avastamist ja nende eest vastutuselevõtmist. Vastavalt Euroopa Liidu toimimise lepingu (ELi toimimise leping) artiklile 346 ei tohi ühtki liikmesriiki kohustada andma teavet, mille avalikustamist ta peab oma oluliste julgeolekuhuvide vastaseks. ***Ühtegi liikmesriiki ei kohustata avaldama teavet, mis on ELi salastatud teave vastavalt nõukogu otsusele 2011/292/EL***[1] ***või vaikimiskokkulepete või mitteametlike vaikimiskokkulepete alla kuuluv teave, näiteks protokoll teabe tundlikkuse märgistamise kohta fooritulede analoogia põhjal.*** **[ME 9]**

---

[1] ***Nõukogu 31. märtsi 2011. aasta otsus 2011/292/EL ELi salastatud teabe kaitseks vajalike julgeolekueeskirjade kohta (ELT L 141, 27.5.2011, lk 17).***

(9) Et saavutada võrgu ja infosüsteemide turvalisuse kõrge tase ja see säilitada, peaks igal liikmesriigil olema riiklik võrgu- ja infoturbe strateegia, milles oleks määratletud strateegilised eesmärgid ja konkreetsed poliitilised meetmed, mida rakendada. Riikide tasemel tuleb ***käesolevas direktiivis sätestatud miinimumnõuete põhjal*** välja töötada olulistele nõuetele vastavad võrgu- ja infoturbe koostöökavad, et saavutada selline reageerimissuutlikkuse tase, mis võimaldaks teha intsidentide korral tulemuslikku ja tõhusat koostööd nii riikide kui ka ELi ~~tasemel~~ ***tasandil, austades ja kaitstes seejuures eraelu ja isikuandmeid***. ***Iga liikmesriik peaks seega olema kohustatud pidama kinni ühistest standarditest, mis puudutavad andmete vormi ja jagatavate ja hinnatavate andmete vahetusvõimalusi. Liikmesriikidel peaks olema õigus paluda Euroopa Võrgu- ja Infoturbeameti (ENISA) koostöövõrgu abi riiklike võrgu- ja infoturbe strateegiate väljatöötamisel, võttes aluseks võrgu- ja infoturbe strateegiate ühise miinimumkava***. **[ME 10]**

(10) Käesoleva direktiivi kohaselt vastuvõetud sätete tõhusa rakendamise huvides tuleks igas liikmesriigis luua või nimetada organ, kes vastutab võrgu- ja infoturbe alaste küsimuste koordineerimise eest ning tegutseb ELi taseme piiriülese koostöö keskusena. Sellistele organitele tuleks anda piisavad tehnilised, rahalised ja inimressursid, mis võimaldaksid neil oma ülesandeid tulemuslikult ja tõhusalt täita ning seeläbi saavutada käesoleva direktiivi eesmärgid.

(10a) ***Arvestades riikide juhtimisstruktuuride erinevusi ning selleks, et kaitsta juba kehtivat valdkondlikku korda või liidu reguleerivaid ja järelevalveasutusi ning et vältida dubleerimist, peaksid liikmesriigid saama käesoleva direktiivi alusel nimetada operaatorite võrkude ja infosüsteemide turbega seotud ülesannete täitmiseks rohkem kui ühe riikliku pädeva asutuse. Kuid sujuva piiriülese koostöö ja suhtluse tagamiseks on vajalik, et iga liikmesriik nimetaks ainult ühe riikliku ühtse kontaktpunkti, kes juhib liidu tasandil piiriülest koostööd, ilma et see piiraks valdkondliku reguleerimiskorra kohaldamist. Kui see on tingitud põhiseaduslikust korrast või muust korrast, peaks liikmesriik saama nimetada ainult ühe asutuse, kes täidab pädeva asutuse ja ühtse kontaktpunkti ülesandeid. Pädevad asutused, ühtsed kontaktpunktid peaksid olema tsiviilorganid, kelle üle teostatakse demokraatlikku kontrolli ning kes ei peaks täitma mingeid ülesandeid luuretegevuse, õiguskaitse või kaitse valdkonnas või olema organisatsiooniliselt seotud mõne nendes valdkondades tegevate organitega.*** **[ME 11]**

(11) Kõik liikmesriigid ***ja operaatorid*** peaksid olema nii tehniliselt kui ka töökorralduse mõttes piisavalt varustatud, et ***igal ajal*** vältida ja avastada võrgu ja infosüsteemidega seotud intsidente ja riske ning neile reageerida ja nende mõju leevendada. ***Haldusasutuste turvasüsteemid peavad olema turvalised ja nende suhtes tuleb kohaldada demokraatlikku kontrolli ja järelevalvet. Üldkohustuslik varustus ja suutlikkus peaks olema kooskõlas ühiselt kokkulepitud tehniliste standardite ja standardse töökorraga.*** Seepärast tuleks kõigis liikmesriikides luua hästi toimivad ja olulistele nõuetele vastavad infoturbeintsidentidega tegelevad ~~meeskonnad~~ ***rühmad (CERTid)***, et kindlustada tulemuslik ja ühilduv suutlikkus tulla toime intsidentide ja riskidega ning tagada ELi tasandil tõhus koostöö. ***Neil CERTidel peaks olema võimalik suhelda omavahel ühiste tehniliste standardite ja SPO põhjal. Olemasolevate infoturbeintsidentidega tegelevate meeskondade (CERTid) erinevate omaduste seisukohalt, mis reageerib erinevatele erialastele vajadustele ja osalistele, peaksid liikmesriigid tagama, et kõikidele käesoleva direktiiviga hõlmatud sektoritele osutaks teenuseid vähemalt üks CERT. Liikmesriigid peaksid seoses CERTide piiriülese koostööga tagama, et CERTidel on piisavad vahendid juba olemasolevates rahvusvahelistes üleeuroopalistes koostöövõrkudes osalemiseks.*** **[ME 12]**

(12) Arvestades liikmesriikide Euroopa foorumi (EFMS) märkimisväärset edu heade poliitiliste tavade üle peetud arutelude ja teabevahetuse soodustamisel, kaasa arvatud küberkriisialase Euroopa koostöö põhimõtete väljatöötamist, peaksid liikmesriigid ja komisjon looma võrgu, mis võimaldaks neil pidevalt suhelda ja toetaks nende koostööd. Turvaline ja tulemuslik koostöömehhanism***, mis vajaduse korral hõlmab operaatorite osalemist,*** peaks võimaldama struktureeritud ja koordineeritud teabevahetust ning probleemide avastamist ja neile reageerimist ELi tasandil. **[ME 13]**

(13) ~~Euroopa Võrgu- ja Infoturbeamet (~~ENISA~~)~~ peaks liikmesriike ja komisjoni abistama, pakkudes neile oma teadmisi ja andes nõu ning toetades parimate tavade vahetamist. Eriti ~~peaks~~ ***peaksid*** komisjon ***ja liikmesriigid*** ENISAga konsulteerima käesoleva direktiivi kohaldamise üle. Et tagada liikmesriikide ja komisjoni tulemuslik ja õigeaegne teavitamine, tuleks varajased hoiatused intsidentide ja riskide kohta edastada koostöövõrgus. Liikmesriikide suutlikkuse ja teadmiste parandamise huvides peaks koostöövõrk pakkuma võimalusi ka parimate tavade vahetamiseks ning abistama oma liikmeid suutlikkuse suurendamisel ja juhtima vastastikuste eksperdihindamiste ja võrgu- ja infoturbe õppuste korraldamist. **[ME 14]**

(13a) Võimaluse korral peaks liikmesriigid saama käesoleva direktiivi sätete kohaldamisel kasutada või kohandada olemasolevat organisatsioonilist struktuuri. **[ME 15]**

(14) Luua tuleks turvaline teabejagamistaristu, mis võimaldaks vahetada koostöövõrgus tundlikku ja konfidentsiaalset teavet. ***Selle eesmärgi saavutamiseks tuleks täielikult kasutada liidus olemasolevaid struktuure.*** Ilma et see piiraks liikmesriikide kohustust teatada koostöövõrgule ELi jaoks olulistest intsidentidest ja riskidest, peaksid liikmesriigid saama juurdepääsu teiste riikide konfidentsiaalsele teabele alles pärast seda, kui nad on tõendanud, et nende tehnilised, finants- ja inimressursid, protsessid ja sidetaristu tagavad nende tulemusliku, tõhusa ja turvalise osalemise võrgu töös**,** ***kasutades läbipaistvaid vahendeid***. **[ME 16]**

(15) Enamiku võrkude ja infosüsteemide operaatorid on eraettevõtjad ning seepärast on avaliku ja erasektori koostöö hädavajalik. Soodustada tuleks operaatorite endi mitteametlikke koostöömehhanisme võrgu- ja infoturbe tagamiseks. Nad peaksid koostööd tegema ka avaliku sektoriga ning jagama ***vastastikku*** teavet ja parimaid tavasid, ~~et saada~~ ***sealhulgas pakkuma*** intsidentide korral ~~pakutavat tegevustoetust~~ ***asjakohast teavet ja tegevustoetust ning strateegiliselt analüüsitud teavet***. ***Selleks et soodustada tulemuslikult teabe ja parimate tavade vahetamist, on tähtis tagada, et sellises teabevahetuses osalevad operaatorid ei oleks oma koostöö tõttu ebasoodsamas olukorras. On vaja piisavaid kaitsemeetmeid, et selline koostöö ei põhjustaks neile operaatoritele suuremaid nõuete mittejärgimisest tulenevaid riske või uusi kohustusi tulenevalt muu hulgas konkurentsi, intellektuaalomandi, andmekaitse või küberkuritegevuse alastest õigusaktidest, samuti suuremaid tegevus- või turvariske.*** **[ME 17]**

(16) Et tagada läbipaistvus ja ELi kodanikke ja operaatoreid nõuetekohaselt teavitada , peaksid ~~pädevad asutused~~ ***ühtsed kontaktpunktid*** looma ühise ***ELi-ülese*** veebisaidi, millel avaldada mittekonfidentsiaalset teavet intsidentide**,** riskide ja ***nende leevendamise võimaluste*** kohta ja ***anda vajaduse korral nõu asjakohaste hooldusmeetmete küsimustes***. ***Veebisaidil olev teave peaks olema kasutatavast seadmest sõltumatult kättesaadav. Sel veebisaidil tuleb piirduda ainult vajalike ja võimalikult anonüümsete isikuandmete avaldamisega***. **[ME 18]**

(17) Kui teavet peetakse konfidentsiaalseks vastavalt ELi ja riikide ärisaladust käsitlevatele eeskirjadele, tuleb käesolevas direktiivis sätestatud toimingute teostamisel ja direktiivi eesmärkide täitmisel selline konfidentsiaalsus tagada.

(18) Lähtudes eelkõige riikide kriisihalduse ~~alastest~~ kogemustest, peaksid komisjon ja liikmesriigid koostöös ENISAga töötama välja ELi võrgu- ja infoturbe koostöökava, milles määratletakse koostöömehhanismid, ***parimad tavad ja tegevusmudelid,*** et ***riske ja intsidente ennetada, avastada, neist teada anda ja nendega*** toime ~~-~~tulla ~~riskide ja intsidentidega~~. Koostöövõrgus edastatavate varajaste hoiatuste puhul tuleks seda kava nõuetekohaselt arvesse võtta. **[ME 19]**

(19) Varajastest hoiatustest tuleks võrgus teatada vaid siis, kui asjaomase intsidendi või riski ulatus või raskusaste on nii olulised või võivad muutuda nii oluliseks, et vajalik on teavitamine või reageerimise koordineerimine ELi tasandil. Seega tuleks varajast hoiatamist kasutada vaid ~~tegelike või võimalike~~ intsidentide või riskide puhul, mille ulatus kasvab kiiresti, mis ületavad riigi reageerimissuutlikkuse või mis mõjutavad mitut liikmesriiki. Nõuetekohase hindamise tarvis tuleks edastada kogu riski või intsidendi hindamiseks vajalik teave koostöövõrgule. **[ME 20]**

(20) Kui ~~pädevad asutused~~ ***ühtsed kontaktpunktid*** on saanud varajase hoiatuse ja seda hinnanud, peaksid nad kokku leppima koordineeritud reageerimises vastavalt ELi võrgu- ja infoturbe koostöökavale. ~~Pädevatele asutustele~~ ***Ühtsetele kontaktpunktidele, ENISAle*** ja komisjonile tuleks teatada koordineeritud reageerimise tulemusena riigi tasandil võetud meetmetest. **[ME 21]**

(21) Arvestades võrgu ja info turvalisusega seotud probleemide globaalsust, on vaja teha tihedamat rahvusvahelist koostööd, et parandada turbestandardeid ja teabevahetust ning edendada ühtset üleilmselt lähenemist võrgu- ja infoturbe küsimustele. ***Sellise rahvusvahelise koostöö raamistik peab vastama Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ***[1] ***ja Euroopa Parlamendi ja nõukogu määrusele (EÜ) nr 45/2001***[2]**. [ME 22]**

---

1 ***Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT L 281, 23.11.1995, lk 31).***

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

(22) Vastutus võrgu ja info turvalisuse tagamise eest lasub suuresti ~~haldusasutustel ja~~ operaatoritel. Asjakohaste regulatiivsete nõuete ja tööstuse vabatahtlike tegutsemisviiside kaudu tuleks levitada ja arendada ~~riskihalduskultuuri~~ ***riskihalduse***, ***tiheda koostöö ja usalduse kultuuri,*** mis hõlmaks riskihindamist ja riskist ***ja pahatahtlikust või juhuslikust intsidendist*** lähtuvalt asjakohaste turvameetmete rakendamist. Samuti on oluline kehtestada ***usaldusväärsed*** võrdsed tingimused, et koostöövõrk saaks tegelikult toimida ja et oleks tagatud kõigi liikmesriikide tulemuslik koostöö. **[ME 23]**

(23) Direktiiviga 2002/21/EÜ on kehtestatud nõue, et üldkasutatavaid elektroonilisi sidevõrke või üldkasutatavaid elektroonilisi sideteenuseid pakkuvad ettevõtjad peavad võtma asjakohased meetmed, et kindlustada nende terviklus ja turvalisus, ning nõuded teatada turvalisuse rikkumisest ja tervikluskaost. Euroopa Parlamendi ja nõukogu direktiivis 2002/58/EÜ[1], on sätestatud nõue, et üldkasutatava elektroonilise sideteenuse pakkuja peab võtma oma teenuste turvalisuse tagamiseks asjakohased tehnilised ja korralduslikud meetmed.

[1] 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).

(24) Neid kohustusi tuleks peale elektroonilise side sektori kohaldada ka ***elutähtsate infrastruktuuride operaatorite suhtes, kes sõltuvad suurel määral info- ja kommunikatsioonitehnoloogiast ning kelle tegevus on äärmiselt oluline, et säilitada majanduse ja ühiskonna jaoks hädavajalikud funktsioonid; nende hulka kuuluvad näiteks elektri-, gaasi-, transpordi- ja krediidiettevõtted, finantsturu taristu ja tervishoiuasutused. Selliste võrkude ja infosüsteemide töö katkestused mõjutaksid siseturgu. Kuigi käesolevas direktiivis sätestatud kohustusi ei tohiks peale elektroonilise side sektori kohaldada ka*** infoühiskonnateenuste peamiste pakkujate suhtes, kes on määratletud Euroopa Parlamendi ja nõukogu direktiivis 98/34/EÜ[1], ning kelle teenustele toetuvad infoühiskonna järgmise tasandi teenused ja tegevus internetis, nagu e-kaubanduse platvormid, internetimaksete lüüsid, sotsiaalvõrgustikud, otsingumootorid, pilvandmetöötluse teenused üldiselt või tarkvarakauplustes. ~~Katkestused sellistes infoühiskonna üldteenustes takistavad ka muude infoühiskonna teenuste pakkumist, mille olulised sisendid sõltuvad just sellistest üldteenustest. Tarkvaraarendajad ja riistvaratootjad ei ole infoühiskonna teenuste pakkujad ja seega jäetakse nemad välja. Need kohustused peaksid laienema ka haldusasutustele ja elutähtsate infrastruktuuride operaatoritele, kes sõltuvad suurel määral info- ja kommunikatsioonitehnoloogiast ning kelle tegevus on äärmiselt oluline, et säilitada majanduse ja ühiskonna jaoks hädavajalikud funktsioonid; nende hulka kuuluvad näiteks elektri- , gaasi- , transpordi- ja krediidiettevõtted, väärtpaberibörsid ja tervishoiuasutused. Selliste võrkude ja infosüsteemide töö katkestused mõjutaksid siseturgu.~~***, võivad kõnealused pakkujad vabatahtlikkuse alusel teavitada pädevat asutust või ühtset kontaktpunkti nendest võrgu turvaintsidentidest, mida nad vajalikuks peavad. Pädev asutus või ühtne kontaktpunkt esitab juhul, kui see on mõistlikult võimalik, intsidendist teatanud operaatoritele strateegilise analüüsitud teabe, mis aitab turvaohtu ületada.*** **[ME 24]**

---

[1] Euroopa Parlamendi ja nõukogu 22. juuni 1998. aasta direktiiv 98/34/EÜ, millega nähakse ette tehnilistest standarditest ja eeskirjadest ning infoühiskonna teenuste eeskirjadest teatamise kord (EÜT L 204, 21.7.1998, lk 37).

(24a) ***Kuigi riist- ja tarkvaratoodete pakkujaid ei ole käesoleva direktiiviga hõlmatud ettevõtjatega samaväärsed ettevõtjad, tugevdavad nende tooted võrgu ja teabesüsteemide turvalisust. Seetõttu on neil tähtis roll operaatorite toetamisel oma võrgu ja teabeinfrastruktuuri turvalisuse tagamises. Pidades silmas, et riist- ja tarkvaratoodete suhtes juba kohaldatakse kehtivaid tootjavastutuse eeskirju, peaksid liikmesriigid tagama nende eeskirjade jõustamise.*** **[ME 25]**

(25) ~~Haldusasutuste ja~~ Operaatorite suhtes kehtestatud tehnilised ja korralduslikud meetmed ei tohiks tähendada, et konkreetset turustatavat info- ja kommunikatsioonitehnoloogilist toodet tuleks projekteerida, arendada või toota konkreetsel viisil. **[ME 26]**

(26) ~~Haldusasutused ja~~ Operaatorid peaksid tagama nende kontrolli all olevate võrkude ja süsteemide turvalisuse. Eelkõige on tegemist privaatvõrkude ja -süsteemidega, mida haldavad kas asutuse enda IT-töötajad või mille turbega seotud teenused ostetakse sisse. Turbe- ja teatamiskohustust tuleks asjaomaste operaatorite ~~ja haldusasutuste~~ suhtes kohaldada olenemata sellest, kas nad haldavad oma võrke ja infosüsteeme ise või ostavad selle teenuse sisse. **[ME 27]**

(27) Vältimaks väikeste operaatorite ja kasutajate ebaproportsionaalset finants- ja halduskoormust, peaksid nõuded olema proportsionaalsed asjaomase võrgu või infosüsteemi puhul esineva riskiga, võttes sealjuures arvesse selliste meetmete kõrget tehnilist taset. Kõnealuseid nõudeid ei tuleks kohaldada mikroettevõtjate suhtes.

(28) Pädevad asutused ***ja ühtsed kontaktpunktid*** peaksid pöörama piisavat tähelepanu mitteametlike ja usaldusväärsete teabejagamiskanalite säilitamisele operaatorite ning avaliku ja erasektori vahel. ***Pädevad asutused ja ühtsed kontaktpunktid peaksid teavitama puudutatud IKT toodete ja teenuste tootjaid ja teenuseosutajaid neile teatatud intsidentidest, millel on oluline mõju.*** Pädevatele asutustele ***ja ühtsetele kontaktpunktidele*** teatatud intsidentide avalikustamisel tuleks seada tasakaalu üldsuse huvi saada ohtudest teada ning kahju, mida selline olukord võib põhjustada intsidendist teatanud ~~haldusasutuse või~~ operaatori mainele ja kaubandustegevusele. Teatamiskohustuse rakendamisel peaksid pädevad asutused ***ja ühtsed kontaktpunktid*** pöörama erilist tähelepanu sellele, et teave toote nõrkuste kohta jääks rangelt konfidentsiaalseks kuni asjakohase turvapaiga ***kasutuselevõtuni*** ~~avaldamiseni~~. ***Reeglina ei tohiks ühtsed kontaktpunktid avaldada intsidentides osalenud üksikisikute isikuandmeid. Ühtsed kontaktpunktid peaksid isikuandmeid avaldama üksnes siis, kui see on soovitud eesmärgi seisukohalt vajalik ja proportsionaalne.*** **[ME 28]**

(29) Pädevatel asutustel peaksid olema oma ülesannete täitmiseks vajalikud vahendid, kaasa arvatud volitused saada operaatoritelt ~~ja haldusasutustelt~~ võrgu või infosüsteemi turvalisuse taseme hindamiseks ***ning intsidentide arvu, tõsiduse ja ulatuse mõõtmiseks*** piisavat teavet ning usaldusväärseid ja põhjalikke andmeid reaalsete intsidentide kohta, mis on mõjutanud võrgu või infosüsteemi tööd. **[ME 29]**

(30) Sageli on intsidendi põhjuseks kuritegelik käitumine. Intsidendi seotust kuriteoga võib kahtlustada ka siis, kui alguses ei ole nende kahtluste kinnitamiseks piisavalt selgeid tõendeid. Sellises olukorras peaks pädevate asutuste***, ühtsete kontaktpunktide*** ja õiguskaitseasutuste asjakohane koostöö ***ning koostöö küberkuritegevuse vastase võitluse Euroopa keskusega (EC3) ja ENISAga*** olema osa tulemuslikust ja igakülgsest reageerimisest turvaintsidentide ohule. Ohutu, turvalise ja vastupidavama keskkonna edendamine eeldab, et intsidentidest, mille puhul kahtlustatakse seotust raske kuriteoga, teatatakse süstemaatiliselt õiguskaitseasutustele. Intsidendi seotust raske kuriteoga tuleks hinnata lähtuvalt liidu õigusaktidest küberkuritegevuse kohta. **[ME 30]**

(31) Sageli on intsidendi tagajärjeks isikuandmete kaitstuse rikkumine. ***Liikmesriigid ja operaatorid peaksid kaitsma salvestatud, töödeldud ja edastatud isikuandmeid juhusliku või ebaseadusliku hävitamise, juhusliku kaotsimineku või muutmise ning loata või ebaseadusliku salvestamise, juurdepääsu, avalikustamise ja levitamise eest ning tagama isikuandmete töötlemise turvapoliitika rakendamise.*** Sellises olukorras peaksid pädevad asutused***, ühtsed kontaktpunktid*** ja andmekaitseasutused omavahel koostööd tegema ja vahetama teavet ~~kõigis asjassepuutuvates küsimustes~~, ***asjakohasel juhul operaatoritega,*** et tulla toime intsidendi tagajärjel toimunud isikuandmetega seotud rikkumisega ***kooskõlas kehtivate andmekaitse-eeskirjadega***. ~~Liikmesriigid rakendavad~~ Turvaintsidentidest teatamise kohustust ***tuleks rakendada*** selliselt, et kui turvaintsidendiga kaasneb isikuandmetega seotud rikkumine ~~üksikisikute kaitset isikuandmete töötlemisel ja selliste andmete vaba liikumist käsitleva Euroopa Parlamendi ja nõukogu määruse[1] tähenduses~~, ***millest tuleb teavitada kooskõlas kohaldatavate liidu andmekaitse-eeskirjadega,*** oleks halduskoormus võimalikult väike. ENISA ~~peab sidet pädevate asutuste ja andmekaitseasutustega ning seega võiks ta aidata~~ ***peaks aitama*** luua teabevahetusmehhanismid ja ~~vormid, et vältida olukorda, kus tuleb kasutada kaht teatamisvormi. Ühtne teatamisvorm hõlbustaks~~ ***ühtse teavitamisvormi, mis hõlbustaks*** isikuandmete rikkumisega seotud intsidentidest teatamist ja vähendaks seega ettevõtjate ja haldusasutuste halduskoormust. **[ME 31]**

~~[1] SEC(2012)72 (final).~~

(32) Turvanõuete standardimine on ***vabatahtlik*** turumajanduslik protsess***, mis peaks võimaldama operaatoritel kasutada alternatiivseid meetmeid, et saavutada vähemalt samaväärseid tulemusi***. Et tagada turvastandardite ühtne kohaldamine, peaksid liikmesriigid julgustama konkreetsete ***koostalitlevate*** standardite järgimist ja vastavust neile, et tagada ELi tasandil turvalisuse kõrge tase. Selleks ***on vaja kaaluda avatud rahvusvaheliste standardite kohaldamist võrgu- ja infoturbele või selliste vahendite kavandamist. Teise sammuna*** võib osutuda vajalikuks harmoneeritud standardite koostamine, mida tuleks teha kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1025/2012[1].***Eelkõige tuleks Euroopa Telekommunikatsioonistandardite Instituuti (ETSI), Euroopa Standardikomiteed (CEN) ja Euroopa Elektrotehnika Standardikomiteed (CENELEC) volitada välja pakkuma tõhusaid ja tulemuslikke ELi avatud turvastandardeid, mille juures tuleks võimalikult vältida tehnoloogilisi eelistusi ning mida peaks väikestel ja keskmise suurusega ettevõtjatel olema kerge järgida. Küberjulgeoleku rahvusvahelised standardid tuleks hoolikalt läbi vaadata, et tagada, et neid ei ole kompromiteeritud ja et nad annavad piisava kaitse, ning kindlustada niimoodi, et küberjulgeoleku standardite õiguspärane järgimine parandab liidu küberjulgeoleku üldist taset, mitte vastupidi.*** **[ME 32]**

(33) Komisjon peaks ***kõigi huvitatud sidusrühmadega konsulteerides*** käesoleva direktiivi sätted regulaarselt läbi vaatama eelkõige selleks, et teha kindlaks, kas neid on vaja muuta seoses ***ühiskonna, poliitika,*** tehnoloogia ja turutingimuste muutumisega. **[ME 33]**

---

[1] 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).

(34) Et koostöövõrk saaks nõuetekohaselt toimida, tuleks komisjonile anda volitused võtta kooskõlas ELi toimimise lepingu artikliga 290 vastu õigusakte, et määratleda ~~kriteeriumid, millele liikmesriik peab vastama, et tal lubataks osaleda turvalises teabevahetussüsteemis,~~ ***ühised ühenduvuse- ja turbestandardid turvalise teabevahetuse infrastruktuuri jaoks ja*** panna paika selliste sündmuste täpsemad kirjeldused, mille puhul tuleks ~~kasuta~~ ***kasutada*** varajast hoiatust~~, ja määratleda asjaolud, mille korral operaatorid ja haldusasutused peavad intsidendist teatama~~.
[ME 34]

(35) On eriti tähtis, et komisjon viiks oma ettevalmistava töö käigus läbi asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil. Komisjon peaks delegeeritud õigusaktide ettevalmistamise ja koostamise ajal tagama asjaomaste dokumentide sama- ja õigeaegse ning nõuetekohase edastamise Euroopa Parlamendile ja nõukogule.

(36) Et tagada käesoleva direktiivi rakendamiseks ühetaolised tingimused, tuleks komisjonile anda rakendusvolitused seoses järgmisega: koostöövõrgu raames toimuv ~~pädevate asutuste~~ ***ühtsete kontaktpunktide*** ja komisjoni koostöö, ~~juurdepääs turvalisele teabevahetustaristule~~ ***ilma et see piiraks olemasolevate koostöömehhanismide tegevust riiklikul tasandil***, ELi võrgu- ja infoturbe koostöökava~~,~~ ***ning suure mõjuga*** intsidentidest ~~üldsusele~~ teatamise ~~vorm ja~~ kord ~~ning võrgu- ja infoturbe jaoks olulised standardid ja/või tehnilised kirjeldused~~. Neid volitusi tuleks teostada vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) nr 182/2011[1]. **[ME 35]**

[1] 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).

(37) Käesoleva direktiivi kohaldamisel peaks komisjon pidama vastavalt vajadusele sidet asjaomaste valdkondlike komiteede ja asjaomaste organitega, mis on loodud ELi tasandil eelkõige ***e-valitsuse,*** energeetika, transpordi***,*** tervishoiu ja ***kaitse*** valdkonnas. **[ME 36]**

(38) Teavet, mida pädev asutus ***või ühtne kontaktpunkt*** peab konfidentsiaalseks vastavalt ärisaladusi käsitlevatele ELi ja siseriiklikele eeskirjadele, tuleks komisjoni***, selle asjaomaste ametite, ühtsete kontaktpunktide ja/või*** ja teiste pädevate asutustega vahetada ainult siis, kui selline teabevahetus on hädavajalik käesoleva direktiivi kohaldamiseks. Vahetada võib ainult teavet, mis on sellise teabevahetuse eesmärgi seisukohast oluline***, vajalik*** ja proportsionaalne ***ning mille puhul tuleb järgida eelmääratletud konfidentsiaalsuse ja turvalisuse kriteeriume vastavalt otsusele 2011/292/EL või vaikimiskokkulepete või mitteametlike vaikimiskokkulepete alla kuuluv teave, näiteks protokoll teabe tundlikkuse märgistamise kohta fooritulede analoogia põhjal***. **[ME 37]**

(39) Koostöövõrgus riskide ja intsidentide kohta teabe jagamine ning intsidentidest riigi pädevatele asutustele ***või ühtsetele kontaktpunktidele*** teatamise nõude järgimine võib eeldada isikuandmete töötlemist. Selline isikuandmete töötlemine on vajalik käesoleva direktiivi eesmärgiks oleva üldiste huvide järgimise jaoks ja on seega õiguspärane vastavalt direktiivi 95/46/EÜ artiklile 7. Nimetatud õiguspärast eesmärki arvestades ei ole tegemist ebaproportsionaalse ega talumatu sekkumisega, mis kahjustaks olemuslikult Euroopa Liidu põhiõiguste harta artikliga 8 tagatud õigust isikuandmete kaitsele. Käesoleva direktiivi kohaldamisel tuleks vajaduse korral kohaldada Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 1049/2001[1]. Kui ELi institutsioonid ja organid töötlevad käesoleva direktiivi kohaldamisel andmeid, peaks see toimuma kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EÜ) nr 45/2001. **[ME 38]**

[1] Euroopa Parlamendi ja nõukogu 30. mai 2001. aasta määrus (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele (EÜT L 145, 31.5.2001, lk 43).

(40) Kuna liikmesriigid üksi ei suuda piisavalt saavutada käesoleva direktiivi eesmärke, st võrgu- ja infoturbe kõrge taseme tagamist ELis, ning tegevuse mõju tõttu on seda parem teha liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kooskõlas nimetatud artiklis sätestatud proportsionaalsuse põhimõttega ei lähe käesolev direktiiv nimetatud eesmärkide saavutamiseks vajalikust kaugemale.

(41) Käesolevas direktiivis järgitakse Euroopa Liidu põhiõiguste harta põhiõigusi ja põhimõtteid, eelkõige õigust eraelu ja edastatavate sõnumite puutumatusele, isikuandmete kaitset, ettevõtlusvabadust ning õigust tõhusale õiguskaitsevahendile kohtus ja õiglasele kohtulikule arutamisele. Käesolevat direktiivi tuleb rakendada kooskõlas nende õiguste ja põhimõtetega.

(41a) Kooskõlas liikmesriikide ja komisjoni 28. septembri 2011. aasta ühise poliitilise deklaratsiooniga selgitavate dokumentide kohta kohustuvad liikmesriigid lisama põhjendatud juhtudel ülevõtmismeetmeid käsitlevale teatele ühe või mitu dokumenti, milles selgitatakse seost direktiivi komponentide ja ülevõtvate siseriiklike õigusaktide vastavate osade vahel. Käesoleva direktiivi puhul leiab seadusandja, et kõnealuste dokumentide edastamine on põhjendatud. **[ME 39]**

(41b) Euroopa andmekaitseinspektoriga konsulteeriti kooskõlas määruse (EÜ) nr 45/2001 artikli 28 lõikega 2 ning ta esitas arvamuse[1] 14. juunil 2013,

ON VASTU VÕTNUD KÄESOLEVA DIREKTIIVI:

[1] ELT C 32, 4.2.2014, lk 19.

I PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese ja reguleerimisala

1. Käesoleva direktiiviga nähakse ette meetmed võrgu- ja infoturbe ühtlaselt kõrge taseme tagamiseks.

2. Selle eesmärgi saavutamiseks tehakse käesoleva direktiiviga järgmist:

   a) sätestatakse kõigile liikmesriikidele kohustused seoses võrke ja infosüsteeme mõjutavate riskide ja intsidentide vältimise ja käsitlemise ning neile reageerimisega;

   b) luuakse liikmesriikidevahelise koostöö mehhanism, et tagada käesoleva direktiivi ühetaoline kohaldamine ELis ning vajaduse korral võrke ja infosüsteeme mõjutavate riskide ja intsidentide koordineeritud**,** tõhus ja ***tulemuslik*** käsitlemine ja neile reageerimine ***asjakohaste sidusrühmade osalusel***; **[ME 40]**

   c) kehtestatakse operaatoritele ~~ja haldusasutustele~~ turvanõuded. **[ME 41]**

3. Käesoleva direktiivi artiklis 14 sätestatud turvanõudeid ei kohaldata direktiivis 2002/21/EÜ osutatud üldkasutatavaid sidevõrke või üldkasutatavaid elektroonilisi sideteenuseid pakkuvate ettevõtjate suhtes, kes peavad täitma konkreetseid turva- ja terviklusnõudeid, mis on sätestatud nimetatud direktiivi artiklites 13a ja 13b, ega usaldusteenuse pakkujate suhtes.

4. Käesolev direktiivi ei piira küberkuritegevust käsitlevate liidu õigusaktide ega nõukogu direktiivi 2008/114/EÜ[1] kohaldamist.

[1] Nõukogu 8. detsembri 2008. aasta direktiiv 2008/114/EÜ Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta (ELT L 345, 23.12.2008, lk 75).

5. Samuti ei piira käesolev direktiiv järgmiste õigusaktide kohaldamist: direktiiv 95/46/EÜ, direktiiv 2002/58/EÜ, ning määrus ***(EÜ) nr 45/2001***. ***Kasutada tohib ainult käesoleva direktiivi eesmärkidel hädavajalikke isikuandmeid ning andmed peavad olema võimalikult anonüümsed, kui mitte täiesti anonüümsed.*** **[ME 42]**

6. Info jagamisega koostöövõrgu raames vastavalt III peatükile ning võrgu- ja infoturbe intsidentidest teatamisega vastavalt artiklile 14 võib kaasneda vajadus töödelda isikuandmeid. Käesoleva direktiiviga taotletavate avaliku huvi eesmärkide saavutamise jaoks vajalikuks töötlemiseks peab olema liikmesriigi luba vastavalt direktiivi 95/46/EÜ artiklile 7 ja direktiivile 2002/58/EÜ selliselt, nagu neid siseriikliku õigusega kohaldatakse.

Artikkel 1a

Isikuandmete kaitse ja töötlemine

1. ***Käesoleva direktiivi kohane isikuandmete töötlemine toimub kooskõlas direktiividega 95/46/EÜ ja 2002/58/EÜ.***

2. ***Käesoleva direktiivi kohane isikuandmete töötlemine komisjoni ja ENISA poolt toimub kooskõlas määrusega (EÜ) nr 45/2001.***

3. ***Käesoleva direktiivi kohane isikuandmete töötlemine Europoli juures tegutseva küberkuritegevuse vastase võitluse Euroopa keskuse poolt toimub vastavalt otsusele 2009/371/JSK[1].***

4. ***Isikuandmete töötlemine on õiglane ja seaduslik ning piirdub üksnes minimaalse andmehulgaga, mis on vajalik nende eesmärkide saavutamiseks, milleks neid andmeid töödeldakse. Neid andmeid säilitatakse vormingus, mis võimaldab tuvastada andmesubjekti isikut mitte kauem, kui on vajalik selle eesmärgi saavutamiseks, milleks neid isikuandmeid töödeldakse.***

5. ***Käesoleva direktiivi artiklis 14 osutatud intsidentidest teatamine ei piira direktiivi 2002/58/EÜ artiklis 4 ja komisjoni määruses (EL) nr 611/2013[2] sätestatud isikuandmetega seotud rikkumisest teatamise normide ja kohustuste kohaldamist.*** **[ME 43]**

---

1 ***Nõukogu 6. aprilli 2009. aasta otsus 2009/371/JSK, millega asutatakse Euroopa Politseiamet (Europol) (ELT L 121, 15.5.2009, lk 37).***

2 ***Komisjoni 24. juuni 2013. aasta määrus (EL) nr 611/2013 meetmete kohta, mida kohaldatakse eraelu puutumatust ja elektroonilist sidet käsitleva Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ kohaselt isikuandmetega seotud rikkumiste teatamise suhtes (ELT L 173, 26.6.2013, lk 2).***

Artikkel 2

Minimaalne ühtlustamine

Miski ei takista liikmesriike võtmast vastu ja säilitamast sätteid, millega tagatakse turvalisuse kõrgem tase, ilma et see piiraks nende ELi õigusest tulenevaid kohustusi.

Artikkel 3

Mõisted

Käesolevas direktiivis kasutatakse järgmisi mõisteid:

(1) „võrk ja infosüsteem” –

a) elektrooniline sidevõrk direktiivis 2002/21/EÜ sätestatud tähenduses ja

b) seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub mõne programmi kohaselt ~~arvutiandmete~~ ***digitaalandmete*** automaatne töötlemine, ning **[ME 44]**

c) ~~arvutiandmed~~ ***digitaalandmed***, mida salvestatakse, töödeldakse, võetakse välja või edastatakse punktides a ja b kirjeldatud komponentide töö, kasutamise, kaitsmise või hooldamise jaoks. **[ME 45]**

(2) „turvalisus” – võrgu ja infosüsteemi võime panna teatava kindlusega vastu õnnetusele või pahatahtlikule tegevusele, mis seab ohtu salvestatud või edastatud andmete või selle võrgu ja infosüsteemi kaudu pakutavate või nende kaudu juurdepääsetavate teenuste käideldavuse, autentsuse, tervikluse ja konfidentsiaalsuse; ***turvalisus hõlmab nõuetekohaseid tehnilisi seadmeid, lahendusi ja töökorda, mis tagavad käesolevas direktiivis sätestatud turvanõuded;*** **[ME 46]**

(3) „risk” – ***mõistlikult tuvastatav*** asjaolu või sündmus, mis võib kahjustada turvalisust; **[ME 47]**

(4) „intsident” – ~~asjaolu või~~ sündmus, mis tegelikult kahjustab turvalisust; **[ME 48]**

~~(5) „infoühiskonna teenus” – teenus direktiivi 98/34/EÜ artikli 1 punkti 2 tähenduses;~~ **[ME 49]**

(6) „võrgu- ja infoturbe koostöökava” – kava, millega luuakse organisatsiooniliste ülesannete, vastutuse ja protseduuride raamistik, et säilitada või taastada võrkude ja infosüsteemide töö neid mõjutava ohu või intsidendi korral;

(7) „intsidentide käsitlemine” – intsidendi ***avastamist, ennetamist,*** analüüsimist ja ohjeldamist ning intsidendile reageerimist toetavad protseduurid; **[ME 50]**

(8) „operaator” –

~~a) muude infoühiskonna teenuste pakkumist võimaldavate infoühiskonna teenuste pakkuja; infoühiskonna teenuste mittetäielik loetelu on esitatud II lisas;~~ **[ME 51]**

b) energeetika, transpordi, panganduse, ~~väärtpaberitega kauplemise~~ ***finantsturu taristu, interneti vahetuspunktide, toiduainete tarneahela*** ja tervishoiu valdkonnas esmatähtsa majandusliku ja ühiskondliku tegevuse säilitamiseks vajaliku ~~elutähtsa~~ ***sellise*** infrastruktuuri operaator***, mille katkestused või hävimine avaldaks liikmesriigis nimetatud funktsioonide täitmata jätmise tõttu suurt mõju***; operaatorite mittetäielik loetelu on esitatud II lisas***, juhul kui asjaomane võrk ja infosüsteem on seotud tema põhiteenustega***; **[ME 52]**

(8a) „olulise mõjuga intsident” – infovõrgu või -süsteemi turvalisust ja pidevust kahjustav intsident, mis toob kaasa majanduse ja ühiskonna jaoks hädavajalike funktsioonide olulise katkestuse; **[ME 53]**

(9) „standard” – määruses (EL) nr 1025/2012 osutatud standard;

(10) „spetsifikatsioon” – määruses (EL) nr 1025/2012 osutatud spetsifikatsioon;

(11) „usaldusteenuse pakkuja” – füüsiline või juriidiline isik, kes pakub elektroonilist teenust, mis seisneb e-allkirjade, e-templite, e-ajatemplite, e-dokumentide, e-andmevahetusteenuste, veebisaitide autentimise ja e-tõendite, sealhulgas e-allkirja ja e-templi jaoks vajalike sertifikaatide loomises, kontrollimises, valideerimises, käsitlemises ja säilitamises.

(11a) „reguleeritud turg” – reguleeritud turg, nagu see on määratletud Euroopa Parlamendi ja nõukogu direktiivi 2004/39/EÜ artikli 4 punktis 14[1]; [ME 54]

(11b) „mitmepoolne kauplemissüsteem” – mitmepoolne kauplemissüsteem, nagu see on määratletud direktiivi 2004/39/EÜ artikli 4 punktis 15; [ME 55]

(11c) „organiseeritud kauplemissüsteem” – mitmepoolne süsteem, mis pole reguleeritud turg, mitmepoolne kauplemissüsteem või keskne osapool, kelle tegevust korraldab investeerimisettevõte või turu korraldaja, kus osakuid võlakirjades, struktureeritud finantstoodetes, lubatud heitkoguse ühikutes või tuletisinstrumentides ostev ja müüv kolmas osapool saab süsteemis suhelda viisil, mis viib lepingu sõlmimiseni kooskõlas direktiivi 2004/39/EÜ II jaotise sätetega. [ME 56]

---

[1] ***Euroopa Parlamendi ja nõukogu 21. aprilli 2004. aasta direktiiv 2004/39/EÜ finantsinstrumentide turgude kohta (ELT L 45, 16.2.2005, lk 18).***

II PEATÜKK
VÕRGU- JA INFOTURBE RIIKLIKUD RAAMISTIKUD

Artikkel 4
Põhimõte

Liikmesriigid tagavad oma territooriumil võrgu ja infosüsteemide turvalisuse kõrge taseme kooskõlas käesoleva direktiiviga.

Artikkel 5
Riiklik võrgu ja infoturbe strateegia ning riiklik võrgu ja infoturbe koostöökava

1. Iga liikmesriik võtab vastu riikliku võrgu- ja infoturbe strateegia, milles määratletakse strateegilised eesmärgid ning konkreetsed poliitilised ja regulatiivsed meetmed, mille abil saavutada võrgu ja info turvalisuse kõrge tase ja seda säilitada. Eelkõige käsitletakse riiklikus võrgu- ja infoturbe strateegias järgmisi küsimusi:

   a) strateegia eesmärkide ja prioriteetide määratlus, lähtudes ajakohasest riski- ja intsidendianalüüsist;

   b) juhtimisraamistik, mille toel strateegia eesmärgid ja prioriteedid ellu viia; see hõlmab valitsusasutuste ja muude asjaosaliste ülesannete ja vastutuse selget määratlust;

c) valmisoleku, reageerimise ja taaste üldmeetmete, kaasa arvatud avaliku ja erasektori koostöö mehhanismide kindlaksmääramine;

d) teadlikkuse suurendamise ning haridus- ja koolitusprogrammide kirjeldus;

e) teadus- ja arendustegevuse kavad ja kirjeldus selle kohta, kuidas neis kavades kajastuvad määratletud prioriteedid.

ea) liikmesriigid võivad paluda ENISA abi oma riiklike võrgu- ja infoturbe strateegiate ja riiklike võrgu- ja infoturbe koostöökavade väljatöötamisel, tuginedes ühisele minimaalsele võrgu- ja infoturbe strateegiale ja koostöökavale. **[ME 57]**

2. Riiklik võrgu- ja infoturbe strateegia sisaldab riiklikku võrgu- ja infoturbe koostöökava, mis vastab vähemalt järgmistele nõuetele:

a) ~~riski hindamise kava~~ ***riskihalduse raamistik***, et ~~teha kindlaks riskid ja hinnata~~ ***luua metoodika riskide kindlakstegemiseks, prioriseerimiseks, hindamiseks ja käsitlemiseks,*** võimalike intsidentide mõju ***hindamine, ennetus- ja kontrollivõimalused ning võimalike vastumeetmete valiku kriteeriumid***; **[ME 58]**

b) ~~kava~~ ***raamistiku*** rakendamises osalevate ***asutuste ja muude*** isikute ülesannete ja vastutuse määratlus; **[ME 59]**

c) vältimise, avastamise, reageerimise, parandamise ja taaste tagamiseks vajalike ja vastavalt hoiatustasemetele kohandatud koostöö- ja teavitusprotsesside määratlus;

d) võrgu- ja infoturbe õppuste ja koolituste plaan, mille põhjal kava kinnistada, valideerida ja katsetada. Omandatud kogemused tuleb dokumenteerida ja kava ajakohastamisel neid arvesse võtta.

3. Riiklik võrgu- ja infoturbe strateegia ning riiklik võrgu- ja infoturbe koostöökava edastatakse komisjonile ~~ühe~~ ***kolme*** kuu jooksul pärast seda, kui need on vastu võetud. **[ME 60]**

Artikkel 6

*Riigi ~~pädev asutus~~ **pädevad asutused ja ühtsed kontaktpunktid** võrgu ja infosüsteemide turbe vallas* **[ME 61]**

1. Iga liikmesriik nimetab võrgu ja infosüsteemide turbe vallas ***ühe või mitu*** oma riigi ~~pädeva asutuse~~ ***pädevat tsiviilasutust*** (edaspidi „pädev asutus ***/ pädevad asutused***"). **[ME 62]**

2. Pädevad asutused jälgivad käesoleva direktiivi rakendamist riigi tasandil ning aitavad kaasa selle ühetaolisele kohaldamisele kogu ELis.

2a. Kui liikmesriik nimetab rohkem kui ühe pädeva asutuse, siis ta nimetab riigi tsiviilasutuse, näiteks pädeva asutuse võrgu ja infosüsteemide turbe valdkonnas riiklikuks ühtseks kontaktpunktiks (edaspidi „ühtne kontaktpunkt"). Kui liikmesriik nimetab ainult ühe pädeva asutuse, siis on see pädev asutus ka ühtne kontaktpunkt. **[ME 63]**

2b. Ühe liikmesriigi pädevad asutused ja ühtne kontaktpunkt teevad tihedat koostööd seoses käesolevas direktiivis sätestatud kohustustega. **[ME 64]**

2c. ***Ühtne kontaktpunkt tagab piiriülese koostöö teiste ühtsete kontaktpunktidega.*** **[ME 65]**

3. Liikmesriigid tagavad, et pädevatel asutustel ***ja ühtsetel kontaktpunktidel*** oleksid piisavad tehnilised, rahalised ja inimressursid, mis võimaldaksid neil oma ülesandeid tulemuslikult ja tõhusalt täita ning seeläbi saavutada käesoleva direktiivi eesmärgid. Liikmesriigid tagavad ~~pädevate asutuste~~ ***ühtsete kontaktpunktide*** tõhusa, tulemusliku ja turvalise koostöö artiklis 8 osutatud koostöövõrgu kaudu. **[ME 66]**

4. Liikmesriigid tagavad, et pädevad asutused ***ja ühtsed kontaktpunktid – kui see on asjakohane käesoleva artikli lõike 2a kohaselt*** **–** saavad kätte ~~haldusasutuste ja~~ operaatorite teated intsidentide kohta vastavalt artikli 14 lõikele 2 ning et neile antakse artiklis 15 osutatud rakendamis- ja jõustamispädevus. **[ME 67]**

4a. ***Kui liidu õigusaktides nähakse ette valdkondlik liidu reguleeriv või järelevalveasutus, muu hulgas võrgu ja infosüsteemide turbe valdkonnas, siis saab see asutus selle sektori asjaomaste operaatorite teated intsidentide kohta vastavalt artikli 14 lõikele 2 ning talle antakse artiklis 15 osutatud rakendamis- ja jõustamispädevus. Kõnealune liidu asutus teeb nende kohustuste valdkonnas tihedat koostööd vastuvõtva liikmesriigi pädevate asutustega ja ühtsete kontaktpunktidega. Vastuvõtva liikmesriigi ühtne kontaktpunkt esindab liidu asutust III peatüki kohustuste puhul.* **[ME 68]**

5. Vajaduse korral konsulteerivad pädevad asutused ***ja ühtsed kontaktpunktid*** riigi asjaomaste õiguskaitseasutuste ja andmekaitseasutustega, ning teevad nendega koostööd. **[ME 69]**

6. Iga liikmesriik teatab komisjonile viivitamata ~~pädeva asutuse~~ ***pädevate asutuste ja ühtse kontaktpunkti*** määramisest, ~~tema~~ ***nende*** ülesannetest ja nende hilisemast muutmisest. Iga liikmesriik avalikustab määratud ~~pädeva asutuse~~ ***pädevad asutused***. **[ME 70]**

Artikkel 7

Infoturbeintsidentidega tegelev meeskond

1. Iga liikmesriik loob ***vähemalt ühe*** infoturbeintsidentidega tegeleva rühma (CERT) ***iga II lisas nimetatud sektori jaoks***, kes vastutab intsidentide ja riskide käsitlemise eest põhjalikult määratletud protseduuri kohaselt ning vastab I lisa punktis 1 osutatud nõuetele. CERTi võib luua pädeva asutuse osana. **[ME 71]**

2. Liikmesriigid tagavad, et CERTil on I lisa punktis 2 osutatud ülesannete tulemuslikuks täitmiseks piisavad tehnilised, rahalised ja inimressursid.

3. Liikmesriigid tagavad, et riigi tasandil on CERTi kasutada turvaline ja vastupidav side- ja infotaristu, mis sobib kokku ja on koostalitlusvõimeline artiklis 9 osutatud turvalise infojagamissüsteemiga.

4. Liikmesriigid teatavad komisjonile, millised on CERTi ressursid, volitused ja intsidentide käsitlemise protsess.

5. ~~CERT tegutseb~~ ***CERTid tegutsevad*** pädeva asutuse ***või ühtse kontaktpunkti*** järelevalve all ning ~~pädev~~ ***see*** asutus kontrollib regulaarselt, kas ~~CERTi~~ ***CERTide*** ressursid, volitused ja intsidentide käsitlemise protsessi tulemuslikkus on piisavad. **[ME 72]**

5a. Liikmesriigid tagavad, et CERTidel on piisavad inim- ja finantsressursid, et osaleda aktiivselt rahvusvahelistes ja eelkõige ELi koostöövõrkudes. **[ME 73]**

5b. CERTidel võimaldatakse ja soovitatakse algatada ühisõppusi teiste CERTidega, kõigi liikmesriikide CERTide ning kolmandate riikide asjaomaste asutustega, samuti rahvusvaheliste institutsioonide, näiteks Põhja-Atlandi Lepingu Organisatsiooni ja Ühendatud Rahvaste Organisatsiooni CERTidega, ning sellistes ühisõppustes osaleda. **[ME 74]**

5c. Liikmesriigid võivad oma riiklike CERTide arendamisel paluda abi ENISA-lt või teistelt liikmesriikidelt. **[ME 75]**

III PEATÜKK

PÄDEVATE ASUTUSTE KOOSTÖÖ

Artikkel 8

Koostöövõrk

1. ~~Pädevad asutused~~ ***Ühtsed kontaktpunktid*** ja komisjon ***ning ENISA*** moodustavad võrgu (edaspidi „koostöövõrk”), et teha koostööd võitlemiseks võrku ja infosüsteeme mõjutavate riskide ja intsidentidega. **[ME 76]**

2. Koostöövõrk võimaldab pidevat teabevahetust komisjoni ja ~~pädevate asutuste~~ ***ühtsete kontaktpunktide*** vahel. Taotluse korral abistab ~~Euroopa Võrgu- ja Infoturbeamet~~ (~~„~~ENISA~~”~~) koostöövõrku oma teadmiste ja nõuannetega. ***Vajaduse korral võib kutsuda operaatoreid ja küberjulgeolekulahenduste pakkujaid osalema koostöövõrgu tegevuses, millele on osutatud lõike 3 punktides g ja i.***

Vajaduse korral teeb võrk koostööd andmekaitseasutustega.

Komisjon teavitab korrapäraselt turvauuringute koostöövõrgustikku ja muid algatuse Horisont 2020 asjakohaseid programme. **[ME 77]**

3. ~~Pädevad asutused~~ ***Ühtsed kontaktpunktid*** teevad koostöövõrgus järgmist:

a) levitavad varajasi hoiatusi riskide ja intsidentide kohta vastavalt artiklile 10;

b) tagavad koordineeritud reageerimise vastavalt artiklile 11;

c) avaldavad ühisel veebisaidil korrapäraselt mittekonfidentsiaalset teavet töös olevate varajaste hoiatuste ja koordineeritud reageerimise kohta;

d) arutavad ja hindavad ~~ühe liikmesriigi või komisjoni taotlusel~~ ühiselt üht või mitut artiklis 5 osutatud riiklikku võrgu- ja infoturbe strateegiat või riiklikku võrgu- ja infoturbe koostöökava käesoleva direktiivi reguleerimisala piires;

e) arutavad ja hindavad ~~liikmesriigi või komisjoni taotlusel~~ ühiselt CERTide töö tulemuslikkust, eelkõige juhul, kui ELi tasandil toimuvad võrgu- ja infoturbe õppused;

f) teevad koostööd ja vahetavad ~~infot~~ ***oskusteavet*** asjakohastel teemadel ***võrgu- ja infoturbe kohta,*** eelkõige andmekaitse, energeetika, transpordi, panganduse, ***finantsturgude*** ja tervishoiu vallas Europoli juures tegutseva küberkuritegevuse vastase võitluse Euroopa keskuse ja muude asjaomaste Euroopa asutustega ~~kõigil väärtpaberitega kauplemise~~;

fa) vajaduse korral teavitavad ELi terrorismivastase võitluse koordinaatorit aruannete abil ning võivad paluda abi koostöövõrgustiku ettevalmistamise ja tegevuse analüüsimisel;

g) vahetavad omavahel ja komisjoniga infot ja parimaid tavasid ning aitavad üksteist võrgu- ja infoturbe alase suutlikkuse loomisel;

~~h) korraldavad vastastikku suutlikkuse ja valmisoleku eksperdihindamisi;~~

i) korraldavad ELi tasandil võrgu- ja infoturbe õppusi ja osalevad vastavalt vajadusele rahvusvahelistel võrgu- ja infoturbe õppustel;

ia) on kaasatud ja konsulteerivad operaatoritega nende võrku ja infosüsteeme kahjustavate ohtude ja intsidentide küsimuses ning vajaduse korral vahetavad selleteemalist teavet;

***ib) töötavad koostöös ENISAga lisaks artikli 14 lõikes 2 sätestatud parameetritele välja sektoripõhiste kriteeriumide suunised olulistest intsidentidest teatamiseks, et saavutada nende ühine tõlgendamine, järjepidev kohaldamine ja sidus rakendamine liidus* [ME 78]**

3a. ***Koostöövõrk avaldab kord aastas eelneva 12 kuu kohta aruande, mis põhineb võrgu tegevusel ja käesoleva direktiivi artikli 14 lõike 4 kohaselt esitatud koondaruandel.*** **[ME 79]**

4. Komisjon kehtestab rakendusaktidega korra, mis hõlbustaks lõigetes 2 ja 3 osutatud koostööd ~~pädevate asutuste~~ ***ühtsete kontaktpunktide, ENISA*** ja komisjoni vahel. ~~Nimetatud~~ ***Kõnealused*** rakendusaktid võetakse vastu artikli 19 ~~lõikes 2~~ ***lõikes 3*** osutatud ~~nõuandemenetlusega~~ ***kontrollimenetluse kohaselt***. **[ME 80]**

Artikkel 9

Turvaline infojagamissüsteem

1. Koostöövõrgus vahetatakse tundlikku ja konfidentsiaalset infot turvalise taristu kaudu.

1a. Turvalise taristu osalejad järgivad kõikides töötlemise etappides muu hulgas asjakohaseid konfidentsiaalsus- ja turvalisusmeetmeid vastavalt direktiivile 95/46/EÜ ja määrusele (EÜ) nr 45/2001. **[ME 81]**

~~2. Komisjonile antakse volitused võtta vastavalt artiklile 18 vastu delegeeritud õigusaktid, et määratleda kriteeriumid millele liikmesriik peab vastama, et tal lubataks osaleda turvalises infojagamissüsteemis; kriteeriumid puudutavad järgmist:~~

~~a) turvalise ja vastupidava ning koostöövõrgu turvalise taristuga koosolu- ja koostalitlusvõimelise side- ja infotaristu käideldavus riigi tasandil vastavalt artikli 7 lõikele 3 ning~~

~~b) piisavate tehniliste, rahaliste ja inimressursside ning protsesside olemasolu pädevas asutuses ja CERTis, mis võimaldaks tulemuslikku, tõhusat ja turvalist osalust turvalises infojagamissüsteemis vastavalt artikli 6 lõikele 3 ning artikli 7 lõigetele 2 ja 3.~~ **[ME 82]**

3. ~~Lähtudes lõigetes 2 ja 3 osutatud kriteeriumidest, võtab komisjon rakendusaktidega vastu otsused liikmesriikide juurdepääsu kohta sellele turvalisele taristule. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 19 lõikes 3 osutatud kontrollimenetlusega.~~ ***Komisjon võtab kooskõlas artikliga 18 delegeeritud õigusaktidega vastu ühised ühenduvuse ja turbestandardid, mida järgivad ühtsed kontaktpunktid enne tundliku ja konfidentsiaalse teabe vahetamist koostöövõrgu raames.*** **[ME 83]**

Artikkel 10

Varajased hoiatused

1. ~~Pädevad asutused~~ ***Ühtsed kontaktpunktid*** ja komisjon annavad koostöövõrgus varajasi hoiatusi riskide ja intsidentide kohta, mis vastavad vähemalt ühele järgmistest tingimustest:

   ~~a) nende ulatus kasvab või võib kasvada kiiresti;~~

   b) ~~need ületavad või võivad~~ ***ühtne kontaktpunkt annab hinnangu, et risk või intsident võib*** ületada riigi ~~reageerimissuulikkuse~~ ***reageerimissuutlikkust***;

   c) ~~need mõjutavad või võivad mõjutada~~ ***ühtsete kontaktpunktide või komisjoni hinnangul mõjutab risk või intsident*** rohkem kui üht liikmesriiki. **[ME 84]**

2. Varajases hoiatuses ~~edastab pädev asutus või~~ ***edastavad ühtsed kontaktpunktid ja*** komisjon ***asjatu viivituseta*** kogu ~~talle~~ ***neile*** teadaoleva asjakohase teabe, mis võib olla riski või intsidendi hindamiseks kasulik. **[ME 85]**

~~3. Komisjon võib mõne liikmesriigi taotlusel või omal algatusel paluda, et liikmesriik esitaks kogu asjakohase teabe konkreetse riski või intsidendi kohta.~~ **[ME 86]**

4. Kui kahtlustatakse, et varajases hoiatuses käsitletav risk või intsident on seotud ***raske*** kuriteoga, ~~teatab pädev asutus või komisjon~~ ***ja kui asjaomane operaator on teatanud kahtlustatavatest raske kuriteoga seotud intsidentidest, millele on osutatud artikli 15 lõikes 4, tagab liikmesriik, et vastavalt vajadusele teatatakse*** sellest Europoli juures tegutsevale küberkuritegevuse vastase võitluse Euroopa keskusele. **[ME 87]**

4a. Koostöövõrgu liikmed ei avalda mis tahes teavet, mida nad on saanud lõikes 1 osutatud riskide ja intsidentide kohta, ilma saamata selleks teavitanud ühtselt kontaktpuntkilt eelnevat heakskiitu.

Enne teabe jagamist koostöövõrgus teavitab ühtne kontaktpunkt oma kavatsusest operaatorit, kellega teave on seotud, ning kui ta peab seda asjakohaseks, siis ta muudab kõnealuse teabe anonüümseks. **[ME 88]**

4b. Kui kahtlustatakse, et varajases hoiatuses käsitletav risk või intsident on tõsist piiriülest tehnilist laadi, teavitab ühtne kontaktpunkt või komisjon sellest ENISAt. **[ME 89]**

5. Komisjonile antakse volitused võtta vastavalt artiklile 18 vastu delegeeritud õigusakte selliste riskide ja intsidentide täpsemate spetsifikatsioonide kohta, mille puhul tuleb esitada käesoleva artikli lõikes 1 osutatud varajane hoiatus.

Artikkel 11

Koordineeritud reageerimine

1. Pärast artiklis 10 osutatud varajast hoiatust lepivad ~~pädevad asutused~~ ***ühtsed kontaktpunktid*** asjakohase info hindamise järel ***asjatu viivituseta*** kokku koordineeritud reageerimises vastavalt artiklis 12 osutatud ELi võrgu- ja infoturbe koostöökavale. **[ME 90]**

2. Koordineeritud reageerimise tulemusena riigi tasandil võetud meetmetest teatatakse koostöövõrgule.

Artikkel 12

ELi võrgu- ja infoturbe koostöökava

1. Komisjonile antakse volitused võtta rakendusaktiga vastu ELi võrgu- ja infoturbe koostöökava. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 19 lõikes 3 osutatud kontrollimenetlusega.

2. ELi võrgu- ja infoturbe koostöökava sisaldab järgmist:

   a) artikli 10 kohaldamiseks:

      – ~~pädevate asutuste~~ ***ühtsete kontaktpunktide*** poolt riskide ja intsidentide kohta kogutava ja jagatava ühilduva ja võrreldava teabe vormingu ning kogumise ja jagamise korra määratlus; **[ME 91]**

      – koostöövõrgus riskidele ja intsidentidele hinnangu andmise protseduuride ja kriteeriumide määratlus;

   b) artikli 11 kohase koordineeritud reageerimise protsessid, kaasa arvatud ülesannete, vastutuse ja koostööprotseduuride kindlaksmääramine;

   c) võrgu- ja infoturbe õppuste ja koolituste plaan, mille põhjal kava kinnistada, valideerida ja katsetada;

   d) liikmesriikide vahelise teadmussiirde programm suutlikkuse suurendamiseks ja vastastikuseks õppimiseks;

   e) liikmesriikidevaheline teadlikkuse suurendamise ja koolitusprogramm.

3. ELi võrgu- ja infoturbe koostöökava võetakse vastu hiljemalt üks aasta pärast käesoleva direktiivi jõustumist ning see vaadatakse regulaarselt läbi. ***Iga läbivaatamise tulemused teatatakse Euroopa Parlamendile.*** **[ME 92]**

3a. Tagatakse liidu võrgu- ja infoturbe koostöökava sidusus artiklis 5 ette nähtud riiklike võrgu- ja infoturbe strateegiate ja koostöökavadega. **[ME 93]**

Artikkel 13

Rahvusvaheline koostöö

EL võib sõlmida rahvusvahelisi lepinguid kolmandate riikide või rahvusvaheliste organisatsioonidega, et võimaldada neil osaleda ja korraldada nende osalus mõningates koostöövõrgu tegevustes, ilma et see piiraks koostöövõrgu võimalusi teha mitteametlikku rahvusvahelist koostööd. Sellises lepingus arvestatakse vajadusega tagada koostöövõrgus ringlevate isikuandmete piisav kaitse***, ilma et kolmandatele pooltele avaldataks ELi kodanike isikuandmeid, ning kehtestatakse järelevalvemenetlus, mida tuleb järgida, et tagada selliste isikuandmete kaitse***. ***Euroopa Parlamenti teavitatakse selliste lepingute üle peetavatest läbirääkimistest. Isikuandmeid tohib edastada liitu mittekuuluvates riikides asuvatele vastuvõtjatele ainult juhul, kui see on kooskõlas direktiivi 95/46/EÜ artiklitega 25 ja 26 ning määruse (EÜ) nr 45/2001 artikliga 9***.* **[ME 94]**

Artikkel 13a

Operaatorite kriitilise tähtsuse tase

Liikmesriikidel on õigus määrata operaatorite kriitilise tähtsuse tase, võttes arvesse sektorite eripära, parameetreid, nagu konkreetse operaatori tähtsus sektori teenuse asjakohase taseme säilitamisel, operaatori osutatava teenuse kasutajate arv ja ajavahemik, milleni operaatori põhiteenuste katkestusel on negatiivne mõju esmatähtsa majandusliku ja sotsiaalse tegevuse säilitamisele. **[ME 95]**

IV PEATÜKK

HALDUSASUTUSTE JA OPERAATORITE VÕRKUDE JA INFOSÜSTEEMIDE TURVE

Artikkel 14

Turvanõuded ja intsidentidest teatamine

1. Liikmesriigid tagavad, et ~~haldusasutused ja~~ operaatorid võtavad vajalikud ***ja proportsionaalsed*** tehnilised ~~ja~~ ***ning*** korralduslikud meetmed, et ***avastada ja tulemuslikult*** hallata riske, mis ohustavad nende kontrollitavate ja nende töös kasutatavate võrkude ja infosüsteemide turvalisust. Tehnika taset arvesse võttes tagatakse nende meetmetega ***olemasolevale ohule vastav*** turvalisuse tase~~, mis on vastavuses konkreetse ohuga~~. Eelkõige võetakse meetmeid, et vältida ***võrkude*** ja ***infosüsteemide turvalisust mõjutavaid intsidente ja*** minimeerida nende ~~asutuste pakutavate põhiteenuste võrku ja infosüsteemi kahjustavate intsidentide~~ mõju ***pakutavatele põhiteenustele*** ning tagada seega neid võrke ja infosüsteeme kasutavate teenuste pidevus. **[ME 96]**

2. Liikmesriigid tagavad, et ~~haldusasutused ja~~ operaatorid teatavad ***põhjendamatu viivituseta*** pädevale asutusele ***või ühtsele kontaktpunktile*** intsidentidest, millel on oluline mõju nende pakutavate põhiteenuste ~~turvalisusele~~ ***pidevusele***. ***Teavitamine ei suurenda teavitava osapoole vastutust.***

Intsidendi mõju kindlaks tegemiseks võetakse arvesse muu hulgas järgmisi parameetreid: **[ME 97]**

a) nende kasutajate arv, kelle põhiteenust mõjutatakse; **[ME 98]**

b) intsidendi kestus; **[ME 99]**

c) intsidendist mõjutatud geograafilise ala ulatus. **[ME 100]**

Neid parameetreid täpsustatakse kooskõlas artikli 8 lõike 3 punktiga ib. **[ME 101]**

2a. ***Operaatorid teavitavad lõigetes 1 ja 2 viidatud intsidentidest selle liikmesriigi pädevale asutusele või ühtsele kontaktpunktile, kus põhiteenusele mõju avaldati. Kui mõjutatakse rohkem kui ühe liikmesriigi põhiteenuseid, hoiatab teate saanud ühtne kontaktpunkt operaatori antud teabe põhjal teisi asjaomaseid ühtseid kontaktpunkte. Operaatorile tuleb võimalikult kiiresti teatada, missuguseid teisi ühtseid kontaktpunkte on intsidendist teavitatud, samuti teavitada teda võetud meetmetest, tulemustest ja muust intsidendiga seoses olulisest teabest.*** **[ME 102]**

2b. ***Kui teade sisaldab isikuandmeid, avaldatakse see ainult teavitatud pädeva asutuse ja ühtse kontaktpunkti vastuvõtjale, kel on vaja neid andmeid töödelda oma ülesannete täitmiseks kooskõlas andmekaitse-eeskirjadega. Avaldatakse vaid nende ülesannete täitmiseks hädavajalikke andmeid.*** **[ME 103]**

2c. ***II lisaga hõlmamata operaatorid võivad teatada artikli 14 lõikes 2 nimetatud intsidentidest vabatahtlikult.*** **[ME 104]**

3. Lõikeid 1 ja 2 kohaldatakse kõigi operaatorite suhtes, kes pakuvad Euroopa Liidus teenuseid.

4. ***Teavitatud pädeva asutuse ja asjaomase operaatoriga konsulteerimise järel võib ühtne kontaktpunkt teavitada üldsust üksikutest intsidentidest,*** kui ~~pädev asutus~~ ***ta*** leiab, et intsidendi ~~avalikustamine on üldsuse huvides, võib ta üldsust teavitada või nõuda, et seda teeks haldusasutus või operaator~~ ***ärahoidmiseks või käimasoleva intsidendiga toimetulemiseks või kui operaator, keda intsident mõjutab, on keeldunud tegelema selle intsidendiga seotud tõsise struktuurilise haavatavusega***.

Enne üldsusele avaldamist tagab teavitatud pädev asutus, et asjaomasel operaatoril on võimalus olla ära kuulatud ning otsus üldsusele avaldamise kohta on täielikult vastavuses üldsuse huviga.

Kui teave üksikute intsidentide kohta tehakse avalikuks, tagab teavitatud pädev asutus või ühtne kontaktpunkt selle muutmise võimalikult anonüümseks.

Pädev asutus või ühtne kontaktpunkt esitab juhul, kui see on mõistlikult võimalik, intsidendist teatanud operaatoritele strateegilise analüüsitud teabe, mis aitab turvaohtu ületada.

Kord aastas esitab ~~pädev asutus~~ ***ühtne kontaktpunkt*** koostöövõrgule koondaruande käesoleva lõike kohaselt saadud teadete***, sealhulgas teadete arvu kohta,*** ja ***käesoleva artikli lõikes 2 loetletud intsidendi parameetrite kohta,*** ja meetmete kohta, mis on võetud kooskõlas käesoleva lõikega. **[ME 105]**

4a. Liikmesriigid julgustavad operaatoreid andma nende ettevõttega seotud intsidentidest vabatahtlikult teada finantsaruannetes. **[ME 106]**

~~5. Komisjonile antakse volitused võtta vastavalt artiklile 18 vastu delegeeritud õigusakte nende asjaolude määratlemiseks, mille korral haldusasutused ja operaatorid peavad intsidentidest teatama.~~ **[ME 107]**

6. ~~Kui lõike 5 alusel vastuvõetud delegeeritud õigusaktides ei ole sätestatud teisiti, võivad~~ Pädevad asutused ***või ühtsed kontaktpunktid võivad*** võtta vastu suuniseid ~~ja vajaduse korral anda välja juhiseid~~ asjaolude kohta, mille korral ~~haldusasutused ja~~ operaatorid peavad intsidentidest teatama. **[ME 108]**

7. Komisjonile antakse volitused määratleda rakendusaktidega lõike 2 kohaldamiseks vajalikud vormingud ja protseduurid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 19 lõikes 3 osutatud kontrollimenetlusega.

8. Lõikeid 1 ja 2 ei kohaldata mikroettevõtjate suhtes, kes on määratletud komisjoni soovituses 2003/361/EÜ[1]***, välja arvatud juhul, kui mikroettevõtja tegutseb vastavalt artikli 3 lõike 8 punkti b kohaselt elutähtsa infrastruktuuri operaatori tütarettevõtjana***. **[ME 109]**

8a. Liikmesriigid võivad otsustada kohaldada haldusasutuste suhtes mutatis mutandis käesolevat artiklit ja artiklit 15. **[ME 110]**

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

Artikkel 15

Rakendamine ja jõustamine

1. Liikmesriigid tagavad, et pädevatel asutustel on ~~kõik~~ ***ja ühtsetel kontaktpunktidel*** on ***vajalikud*** volitused, ~~mida nad vajavad, et uurida juhtumeid, mil haldusasutus või operaator ei täitnud~~ ***et tagada operaatorite*** artiklist 14 ~~tulenevaid kohustusi~~ ***tulenevate kohustuste täitmine***, ja nende juhtumite mõju võrkude ja infosüsteemide turvalisusele. **[ME 111]**

2. Liikmesriigid tagavad, et pädevatel asutustel ***ja ühtsetel kontaktpunktidel*** on volitused nõuda operaatoritelt ~~ja haldusasutustelt~~, et nad: **[ME 112]**

   a) esitaksid oma võrkude ja infosüsteemide turvalisuse hindamiseks vajalikud andmed, sealhulgas dokumenteeritud turvapõhimõtted;

   b) ~~laseksid~~ ***tõendaksid turvapõhimõtete rakendamise tulemuslikkust, näiteks*** kvalifitseeritud ~~sõltumatul asutusel või riigiasutusel teha~~ ***sõltumatu asutuse või riigiasutuse tehtava*** turvaauditi ***tulemuste abil,*** ja avaldaksid ~~selle tulemused~~ ***tõendid*** pädevale asutusele ***või ühtsele kontaktpunktile***. **[ME 113]**

Taotluse saatmisel esitavad pädevad asutused ja ühtsed kontaktpunktid taotluse eesmärgi ja täpsustavad asjakohaselt, millist teavet nõutakse. **[ME 114]**

3. Liikmesriigid tagavad, et pädevatel asutustel ***ja ühtsetel kontaktpunktidel*** on volitused anda operaatoritele ~~ja haldusasutustele~~ siduvaid juhiseid. **[ME 115]**

3a. Erandina käesoleva artikli lõike 2 punktist b võivad liikmesriigid otsustada, et vastavalt vajadusele kas pädevad asutused või ühtsed kontaktpunktid peavad kohaldama teatud operaatorite suhtes teistsugust korda nende elutähtsuse taseme põhjal, mis määratakse kindlaks kooskõlas artikliga 13a. Kui liikmesriigid nii otsustavad:

a) on vastavalt vajadusele kas pädevatel asutustel või ühtsetel kontaktpunktidel volitused esitada operaatoritele asjakohaselt konkreetne taotlus, milles nõutakse, et nad tõendaksid turvapõhimõtete rakendamise tulemuslikkust, näiteks kvalifitseeritud siseaudiitori tehtava turvaauditi tulemuste abil, ja avaldaksid tõendid pädevale asutusele või ühtsele kontaktpunktile;

b) võib pädev asutus või ühtne kontaktpunkt pärast seda, kui operaator on esitanud punktis a osutatud taotluse, nõuda vajaduse korral lisatõendeid või et kvalifitseeritud sõltumatu asutus või riigiasutus teeks lisaauditi.

3b. ***Liikmesriigid võivad otsustada vähendada asjaomase operaatori või haldusasutuse kohta tehtavate auditite arvu ja põhjalikkust, kui turvaaudit näitab järjepidevalt IV peatüki nõuete täitmist.*** **[ME 116]**

4. ***Pädevad asutused ja ühtsed kontaktpunktid teavitavad asjaomaseid operaatoreid võimalusest teatada intsidentidest õiguskaitseasutustele,*** kui kahtlustatakse, et ~~intsident~~ ***need intsidendid*** on seotud raske kuriteoga~~, teatavad pädevad asutused sellest õiguskaitseasutustele~~. **[ME 117]**

5. Kui intsident põhjustab ~~isikuandmetega~~ ***kohaldavate isikuandmete-eeskirjadega*** seotud rikkumise, ***siis, ilma et see piiraks kehtiva andmekaitseõiguse kohaldamist,*** teevad pädevad asutused ***ja ühtsed kontaktpunktid*** selle lahendamisel tihedat koostööd isikuandmete kaitse asutustega. ***Ühtsed kontaktpunktid ja andmekaitseasutused töötavad koostöös ENISAga välja teabevahetusmehhanismid ja ühtse vormi, mida tuleb kasutada nii käesoleva direktiivi artikli 14 lõike 2 kui ka muude liidu andmekaitsealaste õigusaktide kohase teatamise jaoks.*** **[ME 118]**

6. Liikmesriigid tagavad, et kõik käesoleva peatükiga ~~haldusasutustele ja~~ operaatoritele pandud kohustused võib kohtus läbi vaadata. **[ME 119]**

6a. ***Liikmesriigid võivad otsustada kohaldada haldusasutuste suhtes mutatis mutandis artiklit 14 ja käesolevat artiklit.*** **[ME 120]**

Artikkel 16

Standardimine

1. Artikli 14 lõike 1 ühtse kohaldamise tagamiseks julgustavad liikmesriigid ***mis tahes asjaomase tehnoloogia kasutamist piiramata*** võrgu- ja infoturbe seisukohast asjakohaste ***Euroopa Liidu või rahvusvaheliste koostalitlevate*** standardite ja/või spetsifikatsioonide kasutamist. **[ME 121]**

2. Komisjon ~~koostab rakendusaktidega~~ ***volitab asjakohast Euroopa standardiorganisatsiooni asjaomaste sidusrühmadega konsulteerides koostama*** lõikes 1 osutatud standardite ***ja/või spetsifikatsioonide*** nimekirja. Nimekiri avaldatakse *Euroopa Liidu Teatajas*. **[ME 122]**

V PEATÜKK

LÕPPSÄTTED

Artikkel 17

Karistused

1. Liikmesriigid kehtestavad eeskirjad karistuste kohta, mida rakendatakse käesoleva direktiivi kohaselt vastuvõetud siseriiklike õigusnormide rikkumise korral, ning võtavad kõik vajalikud meetmed nende rakendamise tagamiseks. Ettenähtud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad. Liikmesriigid teatavad kõnealustest sätetest komisjonile hiljemalt käesoleva direktiivi ülevõtmise kuupäevaks, samuti teatavad nad viivitamata kõigist neid sätteid mõjutavatest hilisematest muudatustest.

1a. Liikmesriigid tagavad, et käesoleva artikli lõikes 1 osutatud karistusi kohaldatakse ainult siis, kui operaator jätab tahtlikult või raske hooletuse tõttu oma IV peatükist tulenevad kohustused täitmata. **[ME 123]**

2. Liikmesriigid tagavad, et kui turvaintsident puudutab isikuandmeid, on ettenähtud karistused kooskõlas karistustega, mis on sätestatud Euroopa Parlamendi ja nõukogu määruses üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta[1].

[1] SEC(2012) 72.

Artikkel 18

Delegeeritud volituste rakendamine

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

2. Komisjonile antakse õigus võtta vastu artikli 9 lõikes 3 ja artikli 10 lõikes 5 osutatud delegeeritud õigusakte. Komisjon koostab delegeeritud volituste kasutamise kohta aruande hiljemalt üheksa kuud enne viieaastase tähtaja möödumist. Volituste delegeerimist uuendatakse automaatselt samaks ajavahemikuks, välja arvatud juhul, kui Euroopa Parlament või nõukogu esitab selle suhtes vastuväite hiljemalt kolm kuud enne iga ajavahemiku lõppemist.

3. Euroopa Parlament ja nõukogu võivad artikli 9 lõikes 3 ja artikli 10 lõikes 5~~ ja artikli 14 lõikes 5~~ 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 kindlaksmääratud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust. **[ME 124]**

4. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle üheaegselt teatavaks Euroopa Parlamendile ja nõukogule.

5. Artikli 9 lõike 3 ja artikli 10 lõike 5 ~~ja artikli 14 lõike 5~~ 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 vastuväiteid või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväiteid. Kõnealust ajavahemikku võib Euroopa Parlamendi või nõukogu taotlusel kahe kuu võrra pikendada. **[ME 125]**

Artikkel 19

Komiteemenetlus

1. Komisjoni abistab komitee (võrgu- ja infoturbe komitee). Kõnealune komitee on komitee määruse (EL) nr 182/2011 tähenduses.

2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 4.

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

Artikkel 20

Läbivaatamine

Komisjon vaatab korrapäraselt läbi käesoleva direktiivi toimimise***, iseäranis II lisas esitatud loetelu*** ning esitab aruande Euroopa Parlamendile ja nõukogule. Esimene aruanne esitatakse hiljemalt kolm aastat pärast artiklis 21 osutatud ülevõtmise kuupäeva. Selleks võib komisjon paluda, et liikmesriigid esitaksid teavet ilma põhjendamatult viivitamata. **[ME 126]**

Artikkel 21

Ülevõtmine

1. Liikmesriigid võtavad vastu ja avaldavad käesoleva direktiivi järgimiseks vajalikud õigusnormid ja haldussätted hiljemalt [poolteist aastat pärast vastuvõtmist]. Nad edastavad kõnealuste meetmete teksti viivitamata komisjonile.

   Nad hakkavad neid meetmeid kohaldama alates [poolteist aastat pärast vastuvõtmist].

   Kui liikmesriigid need meetmed vastu võtavad, lisavad nad nendesse meetmetesse või nende meetmete ametliku avaldamise korral nende juurde viite käesolevale direktiivile. Sellise viitamise viisi näevad ette liikmesriigid.

2. Liikmesriigid edastavad komisjonile käesoleva direktiiviga reguleeritavas valdkonnas nende poolt vastuvõetud põhiliste siseriiklike õigusnormide teksti.

Artikkel 22

Jõustumine

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

Artikkel 23

Adressaadid

Käesolev direktiiv on adresseeritud liikmesriikidele.

…,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

I LISA

Infoturbeintsidentidega ~~tegelevale meeskonnale~~ ***tegelevatele rühmadele*** (CERT) esitatavad nõuded ja ~~meeskonna~~ ***rühmade*** ülesanded **[ME 127]**

CERTile esitatavad nõuded ja tema ülesanded tuleb määratleda piisavalt ja selgelt ning riigi poliitika ja/või õigusnormid peavad neid toetama. Nõuded hõlmavad järgmist:

1) CERTile esitatavad nõuded

a) ~~CERT peab~~ ***CERTid peavad*** tagama oma sideteenuste käideldavuse kõrge taseme, vältides nõrku lülisid, ning kasutama mitmesuguseid vahendeid, mis võimaldavad ~~tal~~ ***neil*** teistega ja teistel ~~temaga~~ ***nendega igal ajal*** ühendust võtta. Sidekanalid peavad olema selgelt nimetatud ning kasutajatele ja koostööpartneritele hästi teada. **[ME 128]**

b) CERT peab rakendama ja haldama turvameetmeid, et tagada temani jõudva ja tema poolt käideldava teabe konfidentsiaalsus, terviklus, käideldavus ja autentsus.

c) ~~CERTi~~ ***CERTide*** ametiruumide ja ~~tema~~ ***nende*** tööd toetavate infosüsteemide ~~asukoht peab~~ ***asukohad peavad*** olema ~~turvaline~~ ***turvalised ning seal peavad olema turvalised võrguinfosüsteemid***. **[ME 129]**

d) Luua tuleb teenusehalduse kvaliteedisüsteem, et CERTi töö tulemuste põhjal järelmeetmeid võtta ja süsteemi pidevalt paremaks muuta. Süsteem peab põhinema selgelt määratletud parameetritel, mille hulka kuuluvad ka ametlikud teenusetasemed ja peamised tulemuslikkuse näitajad.

e) Talitluspidevus:

- CERTil peab olema taotluste haldamiseks ja suunamiseks sobiv süsteem, et hõlbustada üleandmisi;
- CERTil peab olema piisavalt töötajaid, et tagada alaline kättesaadavus;
- CERTi kasutatava taristu pidevus peab olema tagatud. Selle eesmärgi nimel antakse CERTi kasutusse liiased süsteemid ja varutöökeskkond, et tagada alaline juurdepääs sidevahenditele.

2) CERTi ülesanded

a) CERTi ülesanded peavad sisaldama vähemalt järgmist:

– intsidentide ***tuvastamine ja*** seire riigis, **[ME 130]**

– riskide ja intsidentide kohta varajaste hoiatuste, hoiatuste ja teadaannete esitamine ning teabe levitamine sidusrühmadele,

– intsidentidele reageerimine,

– pidev riskide ja intsidentide analüüsimine ja teadlikkus olukorrast,

– üldsuse teadlikkuse suurendamine interneti kasutamisega seotud riskidest;

– ***aktiivne osalemine liidu ja rahvusvahelistes CERTide koostöövõrkudes;*** **[ME 131]**

– võrgu- ja infoturbealaste kampaaniate korraldamine.

b) CERT peab sisse seadma koostöö erasektoriga.

c) Koostöö hõlbustamiseks peab CERT toetama ühiste või standardtoimingute vastuvõtmist ja kasutamist järgmistes valdkondades:

– intsidentide ja riskide käsitlemise protseduurid,

– intsidentide, riskide ja teabe liigitamise kavad,

– parameetrite süstematiseerimine,

– riskide ja intsidentide kohta vahetatava teabe ja süsteemis kasutatavate nimetuste vormingud.

II LISA

Operaatorite loetelu

~~Vastavalt artikli 3 lõike 8 punktile a:~~

~~1. e-kaubanduse platvormid~~

~~2. Internetimaksete lüüsid~~

~~3. Suhtlusvõrgud~~

~~4. Otsingumootorid~~

~~5. Pilvandmetöötluse teenused~~

~~6. Tarkvarapoed~~

~~Vastavalt artikli 3 lõike 8 punktile b:~~ **[ME 132]**

1. Energeetika

a) Elekter

– ~~Elektri- ja gaasitarnijad~~ ***Tarnijad***

– ~~Elektri- ja/või gaasitarnesüsteemide~~ ***Jaotussüsteemi*** operaatorid ~~ning elektri ja gaasi jaemüüjad~~ ***ja*** lõpptarbijatele ***edasi müüjad***

~~– Maagaasi ülekandesüsteemi, gaasihoidlate ja veeldusjaamade haldurid~~

– Elektrienergia põhivõrguettevõtjad

b) Nafta

– Naftajuhtmed ja naftahoidlad

– ***Nafta tootmise, rafineerimise, töötlemise, hoiustamise ja ülekandmisega tegelevad operaatorid***

c) Gaas

~~– Elektri- ja gaasituru operaatorid~~

– ***Tarnijad***

– ***Jaotussüsteemi operaatorid ja lõpptarbijatele edasi müüjad***

– ***Maagaasi ülekandesüsteemi, gaasihoidlate ja veeldusjaamade süsteemi haldurid***

– ~~Nafta ja maagaasi tootmise, rafineerimise ja töötlemisega tegelevad operaatorid~~ ***Maagaasi tootmis-, rafineerimis- ja töötlemisrajatiste, -hoidlate ja -juhtmete käitajad***

– ***Gaasituru operaatorid*** **[ME 133]**

2. Transport

~~– Lennuettevõtjad (kauba ja reisijate õhuvedu)~~

~~– Meretransporditeenuste osutajad (ettevõtjad, kes tegelevad sõitjate ja kauba vedamisega merel ja rannavetes)~~

~~– Raudtee (taristu haldajad, integreeritud ettevõtjad ja raudteeveoettevõtted)~~

~~– Lennujaamad~~

~~– Sadamad~~

~~– Liikluskorraldusettevõtted~~

~~– Logistika abiteenused: a) ladustamine ja hoiustamine, b) veoste käitlemine ja c) muud transpordi tugiteenused~~

a) ***Maanteetransport***

i) ***Liikluskorraldusettevõtted***

ii) ***Logistika abiteenused:***

– ***ladustamine ja hoiustamine,***

– ***veoste käitlemine ja***

– ***muud transpordi tugiteenused***

b) Raudteetransport

i) Raudtee (taristu haldajad, integreeritud ettevõtjad ja raudteeveoettevõtted)

ii) Liikluskorraldusettevõtted

iii) Logistilised abiteenused:

– *ladustamine ja hoiustamine,*

– *veoste käitlemine ja*

– *muud transpordi tugiteenused*

c) Lennutransport

i) Lennuettevõtjad (kauba ja reisijate õhuvedu)

ii) Lennujaamad

iii) Liikluskorraldusettevõtjad

iv) Logistika abiteenused:

– *ladustamine,*

– *veoste käitlemine ja*

– *muud transpordi tugiteenused*

d) Meretransport

i) Meretransporditeenuste osutajad (ettevõtjad, kes tegelevad sõitjate ja kauba vedamisega sisevetes, merel ja rannavetes) **[ME 134]**

3. Pangandus: krediidiasutused vastavalt Euroopa Parlamendi ja nõukogu direktiivi 2006/48/EÜ[1] artikli 4 lõikele 1.

4. Finantsturu taristu: ~~väärtpaberibörsid~~ ***reguleeritud turud, mitmepoolsed kauplemissüsteemid, organiseeritud kauplemissüsteemid*** ja keskse vastaspoolega kliiringukojad **[ME 135]**

5. Tervishoiusektor: tervishoiuasutused (kaasa arvatud haiglad ja erakliinikud) ning muud tervishoiuteenuste pakkumises osalevad üksused

5a. Vee tootmine ja veega varustamine **[ME 136]**

5b. Toiduainete tarneahel **[ME 137]**

5c. Interneti vahetuspunktid **[ME 138]**

[1] Euroopa Parlamendi ja nõukogu 14. juuni 2006. aasta direktiiv 2006/48/EÜ krediidiasutuste asutamise ja tegevuse kohta (ELT L 177, 30.6.2006, lk 1).