2025/37

15.1.2025

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) 2025/37,

19. detsember 2024,

millega muudetakse määrust (EL) 2019/881 seoses hallatud turbeteenustega

(EMPs kohaldatav tekst)

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

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

pärast konsulteerimist Regioonide Komiteega,

toimides seadusandliku tavamenetluse kohaselt ([2])

ning arvestades järgmist:

(1) Euroopa Parlamendi ja nõukogu määruses (EL) 2019/881 ([3]) on sätestatud Euroopa küberturvalisuse sertifitseerimise kavade kehtestamise raamistik, et kindlustada liidus info- ja kommunikatsioonitehnoloogiatoodete (IKT-toodete), -teenuste ja -protsesside küberturvalisuse piisav tase ning vältida siseturu killustatust seoses küberturvalisuse sertifitseerimise kavadega liidus.

(2) Et tagada liidu kerksus küberrünnete suhtes ja vältida siseturu kaitsetust, on käesoleva määruse eesmärk täiendada Euroopa Parlamendi ja nõukogu määruse (EL) 2024/2847 ([4]) kohast horisontaalset õigusraamistikku, millega kehtestatakse digielemente sisaldavate toodete kohta põhjalikud küberturvalisuse nõuded, sätestades turvalisusega seotud eesmärgid hallatud turbeteenuste ning kõnealuste teenuste kasutamise ja usaldusväärsuse kohta.

(3) Hallatud turbeteenuseid osutavad Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 ([5]) artikli 6 punktis 40 määratletud hallatud turbeteenuse osutajad. Seetõttu peaks käesolevas määruses sätestatud mõiste „hallatud turbeteenused“ määratlus olema kooskõlas direktiivis (EL) 2022/2555 kasutatava mõiste „hallatud turbeteenuse osutaja“ määratlusega. Kõnealused teenused seisnevad nende klientide küberturvalisuse riskihaldusega seotud tegevuse korraldamises või selleks toe pakkumises, ning need on intsidentide ennetamisel ja leevendamisel muutunud üha olulisemaks. Seega käsitatakse selliste teenuste pakkujaid elutähtsate või oluliste üksustena, mis kuuluvad direktiivi (EL) 2022/2555 kohaselt kriitilise tähtsusega sektorisse. Nagu on märgitud kõnealuse direktiivi põhjenduses 86, on hallatud turbeteenuse osutajatel intsidentide ennetamisel, tuvastamisel, lahendamisel ja neist taastumisel üksuste jaoks eriti oluline tugiroll sellistes teenusevaldkondades nagu intsidentidele reageerimine, läbistustestimine, turvaaudit ja konsultatsioonid. Hallatud turbeteenuse osutajad on aga olnud ka ise küberrünnete sihtmärgiks ja kuna nad on oma klientide tegevusse tihedalt lõimitud, kaasneb nendega eriline risk. Seega on tähtis, et direktiivi (EL) 2022/2555 tähenduses elutähtsad ja olulised üksused oleksid hallatud turbeteenuse osutajate valimisel iseäranis hoolikad.

([1]) ELT C 349, 29.9.2023, lk 167.
([2]) Euroopa Parlamendi 24. aprilli 2024. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu 2. detsembri 2024. aasta otsus.
([3]) 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).
([4]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2024. aasta määrus (EL) 2024/2847, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrusi (EL) nr 168/2013 ja (EL) 2019/1020 ning direktiivi (EL) 2020/1828 (küberkerksuse määrus) (ELT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).
([5]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80).

(4) Käesolevas määruses kasutatav hallatud turbeteenuste määratlus sisaldab Euroopa küberturvalisuse sertifitseerimise kavade jaoks kvalifitseeruda võivate hallatud turbeteenuste mittetäielikku loetelu, näiteks intsidentide käsitlemine, läbistustestimine, turvaauditid ja tehnilise toega seotud konsultatsioonid. Hallatud turbeteenused võiksid hõlmata küberturvalisuse teenuseid, mis toetavad intsidentideks valmisolekut, nende ennetamist, tuvastamist, analüüsi, leevendamist, neile reageerimist ja nendest taastumist. Hallatud turbeteenustena võiks käsitada ka küberohuteadmuse esitamist ja tehnilise toega seotud riskide hindamist. Erinevate hallatud turbeteenuste puhul võiks kasutada eraldi Euroopa küberturvalisuse sertifitseerimise kavasid. Kooskõlas selliste kavadega välja antud Euroopa küberturvalisuse sertifikaadid peaksid viitama hallatud turbeteenuse osutajate pakutavatele konkreetsetele hallatud turbeteenustele.

(5) Hallatud turbeteenuse osutajatel võib olla oluline roll ka seoses liidu tegevusega, mis toetab oluliste ja ulatuslike intsidentide korral reageerimist ja esmast taastumist, tuginedes usaldusväärsete erasektori teenuseosutajate teenustele ning sellele, et elutähtsa teenuse osutajaid testitakse võimalike turvanõrkuste suhtes liidu tasandi koordineeritud turberiski hindamise alusel. Hallatud turbeteenuste sertifitseerimisel võiks olla oma osa Euroopa Parlamendi ja nõukogu määruses (EL) 2025/38 ([6]) määratletud usaldusväärsete teenuseosutajate valimisel.

(6) Hallatud turbeteenuste sertifitseerimine ei ole oluline mitte ainult määrusega (EL) 2025/38 loodud ELi küberreservi valikumenetluses, vaid see on ka tähtis kvaliteedinäitaja selliste era- ja avaliku sektori üksuste jaoks, kes kavatsevad neid teenuseid osta. Võttes arvesse hallatud turbeteenuste kriitilist tähtsust ja töödeldavate andmete tundlikkust, võib sertifitseerimine anda potentsiaalsetele klientidele olulisi suuniseid ja kindlust kõnealuste teenuste usaldusväärsuse kohta. Hallatud turbeteenuste Euroopa küberturvalisuse sertifitseerimise kavade eesmärk on aidata vältida siseturu killustumist. Seega on käesoleva määruse eesmärk tõhustada siseturu toimimist.

(7) Hallatud turbeteenuste Euroopa küberturvalisuse sertifitseerimise kavad peaksid aitama neid teenuseid kasutusele võtta ja suurendada hallatud turbeteenuse osutajate vahelist konkurentsi. Ilma et see piiraks eesmärki tagada hallatud turbeteenuse osutajate tehnilised teadmised ning erialane kohusetunne piisaval ja sobival tasemel, peaksid sertifitseerimise kavad seetõttu hõlbustama turule sisenemist ja hallatud turbeteenuste osutamist, lihtsustades võimalikult suurel määral potentsiaalset regulatiivset, haldus- ja finantskoormust, millega teenuseosutajad, eelkõige väikesed ja keskmise suurusega ettevõtjad (VKEd), sealhulgas mikroettevõtjad, võivad hallatud turbeteenuste osutamisel silmitsi seista. Selleks et soodustada hallatud turbeteenuste kasutusele võtmist ja stimuleerida nõudlust nende järele, peaksid Euroopa küberturvalisuse sertifitseerimise kavad aitama muuta sellised teenused kättesaadavamaks eelkõige väiksematele osalejatele, näiteks VKEdele, sealhulgas mikroettevõtjatele, samuti kohalikele ja piirkondlikele omavalitsustele, kelle suutlikkus ja ressursid on väiksemad, kuid kelle puhul on tõenäolisem, et esineb küberturvalisuse rikkumisi, millel on rahaline, õiguslik ning nende mainet ja tegevust puudutav mõju.

(8) Oluline on anda VKEdele, sealhulgas mikroettevõtjatele käesoleva määruse rakendamisel ning küberturvalisuse alaste erioskuste ja erialateadmistega töötajate tööle võtmisel sellist toetust, mida on vaja hallatud turbeteenuste osutamiseks vastavalt käesolevas määruses sätestatud nõuetele. Euroopa Parlamendi ja nõukogu määrusega (EL) 2021/694 ([7]) loodud programmis „Digitaalne Euroopa“ ja muudes asjakohastes liidu programmides on ette nähtud, et komisjon peaks andma kõnealustele ettevõtjatele rahalist ja tehnilist toetust, et nad saaksid panustada liidu majanduskasvu ja küberturvalisuse ühtlase taseme tugevdamisesse liidus, sealhulgas ühtlustades programmi „Digitaalne Euroopa“ ja muude asjakohaste liidu programmide raames antavaid rahalisi toetusi ning toetades VKEsid, sealhulgas mikroettevõtjaid.

(9) Hallatud turbeteenuste Euroopa küberturvalisuse sertifitseerimise kavad peaksid aitama saavutada selliste turvaliste ja kvaliteetsete teenuste kättesaadavust, mis tagavad turvalise digipöörde, samuti peaks see aitama saavutada Euroopa Parlamendi ja nõukogu otsusega (EL) 2022/2481 ([8]) loodud digikümnendi poliitikaprogrammis 2030 seatud

([6]) Euroopa Parlamendi ja nõukogu 19. detsembri 2024. aasta määrus (EL) 2025/38, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks ning millega muudetakse määrust (EL) 2021/694 (kübersolidaarsuse määrus) (ELT L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) 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).

([8]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta otsus (EL) 2022/2481, millega luuakse digikümnendi poliitikaprogramm 2030 (ELT L 323, 19.12.2022, lk 4).

eesmärke, eelkõige seoses eesmärgiga, mille kohaselt peaks 75 % liidu ettevõtjatest hakkama kasutama pilvandmetöötlust, suurandmeid või tehisintellekti, et enam kui 90 % VKEdest, sealhulgas mikroettevõtjatest saavutaks vähemalt digimahukuse algtaseme ja et peamised avalikud teenused oleks internetis kättesaadavad.

(10) Lisaks IKT-toodete, -teenuste või -protsesside kasutuselevõtule võimaldavad hallatud turbeteenused sageli osutada lisateenuseid, mis tuginevad selliste teenuste pakkujate töötajate pädevusele, erialateadmistele ja kogemustele. Turvalisusega seotud eesmärkide hulka peaksid kuuluma nimetatud pädevuse, erialateadmiste ja kogemuste väga kõrge taseme saavutamine ning asjakohased sisemenetlused, et tagada pakutavate hallatud turbeteenuste tipptasemel kvaliteet. Selleks et tagada kõikide hallatud turbeteenuste aspektide kuulumine sihipärastesse Euroopa küberturvalisuse sertifitseerimise kavadesse, on vaja muuta määrust (EL) 2019/881. Arvesse tuleks võtta määruses (EL) 2019/881 ette nähtud hindamise ja läbivaatamise tulemusi ning nende raames antud soovitusi.

(11) Selleks et hõlbustada usaldusväärse siseturu kasvu ja luua samal ajal partnerlusi sarnaselt meelestatud kolmandate riikidega, tuleks määruses (EL) 2019/881 sätestatud Euroopa küberturvalisuse sertifitseerimise raamistikus loodud sertifitseerimise protsessi rakendada viisil, mis hõlbustab rahvusvahelist tunnustamist ja kooskõla rahvusvaheliste standarditega.

(12) Liidus on talendinappus ehk kvalifitseeritud spetsialistide puudus ja liit seisab silmitsi kiiresti muutuvate ohtudega, nagu tunnistati komisjoni 18. aprilli 2023. aasta teatises „Korvata küberturvalisuse valdkonna talendinappus edendamaks ELi konkurentsivõimet, majanduskasvu ja kerksust („Küberturbeoskuste akadeemia“)“. Leidub palju erinevaid õppematerjale ja ametlikke koolitusvõimalusi ning teadmisi on võimalik omandada mitmel viisil: ametlikult, näiteks kõrgkoolis või kursustel õppides, või mitteametlikult, näiteks töökohapõhise õppe või asjaomases valdkonnas saadud töökogemuse kaudu. Et hõlbustada kvaliteetsete hallatud turbeteenuste pakkumist ja saada liidu küberturvalisuse valdkonna töötajate koosseisust parem ülevaade, on seega oluline tugevdada liikmesriikide, komisjoni, määrusega (EL) 2019/881 loodud Euroopa Liidu Küberturvalisuse Ameti (ENISA) ja sidusrühmade, sealhulgas erasektori ja akadeemiliste ringkondade vahelist koostööd avaliku ja erasektori partnerluste arendamise, teadus- ja innovatsioonialgatuste toetamise, ühiste standardite väljatöötamise ja nende vastastikuse tunnustamise ning küberturvalisuse oskuste sertifitseerimise kaudu, sealhulgas Euroopa küberturvalisuse oskuste raamistiku kaudu. Niisugune koostöö hõlbustaks ühtlasi küberturvalisusspetsialistide liikuvust liidus ning küberturvalisusalaste teadmiste ja õppe integreerimist haridusprogrammidesse, tagades samal ajal noortele, sealhulgas ebasoodsas olukorras olevates piirkondades, näiteks saartel, hõredalt asustatud aladel, maapiirkondades ja äärealadel elavatele inimestele võimaluse osaleda töökohapõhises õppes ja praktikal. On oluline, et sellise koostöö eesmärk oleks meelitada sellesse valdkonda rohkem naisi ja tütarlapsi ning aidata kaasa soolise ebavõrdsuse vähendamisele teaduses, tehnoloogias, inseneerias ja matemaatikas, ning et erasektor pakuks töökohapõhist õpet, milles käsitletakse kõige nõutavamaid oskusi, kaasates avaliku halduse asutusi ja idufirmasid ning VKEsid, sealhulgas mikroettevõtjaid. Samuti on oluline, et teenuseosutajad ja liikmesriigid teeksid koostööd ning aitaksid koguda küberturvalisuse tööturu olukorda ja arengut käsitlevaid andmeid.

(13) ENISA-l on oluline roll Euroopa küberturvalisuse sertifitseerimise ettevalmistavate kavade koostamisel. Komisjon peaks liidu üldeelarve projekti ettevalmistamisel hindama ENISA ametikohtade loetelu põhjal vajalikke eelarvevahendeid kooskõlas määruse (EL) 2019/881 artiklis 29 sätestatud menetlusega.

(14) Käesoleva määrusega nähakse ette määruse (EL) 2019/881 sihipärased muudatused, et võimaldada võtta kasutusele Euroopa küberturvalisuse sertifitseerimise kavad hallatud turbeteenuse jaoks. Sellega täpsustatakse ja selgitatakse ka nimetatud määruse teatavaid sätteid, mis käsitlevad kõigi Euroopa küberturvalisuse sertifitseerimise kavade koostamist ja toimimist, et tagada nende läbipaistvus ja avatus. Kõnealused muudatused, mis piirduvad määruse (EL) 2019/881 täpsustamise või selgitamisega, eelkõige muudatused seoses teabega, mida ENISA peab esitama ettevalmistava kava edastamisel, iga ettevalmistava kava jaoks loodud ajutiste töörühmadega ning Euroopa küberturvalisuse sertifitseerimise kavadega seonduva teavitamise ja konsulteerimisega, ei tohiks mingil viisil piirata kõnealuse määruse artikli 67 kohaselt nõutavat laiemat hindamist ja läbivaatamist, eelkõige kõnealuse määruse küberturvalisuse sertifitseerimise raamistikku käsitleva jaotise mõju, tulemuslikkuse ja tõhususe hindamist. Kõnealuse jaotise hindamine ja läbivaatamine peaks põhinema ulatuslikul konsulteerimisel sidusrühmadega ning asjaomaste menetluste täielikul ja põhjalikul analüüsil.

(15) Kuna käesoleva määruse eesmärki, milleks on võimaldada Euroopa küberturvalisuse sertifitseerimise kavade kasutuselevõttu hallatud turbeteenuste jaoks, ei suuda liikmesriigid piisavalt saavutada, küll aga saab seda meetme ulatuse ja toime tõttu 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 määrus nimetatud eesmärgi saavutamiseks vajalikust kaugemale.

(16) Euroopa Andmekaitseinspektoriga konsulteeriti kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([9]) artikli 42 lõikega 1 ning ta esitas arvamuse 10. jaanuaril 2024,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Määruse (EL) 2019/881 muutmine

Määrust (EL) 2019/881 muudetakse järgmiselt.

1) Artikli 1 lõike 1 esimese lõigu punkt b asendatakse järgmisega:

„b) Euroopa küberturvalisuse sertifitseerimise kavade kehtestamise raamistik, et kindlustada liidus IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste küberturvalisuse piisav tase ning vältida siseturu killustatust seoses küberturvalisuse sertifitseerimise kavadega liidus.“

2) Artiklit 2 muudetakse järgmiselt:

a) punktid 9, 10 ja 11 asendatakse järgmisega:

„9) „Euroopa küberturvalisuse sertifitseerimise kava“ – liidu tasandil kindlaks määratud reeglite, tehniliste nõuete, standardite ja menetluste põhjalik kogum, mida kasutatakse konkreetsete IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste sertifitseerimiseks või nende vastavuse hindamiseks;

10) „riiklik küberturvalisuse sertifitseerimise kava“ – riigi ametiasutuse välja töötatud ja kehtestatud reeglite, tehniliste nõuete, standardite ja menetluste põhjalik kogum, mida kasutatakse konkreetse kava kohaldamisalasse kuuluvate IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste sertifitseerimiseks või nende vastavuse hindamiseks;

11) „Euroopa küberturvalisuse sertifikaat“ – asjakohase asutuse välja antud dokument, mis kinnitab, et hinnatud on asjaomase IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse vastavust Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud konkreetsetele turvanõuetele;“;

b) lisatakse järgmine punkt:

„14a) „hallatud turbeteenus“ – kolmandale isikule osutatav teenus, mis seisneb küberturvalisuse riskihaldusega seotud tegevuse, näiteks intsidentide käsitlemise, läbistustestimise, turvaauditite ja tehnilise toega seotud konsultatsioonide, sealhulgas eksperdinõu pakkumise korraldamises või nende korraldamiseks toe pakkumises;“;

c) punktid 20, 21 ja 22 asendatakse järgmisega:

„20) „tehniline spetsifikatsioon“ – dokument, milles nähakse ette IKT-tootele, -teenusele, -protsessile või hallatud turbeteenusele esitatavad tehnilised nõuded või nendega seotud vastavushindamismenetlus;

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

21) „usaldusväärsuse tase“ – alus kindlustundele, et IKT-toode, -teenus, -protsess või hallatud turbeteenus vastab konkreetse Euroopa küberturvalisuse sertifitseerimise kava turvanõuetele, näidates ühtlasi, millisel tasemel on seda hinnatud; usaldusväärsuse tase ei mõõda IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse enda turvalisust;

22) „vastavuse enesehindamine“ – IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuse tootja või pakkuja või hallatud turbeteenuse osutajate tegevus, millega hinnatakse nende IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste vastavust teatavatele Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud nõuetele.“

3) Artikli 4 lõige 6 asendatakse järgmisega:

„6. ENISA edendab Euroopa küberturvalisuse sertifitseerimise kasutamist, et vältida siseturu killustatust. ENISA aitab kaasa Euroopa küberturvalisuse sertifitseerimise raamistiku loomisele ja haldamisele kooskõlas käesoleva määruse III jaotisega, et suurendada IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste küberturvalisuse läbipaistvust ning suurendada seeläbi usaldust digitaalse siseturu vastu ja selle konkurentsivõimet.“

4) Artiklit 8 muudetakse järgmiselt:

a) lõiget 1 muudetakse järgmiselt:

i) sissejuhatav osa asendatakse järgmisega:

„1. ENISA toetab ja edendab käesoleva määruse III jaotises sätestatud IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste küberturvalisuse sertifitseerimise alaste liidu poliitikameetmete arendamist ja rakendamist järgmiselt:“;

ii) punkt b asendatakse järgmisega:

„b) koostab IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste Euroopa küberturvalisuse sertifitseerimise ettevalmistavad kavad („ettevalmistavad kavad“) kooskõlas artikliga 49;“;

b) lõige 3 asendatakse järgmisega:

„3. ENISA koostab ja avaldab suuniseid ning töötab välja häid tavasid IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste küberturvalisuse nõuete kohta, tehes selleks ametlikult, struktureeritult ja läbipaistvalt koostööd riiklike küberturvalisuse sertifitseerimise asutuste ja tööstusega.“;

c) lõige 5 asendatakse järgmisega:

„5. ENISA hõlbustab riskihalduse ning IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste turvalisuse Euroopa ja rahvusvaheliste standardite koostamist ja kasutuselevõtmist.“

5) Artikkel 46 asendatakse järgmisega:

„*Artikkel 46*

Euroopa küberturvalisuse sertifitseerimise raamistik

1. Kehtestatakse Euroopa küberturvalisuse sertifitseerimise raamistik, et parandada siseturu toimimise tingimusi, tõstes liidus küberturvalisuse taset ja võimaldades liidu tasandil ühtlustatud lähenemisviisi Euroopa küberturvalisuse sertifitseerimise kavadele, eesmärgiga luua IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste jaoks digitaalne ühtne turg.

2. Euroopa küberturvalisuse sertifitseerimise raamistik näeb ette mehhanismi, et kehtestada Euroopa küberturvalisuse sertifitseerimise kavad, millega kinnitatakse, et kooskõlas selliste kavadega hinnatud IKT-tooted, -teenused ja -protsessid vastavad kindlaksmääratud turvanõuetele, mille eesmärk on kaitsta salvestatud, edastatud või töödeldud andmete või kõnealuste toodete, teenuste ja protsesside funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust kogu nende olelusringi kestel.

Lisaks kinnitatakse sellega, et kooskõlas selliste kavadega hinnatud hallatud turbeteenused vastavad kindlaksmääratud turvanõuetele, mille eesmärk on kaitsta hallatud turbeteenuste pakkumisega seoses juurdepääsetavate, töödeldavate, salvestatavate või edastatavate andmete käideldavust, autentsust, terviklust ja konfidentsiaalsust, ning et neid hallatud turbeteenuseid pakuvad pidevalt vajaliku pädevuse, erialateadmiste ja kogemustega töötajad, kellel on piisaval ja sobival tasemel tehnilised teadmised ning erialane kohusetunne.“

6) Artiklit 47 muudetakse järgmiselt:

a) lõige 2 asendatakse järgmisega:

„2. Eelkõige sisaldab liidu jooksev tööprogramm IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste või nende kategooriate loetelu, mis võivad saada kasu Euroopa küberturvalisuse sertifitseerimise kava kohaldamisalasse kuulumisest.“;

b) lõiget 3 muudetakse järgmiselt:

i) sissejuhatav osa asendatakse järgmisega:

„3. IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse või nende kategooria lisamine liidu jooksvasse tööprogrammi peab olema põhjendatud vähemalt ühel järgneval alusel:“;

ii) punkt a asendatakse järgmisega:

„a) konkreetse IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse kategooriat hõlmavate riiklike küberturvalisuse sertifitseerimise kavade olemasolu või nende väljatöötamine, eriti seoses killustatuse ohuga;“;

iii) lisatakse järgmine punkt:

„ca) tehnoloogia areng ning rahvusvaheliste küberturvalisuse sertifitseerimise kavade ning rahvusvaheliste standardite ja tööstuses kasutatavate standardite olemasolu ja arendamine;“.

7) Artiklit 49 muudetakse järgmiselt:

a) lõiked 1–4 asendatakse järgmisega:

„1. Artikli 48 kohase komisjoni taotluse põhjal koostab ENISA ettevalmistava kava, mis vastab artiklites 51, 51a, 52 ja 54 sätestatud kohaldatavatele nõuetele.

2. Artikli 48 lõike 2 kohase Euroopa küberturvalisuse sertifitseerimise rühma taotluse põhjal võib ENISA koostada ettevalmistava kava, mis vastab artiklites 51, 51a, 52 ja 54 sätestatud kohaldatavatele nõuetele. Kui ENISA jätab taotluse rahuldamata, peab ta seda põhjendama. Taotluse rahuldamata jätmise otsuse teeb haldusnõukogu.

3. Ettevalmistavat kava koostades konsulteerib ENISA aegsasti kõigi asjaomaste sidusrühmadega ametliku, avatud, läbipaistva ja kaasava konsulteerimisprotsessi raames. Kui ENISA edastab lõike 6 kohaselt komisjonile ettevalmistava kava, esitab ta ühtlasi teabe selle kohta, mil viisil ta on käesolevat lõiget järginud.

4. Iga ettevalmistava kava puhul moodustab ENISA kooskõlas artikli 20 lõikega 4 ajutise töörühma, et pakkuda ENISA-le spetsiifilist nõu ja oskusteavet. Nimetatud ajutistesse töörühmadesse kuuluvad asjakohasel juhul ja ilma et see piiraks artikli 20 lõikes 4 sätestatud menetlusi ja kaalutlusõigust, liikmesriikide ametiasutuste, liidu institutsioonide, organite ja asutuste ning erasektori eksperdid.“;

b) lõige 7 asendatakse järgmisega:

„7. Komisjon võib ENISA koostatud ettevalmistava kava põhjal võtta vastu rakendusakte, millega nähakse ette artiklites 51, 51a, 52 ja 54 sätestatud asjakohastele nõuetele vastavad Euroopa küberturvalisuse sertifitseerimise kavad IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste jaoks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 66 lõikes 2 osutatud kontrollimenetlusega.“

8) Lisatakse järgmine artikkel:

„*Artikkel 49a*

Euroopa küberturvalisuse sertifitseerimise kavasid käsitlev teave ja konsulteerimine

1. Komisjon teeb artiklis 48 osutatud taotlust, milles ta palub ENISA-l koostada ettevalmistav kava või vaadata läbi olemasolev Euroopa küberturvalisuse sertifitseerimise kava, käsitleva teabe avalikult kättesaadavaks.

2. Selle aja jooksul, mil ENISA koostab artikli 49 kohast ettevalmistavat kava, võivad Euroopa Parlament, nõukogu või mõlemad korra kvartalis taotleda komisjonilt kui Euroopa küberturvalisuse sertifitseerimise rühma juhatajalt ja ENISA-lt asjakohase teabe esitamist ettevalmistava kava projekti kohta. ENISA võib Euroopa Parlamendi või nõukogu taotlusel ja kokkuleppel komisjoniga ning ilma et see piiraks artikli 27 kohaldamist, teha Euroopa Parlamendile ja nõukogule kättesaadavaks ettevalmistava kava projekti asjakohased osad nõutava konfidentsiaalsusega kooskõlas oleval ja asjakohasel juhul piiratud viisil.

3. Selleks et tõhustada dialoogi liidu institutsioonide vahel ning aidata kaasa ametlikule, avatud, läbipaistvale ja kaasavale konsultatsiooniprotsessile, võivad Euroopa Parlament, nõukogu või mõlemad kutsuda komisjoni ja ENISAt arutama küsimusi, mis on seotud IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste Euroopa küberturvalisuse sertifitseerimise kavade toimimisega.

4. Asjakohasel juhul võtab komisjon käesoleva määruse hindamisel artikli 67 kohaselt arvesse elemente, mis tulenevad Euroopa Parlamendi ja nõukogu seisukohtadest käesoleva artikli lõikes 3 osutatud küsimustes.“

9) Artiklit 51 muudetakse järgmiselt:

a) pealkiri asendatakse järgmisega:

„IKT-toodete, -teenuste ja -protsesside Euroopa küberturvalisuse sertifitseerimise kavade turvalisusega seotud eesmärgid“;

b) sissejuhatav lause asendatakse järgmisega:

„IKT-toodete, -teenuste või -protsesside Euroopa küberturvalisuse sertifitseerimise kava peab olema koostatud nii, et saavutada kohaldataval juhul vähemalt järgmised turvalisusega seotud eesmärgid:“.

10) Lisatakse järgmine artikkel:

„*Artikkel 51a*

Hallatud turbeteenuste Euroopa küberturvalisuse sertifitseerimise kavade turvalisusega seotud eesmärgid

Hallatud turbeteenuse Euroopa küberturvalisuse sertifitseerimise kava peab olema koostatud nii, et saavutada kohaldataval juhul vähemalt järgmised turvalisusega seotud eesmärgid:

a) hallatud turbeteenuseid pakutakse vajalikul tasemel pädevuse, erialateadmiste ja kogemustega, muu hulgas peavad töötajatel, kelle ülesanne on kõnealuseid teenuseid pakkuda, olema asjaomases valdkonnas piisaval ja sobival tasemel tehnilised teadmised ja pädevus ning piisav ja asjakohane kogemus ning suurim erialane kohusetunne;

b) hallatud turbeteenuse osutaja on kehtestanud sobivad sisemenetlused, mis tagavad, et hallatud turbeteenuseid pakutakse igal ajal piisava ja sobiva kvaliteediga;

c) hallatud turbeteenuste pakkumisega seoses juurdepääsetavad või salvestatavad, edastatavad või muul moel töödeldavad andmed on kaitstud juhusliku või volitamata juurdepääsu, salvestamise, avaldamise, hävitamise, muul viisil töötlemise, kaotsimineku, muutmise või kättesaamatuse eest;

d) füüsilise või tehnilise intsidendi korral taastatakse aegsasti andmete, teenuste ja funktsioonide käideldavus ja neile juurdepääs;

e) volitatud kasutajatel, programmidel ja masinatel on juurdepääs üksnes neile andmetele, teenustele või funktsioonidele, millele neil on õigus juurde pääseda;

f) on dokumenteeritud ja võimalik kontrollida, millal ja kes on pääsenud juurde millistele andmetele, teenustele või funktsioonidele, on neid kasutanud või muul viisil töödelnud;

g) hallatud turbeteenuste pakkumisel kasutatud IKT-tooted, -teenused ja -protsessid on sisseprojekteeritult ja vaikimisi turvalised, neil ei ole teadaolevaid turvanõrkusi ning kohaldataval juhul on neile paigaldatud kõige värskem turvauuendus ning need ei sisalda avalikult teadaolevaid turvanõrkusi.“

11) Artiklit 52 muudetakse järgmiselt:

a) lõige 1 asendatakse järgmisega:

„1. Euroopa küberturvalisuse sertifitseerimise kavas võidakse määrata IKT-toodetele, -teenustele, -protsessidele ning hallatud turbeteenustele üks või mitu järgmist usaldusväärsuse taset: baastase, märkimisväärne tase või kõrge tase. Usaldusväärsuse tase peab vastama IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse ettenähtud kasutamisega seotud riskitasemele, võttes arvesse intsidendi tõenäosust ja mõju.“;

b) lõige 3 asendatakse järgmisega:

„3. Euroopa küberturvalisuse sertifitseerimise kavas määratakse kindlaks igale usaldusväärsuse tasemele vastavad turvanõuded, sealhulgas turvafunktsioonid ja IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse hindamise rangus ja põhjalikkus.“;

c) lõiked 5, 6 ja 7 asendatakse järgmisega:

„5. Euroopa küberturvalisuse sertifikaat või ELi vastavusdeklaratsioon, mis osutab usaldusväärsuse baastasemele, annab kindluse, et IKT-tooted, -teenused, -protsessid või hallatud turbeteenused, mille kohta kõnealune sertifikaat või ELi vastavusdeklaratsioon on välja antud, vastavad asjaomastele turvanõuetele, sealhulgas turvafunktsioonidele, ning et neid on hinnatud tasemel, mille eesmärk on minimeerida intsidentide ja küberrünnete teadaolevaid põhilisi riske. Hindamine hõlmab vähemalt tehnilise dokumentatsiooni läbivaatamist. Kui tehnilise dokumentatsiooni läbivaatamine ei ole asjakohane, tuleb selle asemel kasutada muud samaväärse mõjuga hindamist.

6. Euroopa küberturvalisuse sertifikaat, mis osutab märkimisväärsele usaldusväärsuse tasemele, annab kindluse, et IKT-tooted, -teenused, -protsessid või hallatud turbeteenused, mille kohta kõnealune sertifikaat on välja antud, vastavad asjaomastele turvanõuetele, sealhulgas turvafunktsioonidele, ning et neid on hinnatud tasemel, mille eesmärk on minimeerida teadaolevaid küberturvalisuse riske ning piiratud oskuste ja vahenditega isikute poolt toimepandavate intsidentide ja küberrünnete riske. Hindamine hõlmab vähemalt järgmist: kontroll, mis tõendab, et ei esine avalikult teadaolevaid turvanõrkusi, ning testid, mis tõendavad, et IKT-tooted, -teenused, -protsessid või hallatud turbeteenused täidavad korrektselt vajalikke turvafunktsioone. Kui selline hindamine ei ole asjakohane, tuleb selle asemel kasutada muud samaväärse mõjuga hindamist.

7. Euroopa küberturvalisuse sertifikaat, mis osutab kõrgele usaldusväärsuse tasemele, annab kindluse, et IKT-tooted, -teenused, -protsessid või hallatud turbeteenused, mille kohta kõnealune sertifikaat on välja antud, vastavad asjaomastele turvanõuetele, sealhulgas turbefunktsioonidele, ning et neid on hinnatud tasemel, mille eesmärk on minimeerida märkimisväärsete oskuste ja vahenditega isikute poolt toimepandavate tipptasemel küberrünnete riski. Hindamine hõlmab vähemalt järgmist: kontroll, mis tõendab, et ei esine avalikult teadaolevaid turvanõrkusi, testid, mis tõendavad, et IKT-tooted, -teenused, -protsessid või hallatud turbeteenused täidavad vajalikke turvafunktsioone korrektselt ja tipptasemel ning nende oskuslikele häkkeritele vastupanemise võime hindamine läbistustestimise kaudu. Kui selline hindamine ei ole asjakohane, tuleb selle asemel kasutada muud samaväärse mõjuga hindamist.“

12) Artikli 53 lõiked 1, 2 ja 3 asendatakse järgmisega:

„1. Euroopa küberturvalisuse sertifitseerimise kavas võidakse lubada vastavuse enesehindamise läbiviimist IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja ainuvastutusel. Vastavuse enesehindamine on lubatud üksnes väikese riskiga IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste suhtes, mis vastavad usaldusväärsuse baastasemele.

2. IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja võib anda välja ELi vastavusdeklaratsiooni, milles kinnitatakse, et kavas kindlaks määratud nõuded on täidetud. ELi vastavusdeklaratsiooni väljaandmisega võtab IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja vastutuse IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse vastavuse eest kõnealuses kavas kindlaks määratud nõuetele.

3. IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja hoiab ELi vastavusdeklaratsiooni, tehnilist dokumentatsiooni ja muud asjaomast teavet, mis puudutab IKT-toodete, -teenuste ja -protsesside või hallatud turbeteenuste vastavust kavale, asjaomases Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud tähtaja jooksul kättesaadavana artikli 58 kohaselt määratud riikliku küberturvalisuse sertifitseerimise asutusele. ELi vastavusdeklaratsiooni koopia esitatakse riiklikule küberturvalisuse sertifitseerimise asutusele ja ENISA-le.“

13) Artikli 54 lõiget 1 muudetakse järgmiselt:

a) punkt a asendatakse järgmisega:

„a) sertifitseerimiskava sisu ja ulatus, sealhulgas hõlmatud IKT-toodete, -teenuste ja -protsesside või hallatud turbeteenuste liik või kategooria;“;

b) punkt g asendatakse järgmisega:

„g) konkreetsed hindamiskriteeriumid ja -meetodid, sealhulgas hindamise liigid, tõendamaks, et artiklites 51 ja 51a osutatud turvalisusega seotud kohaldatavad eesmärgid on täidetud;“;

c) punkt j asendatakse järgmisega:

„j) reeglid, mille abil jälgida IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste Euroopa küberturvalisuse sertifikaatide nõuetele või ELi vastavusdeklaratsiooni nõuetele vastavust, sealhulgas mehhanismid, millega kinnitatakse kindlaksmääratud küberturvalisuse nõuete jätkuvat täitmist;“;

d) punkt l asendatakse järgmisega:

„l) reeglid, mis käsitlevad sertifitseeritud või ELi vastavusdeklaratsiooni saanud IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste kava nõuetele mittevastavuse tagajärgi;“;

e) punkt o asendatakse järgmisega:

„o) teave sama liiki või samasse kategooriasse kuuluvaid IKT-tooteid, -teenuseid, -protsesse või hallatud turbeteenuseid, turvanõudeid, hindamiskriteeriumeid ja -meetodeid ning usaldusväärsuse tasemeid hõlmavate riiklike või rahvusvaheliste küberturvalisuse sertifitseerimise kavade kohta;“;

f) punkt q asendatakse järgmisega:

„q) ELi vastavusdeklaratsiooni, tehnilise dokumentatsiooni ning IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootja või pakkuja poolt kättesaadavaks tehtava muu asjaomase teabe kättesaadavuse tähtaeg;“.

14) Artiklit 56 muudetakse järgmiselt:

a) lõige 1 asendatakse järgmisega:

„1. Kui IKT-tooted, -teenused, -protsessid ning hallatud turbeteenused on sertifitseeritud Euroopa küberturvalisuse sertifitseerimise kava kohaselt, mis on vastu võetud vastavalt artiklile 49, eeldatakse, et nad vastavad kõnealuse kava nõuetele.“;

b) lõiget 3 muudetakse järgmiselt:

i) esimene lõik asendatakse järgmisega:

„Komisjon hindab korrapäraselt vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade tulemuslikkust ja kasutamist ning seda, kas konkreetne Euroopa küberturvalisuse sertifitseerimise kava tuleb teha asjakohase liidu õigusaktiga kohustuslikuks, et tagada liidus IKT-toodete, -teenuste ja -protsesside ning alates 4. veebruarist 2025 hallatud turbeteenuse küberturvalisuse piisav tase ning parandada siseturu toimimist. Esimene selline hindamine tuleb läbi viia 31. detsembriks 2023 ja seejärel vähemalt iga kahe aasta järel. Komisjon teeb hindamise tulemuste põhjal kindlaks olemasoleva sertifitseerimiskavaga hõlmatud IKT-tooted, -teenused, -protsessid ning hallatud turbeteenused, mis peavad olema kohustusliku sertifitseerimiskavaga hõlmatud.“;

ii) kolmandat lõiku muudetakse järgmiselt:

— punkt a asendatakse järgmisega:

„a) võtab arvesse mõju, mida avaldavad meetmed kõnealuste IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootjatele või pakkujatele ja kasutajatele kulude seisukohast, ning sotsiaalset ja majanduslikku kasu, mis tuleneb hinnatud IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste turvalisuse taseme eeldatavast paranemisest;“;

— punkt d asendatakse järgmisega:

„d) võtab arvesse rakendamise tähtpäevi, üleminekumeetmeid ja -tähtaegu, eelkõige meetme võimaliku mõju osas IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootjatele ja pakkujatele, sealhulgas VKEde, sealhulgas mikroettevõtjate erihuvid ja -vajadused;“;

c) lõiked 7 ja 8 asendatakse järgmisega:

„7. Füüsiline või juriidiline isik, kes esitab oma IKT-tooted, -teenused, -protsessid või hallatud turbeteenused sertifitseerimiseks, peab tegema artikli 58 kohaselt määratud riiklikule küberturvalisuse sertifitseerimise asutusele, kui kõnealune asutus on Euroopa küberturvalisuse sertifikaati väljaandev asutus, või artiklis 60 osutatud vastavushindamisasutusele kättesaadavaks kogu sertifitseerimiseks vajaliku teabe.

8. Euroopa küberturvalisuse sertifikaadi omanik teavitab lõikes 7 osutatud asutust igast hiljem avastatud turvanõrkusest või nõuete rikkumisest, mis puudutab sertifitseeritud IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse turvalisust ja millel võib olla mõju sertifitseerimisega seotud nõuete täitmisele. Kõnealune asutus edastab selle teabe põhjendamatu viivituseta asjaomasele riiklikule küberturvalisuse sertifitseerimise asutusele.“

15) Artikli 57 lõiked 1 ja 2 asendatakse järgmisega:

„1. Ilma et see piiraks käesoleva artikli lõike 3 kohaldamist, lõpeb riiklike küberturvalisuse sertifitseerimise kavade ja Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenustega seotud menetluste õiguslik toime artikli 49 lõike 7 kohaselt vastu võetud rakendusaktis kindlaks määratud kuupäeval. Riiklikud küberturvalisuse sertifitseerimise kavad ja nendega seotud menetlused, mis käsitlevad Euroopa küberturvalisuse sertifitseerimise kavaga hõlmamata IKT-tooteid, -teenuseid ja -protsesse ning hallatud turbeteenuseid, jäävad kehtima.

2. Liikmesriigid ei kehtesta kehtiva Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT-toodetele, -teenustele, -protsessidele ning hallatud turbeteenustele uusi riiklikke küberturvalisuse sertifitseerimise kavasid.“

16) Artiklit 58 muudetakse järgmiselt:

a) lõiget 7 muudetakse järgmiselt:

i) punktid a ja b asendatakse järgmisega:

„a) teeb koostöös teiste asjaomaste turujärelevalveasutustega järelevalvet artikli 54 lõike 1 punkti j kohaselt Euroopa küberturvalisuse sertifitseerimise kavades sisalduvate reeglite üle, mille kohaselt jälgitakse IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste vastavust selliste Euroopa küberturvalisuse sertifikaatide nõuetele, mis on välja antud tema liikmesriigi territooriumil, ja tagab nende reeglite täitmise;

b) jälgib tema liikmesriigi territooriumil asuvate ja vastavuse enesehindamist tegevate IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootjate või pakkujate kohustuste täitmist, eriti artikli 53 lõigetes 2 ja 3 ning vastavas Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud kohustuste täitmist, ja tagab nende kohustuste täitmise;“;

ii) punkt h asendatakse järgmisega:

„h) teeb koostööd teiste riiklike küberturvalisuse sertifitseerimise asutuste ja muude avaliku sektori asutustega, sealhulgas jagades teavet IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele, ning“;

b) lõige 9 asendatakse järgmisega:

„9. Riiklikud küberturvalisuse sertifitseerimise asutused teevad omavahel ja komisjoniga koostööd, eelkõige vahetavad teavet, kogemusi ja häid tavasid seoses küberturvalisuse sertifitseerimisega ning IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste küberturvalisust puudutavate tehniliste küsimustega.“

17) Artikli 59 lõike 3 punktid b ja c asendatakse järgmisega:

„b) IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste Euroopa küberturvalisuse sertifikaatide nõuetele vastavuse jälgimise reeglite artikli 58 lõike 7 punkti a kohase järelevalve ja täitmise tagamise menetlused;

c) artikli 58 lõike 7 punkti b kohased IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste tootjate või pakkujate kohustuste täitmise jälgimise ja kohustuste täitmise tagamise menetlused;“.

18) Artikli 67 lõiked 2 ja 3 asendatakse järgmisega:

„2. Hindamise raames analüüsitakse ka käesoleva määruse III jaotise sätete, sealhulgas Euroopa küberturvalisuse sertifitseerimise kavade (sealhulgas nende aluseks olevad tõendid) vastuvõtmist võimaldanud menetluste mõju, tulemuslikkust ja tõhusust seoses eesmärgiga tagada IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste piisav küberturvalisuse tase liidus ja parandada siseturu toimimist.

3. Hindamise käigus analüüsitakse, kas on vaja siseturule pääsu käsitlevaid olulisi küberturvalisuse nõudeid, et vältida selliste IKT-toodete, -teenuste, -protsesside ning hallatud turbeteenuste siseturule jõudmist, mis ei vasta põhilistele küberturvalisuse nõuetele.“

19) Lisa muudetakse kooskõlas käesoleva määruse lisaga.

Artikkel 2

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

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 19. detsember 2024

Euroopa Parlamendi nimel	*Nõukogu nimel*
eesistuja	*eesistuja*
R. METSOLA	BÓKA J.

LISA

Määruse (EL) 2019/881 lisa muudetakse järgmiselt:

1) punktid 2–5 asendatakse järgmisega:

„2. Vastavushindamisasutus on kolmandast isikust asutus, kes on sõltumatu organisatsioonist ja IKT-tootest, -teenusest, -protsessist või hallatud turbeteenustest, mida ta hindab.

3. Asutust, mis kuulub ettevõtjate ühendusse või kutseliitu, mis esindab ettevõtjaid, kes on seotud tema hinnatavate IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste projekteerimise, tootmise, pakkumise, monteerimise, kasutamise või hooldamisega, võib pidada vastavushindamisasutuseks tingimusel, et tõendatud on tema sõltumatus ning huvide konflikti puudumine.

4. Vastavushindamisasutus, selle kõrgem juhtkond ja vastavushindamisülesannete täitmise eest vastutavad töötajad ei tohi olla hinnatava IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse projekteerija, tootja, pakkuja, paigaldaja, ostja, omanik, kasutaja, hooldaja ega ühegi nimetatud isiku volitatud esindaja. Keeld ei välista vastavushindamisasutuse tegevuseks vajalike hinnatavate IKT-toodete kasutamist ega nende IKT-toodete kasutamist isiklikul otstarbel.

5. Vastavushindamisasutus, selle kõrgem juhtkond ja vastavushindamisülesannete täitmise eest vastutavad töötajad ei tohi olla otseselt seotud hinnatavate IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste projekteerimise, tootmise või konstrueerimise, pakkumise, turustamise, paigaldamise, kasutamise või hooldusega ega esindada ühtegi isikut, kes nimetatud tegevusega tegeleb. Vastavushindamisasutus, selle kõrgem juhtkond ja vastavushindamisülesannete täitmise eest vastutavad töötajad ei tohi osaleda tegevuses, mis võib seada kahtluse alla nende otsuste sõltumatuse ja usaldusväärsuse nende tehtavates vastavushindamistoimingutes. Keeld kehtib eelkõige nõustamisteenuste puhul.“;

2) punkti 10 muudetakse järgmiselt:

a) sissejuhatav osa asendatakse järgmisega:

„10. Vastavushindamisasutuse käsutuses peavad alati olema kõigile IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste liikidele, kategooriatele või alamkategooriatele ning kõigile vastavushindamismenetlustele vastavad järgmised vajalikud vahendid:“;

b) punkt c asendatakse järgmisega:

„c) toimingute tegemise menetlused, mis võtavad asjakohaselt arvesse ettevõtja suurust, tegutsemisvaldkonda, tema struktuuri, IKT-toote, -teenuse, -protsessi või hallatud turbeteenuse tehnoloogia keerukuse astet ning seda, kas tegemist on mass- või seeriatootmisega.“;

3) punktid 19 ja 20 asendatakse järgmisega:

„19. Vastavushindamisasutus peab vastama asjakohase, määruse (EÜ) nr 765/2008 artikli 2 punktis 9 määratletud harmoneeritud standardi nõuetele IKT-toodete, -teenuste, -protsesside või hallatud turbeteenuste sertifitseerimist läbiviivate vastavushindamisasutuste akrediteerimiseks.

20. Vastavushindamisasutus peab tagama, et vastavushindamiseks kasutatavad katselaborid vastavad asjakohase, määruse (EÜ) nr 765/2008 artikli 2 punktis 9 määratletud harmoneeritud standardi nõuetele katselaborite akrediteerimiseks.“

Käesoleva õigusakti kohta on tehtud avaldus, mis on kättesaadav ELTs C, C/2025/307, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/307/oj.