EUROOPA LIIT

EUROOPA PARLAMENT **NÕUKOGU**

Brüssel, 25. september 2024
(OR. en)

2022/0272(COD) **PE-CONS 100/23**

CYBER 328
JAI 1731
DATAPROTECT 391
TELECOM 409
MI 1168
CSC 579
CSCI 215
CODEC 2601

SEADUSANDLIKUD AKTID JA MUUD DOKUMENDID

Teema:	EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, 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)

EUROOPA PARLAMENDI JA NÕUKOGU
MÄÄRUS (EL) 2024/…,

…,

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)

(EMPs kohaldatav tekst)

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eelkõige 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]

---

1 ELT C 100, 16.3.2023, lk 101.

2 Euroopa Parlamendi 12. märtsi 2024. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu … otsus.

ning arvestades järgmist:

(1) Küberturvalisus on üks liidu ees seisvaid peamisi probleeme. Ühendatud seadmete arv ja mitmekesisus kasvab lähiaastatel hüppeliselt. Küberründed on avalikku huvi pakkuv küsimus, kuna need avaldavad olulist mõju mitte ainult liidu majandusele, vaid ka demokraatiale ning tarbijate ohutusele ja tervisele. Seepärast on vaja tugevdada liidu lähenemisviisi küberturvalisusele, tegeleda küberkerksuse küsimusega liidu tasandil ning parandada siseturu toimimist, kehtestades selleks ühtse õigusraamistiku, mis käsitleb digielemente sisaldavate toodete liidu turule laskmise jaoks olulisi küberturvalisuse nõudeid. Käsitleda tuleks kaht suurt probleemi, mis tekitavad kasutajate ja ühiskonna jaoks lisakulusid: ühest küljest digielemente sisaldavate toodete küberturvalisuse madal tase, millest annavad märku laialdaselt levinud nõrkused ning nende kõrvaldamiseks vajalike turvauuenduste ebapiisav ja ebajärjekindel pakkumine, ja teisalt see, et kasutajate arusaamine teabest ja juurdepääs sellele on ebapiisav, mis ei lase neil valida piisava küberturvalisusega tooteid või neid turvaliselt kasutada.

(2) Käesoleva määruse eesmärk on kehtestada turvaliste digielemente sisaldavate toodete väljatöötamise piirtingimused, tagades, et turule lastavatel riist- ja tarkvaratoodetel on vähem nõrkusi ja et tootjad suhtuvad turvalisusse kogu toote elutsükli jooksul tõsiselt. Ühtlasi on selle eesmärk luua tingimused, et kasutajad saaksid digielemente sisaldavaid tooteid valides ja kasutades võtta arvesse küberturvalisust, näiteks suurendades läbipaistvust seoses turul kättesaadavaks tehtud digielemente sisaldavate toodete toe kestusega.

(3) Kehtiv asjakohane liidu õigus sisaldab mitut horisontaalsete normide kogumit, mis käsitlevad küberturvalisusega seotud teatavaid aspekte eri vaatenurkadest, sealhulgas digitaalse tarneahela turvalisuse parandamise meetmed. Küberturvalisust käsitlev kehtiv liidu õigus, sealhulgas Euroopa Parlamendi ja nõukogu määrus (EL) 2019/881[3] ning Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555[4], ei reguleeri siiski otseselt digielemente sisaldavate toodete turvalisuse kohustuslikke nõudeid.

---

[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 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) Kehtivat liidu õigust kohaldatakse küll teatavate digielemente sisaldavate toodete suhtes, kuid puudub horisontaalne liidu õigusraamistik, milles sätestatakse kõigi digielemente sisaldavate toodete jaoks põhjalikud küberturvalisuse nõuded. Liidu ja liikmesriikide tasandi senised õigusaktid ja algatused on küberturvalisusega seoses kindlaks tehtud probleeme ja riske käsitlenud vaid osaliselt ning seega on siseturul loodud seadusandlik killustatus, mis suurendab nii selliste toodete tootjate kui ka kasutajate õiguskindlusetust ja tekitab ettevõtete ja organisatsioonide jaoks tarbetu koormuse täita samalaadsete toodete puhul paljusid eri nõudeid ja kohustusi. Selliste toodete küberturvalisusel on eriti tugev piiriülene aspekt, sest ühes liikmesriigis või kolmandas riigis valmistatud digielemente sisaldavaid tooteid kasutavad organisatsioonid ja tarbijad sageli kõikjal siseturul. See tähendab, et kõnealust valdkonda on vaja reguleerida liidu tasandil, et tagada ühtlustatud õigusraamistik ja õiguskindlus kasutajatele, organisatsioonidele ja ettevõtetele, sealhulgas mikroettevõtjatele ning väikestele ja keskmise suurusega ettevõtjatele, nagu on määratletud komisjoni soovituse 2003/361/EÜ[5] lisas. Liidu õigusliku keskkonna ühtlustamiseks tuleks kehtestada digielemente sisaldavate toodete küberturvalisuse horisontaalsed nõuded. Ühtlasi tuleks kogu liidus tagada ettevõtjate ja kasutajate jaoks õiguskindlus, samuti siseturu parem ühtlustamine ja proportsionaalsus mikro-, väikeste ja keskmise suurusega ettevõtjate jaoks, luues sellele turule siseneda soovivate ettevõtjate jaoks paremini toimivad tingimused.

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

(5) Mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate puhul tuleks ettevõtja kategooria kindlaksmääramisel kohaldada komisjoni soovituse 2003/361/EÜ lisa sätteid täies ulatuses. Seetõttu tuleks töötajate arvu ja rahaliste ülemmäärade arvutamisel ettevõtjate kategooriate kindlaksmääramiseks kohaldada ka komisjoni soovituse 2003/361/EÜ lisa artikli 6 sätteid, mis käsitlevad ettevõtja andmete kindlakstegemist teatavat liiki ettevõtjate, näiteks partnerettevõtjate või sidusettevõtjate puhul.

(6) Komisjon peaks andma suuniseid, et abistada ettevõtjaid, eelkõige mikroettevõtjaid ning väikeseid ja keskmise suurusega ettevõtjaid käesoleva määruse kohaldamisel. Sellised suunised peaksid muu hulgas hõlmama käesoleva määruse kohaldamisala, eelkõige andmete kaugtöötlust ja selle mõju vaba ja avatud lähtekoodiga tarkvara arendajatele, digielemente sisaldavate toodete toe kestuse kindlaksmääramiseks kasutatavate kriteeriumide kohaldamist, käesoleva määruse ja muu liidu õiguse koostoimet ning olulise muudatuse käsitlust.

(7) Liidu tasandil on mitmetes programmilistes ja poliitilistes dokumentides, näiteks komisjoni ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja 16. detsembri 2020. aasta ühisteatises „ELi küberturvalisuse strateegia digikümnendi jaoks“, nõukogu 2. detsembri 2020. aasta järeldustes ühendatud seadmete küberturvalisuse kohta ja 23. mai 2022. aasta järeldustes Euroopa Liidu kübervaldkonna positsiooni arendamise kohta ning Euroopa Parlamendi 10. juuni 2021. aasta resolutsioonis ELi küberturvalisuse strateegia kohta digikümnendi jaoks[6], nõutud, et digitaalsete või ühendatud toodete jaoks kehtestataks liidu küberturvalisuse erinõuded, kusjuures mitu kolmandat riiki on selle probleemi lahendamiseks omal algatusel juba meetmeid võtnud. Euroopa tuleviku konverentsi lõpparuandes soovisid kodanikud ELi rolli tugevdamist küberohtudega võitlemisel. Et liidul oleks küberturvalisuse valdkonnas juhtiv rahvusvaheline roll, on oluline kehtestada ambitsioonikas õigusraamistik.

(8) Kõigi siseturule lastavate digielemente sisaldavate toodete üldise küberturvalisuse taseme tõstmiseks tuleb kehtestada nende toodete eesmärgipärased ja tehnoloogianeutraalsed olulised küberturvalisuse nõuded, mis kehtivad horisontaalselt.

---

[6] ELT C 67, 8.2.2022, lk 81.

(9) Teatavatel tingimustel võivad kõik digielemente sisaldavad tooted, mis on integreeritud või ühendatud suuremate elektrooniliste infosüsteemidega, olla kuritahtlike isikute jaoks ründevektor. Seetõttu võib ka riistvara ja tarkvara, mille tähtsust ei peeta nii kriitiliseks, hõlbustada seadme või võrgu esialgset kahjustamist ja võimaldada kuritahtlikul isikul saada süsteemile eelisjuurdepääsu või liikuda süsteemide vahel lateraalselt. Seepärast peaksid tootjad tagama, et kõik digielemente sisaldavad tooted projekteeritakse ja neid arendatakse kooskõlas käesolevas määruses sätestatud oluliste küberturvalisuse nõuetega. See kohustus käib nii nende toodete kohta, mida saab ühendada füüsiliselt riistvaralise liidese kaudu, kui ka toodete kohta, mis ühendatakse loogiliselt, näiteks võrgupesa, toru, faili, rakendusliidese või muud liiki tarkvaraliidese kaudu. Küberohud võivad enne teatava sihtmärgini jõudmist levida mitmesuguste digielemente sisaldavate toodete kaudu, näiteks mitmest nõrkuse ärakasutamisest tekitatud ahelas, ja seepärast peaksid tootjad tagama ka selliste digielemente sisaldavate toodete küberturvalisuse, mis on teiste seadmete või võrkudega ühendatud üksnes kaudselt.

(10) Küberturvalisuse nõuete sätestamisega digielemente sisaldavate toodete turule laskmise jaoks on kavas suurendada nende toodete küberturvalisust nii tarbijate kui ka ettevõtjate jaoks. Nende nõuetega tagatakse samuti küberturvalisusega arvestamine kogu tarneahela ulatuses, mis muudab digielemente sisaldavad lõpptooted ja nende komponendid turvalisemaks. See hõlmab ka vähekaitstud tarbijatele mõeldud digielemente sisaldavate toodete, näiteks mänguasjade ja beebimonitorisüsteemide turule laskmise nõudeid. Digielemente sisaldavad tarbekaubad, mis on käesolevas määruses liigitatud digielemente sisaldavateks olulisteks toodeteks, kujutavad endast suuremat küberriski, kuna need täidavad funktsiooni, millega kaasneb märkimisväärne risk, et avalduv kahjulik mõju on intensiivsem ja võib kahjustada niisuguste toodete kasutajate tervist, turvalisust või ohutust, ning nende suhtes tuleks kohaldada rangemat vastavushindamismenetlust. See kehtib selliste toodete suhtes nagu nutikodu tooted, millel on turvafunktsioonid, nagu arukad ukselukud, beebimonitorisüsteemid ja häiresüsteemid, andmesideühendusega mänguasjad ja isiklik kaasaskantav terviseseiretehnoloogia. Lisaks aitavad rangemad vastavushindamismenetlused, mille peavad läbima muud käesolevas määruses digielemente sisaldavateks olulisteks või kriitilise tähtsusega toodeteks liigitatud digielemente sisaldavad tooted, vältida nõrkuste ärakasutamise võimalikku kahjulikku mõju tarbijatele.

(11) Käesoleva määruse eesmärk on tagada digielemente sisaldavate toodete ja nende integreeritud andmete kaugtöötluslahenduste küberturvalisuse kõrge tase. Sellised andmete kaugtöötluslahendused tuleks määratleda kui distantsilt toimuv andmetöötlus, mille jaoks tarkvara on projekteerinud ja arendanud asjaomase digielemente sisaldava toote tootja või on seda tehtud tema nimel, ning mille puudumine ei laseks digielemente sisaldaval tootel täita üht oma funktsioonidest. Niisuguse lähenemisega tagatakse, et tootjad on sellised tooted igakülgselt piisavalt turvanud, olenemata sellest, kas andmeid töödeldakse või salvestatakse kohapeal kasutaja seadmes või tootja poolt kaugühenduse teel. Samal ajal kuulub kaugtöötlemine või -salvestamine käesoleva määruse kohaldamisalasse ainult niivõrd, kuivõrd see on vajalik digielemente sisaldava toote funktsioonide täitmiseks. Selline kaugtöötlemine või -salvestamine hõlmab olukorda, kus mobiilirakendus vajab juurdepääsu rakendusliidesele või andmebaasile, mida pakub tootja välja töötatud teenus. Sellisel juhul kuulub teenus andmete kaugtöötluslahendusena käesoleva määruse kohaldamisalasse. Käesoleva määruse kohaldamisalasse kuuluvaid andmete kaugtöötluslahendusi käsitlevad nõuded ei hõlma seega tehnilisi, operatiiv- ega korralduslikke meetmeid, mille eesmärk on ohjata riske, mis ohustavad tootja võrgu- ja infosüsteemide turvalisust tervikuna.

(12) Pilvelahendused on käesoleva määruse tähenduses andmete kaugtöötluslahendused üksnes siis, kui need vastavad käesolevas määruses sätestatud määratlusele. Näiteks kuuluvad käesoleva määruse kohaldamisalasse nutikodu seadmete tootjate pakutavad pilvefunktsioonid, mis võimaldavad kasutajatel seadet kaugjuhtida. Teisalt ei kuulu käesoleva määruse kohaldamisalasse veebisaidid, mis ei toeta digielemente sisaldava toote funktsioone, või pilveteenused, mis on projekteeritud ja välja töötatud muul kui digielemente sisaldava toote tootja vastutusel. Pilvandmetöötluse teenuste ja pilveteenuste mudelite, sh tarkvara teenusena (SaaS), platvorm teenusena (PaaS) ja taristu teenusena (IaaS), suhtes kohaldatakse direktiivi (EL) 2022/2555. Liidus pilvandmetöötlusteenuseid osutavad üksused, mis on komisjoni soovituse 2003/361/EÜ lisa artikli 2 tähenduses keskmise suurusega ettevõtjad või ületavad kõnealuse artikli lõikes 1 sätestatud keskmise suurusega ettevõtjate ülemmäärasid, kuuluvad kõnealuse direktiivi kohaldamisalasse.

(13) Kooskõlas käesoleva määruse eesmärgiga kõrvaldada digielemente sisaldavate toodete vaba liikumise takistused, ei tohiks liikmesriigid takistada käesoleva määrusega hõlmatud küsimustes käesoleva määruse nõuetele vastavate digielemente sisaldavate toodete turul kättesaadavaks tegemist. Seetõttu ei tohi liikmesriigid käesoleva määrusega ühtlustatud küsimustes kehtestada digielemente sisaldavate toodete turul kättesaadavaks tegemisele täiendavaid küberturvalisuse nõudeid. Iga avaliku või erasektori üksus võib siiski kehtestada lisaks käesolevas määruses sätestatud nõuetele täiendavaid nõudeid digielemente sisaldavate toodete hankimiseks või kasutamiseks oma erieesmärkidel ning võib seetõttu otsustada kasutada digielemente sisaldavaid tooteid, mis vastavad rangematele või konkreetsematele küberturvalisuse nõuetele kui need, mida kohaldatakse käesoleva määruse alusel turul kättesaadavaks tegemise suhtes. Ilma et see piiraks Euroopa Parlamendi ja nõukogu direktiivide 2014/24/EL[7] ja 2014/25/EL[8] kohaldamist, peaksid liikmesriigid selliste digielemente sisaldavate toodete hankimisel, mis peavad vastama käesolevas määruses sätestatud olulistele küberturvalisuse nõuetele, sealhulgas nõrkuste käsitlemisega seotud nõuetele, tagama, et niisuguseid nõudeid võetakse hankemenetluses arvesse ning et arvesse võetakse ka tootjate suutlikkust tulemuslikult kohaldada küberturvalisuse meetmeid ja hallata küberohte.

---

[7] Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/24/EL riigihangete kohta ja direktiivi 2004/18/EÜ kehtetuks tunnistamise kohta (ELT L 94, 28.3.2014, lk 65).

[8] Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/25/EL, milles käsitletakse vee-, energeetika-, transpordi- ja postiteenuste sektoris tegutsevate üksuste riigihankeid ja millega tunnistatakse kehtetuks direktiiv 2004/17/EÜ (ELT L 94, 28.3.2014, lk 243).

Lisaks on direktiivis (EL) 2022/2555 sätestatud küberturvalisuse riskijuhtimismeetmed kõnealuse direktiivi artiklis 3 osutatud elutähtsate ja oluliste üksuste jaoks, mis võivad hõlmata tarneahela turvameetmeid, milleks on vaja, et sellised üksused kasutaksid digielemente sisaldavaid tooteid, mis vastavad käesolevas määruses sätestatutest rangematele küberturvalisuse nõuetele. Kooskõlas direktiiviga (EL) 2022/2555 ja selle minimaalse ühtlustamise põhimõttega võivad liikmesriigid seega kehtestada täiendavaid küberturvalisuse nõudeid IKT-toodete kasutamisele elutähtsate või oluliste üksuste poolt vastavalt kõnealusele direktiivile, et tagada kõrgem küberturvalisuse tase, tingimusel et sellised nõuded on kooskõlas liikmesriikide kohustustega, mis on sätestatud liidu õiguses. Küsimused, mida käesolev määrus ei hõlma, võivad hõlmata digielemente sisaldavate toodete ja nende tootjatega seotud mittetehnilisi tegureid. Seepärast võivad liikmesriigid kehtestada riiklikke meetmeid, sealhulgas piiranguid digielemente sisaldavatele toodetele või selliste toodete tarnijatele, mis võtavad arvesse mittetehnilisi tegureid. Selliste teguritega seotud riiklikud meetmed peavad olema liidu õigusega kooskõlas.

(14) Käesolev määrus ei tohiks piirata liikmesriikide vastutust riikliku julgeoleku tagamise eest kooskõlas liidu õigusega. Liikmesriikidel peaks olema võimalik kohaldada riikliku julgeoleku või kaitse eesmärkidel hangitavate või kasutatavate digielemente sisaldavate toodete suhtes lisameetmeid, tingimusel et sellised meetmed on kooskõlas liikmesriikide kohustustega, mis on sätestatud liidu õiguses.

(15) Käesolevat määrust kohaldatakse ettevõtjate suhtes üksnes seoses digielemente sisaldavate toodetega, mis on turul kättesaadavaks tehtud ja mida seega tarnitakse liidu turul äritegevuse käigus levitamiseks või kasutamiseks. Äritegevuse käigus toimuvat tarnimist võib iseloomustada mitte üksnes digielemente sisaldava toote eest hinna küsimine, vaid ka tehniliste tugiteenuste eest hinna küsimine, kui see ei täida ainult tegelike kulude katmise eesmärki, kui selle eest on kavatsus tulu teenida näiteks tarkvaraplatvormi pakkumisega, mille kaudu tootja teenib tulu muude teenuste eest, nõudes kasutamise eeltingimusena isikuandmete töötlemist muul otstarbel kui üksnes tarkvara turvalisuse, ühilduvuse või koostalitlusvõime parandamiseks, või võttes vastu annetusi, mis ületavad digielemente sisaldava toote projekteerimise, väljatöötamise ja pakkumisega seotud kulusid. Annetuste vastuvõtmist kasumi saamise kavatsuseta ei tohiks käsitada äritegevusena.

(16) Digielemente sisaldavaid tooteid, mida pakutakse sellise teenuse osutamise raames, mille eest võetakse tasu üksnes selle teenuse osutamisega otseselt seotud tegelike kulude katmiseks, näiteks teatavate digielemente sisaldavate toodete puhul, mida pakuvad avalikud haldusüksused, ei tohiks käsitada üksnes nendel põhjustel käesoleva määruse tähenduses äritegevusena. Lisaks ei tohiks digielemente sisaldavaid tooteid, mille avalik haldusüksus on välja töötanud või mida ta on muutnud üksnes oma tarbeks, käsitada käesoleva määruse tähenduses turul kättesaadavaks tehtutena.

(17) Avalikult jagatav tarkvara ja andmed, mille puhul kasutajad saavad neile või nende muudetud versioonidele vabalt juurde pääseda, neid kasutada, muuta ja edasi levitada, võivad aidata kaasa teadusuuringutele ja innovatsioonile turul. Selleks et edendada vaba ja avatud lähtekoodiga tarkvara arendamist ja kasutuselevõttu, eelkõige mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate, sealhulgas idufirmade, üksikisikute, mittetulundusühenduste ja akadeemiliste teadusorganisatsioonide poolt, tuleks käesoleva määruse kohaldamisel selliste digielemente sisaldavate toodete suhtes, mida käsitatakse äritegevuse käigus levitamiseks või kasutamiseks tarnitava vaba ja avatud lähtekoodiga tarkvarana, võtta arvesse vaba ja avatud lähtekoodiga tarkvara litsentside alusel levitatava ja arendatava tarkvara erinevate arendusmudelite olemust.

(18) Vaba ja avatud lähtekoodiga tarkvara on tarkvara, mille lähtekoodi jagatakse avalikult ja mis tehakse kättesaadavaks sellise litsentsi alusel, mis annab kõik õigused teha see vabalt kättesaadavaks, kasutatavaks, muudetavaks ja levitatavaks. Vaba ja avatud lähtekoodiga tarkvara arendatakse, hallatakse ja levitatakse avatult, sealhulgas veebiplatvormide kaudu. Käesoleva määruse kohaldamisalasse kuuluvate ettevõtjate puhul peaks käesoleva määruse kohaldamisalasse kuuluma üksnes turul kättesaadavaks tehtud vaba ja avatud lähtekoodiga tarkvara, mida seetõttu tarnitakse levitamiseks või äritegevuse käigus kasutamiseks. Seetõttu ei tohiks selle kindlaksmääramisel, kas niisuguse tegevuse olemus on äriline või mitte, võtta arvesse üksnes asjaolusid, mille korral digielemente sisaldavat toodet on arendatud, või seda, kuidas arendamist on rahastatud. Täpsemalt ei tohiks käesoleva määruse kohaldamisel ja seoses selle kohaldamisalasse kuuluvate ettevõtjatega käsitada äritegevusena selliste digielemente sisaldavate toodete pakkumist, mida käsitatakse vaba ja avatud lähtekoodiga tarkvarana, millega tootjad ei teeni tulu, et tagada arendus- ja tarneetappide selge eristamine. Lisaks tuleks selliste digielemente sisaldavate toodete tarnimist, mida käsitatakse teiste tootjate poolt nende digielemente sisaldavatesse toodetesse integreerimiseks mõeldud vaba ja avatud lähtekoodiga tarkvara komponentidena, käsitada turul kättesaadavaks tegemisena üksnes juhul, kui komponendi algne tootja teenib sellega tulu. Näiteks ei tohiks ainuüksi asjaolu, et digielemente sisaldav avatud lähtekoodiga tarkvaratoode saab tootjatelt rahalist toetust või et tootjad aitavad kaasa sellise toote arendamisele, tähendada iseenesest seda, et niisugune tegevus on ärilist laadi.

Samuti ei tohiks ainuüksi regulaarsete versioonide olemasolu iseenesest tuua kaasa järeldust, et digielemente sisaldavat toodet tarnitakse äritegevuse käigus. Käesoleva määruse kohaldamisel ei tohiks vaba ja avatud lähtekoodiga tarkvarana käsitatavate digielemente sisaldavate toodete väljatöötamist mittetulundusühenduste poolt samuti käsitada äritegevusena, kui organisatsioon on loodud viisil, mis tagab, et kogu tulu, millest on maha arvestatud kulud, kasutatakse mittetulunduslike eesmärkide saavutamiseks. Käesolevat määrust ei kohaldata füüsiliste või juriidiliste isikute suhtes, kes panustavad lähtekoodiga sellistesse digielemente sisaldavatesse toodetesse, mida käsitatakse vaba ja avatud lähtekoodiga tarkvarana ja mis ei kuulu nende vastutusalasse.

(19) Võttes arvesse, kui olulised on paljud sellised digielemente sisaldavad tooted, mida käsitatakse vaba ja avatud lähtekoodiga tarkvarana ning mida avaldatakse, kuid ei tehta turul kättesaadavaks käesoleva määruse tähenduses, tuleks juriidiliste isikute suhtes, kes pakuvad pidevat tuge niisuguste toodete arendamisel, mis on mõeldud äritegevuseks, ja kellel on peamine roll niisuguste toodete elujõulisuse tagamisel (avatud lähtekoodiga tarkvara korraldajad), kohaldada lihtsamat ja kohandatud regulatiivset korda. Avatud lähtekoodiga tarkvara korraldajad hõlmavad nii teatavaid sihtasutusi kui ka üksusi, mis arendavad ja avaldavad vaba ja avatud lähtekoodiga tarkvara seoses äritegevusega, sealhulgas mittetulunduslikud üksused. Regulatiivses korras peaks võtma arvesse nende eripära ja vastavust kehtestatud kohustuste liigile. See peaks hõlmama üksnes niisuguseid digielemente sisaldavaid tooteid, mida käsitatakse vaba ja avatud lähtekoodiga tarkvarana ning mis on lõppkokkuvõttes ette nähtud äritegevuseks, näiteks integreerimiseks äriteenustesse või digielemente sisaldavatesse toodetesse, millega teenitakse tulu. Kõnealuse regulatiivse korra kohaldamisel hõlmab kavatsus integreerida tulu teenivatesse digielemente sisaldavatesse toodetesse juhtumeid, kus tootjad, kes integreerivad komponendi oma digielemente sisaldavatesse toodetesse, panustavad selle komponendi korrapärasesse arendamisse või annavad korrapärast rahalist abi, et tagada tarkvaratoote toimepidevus. Pidev toetus digielemente sisaldava toote arendamiseks hõlmab muu hulgas tarkvaraarenduse koostööplatvormide majutamist ja haldamist, lähtekoodi või tarkvara majutamist, selliste digielemente sisaldavate toodete juhtimist või haldamist, mida käsitatakse vaba ja avatud lähtekoodiga tarkvarana, ning selliste toodete arendamise juhtimist. Arvestades, et lihtsama ja kohandatud regulatiivse korraga ei kehtestata nendele, kes tegutsevad avatud lähtekoodiga tarkvara korraldajatena, samu kohustusi kui nendele, kes tegutsevad käesoleva määruse kohaldamisalasse kuuluvate tootjatena, ei tohiks neil lubada CE-vastavusmärgise kinnitamist digielemente sisaldavatele toodetele, mille arendamist nad toetavad.

(20) Kui digielemente sisaldavaid tooteid avatud hoidlates üksnes majutatakse, sealhulgas paketihaldurite kaudu või koostööplatvormidel, ei tähenda see iseenesest digielemente sisaldava toote turul kättesaadavaks tegemist. Selliste teenuste osutajaid tuleks käsitada turustajatena ainult siis, kui nad teevad niisuguse tarkvara turul kättesaadavaks ja seega tarnivad seda liidu turul äritegevuse käigus levitamiseks või kasutamiseks.

(21) Selleks et toetada ja hõlbustada nende tootjate hoolsuskohustust, kes integreerivad oma digielemente sisaldavatesse toodetesse, mille suhtes ei kohaldata käesolevas määruses sätestatud olulisi küberturvalisuse nõudeid, vaba ja avatud lähtekoodiga tarkvara komponendid, peaks komisjonil olema võimalik kehtestada vabatahtlikud turvalisuse tõendamise programmid kas käesolevat määrust täiendava delegeeritud õigusaktiga või nõudes määruse (EL) 2019/881 artikli 48 kohast Euroopa küberturvalisuse sertifitseerimise kava, milles võetakse arvesse vaba ja avatud lähtekoodiga tarkvara arendusmudelite eripära. Turvalisuse tõendamise programmid tuleks kavandada nii, et turvalisuse tõendamist saaksid algatada või rahastada mitte ainult füüsilised või juriidilised isikud, kes arendavad vaba ja avatud lähtekoodiga tarkvarana käsitatavat digielemente sisaldavat toodet või aitavad sellele kaasa, vaid ka kolmandad isikud, näiteks tootjad, kes integreerivad sellised tooted oma digielemente sisaldavatesse toodetesse, kasutajad, või liidu ja liikmesriikide haldusasutused.

(22) Võttes arvesse käesoleva määruse avaliku küberturvalisuse eesmärke ja selleks, et parandada liikmesriikide olukorrateadlikkust seoses liidu sõltuvusega tarkvarakomponentidest ning eelkõige potentsiaalselt vaba ja avatud lähtekoodiga tarkvara komponentidest, peaks käesoleva määrusega loodud spetsiaalne halduskoostöörühm (ADCO) saama otsustada, kas viia ühiselt läbi liidu sõltuvuse hindamine. Turujärelevalveasutustel peaks olema võimalik nõuda, et ADCO kehtestatud digielemente sisaldavate toodete kategooriate tootjad esitaksid käesoleva määruse kohaselt koostatud tarkvara koostenimekirjad. Selleks et kaitsta tarkva koostenimekirjade konfidentsiaalsust, peaksid turujärelevalveasutused esitama ADCO-le sõltuvuse kohta asjakohase anonüümitud koondteabe.

(23) Käesoleva määruse rakendamise tulemuslikkus sõltub ka piisavate küberturvalisuse alaste oskuste olemasolust. Liidu tasandil tunnistati erinevates programmilistes ja poliitikadokumentides, sealhulgas komisjoni 18. aprilli 2023. aasta teatises „Korvata küberturvalisuse valdkonna talendinappus edendamaks ELi konkurentsivõimet, majanduskasvu ja kerksust“ ning nõukogu 22. mai 2023. aasta järeldustes ELi küberkaitsepoliitika kohta, et liidus esineb küberturvalisuse oskuste nappus, ja vajadust tegeleda selliste probleemidega esmajärjekorras nii avalikus kui ka erasektoris. Käesoleva määruse tulemusliku rakendamise tagamiseks peaksid liikmesriigid tagama piisavate vahendite olemasolu turujärelevalveasutuste ja vastavushindamisasutuste vajalike töötajate jaoks, et nad saaksid täita käesolevas määruses sätestatud ülesandeid. Need meetmed peaksid suurendama küberturvalisuse valdkonna töötajate liikuvust ja nende seonduvaid karjäärivõimalusi. Samuti peaksid need aitama muuta küberturvalisuse valdkonna tööjõu kerksamaks ja kaasavamaks, seda ka soolises aspektis. Seepärast peaksid liikmesriigid võtma meetmeid tagamaks, et neid ülesandeid täidavad piisavalt koolitatud ja vajalike küberturvalisuse alaste oskustega spetsialistid. Samuti peaksid tootjad tagama, et nende töötajatel on käesolevas määruses sätestatud kohustuste täitmiseks vajalikud oskused. Liikmesriigid ja komisjon peaksid kooskõlas oma õiguste ja pädevustega ning neile käesoleva määrusega antud spetsiaalsete ülesannetega võtma meetmeid, et toetada tootjaid, eelkõige mikroettevõtjaid ning väikeseid ja keskmise suurusega ettevõtjaid, sealhulgas idufirmasid, ka sellistes valdkondades nagu oskuste arendamine, et nad saaksid täita käesolevas määruses sätestatud kohustusi. Kuna direktiivis (EL) 2022/2555 nõutakse, et liikmesriigid võtaksid oma riiklike küberturvalisuse strateegiate raames poliitikameetmed, millega edendatakse ja töötatakse välja küberturvalisuse alast ning küberturvalisusega seotud oskuste alast koolitust, võivad liikmesriigid selliste strateegiate vastuvõtmisel kaaluda ka käesolevast määrusest tulenevate küberturvalisusega seotud oskuste vajaduste, sealhulgas ümberõppe ja täiendõppega seotud vajaduste rahuldamist.

(24) Turvaline internet on elutähtsa taristu ja ühiskonna kui terviku toimimiseks hädavajalik. Direktiivi (EL) 2022/2555 eesmärk on tagada kõnealuse direktiivi artiklis 3 osutatud elutähtsate ja oluliste üksuste, sealhulgas avatud interneti tuumteenuseid toetavate, internetiühendust tagavate ja internetiteenuseid osutatavate digitaristu pakkujate osutatavate teenuste küberturvalisuse kõrge tase. Seepärast on oluline, et digielemente sisaldavad tooted, mida digitaristu pakkujad vajavad, et tagada interneti toimimine, oleksid välja töötatud turvalisel viisil ja et need vastaksid väljakujunenud internetiturvalisuse standarditele. Käesolevat määrust kohaldatakse kõigi ühendatavate riistvara- ja tarkvaratoodete suhtes ning ühtlasi on selle määruse eesmärk aidata digitaristu pakkujatel täita direktiivist (EL) 2022/2555 tulenevaid tarneahela nõudeid, tagades, et nende teenuste osutamiseks kasutatavate digielemente sisaldavate toodete väljatöötamine toimub turvalisel viisil ning neil on juurdepääs selliste toodete õigeaegsetele turvauuendustele.

(25) Euroopa Parlamendi ja nõukogu määrusega (EL) 2017/745[9] on kehtestatud õigusnormid meditsiiniseadmete kohta ning Euroopa Parlamendi ja nõukogu määrusega (EL) 2017/746[10] in vitro diagnostikameditsiiniseadmete kohta. Nendes määrustes on käsitletud küberriske ja järgitud lähenemisviise, mida puudutatakse ka käesolevas määruses. Konkreetsemalt on määrustes (EL) 2017/745 ja (EL) 2017/746 sätestatud olulised nõuded selliste meditsiiniseadete jaoks, mis toimivad elektroonilise süsteemi kaudu või on ise tarkvara. Neis määrustes käsitletakse ka teatavat sisseehitamata tarkvara ja kogu elutsüklit hõlmavat lähenemisviisi. Need nõuded kohustavad tootjaid kohaldama oma toodete väljatöötamisel ja loomisel riskijuhtimise põhimõtteid ning kehtestama IT-turvalisuse meetmete alased nõuded ja asjaomased vastavushindamismenetlused. Peale selle kehtivad alates 2019. aasta detsembrist meditsiiniseadmete küberturvalisuse kohta erijuhised, millega antakse meditsiiniseadmete, sealhulgas in vitro diagnostikaseadmete tootjatele juhised selle kohta, kuidas täita küberturvalisuse osas kõiki nende määruste I lisas sätestatud asjaomaseid olulisi nõudeid. Seega ei peaks digielemente sisaldavad tooted, mille suhtes kohaldatakse üht neist määrustest, kuuluma käesoleva määruse kohaldamisalasse.

---

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

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

(26) Digielemente sisaldavad tooted, mis on välja töötatud või mida on muudetud üksnes riikliku julgeoleku või kaitse otstarbel, või tooted, mis on spetsiaalselt projekteeritud salastatud teabe töötlemiseks, ei kuulu käesoleva määruse kohaldamisalasse. Liikmesriike julgustatakse tagama kõnealustele toodetele sama või kõrgema kaitsetaseme kui käesoleva määruse kohaldamisalasse kuuluvate toodete puhul.

(27) Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/2144[11] on ette nähtud sõidukite ning nende süsteemide ja osade tüübikinnituse nõuded, millega kehtestati teatavad küberturvalisuse nõuded (muu hulgas sertifitseeritud küberturvalisuse haldamise süsteemide käitamise ja tarkvarauuenduste kohta), mis hõlmavad organisatsiooni põhimõtteid ja protseduure sõidukite, seadmete ja teenuste kogu olelusringi ja elutsükliga seotud küberriskide jaoks kooskõlas kohaldatavate ÜRO eeskirjadega tehniliste spetsifikatsioonide ja küberturvalisuse kohta, eelkõige ÜRO eeskirjaga nr 155 (ühtsed sätted, mis käsitlevad sõidukite tüübikinnitust seoses küberturvalisuse ja küberturvalisuse haldamise süsteemiga), ning millega on ette nähtud konkreetsed vastavushindamismenetlused.

---

[11] Euroopa Parlamendi ja nõukogu 27. novembri 2019. aasta määrus (EL) 2019/2144, mis käsitleb mootorsõidukite ja nende haagiste ning mootorsõidukite jaoks ette nähtud süsteemide, osade ja eraldi seadmestike tüübikinnituse nõudeid seoses nende üldise ohutuse ning sõitjate ja vähekaitstud liiklejate kaitsega ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) 2018/858 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 78/2009, (EÜ) nr 79/2009 ja (EÜ) nr 661/2009 ning komisjoni määrused (EÜ) nr 631/2009, (EL) nr 406/2010, (EL) nr 672/2010, (EL) nr 1003/2010, (EL) nr 1005/2010, (EL) nr 1008/2010, (EL) nr 1009/2010, (EL) nr 19/2011, (EL) nr 109/2011, (EL) nr 458/2011, (EL) nr 65/2012, (EL) nr 130/2012, (EL) nr 347/2012, (EL) nr 351/2012, (EL) nr 1230/2012 ja (EL) 2015/166 (ELT L 325, 16.12.2019, lk 1).

Lennunduse valdkonnas on Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139[12] põhieesmärk luua ja säilitada liidus tsiviillennundusohutuse ühtlaselt kõrge tase. Nimetatud määrusega on loodud lennundustoodete, osade ja seadmete, sealhulgas tarkvara lennukõlblikkuse oluliste nõuete raamistik, mis hõlmab kohustust kaitsta infoturvaohtude eest. Määruse (EL) 2018/1139 kohane sertifitseerimismenetlus tagab sellise usaldusväärsuse taseme, mille poole käesoleva määrusega püüeldakse. Seega ei peaks käesolevas määruses sätestatud olulised küberturvalisuse nõuded ja vastavushindamismenetlused kehtima digielemente sisaldavate toodete suhtes, mille suhtes kohaldatakse määrust (EL) 2019/2144, ja määruse (EL) 2018/1139 kohaselt sertifitseeritud toodete suhtes.

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

(28) Käesoleva määrusega nähakse ette horisontaalsed küberturvalisuse normid, mis ei piirdu konkreetsete sektorite või vaid teatavate digielemente sisaldavate toodetega. Sellegipoolest võib kehtestada sektori- või tootespetsiifilisi liidu norme, millega nähakse ette kõiki või mõningaid käesolevas määruses sätestatud oluliste küberturvalisuse nõuetega hõlmatud riske käsitlevad nõuded. Sellisel juhul võib käesoleva määruse kohaldamine digielemente sisaldavate toodete suhtes, mida reguleerivad muud liidu normid, millega nähakse ette kõiki või mõningaid käesolevas määruses sätestatud oluliste küberturvalisuse nõuetega hõlmatud riske käsitlevad nõuded, olla piiratud või välistatud, kui selline piiramine või välistamine on kooskõlas selliste toodete suhtes kehtiva üldise õigusraamistikuga ja kui valdkondlike õigusnormidega saavutatakse vähemalt samasugune kaitse tase, nagu on ette nähtud käesoleva määrusega. Komisjonil peaks olema õigus võtta käesoleva määruse täiendamiseks vastu delegeeritud õigusakte ning määrata kindlaks sellised tooted ja normid. Kehtiva liidu õiguse kohta, mille suhtes tuleks kohaldada sellist piirangut või välistust, sisaldab käesolev määrus konkreetsed sätted, et selgitada määruse suhet kõnealuse liidu õigusega.

(29) Tagamaks, et turul kättesaadavaks tehtud, digielemente sisaldavaid tooteid on võimalik tulemuslikult parandada ja nende vastupidavust pikendada, tuleks varuosade jaoks ette näha erand. Kõnealune erand peaks kehtima nii selliste varuosade suhtes, millega parandada enne käesoleva määruse kohaldamise alguskuupäeva kättesaadavaks tehtud varasemaid tooteid, kui ka varuosade suhtes, mis on käesoleva määruse kohase vastavushindamismenetluse juba läbinud.

(30) Komisjoni delegeeritud määruses (EL) 2022/30[13] on sätestatud, et teatavate raadioseadmete suhtes kohaldatakse mitmeid Euroopa Parlamendi ja nõukogu direktiivi 2014/53/EL[14] artikli 3 lõike 3 punktides d, e ja f sätestatud olulisi nõudeid, mis käsitlevad võrgu kahjustamist, võrgu ressursside kuritarvitamist, isikuandmeid ja eraelu puutumatust ning pettusi. Komisjoni 5. augusti 2022. aasta rakendusotsuses C(2022)5637 Euroopa Standardikomiteele ja Euroopa Elektrotehnika Standardikomiteele esitatud standardimistaotluse kohta on sätestatud nõuded konkreetsete standardite väljatöötamise kohta, et veelgi täpsustada, kuidas neid olulisi nõudeid tuleks käsitleda. Käesolevas määruses sätestatud olulised küberturvalisuse nõuded sisaldavad kõiki direktiivi 2014/53/EL artikli 3 lõike 3 punktides d, e ja f osutatud oluliste nõuete elemente. Lisaks on käesolevas määruses sätestatud olulised küberturvalisuse nõuded kooskõlas standardimistaotluses loetletud konkreetsete standardite nõuete eesmärkidega. Seega kui komisjon tunnistab delegeeritud määruse (EL) 2022/30 kehtetuks või muudab seda nii, et määrust ei kohaldata enam teatavate käesoleva määruse kohaldamisalasse kuuluvate toodete suhtes, peaksid komisjon ja Euroopa standardiorganisatsioonid võtma arvesse standardimistööd, mis on tehtud seoses rakendusotsusega C(2022)5637, et valmistada ette ja töötada välja käesoleva määruse rakendamist hõlbustavad harmoneeritud standardid. Käesoleva määruse kohaldamiseks ette nähtud üleminekuperioodi jooksul peaks komisjon andma suuniseid tootjatele, kelle suhtes kohaldatakse käesolevat määrust ja kelle suhtes kohaldatakse ka delegeeritud määrust (EL) 2022/30, et hõlbustada nende kahe määruse järgimise tõendamist.

---

[13] Komisjoni 29. oktoobri 2021. aasta delegeeritud määrus (EL) 2022/30, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi 2014/53/EL seoses nimetatud direktiivi artikli 3 lõike 3 punktides d, e ja f osutatud oluliste nõuete kohaldamisega (ELT L 7, 12.1.2022, lk 6).

[14] Euroopa Parlamendi ja nõukogu 16. aprilli 2014. aasta direktiiv 2014/53/EL raadioseadmete turul kättesaadavaks tegemist käsitlevate liikmesriikide õigusaktide ühtlustamise kohta ja millega tunnistatakse kehtetuks direktiiv 1999/5/EÜ (ELT L 153, 22.5.2014, lk 62).

(31) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2024/…[15+] täiendab käesolevat määrust. Selles direktiivis on sätestatud tootevastutuse normid, et kahju kannatanud isik saaks nõuda kahju hüvitamist, kui kahju on põhjustanud puudusega toode. Direktiivis on sätestatud põhimõte, et toote tootja vastutab kahju eest, mille on põhjustanud tema toote puudulik ohutus olenemata süüst („mittesüüline vastutus“). Kui selline puudulik ohutus seisneb toote turule laskmise järgsete turvauuenduste puudumises ja see põhjustab kahju, võib see kaasa tuua tootja vastutuse. Käesolevas määruses tuleks sätestada tootjate kohustused, mis on seotud selliste turvauuenduste pakkumisega.

---

15 Euroopa Parlamendi ja nõukogu … direktiiv (EL) 2024/… (ELT …, ELI: …).

+ ELT: palun sisestada teksti dokumendis (2022/0302(COD)) sisalduva direktiivi number ning esitada joonealuses märkuses kõnealuse direktiivi kuupäev, number, pealkiri ja ELT avaldamisviide.

(32) Käesolev määrus ei tohiks piirata Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679[16] kohaldamist, sealhulgas sätteid, mis on seotud selliste andmekaitse sertifitseerimismehhanismide ning andmekaitsepitserite ja -märgiste kasutuselevõtuga, mille abil saab tõendada, et vastutavate töötlejate ja volitatud töötlejate isikuandmete töötlemise toimingud vastavad kõnealusele määrusele. Digielemente sisaldavatesse toodetesse võib selliseid toiminguid integreerida. Lõimitud ja vaikimisi andmekaitse ning küberturvalisus üldiselt on määruse (EL) 2016/679 olulised elemendid. Käesolevas määruses sätestatud olulised küberturvalisuse nõuded kaitsevad tarbijaid ja organisatsioone küberriskide eest ning aitavad seega parandada isikuandmete kaitset ja üksikisikute eraelu kaitset. Komisjoni, Euroopa standardiorganisatsioonide, Euroopa Liidu Küberturvalisuse Ameti (ENISA), määrusega (EL) 2016/679 loodud Euroopa Andmekaitsenõukogu ja riiklike andmekaitse järelevalveasutuste vahelises koostöös tuleks kaaluda koostoimet nii küberturvalisuse aspektide standardimise kui ka sertifitseerimise vallas. Käesoleva määruse ja liidu andmekaitseõiguse koostoimesse tuleks panustada ka turujärelevalve ja nõuete täitmise tagamise valdkonnas. Seda eesmärki silmas pidades peaksid käesoleva määruse kohaselt määratud riiklikud turujärelevalveasutused tegema koostööd liidu andmekaitseõiguse kohaldamise üle järelevalvet tegevate asutustega. Viimastel peaks samuti olema juurdepääs oma ülesannete täitmiseks vajalikule teabele.

---

[16] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

(33) Kui Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014[17] artikli 5a lõikes 2 osutatud Euroopa digiidentiteedikukrute pakkujate tooted kuuluvad käesoleva määruse kohaldamisalasse, peaksid nad täitma nii käesolevas määruses sätestatud olulisi horisontaalseid küberturvalisuse nõudeid kui ka määruse (EL) nr 910/2014 artiklis 5a sätestatud spetsiifilisi turvanõudeid. Nõuete täitmise hõlbustamiseks peaksid digiidentiteedikukrute pakkujad saama tõendada Euroopa digiidentiteedikukru vastavust käesolevas määruses ja määruses (EL) nr 910/2014 sätestatud nõuetele sedasi, et lasevad oma tooted sertifitseerida määruse (EL) 2019/881 alusel loodud sellise Euroopa küberturvalisuse sertifitseerimise kava kohaselt, mille kohta komisjon on delegeeritud õigusaktiga näinud ette käesolevale määrusele vastavuse eelduse, kuivõrd sertifikaat või selle osad hõlmavad neid nõudeid.

[17] Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.8.2014, lk 73).

(34) Kui tootjad integreerivad projekteerimis- ja arendusetapis digielemente sisaldavatesse toodetesse kolmandatelt isikutelt hangitud komponente, peaksid nad selleks, et tagada toodete projekteerimine, arendamine ja tootmine kooskõlas käesolevas määruses sätestatud oluliste küberturvalisuse nõuetega, rakendama hoolsuskohustust nende komponentide suhtes, sealhulgas vaba ja avatud lähtekoodiga tarkvarakomponentide suhtes, mida ei ole turul kättesaadavaks tehtud. Hoolsuskohustuse asjakohane tase sõltub konkreetse komponendi laadist ja sellega seotud küberriski tasemest ning seepärast tuleks selle puhul võtta arvesse ühte või mitut järgmistest meetmetest: kui see on kohaldatav, selle kontrollimine, kas komponendi tootja on tõendanud vastavust käesolevale määrusele, sealhulgas kontrollides, kas komponendil on juba CE-vastavusmärgis; selle kontrollimine, et komponent saab korrapäraselt turvauuendusi, näiteks kontrollides selle turvauuenduste ajalugu; selle kontrollimine, et komponent ei sisalda nõrkusi, mis on registreeritud direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasis või muudes avalikult kättesaadavates nõrkuste andmebaasides, või täiendavate turvatestide tegemine. Käesolevas määruses sätestatud nõrkuste käsitlemise kohustusi, mida tootjad peavad täitma digielemente sisaldava toote turule laskmisel ja toe kestuse vältel, kohaldatakse digielemente sisaldavate toodete suhtes tervikuna, sealhulgas kõigi integreeritud komponentide suhtes. Kui digielemente sisaldava toote tootja teeb hoolsuskohustuse täitmise käigus komponendis, sealhulgas vaba ja avatud lähtekoodiga komponendis kindlaks nõrkuse, peaks ta teavitama sellest komponenti tootvat või hooldavat isikut või üksust, tegelema nõrkusega ja selle kõrvaldama, ning esitama isikule või üksusele kasutatud turvaparanduse, kui see on kohaldatav.

(35) Kohe pärast käesoleva määruse kohaldamiseks ette nähtud üleminekuperioodi ei pruugi sellise digielemente sisaldava toote tootja, millesse on integreeritud üks või mitu komponenti, mis on hangitud kolmandatelt isikutelt, kelle suhtes samuti käesolevat määrust kohaldatakse, olla võimeline oma hoolsuskohustuse raames kontrollima, et nende komponentide tootjad on tõendanud vastavust käesolevale määrusele, kontrollides näiteks seda, kas komponentidel on juba CE-vastavusmärgis. Nii võib see olla juhul, kui komponendid on integreeritud enne, kui käesolevat määrust hakatakse kohaldama nende komponentide tootjate suhtes. Sellisel juhul peaks niisuguseid komponente integreeriv tootja rakendama hoolsuskohustust muul viisil.

(36) Digielemente sisaldavatel toodetel peaks olema CE-vastavusmärgis, mis näitab nähtavalt, loetavalt ja kustutamatult nende vastavust käesolevale määrusele, et nad saaksid siseturul vabalt liikuda. Liikmesriigid ei tohiks luua põhjendamatuid tõkkeid käesolevas määruses sätestatud nõuetele vastavate ja CE-vastavusmärgisega digielemente sisaldavate toodete turule laskmisele. Lisaks ei tohiks liikmesriigid takistada käesolevale määrusele mittevastavate digielemente sisaldavate toodete, sealhulgas nende prototüüpide esitlemist ega kasutamist messidel, näitustel ja esitlustel või muudel samalaadsetel üritustel, kui toodet esitletakse nähtava sildiga, millel on selgelt märgitud, et toode ei vasta käesolevale määrusele ning seda ei tehta turul kättesaadavaks enne, kui see vastab käesoleva määruse nõuetele.

(37) Tagamaks et tootjad saavad tarkvara testimiseks välja lasta enne, kui nende digielemente sisaldavate toodete suhtes kohaldatakse vastavushindamist, ei tohiks liikmesriigid takistada lõpetamata tarkvara, näiteks alfaversioonide, beetaversioonide või kandidaatversioonide kättesaadavaks tegemist, tingimusel et lõpetamata tarkvara tehakse kättesaadavaks üksnes selle testimiseks ja tagasiside kogumiseks vajaliku aja jooksul. Tootjad peaksid tagama, et kirjeldatud tingimustel kättesaadavaks tehtud tarkvara lastakse välja üksnes pärast riskihindamist ja et see vastab võimalikult suures ulatuses digielemente sisaldavate toodete omaduste kohta käesolevas määruses sätestatud turvanõuetele. Samuti peaksid tootjad võimalikult suures ulatuses rakendama nõrkuste käsitlemise nõudeid. Tootjad ei tohiks sundida kasutajaid paigaldama üksnes testimiseks välja lastud versioone.

(38) Tagamaks et digielemente sisaldavad tooted ei põhjusta turule laskmisel inimestele ja organisatsioonidele küberriske, tuleks selliste toodete jaoks kehtestada olulised küberturvalisuse nõuded. Neid olulisi küberturvalisuse nõudeid, sealhulgas nõrkuste käsitlemise nõudeid kohaldatakse turule laskmisel iga digielemente sisaldava üksiktoote suhtes, olenemata sellest, kas digielemente sisaldav toode on toodetud eraldiseisva tooteühikuna või tooteseeriana. Näiteks ühe tootetüübi puhul peaks iga digielemente sisaldav üksiktoode olema saanud kõik kättesaadavad turvapaigad või -uuendused, et käsitleda asjakohaseid turvaprobleeme, kui toode turule lastakse. Kui hiljem muudetakse digielemente sisaldavat toodet füüsiliste või digitaalsete vahenditega, mida tootja esialgses riskihindamises ette ei näinud ja mis võib tähendada, et toode ei vasta enam asjakohastele olulistele küberturvalisuse nõuetele, tuleks seda pidada oluliseks muutmiseks. Näiteks parandused võib ühildada hooldustöödega, eeldusel et need ei muuda juba turule lastud, digielemente sisaldavat toodet viisil, mis mõjutaks vastavust kohaldatavatele nõuetele või muudaks kavandatud otstarvet, millest lähtuvalt on toodet hinnatud.

(39) Nagu füüsilise parandamise või muutmise korral, tuleks digielemente sisaldavat toodet käsitada tarkvara muutmise tagajärjel oluliselt muudetud tootena, kui tarkvarauuendusega muudetakse toote sihtotstarvet ning selliseid muudatusi ei olnud tootja esialgses riskihindamises ette näinud, või kui tarkvarauuenduse tõttu on ohu laad muutunud või küberriski tase tõusnud, ja toote ajakohastatud versioon tehakse turul kättesaadavaks. Kui turvauuendus, mille eesmärk on vähendada digielemente sisaldava toote küberriski taset, ei muuda digielemente sisaldava toote sihtotstarvet, ei käsitata seda olulise muudatusena. See hõlmab tavaliselt olukordi, kus turvauuendusega kaasneb lähtekoodi vähene kohandamine. Näiteks võib see olla nii juhul, kui turvauuendusega käsitletakse teadaolevat nõrkust, sealhulgas muutes digielemente sisaldava toote funktsioone või toimivust üksnes selleks, et küberriski taset alandada. Vähemtähtsat funktsioonide uuendust, nagu visuaalsed täiendus, uute piktogrammide või uute keelte kogumi lisamine kasutajaliidesesse, ei tohiks üldjuhul pidada olulisteks muudatusteks. Seevastu juhul, kui omaduste uuendusega muudetakse digielemente sisaldava toote algseid kavandatud funktsioone või tüüpi või toimivust ja see vastab nimetatud kriteeriumidele, tuleks seda käsitada olulise muudatusena, kuna uute omaduste lisamine toob tavaliselt kaasa laiema ründepinna, mis suurendab seetõttu küberriski. Näiteks võib see olla nii juhul, kui rakendusele lisatakse uus sisendelement, mistõttu tootja peab tagama sisendi piisava valideerimise. Selle hindamisel, kas omaduse uuendamist peetakse oluliseks muudatuseks, ei ole oluline, kas see esitatakse eraldi uuendusena või koos turvauuendusega. Komisjon peaks andma välja suunised selle kohta, kuidas määrata kindlaks, milline on oluline muudatus.

(40) Võttes arvesse tarkvaraarenduse olemuslikku korduvust, peaks tootjatel, kes on toote hilisema olulise muudatuse tõttu turule lasknud tarkvaratoote hilisemad versioonid, olema võimalik pakkuda toe kestuse jooksul turvauuendusi üksnes selle tarkvaratoote versioonile, mille nad on viimati turule lasknud. Nad peaksid saama seda teha üksnes juhul, kui asjaomaste varasemate tooteversioonide kasutajatel on tasuta juurdepääs viimasele turule lastud tooteversioonile ning nad ei kanna lisakulusid seoses selle riist- või tarkvarakeskkonna kohandamisega, milles nad toodet kasutavad. See võib olla nii näiteks juhul, kui lauaarvuti operatsioonisüsteemi uuendamiseks ei ole vaja uut riistvara, näiteks kiiremat kesktöötlusseadet või rohkem mälu. Sellegipoolest peaks tootja toe kestuse jooksul jätkuvalt täitma muid nõrkuste käsitlemise nõudeid, nagu nõrkuste avalikustamise koordineeritud poliitika või meetmed, mis hõlbustavad teabe jagamist võimalike nõrkuste kohta kõigi turule lastud tarkvaratoote hilisemate oluliselt muudetud versioonide puhul. Tootjatel peaks olema võimalik pakkuda väiksemaid turva- või funktsiooniuuendusi, mis ei ole olulised muudatused, üksnes sellise tarkvaratoote viimase versiooni või allversiooni puhul, mida ei ole oluliselt muudetud. Samas juhul kui riistvaratoode, näiteks nutitelefon, ei sobi kokku niisuguse operatsioonisüsteemi viimase versiooniga, millega see algselt tarniti, peaks tootja jätkama toe kestuse jooksul turvauuenduste pakkumist vähemalt selle operatsioonisüsteemi viimasele ühilduvale versioonile.

(41) Liidu ühtlustamisõigusaktidega reguleeritud toodete olulise muutmise laialdaselt juurdunud mõistega kooskõlas on otstarbekas kontrollida digielemente sisaldava toote vastavust ja asjakohasel juhul teha sellele uus vastavushindamine alati, kui leiab aset oluline muudatus, mis võib mõjutada digielemente sisaldava toote vastavust käesolevale määrusele, või kui selle toote sihtotstarve muutub. Kui see on asjakohane, tuleb juhul, kui tootja võtab ette vastavushindamise, millesse on kaasatud kolmas isik, teavitada seda kolmandat isikut muudatusest, mis võib kaasa tuua olulise muudatuse.

(42) Euroopa Parlamendi ja nõukogu määruse (EL) 2024/1781[18] artikli 2 punktides 18, 19 ja 20 määratletud digielemente sisaldava toote „taastamine“, „hooldus“ ja „parandamine“ ei pruugi põhjustada toote olulist muutmist, näiteks siis, kui sihtotstarvet ja funktsioone ei muudeta ja riski taset ei mõjutata. Digielemente sisaldava toote uuendamine tootja poolt võib siiski põhjustada muudatusi kõnealuse toote projektis ja arendamises ning võib seega mõjutada selle kavandatud otstarvet ja vastavust käesolevas määruses sätestatud nõuetele.

[18] Euroopa Parlamendi ja nõukogu 13. juuni 2024. aasta määrus (EL) 2024/1781, millega kehtestatakse kestlike toodete ökodisainինõuete sätestamise raamistik, muudetakse direktiivi (EL) 2020/1828 ja määrust (EL) 2023/1542 ning tunnistatakse kehtetuks direktiiv 2009/125/EÜ (ELT L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

(43) Digielemente sisaldavaid tooteid peaks käsitama olulistena, kui toote võimalike nõrkuste ärakasutamise kahjulik mõju võib olla tõsine muu hulgas küberturvalisusega seotud funktsioonide või sellise funktsiooni tõttu, millega kaasneb märkimisväärne kahjuliku mõju risk seoses selle intensiivsuse ja võimega häirida, kontrollida või kahjustada suurt hulka muid digielemente sisaldavaid tooteid või kasutajate tervist, turvalisust või ohutust otsese manipuleerimise teel, näiteks kesksüsteemi funktsiooni, sealhulgas võrguhalduse, konfiguratsiooni kontrolli, virtualiseerimise või isikuandmete töötlemise tõttu. Turvalisusprobleemide leviku tarneahelas võivad kaasa tuua eeskätt selliste digielemente sisaldavate toodete nõrkused, mille funktsioonid on seotud küberturvalisusega (näiteks buutimishaldurid). Intsidendi mõju tõsidus võib suureneda ka siis, kui toode täidab peamiselt kesksüsteemi funktsiooni, sealhulgas võrguhaldus, konfiguratsiooni kontroll, virtualiseerimine või isikuandmete töötlemine.

(44) Teatavate digielemente sisaldavate toodete kategooriate suhtes tuleks kohaldada rangemaid vastavushindamismenetlusi, jäädes oma lähenemises siiski proportsionaalseks. Sel otstarbel tuleks digielemente sisaldavad olulised tooted jagada kahte klassi, lähtudes nende tootekategooriatega seotud küberriskide tasemest. II klassi kuuluvaid, digielemente sisaldavaid olulisi tooteid hõlmava võimaliku intsidendi kahjulik mõju võib olla suurem kui I klassi kuuluvaid, digielemente sisaldavaid olulisi tooteid hõlmava intsidendi puhul näiteks johtuvalt toote küberturvalisusega seotud funktsiooni laadist või muu funktsiooni täitmise tõttu, millega kaasneb märkimisväärne kahjuliku mõju risk. Sellise suurema kahjuliku mõju märgina võivad II klassi kuuluvad digielemente sisaldavad tooted kas täita küberturvalisusega seotud funktsiooni või muud funktsiooni, millega kaasneb märkimisväärne kahjuliku mõju risk, mis on suurem kui I klassi toodete puhul, või mis vastavad mõlemale eespool nimetatud kriteeriumile. Seepärast tuleks II klassi kuuluvate digielemente sisaldavate oluliste toodete suhtes kohaldada rangemat vastavushindamismenetlust.

(45) Käesolevas määruses osutatud digielemente sisaldavaid olulisi tooteid tuleks mõista kui tooteid, millel on käesolevas määruses sätestatud digielemente sisaldavate oluliste toodete kategooria põhifunktsionaalsus. Näiteks sätestatakse käesolevas määruses digielemente sisaldavate oluliste toodete kategooriad, mis on nende põhifunktsiooni järgi määratletud II klassi tulemüüride või sissetungitõrje- ja tuvastussüsteemidena. Sellest tulenevalt kohaldatakse tulemüüride ning sissetungitõrje- ja tuvastussüsteemide suhtes kohustuslikku kolmanda isiku vastavushindamist. See ei kehti aga muude digielemente sisaldavate toodete suhtes, mis ei ole liigitatud digielemente sisaldavateks olulisteks toodeteks, millesse võivad olla integreeritud tulemüürid või sissetungitõrje- ja tuvastussüsteemid. Komisjon peaks võtma vastu rakendusakti, et täpsustada I ja II klassi kuuluvate digielemente sisaldavate oluliste toodete kategooriate tehnilist kirjeldust, nagu on sätestatud käesolevas määruses.

(46) Käesolevas määruses sätestatud, digielemente sisaldavate kriitilise tähtsusega toodete kategooriatel on küberturvalisusega seotud funktsioonid ja need täidavad funktsiooni, millega kaasneb märkimisväärne kahjuliku mõju risk seoses nende intensiivsuse ja võimega otsese manipuleerimise kaudu häirida, kontrollida või kahjustada paljusid muid digielemente sisaldavaid tooteid. Lisaks käsitatakse neid digielemente sisaldavaid toote kategooriaid direktiivi (EL) 2022/2555 artikli 3 lõikes 1 osutatud elutähtsate üksuste jaoks kriitilise tähtsusega sõltuvusena. Digielemente sisaldavate kriitilise tähtsusega toodete kategooriate puhul, mis on sätestatud käesoleva määruse lisas, kasutatakse nende tähtsuse tõttu juba laialdaselt erinevaid sertifitseerimise vorme ning need on hõlmatud ka Euroopa ühise kriteeriumidel põhineva küberturvalisuse sertifitseerimise kavaga (EUCC), mis on sätestatud komisjoni rakendusmääruses (EL) 2024/482[19]. Seepärast võib digielemente sisaldavate kriitilise tähtsusega toodete ühise ja piisava küberturvalisuse kaitse tagamiseks liidus olla piisav ja proportsionaalne kohaldada selliste tootekategooriate suhtes kohustuslikku Euroopa küberturvalisuse sertifitseerimist delegeeritud õigusaktiga, kui neid tooteid hõlmav asjakohane Euroopa küberturvalisuse sertifitseerimise kava on juba loodud ja komisjon on hinnanud kavandatava kohustusliku sertifitseerimise võimalikku mõju turule. Hindamisel tuleks kaaluda nii pakkumise kui ka nõudluse poolt, sealhulgas seda, kas asjaomaste digielemente sisaldavate toodete järele on piisav nõudlus nii liikmesriikide kui ka kasutajate poolt, et nõuda Euroopa küberturvalisuse sertifitseerimist, samuti seda, millisel otstarbel digielemente sisaldavaid tooteid kavatsetakse kasutada, sealhulgas direktiivi (EL) 2022/2555 artikli 3 lõikes 1 osutatud elutähtsate üksuste kriitilise tähtsusega sõltuvust nendest. Hindamise käigus tuleks analüüsida ka kohustusliku sertifitseerimise võimalikku mõju nende toodete kättesaadavusele siseturul ning liikmesriikide suutlikkust ja valmisolekut asjakohaste Euroopa küberturvalisuse sertifitseerimise kavade rakendamiseks.

---

[19] Komisjoni 31. jaanuari 2024. aasta rakendusmäärus (EL) 2024/482, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega (ELT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(47) Delegeeritud õigusaktides, millega nõutakse Euroopa küberturvalisuse kohustuslikku sertifitseerimist, tuleks kindlaks määrata need digielemente sisaldavad tooted, millel on käesolevas määruses sätestatud digielemente sisaldavate kriitilise tähtsusega toodete kategooria põhifunktsioonid ja mille suhtes kohaldatakse kohustuslikku sertifitseerimist, ning nõutav usaldusväärsuse tase, mis peaks olema vähemalt „märkimisväärne“. Nõutav usaldusväärsuse tase peaks olema proportsionaalne digielemente sisaldava tootega seotud küberriski tasemega. Näiteks kui digielemente sisaldaval tootel on käesolevas määruses sätestatud digielemente sisaldava kriitilise tähtsusega toodete kategooria põhifunktsioonid ja see on ette nähtud kasutamiseks tundlikus või kriitilises keskkonnas, nagu direktiivi (EL) 2022/2555 artikli 3 lõikes 1 osutatud elutähtsate üksuste poolt kasutamiseks mõeldud toodete puhul, võib see vajada kõrgeimat usaldusväärsuse taset.

(48) Selleks et tagada liidus niisuguste digielemente sisaldavate toodete ühine ja piisav küberturvalisuse kaitse, millel on käesolevas määruses sätestatud, digielemente sisaldava kriitilise tähtsusega toodete kategooria põhifunktsioonid, tuleks komisjonile anda samuti õigus võtta vastu delegeeritud õigusakte käesoleva määruse muutmiseks, et lisada või kõrvaldada selliste digielemente sisaldavate kriitilise tähtsusega toodete kategooriaid, mille puhul võib tootjatelt nõuda Euroopa küberturvalisuse sertifikaadi omandamist määruse (EL) 2019/881 kohase Euroopa küberturvalisuse sertifitseerimise kava alusel, et tõendada vastavust käesolevale määrusele. Nendele kategooriatele võib lisada digielemente sisaldavate kriitilise tähtsusega toodete uue kategooria, kui direktiivi (EL) 2022/2555 artikli 3 lõikes 1 osutatud elutähtsatel üksustel on neist kriitilise tähtsusega sõltuvus, või kui see võiks intsidentide mõjutamise korral või ärakasutatavate nõrkuste sisaldamise korral põhjustada häireid kriitilise tähtsusega tarneahelates. Digielemente sisaldavate kriitilise tähtsusega toodete kategooriate delegeeritud õigusaktiga lisamise või kõrvaldamise vajaduse hindamisel peaks komisjonil olema võimalik võtta arvesse, kas liikmesriigid on riigi tasandil kindlaks määranud sellised digielemente sisaldavad tooted, millel on direktiivi (EL) 2022/2555 artikli 3 lõikes 1 osutatud elutähtsate üksuste kerksuse seisukohast kriitilise tähtsusega roll ja mis puutuvad üha rohkem kokku tarneahela küberrünnetega, millel võib olla tõsine häiriv mõju. Lisaks peaks komisjonil olema võimalik võtta arvesse direktiivi (EL) 2022/2555 artikli 22 kohaselt tehtud liidu tasandi kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamisi.

(49) Komisjon peaks tagama, et käesoleva määruse rakendamiseks meetmete ettevalmistamisel konsulteeritakse struktureeritult ja korrapäraselt paljude asjaomaste sidusrühmadega. Eelkõige tuleks seda teha juhul, kui komisjon hindab vajadust digielemente sisaldavate oluliste või kriitilise tähtsusega toodete kategooriate loetelude võimaliku ajakohastamise järele, mille puhul tuleks konsulteerida asjaomaste tootjatega ja võtta arvesse nende seisukohti, et analüüsida küberriske ning selliste tootekategooriate olulisteks või kriitilise tähtsusega liigitamise kulude ja tulude tasakaalu.

(50) Käesolevas määruses käsitletakse küberriske sihipäraselt. Digielemente sisaldavad tooted võivad siiski põhjustada muid ohutusriske, mis ei ole alati seotud küberturvalisusega, vaid võivad tuleneda turvarikkumisest. Selliste riskide suhtes tuleks ka edaspidi kohaldada muid asjakohaseid liidu ühtlustamisõigusakte kui käesolev määrus. Kui muid liidu ühtlustamisõigusakte peale käesoleva määruse ei kohaldata, tuleks nende riskide suhtes kohaldada Euroopa Parlamendi ja nõukogu määrust (EL) 2023/988[20]. Käesoleva määruse sihipärasust arvestades tuleks seega käesoleva määrusega hõlmamata ohutusriskide osas erandina määruse (EL) 2023/988 artikli 2 lõike 1 kolmanda lõigu punktist b kohaldada digielemente sisaldavate toodete suhtes määruse (EL) 2023/988 III peatüki 1. jaotist, V ja VII peatükki ja peatükke IX–XI, kui nende toodete suhtes ei kohaldata muude liidu ühtlustamisõigusaktidega kui käesoleva määrusega kehtestatud erinõudeid määruse (EL) 2023/988 artikli 3 punkti 27 tähenduses.

---

[20] Euroopa Parlamendi ja nõukogu 10. mai 2023. aasta määrus (EL) 2023/988, milles käsitletakse üldist tooteohutust ja millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 1025/2012 ja Euroopa Parlamendi ja nõukogu direktiivi (EL) 2020/1828 ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2001/95/EÜ ja nõukogu direktiiv 87/357/EMÜ (ELT L 135, 23.5.2023, lk 1).

(51) Digielemente sisaldavad tooted, mis on vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2024/1689[21] artiklile 6 liigitatud suure riskiga tehisintellektisüsteemiks ja mis kuuluvad käesoleva määruse kohaldamisalasse, peaksid vastama käesolevas määruses sätestatud olulistele küberturvalisuse nõuetele. Kui sellised suure riskiga tehisintellektisüsteemid vastavad käesolevas määruses sätestatud olulistele küberturvalisuse nõuetele, tuleks need lugeda määruse (EL) 2024/1869 artiklis 15 sätestatud küberturvalisuse nõuetele vastavaks, kuivõrd käesoleva määruse alusel välja antud ELi vastavusdeklaratsioon või selle osad hõlmavad neid nõudeid. Selleks tuleks selliste küberriskide hindamisel, mis on seotud digielemente sisaldava tootega, mis on määruse (EL) 2024/1869 kohaselt liigitatud suure riskiga tehisintellektisüsteemiks, mida tuleb võtta arvesse sellise toote kavandamis-, projekteerimis-, arendamis-, tootmis-, tarne- ja hooldusetapis, nagu on nõutud käesoleva määrusega, võtta arvesse tehisintellektisüsteemi küberkerksust ohustavaid riske seoses volitamata kolmandate isikute katsetega muuta selle kasutamist, käitumist või toimivust, sealhulgas tehisintellektile omaseid nõrkusi, nagu andmemürgitus või vasturünded, ning asjakohasel juhul riske põhiõigustele kooskõlas määrusega (EL) 2024/1869. Mis puudutab käesoleva määruse kohaldamisalasse kuuluva ja suure riskiga tehisintellektisüsteemiks liigitatud, digielemente sisaldava toote oluliste küberturvalisuse nõuetega seotud vastavushindamismenetlusi, siis tuleks käesoleva määruse asjaomaste sätete asemel reeglina kohaldada määruse (EL) 2024/1869 artiklit 43.

---

[21] Euroopa Parlamendi ja nõukogu 13. juuni 2024. aasta määrus (EL) 2024/1689, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ja muudetakse määrusi (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ja direktiivid 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellektimäärus) (ELT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Sellise reegli tagajärjel ei tohiks siiski väheneda käesolevas määruses osutatud digielemente sisaldavate oluliste või kriitilise tähtsusega toodete usaldusväärsuse vajalik tase. Seepärast tuleks erandina sellest reeglist kohaldada suure riskiga tehisintellektisüsteemide suhtes, mis kuuluvad määruse (EL) 2024/1869 kohaldamisalasse ning mis on ühtlasi käesolevas määruses osutatud digielemente sisaldavad olulised või kriitilise tähtsusega tooted ning mille suhtes kohaldatakse määruse (EL) 2024/1689 VI lisas osutatud sisekontrollil põhinevat vastavushindamismenetlust, käesoleva määrusega ette nähtud vastavushindamismenetlust selles osas, mis puudutab käesolevas määruses sätestatud olulisi nõudeid. Sellisel juhul tuleks kõigis muudes määrusega (EL) 2024/1689 hõlmatud aspektides kohaldada asjaomaseid sätteid, mis käsitlevad kõnealuse määruse VI lisas sätestatud sisekontrollil põhinevat vastavushindamismenetlust.

(52) Siseturule lastavate digielemente sisaldavate toodete turvalisuse parandamiseks on vaja kehtestada olulised küberturvalisuse nõuded, mida selliste toodete suhtes kohaldatakse. Need olulised küberturvalisuse nõuded ei tohiks piirata direktiivi (EL) 2022/2555 artikliga 22 ettenähtud liidu tasandi kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamiste kohaldamist, milles võetakse arvesse nii tehnilisi kui ka vajaduse korral mittetehnilisi riskitegureid, näiteks tarnijate lubamatut mõjutamist kolmanda riigi poolt. Samuti ei tohiks need piirata liikmesriikide õigust sätestada täiendavaid nõudeid, milles võetakse kerksuse kõrge taseme tagamiseks arvesse mittetehnilisi tegureid, kaasa arvatud neid, mis on määratletud komisjoni soovituses (EL) 2019/534[22], ELi 5G-võrkude küberturvalisuse koordineeritud riskihindamise aruandes ja direktiivi (EL) 2022/2555 artikli 14 kohaselt loodud koostöörühma kokkulepitud 5G-küberturvalisuse ELi meetmepaketis.

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

(53) Selliste Euroopa Parlamendi ja nõukogu määruse (EL) 2023/1230[23] kohaldamisalasse kuuluvate toodete tootjad, mis on ühtlasi digielemente sisaldavad tooted käesoleva määruse tähenduses, peaksid vastama nii käesolevas määruses sätestatud olulistele nõuetele kui ka määruses (EL) 2023/1230 sätestatud olulistele tervisekaitse- ja ohutusnõuetele. Käesolevas määruses sätestatud olulised küberturvalisuse nõuded ja määruses (EL) 2023/1230 sätestatud teatavad küberturvalisuse olulised nõuded võivad käsitleda sarnaseid küberriske. Seepärast võib käesolevas määruses sätestatud oluliste nõuete täitmine hõlbustada vastavust olulistele küberturvalisuse nõuetele, mis hõlmavad ka teatavaid küberriske, nagu on sätestatud määruses (EL) 2023/1230, eelkõige sellistele nõuetele, mis on seotud rikkumise eest kaitsmisega ning juhtsüsteemide ohutuse ja töökindlusega, nagu on sätestatud kõnealuse määruse III lisa punktides 1.1.9 ja 1.2.1. Tootja peab sellist koostoimet tõendama, näiteks kohaldades harmoneeritud standardeid, kui need on kättesaadavad, või muid tehnilisi spetsifikatsioone, mis hõlmavad asjaomaseid olulisi nõudeid pärast kõnealuseid küberriske hõlmavat riskihindamist. Tootja peaks samuti järgima käesolevas määruses ja määruses (EL) 2023/1230 sätestatud kohaldatavaid vastavushindamismenetlusi. Komisjon ja Euroopa standardiorganisatsioonid peaksid ettevalmistustöös, mis toetab käesoleva määruse ja määruse (EL) 2023/1230 rakendamist ja sellega seotud standardimisprotsesse edendama järjepidevust selles osas, kuidas küberriske tuleb hinnata ja kuidas need riskid peavad olema hõlmatud harmoneeritud standarditega, pidades silmas asjakohaseid olulisi küberturvalisuse nõudeid.

---

[23] Euroopa Parlamendi ja nõukogu 14. juuni 2023. aasta määrus (EL) 2023/1230, mis käsitleb masinaid ning millega tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2006/42/EÜ ja nõukogu direktiiv 73/361/EMÜ (ELT L 165, 29.6.2023, lk 1).

Eelkõige peaksid komisjon ja Euroopa standardiorganisatsioonid võtma käesolevat määrust arvesse harmoneeritud standardite ettevalmistamisel ja väljatöötamisel, et hõlbustada määruse (EL) 2023/1230 rakendamist, eelkõige seoses kõnealuse määruse III lisa punktides 1.1.9 ja 1.2.1 sätestatud küberturvalisuse aspektidega, mis on seotud rikkumise eest kaitsmisega ning juhtsüsteemide ohutuse ja töökindlusega. Komisjon peaks andma suuniseid, et toetada käesoleva määruse kohaldamisalasse kuuluvaid tootjaid, kelle suhtes kohaldatakse ka määrust (EL) 2023/1230, eelkõige selleks, et hõlbustada käesolevas määruses ja määruses (EL) 2023/1230 sätestatud asjakohastele olulistele nõuetele vastavuse tõendamist.

(54) Tagamaks et digielemente sisaldavad tooted on turvalised nii turule laskmise ajal kui ka aja jooksul, mil digielemente sisaldavat toodet eeldatavasti kasutatakse, tuleb kehtestada nõrkuste käsitlemise olulised küberturvalisuse nõuded ja olulised küberturvalisuse nõuded, mis puudutavad digielemente sisaldavate toodete omadusi. Tootjad peaksid täitma kõiki nõrkuste käsitlemisega seotud olulisi nõudeid toote toe kestuse jooksul, ning samas peaksid nad kindlaks tegema, millised muud toote omadustega seotud olulised küberturvalisuse nõuded on asjaomase digielemente sisaldava toote tüübi puhul asjakohased. Sel otstarbel peaksid tootjad korraldama digielemente sisaldava tootega seotud küberriskide hindamise, et teha kindlaks asjaomased riskid ja asjaomased olulised küberturvalisuse nõuded, et teha oma digielemente sisaldavad tooted kättesaadavaks ilma teadaolevate ärakasutatavate nõrkusteta, mis võivad mõjutada nende toodete turvalisust, ning kohaldada sobivaid harmoneeritud standardeid, ühtseid spetsifikatsioone ning Euroopa või rahvusvahelisi standardeid nõuetekohaselt.

(55) Kui digielemente sisaldava toote suhtes ei kohaldata teatavaid olulisi küberturvalisuse nõudeid, peaks tootja lisama tehnilises dokumentatsioonis sisalduvasse küberriskide hindamisse selge põhjenduse. Nii võib toimida juhul, kui mõni oluline küberturvalisuse nõue ei ole kooskõlas digielemente sisaldava toote olemusega. Näiteks võib digielemente sisaldava toote sihtotstarbeks vaja olla, et tootja järgiks üldtunnustatud koostalitlusvõime standardeid, isegi kui selle turvaomadusi ei peeta enam tehnika tasemele vastavaks. Samamoodi nõutakse muu liidu õigusega tootjatelt spetsiaalsete koostalitlusnõuete kohaldamist. Kui digielemente sisaldava toote suhtes mõnda olulist küberturvalisuse nõuet ei kohaldata, kuid tootja on seoses selle olulise küberturvalisuse nõudega tuvastanud küberriskid, peaks ta võtma meetmeid nende riskide käsitlemiseks muul viisil, näiteks piirates toote sihtotstarvet usaldusväärse keskkonnaga või teavitades kasutajaid nendest riskidest.

(56) Üks olulisemaid meetmeid, mida kasutajad saavad võtta oma digielemente sisaldavate toodete kaitsmiseks küberrünnete eest, on paigaldada võimalikult kiiresti uusimad kättesaadavad turvauuendused. Seepärast peaksid tootjad projekteerima oma tooteid ja kehtestama protsesse nii, et tagatakse, et digielemente sisaldavad tooted sisaldavad funktsioone, mis võimaldavad turvauuendustest automaatselt teatada, neid levitada, alla laadida ja paigaldada, eelkõige tarbekaupade puhul. Samuti peaksid nad andma võimaluse kiita viimase sammuna heaks turvauuenduste allalaadimine ja paigaldamine. Kasutajatel peaks säilima võimalus automaatsed uuendused desaktiveerida, kasutades selget ja kergesti kasutatavat mehhanismi, mida toetavad selged juhised selle kohta, kuidas kasutajad saavad neist loobuda. Käesoleva määruse lisas sätestatud automaatsete uuendustega seotud nõudeid ei kohaldata selliste digielemente sisaldavate toodete suhtes, mis on peamiselt ette nähtud komponentidena muudesse toodetesse integreerimiseks. Neid ei kohaldata ka niisuguste digielemente sisaldavate toodete suhtes, mille puhul kasutajad ei eeldaks mõistlikkuse piires automaatseid uuendusi, sealhulgas digielemente sisaldavate toodete suhtes, mis on ette nähtud kasutamiseks professionaalsetes IKT-võrkudes, ning eelkõige kriitilise tähtsusega ja tööstuskeskkondades, kus automaatne uuendus võib häirida toimimist. Olenemata sellest, kas digielemente sisaldav toode on projekteeritud saama automaatseid uuendusi või mitte, peaks tootja teavitama kasutajaid nõrkustest ja tegema turvauuendused viivitamata kättesaadavaks. Kui digielemente sisaldaval tootel on kasutajaliides või sarnane tehniline vahend, mis võimaldab otsest suhtlust kasutajatega, peaks tootja neid omadusi kasutama, et teavitada kasutajaid sellest, et nende digielemente sisaldava toote toe kestus on lõppenud. Teavitused peaksid piirduma sellega, mis on vajalik, et tagada selle teabe tulemuslik vastuvõtmine, ega tohiks avaldada kahjulikku mõju digielemente sisaldava toote kasutajakogemusele.

(57) Selleks et parandada nõrkuste käsitlemise protsesside läbipaistvust ja tagada, et kasutajatelt ei nõuta uute funktsioonidega seotud uuenduste paigaldamist üksnes viimaste turvauuenduste saamise eesmärgil, peaksid tootjad tagama, et uusi turvauuendusi pakutakse funktsiooniuuendustest eraldi, kui see on tehniliselt teostatav.

(58) Komisjoni ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja 20. juuni 2023. aasta ühisteatises „Euroopa majandusjulgeoleku strateegia“ märgiti, et liit peab liidu majandusjulgeoleku ühise strateegilise raamistiku kaudu maksimeerima oma majanduslikust avatusest saadavat kasu ja samas minimeerima riske, mis tulenevad majanduslikust sõltuvusest suure riskiga tarnijatest. Sõltuvus digielemente sisaldavate toodete suure riskiga tarnijatest võib kujutada endast strateegilist riski, millega tuleb tegeleda liidu tasandil, eriti juhul, kui digielemente sisaldavad tooted on ette nähtud kasutamiseks direktiivi (EL) 2022/2555 artikli 3 lõikes 1 osutatud elutähtsate üksuste poolt. Sellised riskid võivad olla seotud, kuid mitte piirduda tootja suhtes kohaldatava jurisdiktsiooniga, tema äriomandi tunnustega ja kontrolli seotusega selle kolmanda riigi valitsusega, kus ta on asutatud, eelkõige juhul, kui kolmas riik tegeleb majandusspionaažiga või käitub küberruumis vastutustundetult ning kui tema õigusaktid võimaldavad lubada meelevaldset juurdepääsu mis tahes ettevõtte tegevusele või andmetele, sealhulgas tundlikele äriandmetele, ning nendega võidakse kehtestada luurega seotud kohustusi ilma demokraatliku kontrolli ja tasakaalu, järelevalvemehhanismide, nõuetekohase menetluse või sõltumatute kohtuasutuste poole pöördumise õiguseta. Küberriski olulisuse kindlaksmääramisel käesoleva määruse tähenduses peaksid komisjon ja turujärelevalveasutused vastavalt oma käesolevas määruses sätestatud kohustustele võtma arvesse ka mittetehnilisi riskitegureid, eelkõige neid, mis on tehtud kindlaks direktiivi (EL) 2022/2555 artikli 22 kohaselt tehtud liidu tasandi kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamise tulemusel.

(59) Selleks et tagada digielemente sisaldavate toodete turvalisus pärast nende turule laskmist, peaksid tootjad määrama kindlaks toe kestuse, mis kajastaks digielemente sisaldava toote eeldatavat kasutusaega. Toe kestuse kindlaksmääramisel peaks tootja võtma eelkõige arvesse kasutajate mõistlikke ootusi, toote olemust ja asjakohast liidu õigust, millega määratakse kindlaks digielemente sisaldavate toodete kasutusiga. Tootjatel peaks olema võimalik arvesse võtta ka muid asjakohaseid tegureid. Kriteeriume tuleks kohaldada nii, et toe kestuse kindlaksmääramisel oleks tagatud proportsionaalsus. Taotluse korral tuleks tootjal esitada turujärelevalveasutustele teave, mida digielemente sisaldava toote toe kestuse kindlaksmääramisel arvesse võeti.

(60) Toe kestus, mille jooksul tootja tagab nõrkuste tõhusa käsitlemise, ei tohiks olla lühem kui viis aastat, välja arvatud juhul, kui digielemente sisaldava toote kasutusiga on lühem kui viis aastat, millisel juhul peaks tootja tagama nõrkuste käsitlemise kogu kasutusea jooksul. Kui digielemente sisaldava toote mõistlikult eeldatav kasutusaeg on pikem kui viis aastat, nagu see on sageli riistvarakomponentide, nagu emaplaadid või mikroprotsessorid, võrguseadmete, nagu ruuterid, modemid või kommutaatorid, ning tarkvara puhul, nagu operatsioonisüsteemid või videomontaaži vahendid, peaksid tootjad tagama toe pikema kestuse. Sageli kasutatakse just digielemente sisaldavaid tooteid, mis on ette nähtud kasutamiseks tööstuskeskkonnas, näiteks tööstuslikke juhtsüsteeme, märkimisväärselt pikema aja jooksul. Tootjal peaks olema võimalik kehtestada alla viie aasta pikkune toe kestus üksnes juhul, kui see on põhjendatud asjaomase digielemente sisaldava toote olemusega ja kui seda toodet kasutatakse eeldatavasti vähem kui viis aastat, ning sellisel juhul peaks toe kestus vastama eeldatavale kasutusajale. Näiteks võib pandeemia ajal kasutamiseks mõeldud kontaktide jälgimise rakenduse kasutusiga piirduda pandeemia kestusega. Lisaks on tarkvararakendusi, mida on nende olemusest tulenevalt võimalik teha kättesaadavaks üksnes tellimismudeli alusel, eelkõige juhul, kui rakendus muutub pärast tellimuse lõppemist kasutajale kättesaamatuks ning ei ole seetõttu enam kasutusel.

(61) Selleks, et nõrkusi oleks võimalik käsitleda ka pärast toe kestuse lõppu, peaksid tootjad digielemente sisaldavate toodete toe kestuse lõppemisel kaaluma selliste digielemente sisaldavate toodete lähtekoodi kättesaadavaks tegemist kas teistele ettevõtjatele, kes kohustuvad jätkama nõrkuste käsitlemise teenuste osutamist, või üldsusele. Juhul kui tootjad avaldavad lähtekoodi teistele ettevõtjatele, peaks neil olema võimalik kaitsta digielemente sisaldava toote omandiõigust ja takistada lähtekoodi levitamist üldsusele, näiteks lepingupõhiste kokkulepete kaudu.

(62) Tagamaks, et tootjad kogu liidus määravad võrreldavate digielemente sisaldavate toodete jaoks sarnase toe kestuse, peaks ADCO avaldama statistikat tootjate poolt digielemente sisaldavate toodete kategooriate jaoks kindlaks määratud keskmise toe kestuse kohta ja andma välja suunised, milles on märgitud asjakohased toe kestused selliste kategooriate jaoks. Selleks et tagada ühtlustatud lähenemisviis kogu siseturul, peaks komisjonil olema võimalik võtta vastu delegeeritud õigusakte, et määrata kindlaks konkreetsete tootekategooriate minimaalse toe kestus, kui turujärelevalveasutuste esitatud andmed viitavad sellele, et tootjate määratud toe kestus ei vasta süstemaatiliselt käesolevas määruses sätestatud toe kestuse määramise kriteeriumidele või et eri liikmesriikide tootjad määravad neile põhjendamatult erinevaid toe kestusi.

(63) Tootjad peaksid looma ühtse kontaktpunkti, mis võimaldab kasutajatel nendega hõlpsalt suhelda, sealhulgas digielemente sisaldava toote nõrkustest teatamiseks ja nende kohta teabe saamiseks. Tootjad peaksid muutma selle ühtse kontaktpunkti kasutajatele kergesti juurdepääsetavaks, osutama selgelt selle kättesaadavusele ning hoidma seda teavet ajakohastatuna. Kui tootjad otsustavad pakkuda automatiseeritud vahendeid, nt vestlusaknaid, peaksid nad pakkuma ka telefoninumbrit või mõnda muud digitaalset kontaktvahendit, näiteks e-posti aadressi või kontaktvormi. Ühtne kontaktpunkt ei tohiks tugineda üksnes automatiseeritud vahenditele.

(64) Tootjad peaksid tegema oma digielemente sisaldavad tooted turul kättesaadavaks vaikimisi turvalise konfiguratsiooniga ja pakkuma kasutajatele turvauuendusi tasuta. Tootjatel peaks olema võimalik nendest olulistest küberturvalisuse nõuetest kõrvale kalduda üksnes seoses konkreetsele ärikasutajale kohandatud spetsiaalselt valmistatud toodetega, mille puhul nii tootja kui ka kasutaja on sõnaselgelt nõustunud teistsuguste lepingutingimustega.

(65) Tootjad peaksid samal ajal ühtse teatamisplatvormi kaudu teavitama nii koordinaatoriks määratud küberintsidentidele reageerimise üksust (CSIRT) kui ka ENISAt digielemente sisaldavates toodetes sisalduvatest aktiivselt ärakasutatavatest nõrkustest ning tõsistest intsidentidest, mis mõjutavad nende toodete turvalisust. Teated tuleks esitada koordinaatoriks määratud CSIRTi teavitusahela lõpp-punkti kaudu ja need peaksid olema samaaegselt ka ENISA-le kättesaadavad.

(66) Tootjad peaksid teavitama aktiivselt ärakasutatavatest nõrkustest, tagamaks et koordinaatoriteks määratud CSIRTidel ja ENISA-l on piisav ülevaade sellistest nõrkustest ja neile antakse teave, mida need vajavad oma direktiivis (EL) 2022/2555 sätestatud ülesannete täitmiseks ning kõnealuse direktiivi artiklis 3 osutatud elutähtsate ja oluliste üksuste küberturvalisuse üldise taseme tõstmiseks, ning tagamaks et turujärelevalveasutused tegutsevad tulemuslikult. Digielemente sisaldavaid tooteid turustatakse enamasti kõikjal siseturul ja seega tuleks digielemente sisaldava toote iga ärakasutatavat nõrkust käsitada ohuna siseturu toimimisele. ENISA peaks kokkuleppel tootjaga avalikustama parandatud nõrkused direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasis. Euroopa nõrkuste andmebaas aitab tootjatel tuvastada teadaolevaid ärakasutuslikke nõrkusi oma toodetes, tagamaks et turule pääsevad ainult turvalised tooted.

(67) Tootjad peaksid koordinaatoriks määratud CSIRTi ja ENISA-t teavitama ka kõigist tõsistest intsidentidest, mis mõjutavad digielemente sisaldava toote turvalisust. Tagamaks, et kasutajad saavad nende digielemente sisaldavaid tooteid mõjutavatele tõsistele intsidentidele kiiresti reageerida, peaksid tootjad teavitama sellistest intsidentidest ka oma kasutajaid ning, kui see on asjakohane, teavitama neid ka parandusmeetmetest, mida kasutajad saavad võtta intsidendi mõju leevendamiseks; näiteks võivad tootjad avaldada asjakohase teabe oma veebisaidil või, kui neil on võimalik oma kasutajatega ühendust võtta ja kui see on küberriskide seisukohast põhjendatud, pöörduda otse kasutajate poole.

(68) Aktiivselt ärakasutatavad nõrkused puudutavad selliseid juhte, mille puhul tootja teeb kindlaks, et tema kasutajaid või muid füüsilisi või juriidilisi isikuid mõjutav turvarikkumine on tingitud sellest, et kuritahtlik isik on ära kasutanud viga mõnes digielemente sisaldavas tootes, mille tootja on turul kättesaadavaks teinud. Sellised nõrkused võivad endast kujutada näiteks puudusi toote identifitseerimis- ja autentimisfunktsioonides. Kohustuslikku teavitamist ei peaks kohaldama nõrkuste puhul, mis tuvastatakse ilma kuritahtliku kavatsuseta heauskse testimise, uurimise, parandamise või avalikustamise eesmärgil, et edendada süsteemi omaniku ja selle kasutajate turvalisust või ohutust. Digielemente sisaldava toote turvalisust mõjutavad tõsised intsidendid on aga olukorrad, kus küberintsident mõjutab tootja arendus-, tootmis- või hooldusprotsesse nii, et see võib suurendada küberriski kasutajate või muude isikute jaoks. Selline tõsine intsident võib hõlmata olukorda, kus ründaja on edukalt sisestanud ründekoodi väljastuskanalisse, mille kaudu tootja saadab kasutajatele turvauuendusi.

(69) Tagamaks, et teateid saab kiiresti levitada kõigile asjaomastele CSIRTidele, kes on määratud koordinaatoriteks, ja võimaldamaks tootjatel esitada üks teade igas teavitusprotsessi etapis, peaks ENISA looma ühtse teatamisplatvormi koos teavitusahela riigisiseste lõpp-punktidega. Ühtse teatamisplatvormi igapäevast tegevust peaks haldama ja töökorras hoidma ENISA. Koordinaatoriteks määratud CSIRTid peaksid teavitama oma turujärelevalveasutusi teatatud nõrkustest või intsidentidest. Ühtne teatamisplatvorm tuleks kavandada nii, et see tagaks teavituste konfidentsiaalsuse, eelkõige seoses selliste nõrkustega, mille turvauuendus ei ole veel kättesaadav. Lisaks peaks ENISA kehtestama menetlused teabe turvaliseks ja konfidentsiaalseks käsitlemiseks. ENISA peaks kogutud teabe põhjal koostama iga kahe aasta järel tehnilise aruande küberriskide värskete suundumuste kohta digielemente sisaldavates toodetes ning esitama selle direktiivi (EL) 2022/2555 artikli 14 alusel loodud koostöörühmale.

(70) Erandlikel asjaoludel ja eelkõige tootja taotlusel peaks algse teavituse saanud CSIRTil olema võimalik teha otsus selle edastamine teistele asjaomastele koordinaatoriteks määratud CSIRTidele ühtse aruandlusplatvormi kaudu edasi lükata, kui seda saab põhjendada küberturvalisusega seotud põhjustega ja üksnes rangelt vajalikuks ajavahemikuks. Koordinaatoriks määratud CSIRT peaks viivitamata teavitama ENISAt oma edasilükkamisotsusest, selle põhjustest ning sellest, millal ta kavatseb teavituse edastada. Komisjon peaks delegeeritud õigusaktiga välja töötama nende tingimuste kirjeldused, millal tohiks kohaldada küberturvalisusega seotud põhjuseid, ning tegema selle delegeeritud õigusakti eelnõu ettevalmistamisel koostööd direktiivi (EL) 2022/2555 artikli 15 kohaselt loodud CSIRTide võrgustikuga ja ENISAga. Küberturvalisusega seotud põhjused hõlmavad näiteks käimasolevat nõrkuste koordineeritud avalikustamise menetlust või olukordi, kus lähemal ajal on oodata tootja pakutavat leevendusmeedet ja andmete kohese edastamisega ühtse teatamisplatvormi kaudu kaasnevad küberriskid kaaluvad üles sellest saadava kasu. ENISA-l peaks koordinaatoriks määratud CSIRTi taotluse korral olema võimalik toetada seda CSIRTi küberturvalisusega seotud põhjuste kohaldamisel teavituse edastamise edasilükkamise osas selle teabe põhjal, mille ENISA on saanud kõnealuselt CSIRTilt otsuse kohta jätta teade nendel küberturvalisusega seotud põhjustel edastamata. Ka ei peaks ENISA eriti erandlikel asjaoludel samaaegselt saama aktiivselt ärakasutatava nõrkuse teavituse kõiki üksikasju.

Nii oleks see juhul, kui tootja märgib oma teates, et kuritahtlik isik on teatatud nõrkust aktiivselt ära kasutanud ja et kättesaadava teabe kohaselt ei ole see toimunud üheski teises liikmesriigis peale selle, kus koordinaatoriks on määratud CSIRT, keda tootja nõrkusest teavitas, juhul kui teatatud nõrkuse kohene edastamine tooks tõenäoliselt kaasa teabe esitamise, mille avalikustamine oleks vastuolus nimetatud liikmesriigi oluliste huvidega, või kui teatatud nõrkus kujutab endast vahetut ja suurt küberriski, mis tuleneb selle teabe edastamisest. Sellistel juhtudel saab ENISA samaaegselt juurdepääsu üksnes teabele selle kohta, et tootja on esitanud teavituse, üldteabele asjaomase digielemente sisaldava toote kohta, teabele ärakasutamise üldise laadi kohta ja teabele selle kohta, et tootja on tõstatanud nimetatud turvakaalutlused ja et teavituse täieliku sisu edastamine on seetõttu peatatud. Seejärel tuleks täielik teavitus teha ENISA-le ja teistele koordinaatoriteks määratud asjaomastele CSIRTidele kättesaadavaks siis, kui algse teavituse saanud koordinaatoriks määratud CSIRT leiab, et käesolevas määruses sätestatud eriti erandlikest asjaoludest tulenevaid turvalisuse kaalutlusi enam ei eksisteeri. Kui ENISA leiab kättesaadava teabe põhjal, et esineb süsteemne risk, mis mõjutab siseturu turvalisust, peaks ENISA soovitama teavituse saanud CSIRTil edastada teavitus täies mahus teistele koordinaatoriteks määratud CSIRTidele ja ENISA-le endale.

(71) Kui tootjad teavitavad aktiivselt ärakasutatavast nõrkusest või tõsisest intsidendist, mis mõjutab digielemente sisaldava toote turvalisust, peaksid nad märkima, kui tundlikuks nad esitatud teavet peavad. Algse teavituse saanud koordinaatoriks määratud CSIRT peaks seda teavet arvesse võtma, kui ta hindab, kas teavitusest tuleneb erandlikke asjaolusid, mis õigustavad küberturvalisusega seotud põhjendatud alustel viivitusi selle edastamisel teistele asjaomastele koordinaatoriteks määratud CSIRTidele. Samuti peaks ta seda teavet arvesse võtma, kui ta hindab, kas aktiivselt ärakasutatavast nõrkusest teatamine võib põhjustada eriti erandlikke asjaolusid, mis õigustaks seda, et teadet ei tehta täies ulatuses samaaegselt kättesaadavaks ENISA-le. Ühtlasi peaks koordinaatoriteks määratud CSIRTidel olema võimalik võtta seda teavet arvesse, kui nad määravad kindlaks asjakohaseid meetmeid sellistest nõrkustest ja intsidentidest tulenevate riskide maandamiseks.

(72) Selleks et lihtsustada käesoleva määruse alusel nõutava teabe esitamist, ning võttes arvesse muid täiendavaid teavitusnõudeid, mis on sätestatud liidu õiguses, näiteks määruses (EL) 2016/679, Euroopa Parlamendi ja nõukogu määruses (EL) 2022/2554[24], Euroopa Parlamendi ja nõukogu direktiivis 2002/58/EÜ[25] ja direktiivis (EL) 2022/2555, ning vähendada üksuste halduskoormust, julgustatakse liikmesriike kaaluma selliste teavitusnõuete jaoks ühtsete kontaktpunktide loomist riigi tasandil. Selliste ühtsete riiklike kontaktpunktide kasutamine turvaintsidentidest teatamiseks määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ alusel ei tohiks mõjutada määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ sätete, eelkõige nendes osutatud asutuste sõltumatust käsitlevate sätete kohaldamist. Käesolevas määruses osutatud ühtse teatamisplatvormi loomisel peaks ENISA võtma arvesse võimalust, et käesolevas määruses osutatud teavitusahela riigisisesed lõpp-punktid integreeritakse riiklikesse ühtsetesse kontaktpunktidesse, mis võivad integreerida ka muid liidu õiguse kohaselt nõutavaid teavitusi.

---

[24] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1).

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

(73) Käesolevas määruses osutatud ühtse teatamisplatvormi loomisel ning selleks, et kasutada ära varasemaid kogemusi, peaks ENISA konsulteerima teiste liidu institutsioonide või asutustega, kes haldavad platvorme või andmebaase, mille suhtes kohaldatakse rangeid turvanõudeid, näiteks Vabadusel, Turvalisusel ja Õigusel Rajaneva Ala Suuremahuliste IT-süsteemide Operatiivjuhtimise Euroopa Liidu Ametiga (eu-LISA). ENISA peaks analüüsima ka võimalikku vastastikust täiendavust direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasiga.

(74) Tootjatel ning muudel füüsilistel ja juriidilistel isikutel peaks olema võimalik koordinaatoriks määratud CSIRTi või ENISAt vabatahtlikult teavitada kõigist digielemente sisaldavas tootes sisalduvatest nõrkustest, küberohtudest, mis võivad mõjutada digielemente sisaldava toote riskiprofiili, kõigist intsidentidest, mis avaldavad mõju digielemente sisaldava toote turvalisusele, ning intsidendiohtudest, mis oleksid võinud sellise intsidendi põhjustada.

(75) Liikmesriigid peaksid kooskõlas riigisisese õigusega püüdma võimalikult suures ulatuses lahendada probleeme, millega puutuvad kokku nõrkuste valdkonnas uuringuid läbi viivad isikud, sealhulgas probleeme, mis on seotud nende võimaliku kriminaalvastutusega. Võttes arvesse, et mõnes liikmesriigis võib nõrkuste valdkonnas uuringuid läbi viivate füüsiliste ja juriidiliste isikute suhtes kohaldada kriminaal- ja tsiviilvastutust, soovitatakse liikmesriikidel võtta vastu suunised, mis käsitlevad infoturbeuurijate nende tegevuse eest vastutusele võtmisest loobumist ja tsiviilvastutusest vabastamist.

(76) Digielemente sisaldavate toodete tootjad peaksid kehtestama nõrkuste koordineeritud avalikustamise põhimõtted, et üksikisikutel või üksustel oleks lihtsam nõrkustest teatada kas otse tootjale või kaudselt ja taotluse korral anonüümselt CSIRTide kaudu, kes on määratud kooskõlas direktiivi (EL) 2022/2555 artikli 12 lõikega 1 nõrkuste koordineeritud avalikustamise koordinaatoriteks. Tootjate nõrkuste koordineeritud avalikustamise põhimõtetes tuleks kirjeldada struktureeritud protsessi, mille kohaselt nõrkusest teatatakse tootjale nii, et tootja saaks sellised nõrkused diagnoosida ja kõrvaldada enne, kui üksikasjalik teave nõrkuse kohta avalikustatakse kolmandatele isikutele või avalikkusele. Lisaks peaksid tootjad kaaluma oma turbepõhimõtete avaldamist masinloetavas vormingus. Arvestades et teavet laialdaselt kasutatavates digielemente sisaldavates toodetes esinevate ärakasutamist võimaldavate nõrkuste kohta võidakse mustal turul müüa kõrge hinnaga, peaksid selliste toodete tootjad saama oma nõrkuste koordineeritud avalikustamise põhimõtete raames kasutada programme, millega motiveerida nõrkustest teatama, tagades üksikisikutele või üksustele nende töö eest tunnustuse ja kompensatsiooni. Siinkohal viidatakse niinimetatud puugipreemia programmidele.

(77) Hõlbustamaks nõrkuste analüüsimist, peaksid tootjad nimetama ja dokumenteerima digielemente sisaldavate toodete komponendid ning koostama tarkvara koostenimekirja. Tarkvara koostenimekiri võib anda tarkvara tootjatele, ostjatele ja käitajatele teabe, mis parandab nende arusaamist tarneahelast, mis on kasulik mitmes mõttes – eeskätt aitab see tootjatel ja kasutajatel ajada värskelt ilmnenud nõrkuste ja küberriskide jälgi. Tootjate jaoks on eriti oluline tagada, et nende digielemente sisaldavad tooted ei sisaldaks kolmandate isikute välja töötatud kaitsetuid komponente. Tootjad ei peaks olema kohustatud tarkvara koostenimekirja avalikustama.

(78) Internetimüügiga seotud uute keerukate ärimudelite puhul võib internetis tegutsev ettevõtja osutada mitmesuguseid teenuseid. Digielemente sisaldava tootega seoses osutatavate teenuste laadist olenevalt võib sama üksus kuuluda erinevatesse ärimudelite või ettevõtjate kategooriatesse. Kui üksus pakub konkreetse digielemente sisaldava toote jaoks üksnes veebipõhiseid vahendusteenuseid ja on vaid internetipõhise kauplemiskoha pakkuja, nagu on määratletud määruse (EL) 2023/988 artikli 3 punktis 14, ei kvalifitseeru ta ühessegi käesolevas määruses määratletud liiki kuuluvaks ettevõtjaks. Kui sama üksus on internetipõhise kauplemiskoha pakkuja ja tegutseb mingite digielemente sisaldavate toodete müügi puhul käesolevas määruses määratletud ettevõtjana, tuleks tema suhtes kohaldada käesolevas määruses seda liiki ettevõtjate suhtes sätestatud kohustusi. Näiteks kui internetipõhise kauplemiskoha pakkuja turustab ka digielemente sisaldavat toodet, siis selle toote müügi puhul käsitatakse teda turustajana. Samuti kui kõnealune üksus müüb digielemente sisaldavaid tooteid omaenda kaubamärgi all, kvalifitseerub ta tootjaks ja peab seega täitma tootjatele kohaldatavaid nõudeid. Samuti võivad mõned üksused kvalifitseeruda Euroopa Parlamendi ja nõukogu määruse (EL) 2019/1020[26] artikli 3 punktis 11 määratletud ekspediitorteenuse osutajateks, kui nad selliseid teenuseid pakuvad. Selliseid juhtumeid on vaja hinnata iga kord eraldi. Võttes arvesse internetipõhiste kauplemiskohtade olulist rolli e-kaubanduse võimaldamisel, peaksid nad püüdma teha koostööd liikmesriikide turujärelevalveasutustega, et aidata tagada internetipõhiste kauplemiskohtade kaudu ostetud digielemente sisaldavate toodete vastavus käesolevas määruses sätestatud küberturvalisuse nõuetele.

[26] Euroopa Parlamendi ja nõukogu 20. juuni 2019. aasta määrus (EL) 2019/1020 turujärelevalve ja toodete vastavuse kohta ning millega muudetakse direktiivi 2004/42/EÜ ja määruseid (EÜ) nr 765/2008 ja (EL) nr 305/2011 (ELT L 169, 25.6.2019, lk 1).

(79) Et vastavust käesoleva määruse nõuetele oleks lihtsam hinnata, tuleks eeldada vastavust juhul, kui digielemente sisaldav toode on vastavuses harmoneeritud standarditega, milles pannakse käesolevas määruses sätestatud olulised küberturvalisuse nõuded üksikasjalike tehniliste spetsifikatsioonide vormi ja mis on vastu võetud kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1025/2012[27]. Nimetatud määrusega sätestatakse menetlus vastuväidete esitamiseks harmoneeritud standarditele, kui need standardid ei vasta täielikult käesolevas määruses sätestatud nõuetele. Standardimise protsess peaks tagama huvide tasakaalustatud esindatuse ja kodanikuühiskonna sidusrühmade, sealhulgas tarbijaühenduste tulemusliku osalemise. Arvesse tuleks võtta ka rahvusvahelisi standardeid, mis vastavad käesolevas määruses sätestatud oluliste küberturvalisuse nõuetega taotletava küberturvalisuse kaitse tasemele, et hõlbustada harmoneeritud standardite väljatöötamist ja käesoleva määruse rakendamist ning hõlbustada nõuete täitmist ettevõtjate, eelkõige mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate ning ülemaailmselt tegutsevate ettevõtjate jaoks.

---

[27] 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).

(80) Käesoleva määruse tulemusliku rakendamise seisukohalt on eriti oluline harmoneeritud standardite õigeaegne väljatöötamine käesoleva määruse kohaldamiseks ette nähtud üleminekuperioodil ning nende kättesaadavus enne määruse kohaldamise alguskuupäeva. Eelkõige kehtib see digielemente sisaldavate oluliste toodete puhul, mis kuuluvad I klassi. Harmoneeritud standardite kättesaadavus võimaldab selliste toodete tootjatel teha vastavushindamisi sisekontrollimenetluse kaudu, vältides nii kitsaskohti ja viivitusi vastavushindamisasutuste tegevuses.

(81) Määrusega (EL) 2019/881 on kehtestatud IKT-toodete, IKT-protsesside ja IKT-teenuste Euroopa küberturvalisuse sertifitseerimise vabatahtlik raamistik. Euroopa küberturvalisuse sertifitseerimise kavad annavad kasutajatele ühtse usaldusraamistiku käesoleva määruse kohaldamisalasse kuuluvate digielemente sisaldavate toodete kasutamiseks. Käesolev määrus peaks seetõttu tekitama koostoime määrusega (EL) 2019/881. Et vastavust käesoleva määruse nõuetele oleks lihtsam hinnata, eeldatakse, et digielemente sisaldavad tooted, mis on sertifitseeritud või mille kohta on välja antud vastavusdeklaratsioon määruse (EL) 2019/881 kohase Euroopa küberturvalisuse kava alusel, mille komisjon on rakendusaktis kindlaks määranud, vastavad käesolevas määruses sätestatud olulistele küberturvalisuse nõuetele niivõrd, kuivõrd Euroopa küberturvalisuse sertifikaat või vastavusdeklaratsioon või nende osa hõlmavad neid nõudeid. Uute Euroopa küberturvalisuse sertifitseerimise kavade vajadust digielemente sisaldavate toodete jaoks tuleks hinnata käesoleva määruse alusel, sealhulgas liidu jooksva tööprogrammi ettevalmistamisel kooskõlas määrusega (EL) 2019/881. Kui on vajadus uue digielemente sisaldavaid tooteid hõlmava kava järele, sealhulgas selleks, et hõlbustada käesoleva määruse järgimist, võib komisjon paluda ENISA-l valmistada ette kavade kandidaatversioonid kooskõlas määruse (EL) 2019/881 artikliga 48. Sellistes tulevastes Euroopa küberturvalisuse sertifitseerimise kavades, mis hõlmavad digielemente sisaldavaid tooteid, tuleks arvesse võtta käesolevas määruses sätestatud olulisi küberturvalisuse nõudeid ja vastavushindamismenetlusi ning hõlbustada käesoleva määruse järgimist. Euroopa küberturvalisuse sertifitseerimise kavade puhul, mis jõustuvad enne käesoleva määruse jõustumist, võib olla vaja täiendavaid täpsustusi selle kohta, kuidas kohaldada vastavuse eeldamist.

Komisjonil peaks olema õigus delegeeritud õigusaktidega täpsustada, millistel tingimustel Euroopa küberturvalisuse sertifitseerimise kavasid võib kasutada, et tõendada vastavust käesolevas määruses sätestatud olulistele küberturvalisuse nõuetele. Lisaks, et vältida põhjendamatu halduskoormuse tekitamist, ei tohiks tootjatele panna kolmanda isiku tehtava vastavushindamise kohustust, mis on käesoleva määrusega vastavate nõuete puhul ette nähtud, juhul kui nende Euroopa küberturvalisuse sertifitseerimise kavade alusel on välja antud vähemalt märkimisväärsele usaldusväärsuse tasemele osutav Euroopa küberturvalisuse sertifikaat.

(82) Pärast seda, kui on jõustunud komisjoni rakendusmäärus (EL) 2024/482, mis puudutab käesoleva määruse kohaldamisalasse kuuluvaid tooteid, näiteks riistvara turvamooduleid ja mikroprotsessoreid, peaks komisjonil olema võimalik delegeeritud õigusaktiga täpsustada, kuidas Euroopa küberturvalisuse sertifitseerimise kava võimaldab eeldada vastavust käesolevas määruses või selle osades sätestatud olulistele küberturvalisuse nõuetele. Lisaks võib sellises delegeeritud õigusaktis täpsustada, kuidas Euroopa küberturvalisuse sertifitseerimise kava alusel välja antud sertifikaat vabastab tootja kolmanda isiku tehtava vastavushindamise kohustusest, mis on vastavate nõuete puhul käesoleva määruse kohaselt nõutav.

(83) Praegune Euroopa standardimisraamistik, mis põhineb uue lähenemisviisi põhimõtetel, mis on sätestatud nõukogu 7. mai 1985. aasta resolutsioonis uue lähenemisviisi kohta tehnilisele ühtlustamisele ja standarditele, ning määrusel (EL) nr 1025/2012, kujutab endast vaikimisi raamistikku selliste standardite väljatöötamiseks, mille puhul eeldatakse vastavust käesolevas määruses ette nähtud olulistele küberturvalisuse nõuetele. Euroopa standardid peaksid olema turupõhised, nendes peaks olema võetud arvesse avalikku huvi ning poliitikaeesmärke, mis on selgelt sätestatud ühele või mitmele Euroopa standardiorganisatsioonile esitatud komisjoni taotluses koostada kindlaksmääratud tähtaja jooksul harmoneeritud standardid, ning need peaksid põhinema konsensusel. Asjakohaste viidete puudumisel harmoneeritud standarditele peaks komisjonil olema siiski õigus võtta vastu rakendusakte, milles sätestatakse käesoleva määruse oluliste küberturvalisuse nõuete ühtsed spetsifikatsioonid, tingimusel et ta võtab seda tehes igakülgselt arvesse standardiorganisatsioonide rolli ja ülesandeid ning et seda kasutatakse erandliku varulahendusena, et tootjal oleks kergem täita oma kohustust järgida olulisi küberturvalisuse nõudeid, kui standardimisprotsess on takistatud või kui asjakohaste harmoneeritud standardite kehtestamine viibib. Kui selline viivitus on tingitud kõnealuse standardi tehnilisest keerukusest, peaks komisjon seda enne ühtsete spetsifikatsioonide kehtestamise kaalumist arvesse võtma.

(84) Et kehtestada kõige tõhusamalt ühtsed spetsifikatsioonid, mis hõlmavad käesoleva määruse olulisi küberturvalisuse nõudeid, peaks komisjon kaasama sellesse protsessi asjaomased sidusrühmad.

(85) Mõistlik ajavahemik, mis puudutab harmoneeritud standardite viidete avaldamist *Euroopa Liidu Teatajas* vastavalt määrusele (EL) nr 1025/2012, tähendab eeldatavat ajavahemikku, mille jooksul viide standardile, selle parandusele või muudatusele avaldatakse *Euroopa Liidu Teatajas*, ning see ei tohiks olla pikem kui üks aasta pärast Euroopa standardi koostamise tähtaega, mis on kehtestatud vastavalt määrusele (EL) nr 1025/2012.

(86) Et vastavust käesolevas määruses sätestatud olulistele küberturvalisuse nõuetele oleks lihtsam hinnata, tuleks eeldada vastavust juhul, kui digielemente sisaldav toode on vastavuses ühtsete spetsifikatsioonidega, mille komisjon on vastu võtnud käesoleva määruse kohaselt, et esitada nende nõuete üksikasjalikud tehnilised spetsifikatsioonid.

(87) Määruse (EL) 2019/881 kohaselt vastu võetud harmoneeritud standardite, ühtsete spetsifikatsioonide või Euroopa küberturvalisuse sertifitseerimise kavade kohaldamine, millega nähakse ette vastavuseeldus digielemente sisaldavate toodete suhtes kohaldatavatele olulistele küberturvalisuse nõuetele, hõlbustab tootjatel teha vastavushindamist. Kui tootja otsustab teatavate nõuete puhul selliseid vahendeid mitte kohaldada, peab ta oma tehnilises dokumentatsioonis märkima, kuidas vastavus saavutatakse muul viisil. Lisaks hõlbustaks määruse (EL) 2019/881 kohaselt vastu võetud harmoneeritud standardite, ühtsete spetsifikatsioonide või Euroopa küberturvalisuse sertifitseerimise kavade kohaldamine, mis tagavad vastavuseelduse tootjate poolt, turujärelevalveasutustel digielemente sisaldavate toodete vastavuse kontrollimist. Seepärast julgustatakse digielemente sisaldavate toodete tootjaid kohaldama selliseid harmoneeritud standardeid, ühtseid spetsifikatsioone või Euroopa küberturvalisuse sertifitseerimise kavasid.

(88) Tootjad peaksid koostama ELi vastavusdeklaratsiooni, milles esitatakse käesoleva direktiivi kohaselt nõutav teave digielemente sisaldava toote vastavuse kohta käesolevas direktiivis sätestatud olulistele küberturvalisuse nõuetele ja, kui see on asjakohane, muudele asjaomastele liidu ühtlustamisõigusaktidele, mille kohaldamisalasse digielemente sisaldav toode kuulub. Tootjatelt võidakse ELi vastavusdeklaratsiooni koostamist nõuda ka liidu muude õigusaktidega. Selleks et tagada turujärelevalve eesmärgil tõhus juurdepääs teabele, tuleks koostada ühtne ELi vastavusdeklaratsioon, mis kajastaks vastavust kõigile asjaomastele liidu õigusaktidele. Ettevõtjate halduskoormuse vähendamiseks peaks olema võimalik, et kõnealune ühtne ELi vastavusdeklaratsioon on asjaomastest üksikutest vastavusdeklaratsioonidest koostatud toimik.

(89) Toote vastavust näitav CE-vastavusmärgis on üldisemas mõttes kogu vastavushindamise menetluse nähtav tulem. CE-vastavusmärgise kasutamist reguleerivad üldpõhimõtted on sätestatud Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 765/2008[28]. Käesolevas määruses tuleks sätestada õigusnormid selle kohta, kuidas kinnitada CE-vastavusmärgis digielemente sisaldavatele toodetele. CE-vastavusmärgis peaks olema ainus märgis, mis tagab, et digielemente sisaldavad tooted vastavad käesolevas määruses sätestatud nõuetele.

---

[28] Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määrus (EÜ) nr 765/2008, millega sätestatakse akrediteerimise nõuded ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 (ELT L 218, 13.8.2008, lk 30).

(90) Et ettevõtjad saaksid tõendada vastavust käesolevas määruses sätestatud olulistele küberturvalisuse nõuetele ja et turujärelevalveasutused saaksid tagada, et turul kättesaadavaks tehtud digielemente sisaldavad tooted vastavad neile nõuetele, on vaja ette näha vastavushindamismenetlused. Euroopa Parlamendi ja nõukogu otsusega nr 768/2008/EÜ[29] on kehtestatud vastavushindamismenetluste moodulid, arvestades kaasnevaid riske ja vajaliku turvalisuse taset. Sektoritevahelise ühtsuse tagamiseks ja ühekordsetest lahendustest hoidumiseks peaksid vastavushindamismenetlused, mis on piisavad, et kontrollida digielemente sisaldavate toodete vastavust käesolevas määruses sätestatud olulistele küberturvalisuse nõuetele, olema loodud nimetatud moodulite põhjal. Vastavushindamismenetlustega tuleks uurida ja kontrollida nii toote kui ka protsessiga seotud nõudeid, mis katavad kogu digielemente sisaldava toote elutsüklit, sh digielemente sisaldava toote kavandamine, projekteerimine, arendamine või tootmine, testimine ja hooldus.

[29] Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta otsus nr 768/2008/EÜ toodete turustamise ühise raamistiku kohta ja millega tunnistatakse kehtetuks nõukogu otsus 93/465/EMÜ (ELT L 218, 13.8.2008, lk 82).

(91) Käesolevas määruses digielemente sisaldavate oluliste või kriitilise tähtsusega toodete loetelus mittesisalduvate digielemente sisaldavate toodete vastavushindamise võib teha tootja omal vastutusel, järgides otsuse 768/2008/EÜ moodulil A põhinevat sisekontrollimenetlust kooskõlas käesoleva määrusega. See kehtib ka juhul, kui tootja otsustab kohaldatava harmoneeritud standardi, ühtse spetsifikatsiooni või Euroopa küberturvalisuse sertifitseerimise kava täielikult või osaliselt kohaldamata jätta. Tootjale jääb ka vabadus valida rangem vastavushindamismenetlus, millesse on kaasatud kolmas isik. Sisekontrolli vormis toimuva vastavushindamismenetluse raames tagab tootja ja kinnitab oma ainuvastutusel, et digielemente sisaldav toode ja tootja protsessid vastavad käesolevas määruses sätestatud kohaldatavatele olulistele küberturvalisuse nõuetele. Kui digielemente sisaldav oluline toode on klassifitseeritud I klassi tooteks, on käesolevas määruses sätestatud olulistele küberturvalisuse nõuetele vastavuse tõendamiseks vaja täiendavat kindlust. Kui tootja soovib teha vastavushindamist omal vastutusel (moodul A), peaks ta kohaldama määruse (EL) 2019/881 alusel vastu võetud harmoneeritud standardeid, ühtseid spetsifikatsioone või Euroopa küberturvalisuse sertifitseerimise kavasid, mille komisjon on kindlaks määratud rakendusaktiga. Kui tootja selliseid harmoneeritud standardeid, ühtseid spetsifikatsioone või Euroopa küberturvalisuse sertifitseerimise kavasid ei kohalda, peaks ta kohaldama vastavushindamist, millesse on kaasatud kolmas isik (moodulite B ja C või mooduli H põhjal). Võttes arvesse tootjate halduskoormust ja asjaolu, et küberturvalisusel on nii materiaalsete kui ka immateriaalsete digielemente sisaldavate toodete projekteerimise ja arendamise etapis oluline koht, on digielemente sisaldavate oluliste toodete proportsionaalse ja tulemusliku vastavushindamismenetluse jaoks kõige sobivamaks valitud otsuse nr 768/2008/EÜ moodulitel B ja C või H põhinevad vastavushindamismenetlused.

Tootja, kes teeb vastavushindamismenetluse koos kolmanda isikuga, võib valida menetluse, mis sobib kõige paremini tema projekteerimis- ja tootmisprotsessiga. Arvestades, et II klassi liigitatud digielemente sisaldavate oluliste toodete kasutamisega on seotud veelgi suurem küberrisk, peaks nende vastavushindamisse olema alati kaasatud kolmas isik, isegi kui toode täielikult või osaliselt vastab harmoneeritud standarditele, ühtsetele spetsifikatsioonidele või Euroopa küberturvalisuse sertifitseerimise kavadele. Vaba ja avatud lähtekoodiga tarkvaraks kvalifitseeruvate oluliste digielemente sisaldavate toodete tootjad peaksid saama järgida moodulil A põhinevat sisekontrollimenetlust, tingimusel et nad teevad tehnilise dokumentatsiooni üldsusele kättesaadavaks.

(92) Kui digielemente sisaldavate materiaalsete toodete loomiseks on tavaliselt vaja teha palju tööd nii projekteerimise, arendamise kui ka toomise etapis, siis tarkvara kujul loodavate digielemente sisaldavate toodete puhul keskendutakse peaaegu eranditult projekteerimisele ja arendamisele ning tootmine mängib väiksemat rolli. Paljudel juhtudel tuleb tarkvaratooted enne turule laskmist siiski kompileerida, ehitada, pakendada, teha allalaadimiseks kättesaadavaks või kopeerida füüsilisele andmekandjale. Kui kohaldatakse asjaomast vastavushindamismenetlust, et kontrollida toote vastavust käesolevas määruses sätestatud olulistele küberturvalisuse nõuetele projekteerimise, arendamise ja tootmise etapis, tuleks loetletud toiminguid käsitada tootmisega samaväärse tegevusena.

(93) Seoses mikro- ja väikeettevõtjatega on proportsionaalsuse tagamiseks asjakohane leevendada halduskulusid, ilma et see mõjutaks käesoleva määruse kohaldamisalasse kuuluvate digielemente sisaldavate toodete küberturvalisuse kaitse taset või võrdseid võimalusi tootjate jaoks. Seepärast on asjakohane, et komisjon kehtestaks mikro- ja väikeettevõtjate vajadustele suunatud lihtsustatud tehnilise dokumentatsiooni vormi. Komisjoni poolt vastu võetud lihtsustatud tehnilise dokumentatsiooni vorm peaks hõlmama kõiki tehnilise dokumentatsiooniga seotud käesolevas määruses sätestatud kohaldatavaid elemente ja täpsustama, kuidas mikro- või väikeettevõtja saaks kokkuvõtlikult esitada nõutud elemente, näiteks esitada digielemente sisaldava toote projekteerimise, arendamise ja tootmise kirjelduse. Nii aitaks vorm vähendada vastavusega seotud halduskoormust, andes asjaomastele ettevõtjatele õiguskindluse nõutava teabe ulatuse ja üksikasjalikkuse suhtes. Mikro- ja väikeettevõtjatele tuleks anda võimalus esitada tehnilise dokumentatsiooniga seotud kohaldatavaid elemente ka ulatuslikumal kujul, mitte kasutada pakutavat lihtsustatud tehnilist vormi.

(94) Innovatsiooni edendamiseks ja kaitsmiseks on oluline võtta eraldi arvesse mikro- või väikeettevõtjatest tootjate või väikeste ja keskmise suurusega ettevõtjate, eelkõige mikro- ja väikeettevõtjate, sealhulgas idufirmade huve. Selleks võiksid liikmesriigid töötada välja algatusi, mis on suunatud mikro- või väikeettevõtjatest tootjatele, sealhulgas koolituse, teadlikkuse suurendamise, teabevahetuse, testimise ja kolmandate isikute vastavushindamistoimingute ning testkeskkondade loomise kohta. Kohustuslike dokumentide, näiteks käesoleva määruse kohaselt nõutava tehnilise dokumentatsiooni ning kasutajale vajaliku teabe ja juhistega, samuti ametiasutustega suhtlemisega seotud tõlkekulud võivad tootjate, eelkõige väiksemate tootjate jaoks kujutada märkimisväärseid väljaminekuid. Seepärast võiksid liikmesriigid arvestada, et üks nende poolt asjaomaste tootjate dokumentatsiooni ja tootjatega suhtlemise jaoks kindlaks määratud ja neile vastuvõetavatest keeltest on keel, mis on üldjoontes arusaadav võimalikult suurele arvule kasutajatele.

(95) Käesoleva määruse sujuva rakendamise tagamiseks peaksid liikmesriigid püüdma enne käesoleva määruse kohaldamise alguskuupäeva tagada, et kolmandate isikute poolse vastavushindamise läbiviimiseks oleks piisaval arvul teada antud asutusi. Komisjon peaks abistama selles osas liikmesriike ja teisi asjaosalisi, et vältida kitsaskohti ja takistusi tootjate turule sisenemisel. Liikmesriikide juhitud ja vajadusel komisjoni poolt toetatav suunatud koolitustegevus võib aidata kaasa kvalifitseeritud spetsialistide kättesaadavusele, sealhulgas käesoleva määruse kohaselt teada antud asutuste tegevuse toetamisele. Võttes arvesse kolmandate isikute poolse vastavushindamisega kaasneda võivaid kulusid, tuleks kaaluda selliste liidu ja liikmesriikide tasandi algatuste rahastamist, mille eesmärk on leevendada selliseid kulusid mikro- ja väikeettevõtjate jaoks.

(96) Proportsionaalsuse tagamiseks peaksid vastavushindamisasutused vastavushindamismenetluste tasude kehtestamisel võtma arvesse mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate, sealhulgas idufirmade erihuve ja vajadusi. Eelkõige peaksid vastavushindamisasutused kohaldama käesolevas määruses sätestatud asjakohast kontrollimenetlust ja testimisi ainult siis, kui see on asjakohane ja järgides riskipõhist lähenemisviisi.

(97) Regulatiivliivakastide eesmärk peaks olema edendada innovatsiooni ja ettevõtjate konkurentsivõimet, luues kontrollitud testkeskkonnad enne digielemente sisaldavate toodete turule laskmist. Regulatiivliivakastid peaksid aitama parandada kõigi käesoleva määruse kohaldamisalasse kuuluvate osalejate õiguskindlust ning hõlbustama ja kiirendama digielemente sisaldavate toodete pääsu liidu turule, eelkõige juhul, kui neid pakuvad mikro- ja väikeettevõtjad, sealhulgas idufirmad.

(98) Et digielemente sisaldav toode saaks läbida kolmanda isiku tehtava vastavushindamise, peaksid riikide teavitavad asutused teatama komisjonile ja teistele liikmesriikidele vastavushindamisasutuste nimed, tingimusel et need asutused vastavad teatavatele nõuetele eeskätt sõltumatuse, pädevuse ja huvide konflikti puudumise vallas.

(99) Digielemente sisaldavate toodete vastavushindamise kvaliteedi ühtlase taseme tagamiseks on vaja kehtestada nõuded ka teavitavate asutuste kohta ja muude teada antud asutuste hindamisse, teavitamisse ja nende järelevalvesse kaasatud asutuste kohta. Käesolevas määruses esitatud süsteemi peaks täiendama määrusega (EÜ) nr 765/2008 ette nähtud akrediteerimissüsteem. Kuna akrediteerimine on vastavushindamisasutuse pädevuse kontrollimise põhiline vahend, siis tuleks seda kasutada ka teavitamise eesmärgil.

(100) Vastavushindamisasutusi, mis on akrediteeritud ja millest on teada antud liidu õiguse alusel, millega kehtestatakse käesolevas määruses sätestatud nõuetega sarnased nõuded, näiteks vastavushindamisasutust, millest on teada antud määruse (EL) 2019/881 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava raames või delegeeritud määruse (EL) 2022/30 alusel, tuleks käesoleva määruse alusel uuesti hinnata ja neist teada anda. Asjaomased asutused võivad siiski kindlaks määrata sünergia kattuvate nõuete osas, et vältida tarbetut finants- ja halduskoormust ning tagada sujuv ja õigeaegne teatamisprotsess.

(101) Määrusega (EÜ) nr 765/2008 ettenähtud läbipaistev akrediteerimine, mis tagab vastavussertifikaatide usaldusväärsuse vajaliku taseme, peaks kogu liidus kujunema riikide ametiasutuste jaoks eelistatud vahendiks, millega tõendada vastavushindamisasutuste tehnilist pädevust. Riiklikud asutused võivad siiski olla seisukohal, et neil on asjakohased vahendid, et kõnealune hindamine ise läbi viia. Teiste riiklike asutuste läbiviidud hindamiste piisava usaldusväärsuse tagamiseks tuleks neil sellisel juhul esitada komisjonile ja teistele liikmesriikidele dokumentaalsed tõendid selle kohta, et hinnatud vastavushindamisasutused täidavad asjakohaste õigusaktidega kehtestatud nõudeid.

(102) Vastavushindamisasutused kasutavad vastavushindamise mõne toimingu tegemiseks sageli alltöövõtjaid või tütarettevõtjaid. Turule lastava digielemente sisaldava toote ettenähtud kaitsetaseme tagamiseks on oluline, et vastavushindamisse kaasatud alltöövõtjad ja tütarettevõtjad vastaksid vastavushindamise ülesannete täitmisel samadele nõuetele kui teada antud asutused.

(103) Teavitav asutus peaks saatma vastavushindamisasutuse kohta teate komisjonile ja teistele liikmesriikidele teada antud ja määratud organisatsioonide uue teabesüsteemi (NANDO) kaudu. NANDO on komisjoni arendatav ja hallatav elektroonilise teavitamise töövahend, mis sisaldab kõigi teada antud asutuste loetelu.

(104) Et teada antud asutused võivad oma teenuseid pakkuda kogu liidus, peaksid teised liikmesriigid ja komisjon saama võimaluse esitada teada antud asutuse kohta vastuväiteid. Seega on oluline näha ette ajavahemik, mille jooksul saaks lahendada kõik võimalikud vastavushindamisasutuste pädevust puudutavad kahtlused või probleemid, enne kui nad alustavad tegevust teada antud asutustena.

(105) Konkurentsivõime tagamiseks on oluline, et teada antud asutused kohaldaksid vastavushindamisi ilma ettevõtjaid liigselt koormamata. Samal põhjusel ja ettevõtjate võrdse kohtlemise tagamiseks tuleb tagada vastavushindamismenetluste tehnilise kohaldamise järjekindlus. Seda peaks saama kõige paremini saavutada otstarbeka koordineerimise ja koostööga teada antud asutuste vahel.

(106) Liidu õiguse asjakohase ja ühetaolise kohaldamise tagamisel on oluline vahend turujärelevalve. Seepärast on otstarbekas kehtestada õigusraamistik turujärelevalve sobival viisil teostamise jaoks. Käesoleva määruse kohaldamisalasse kuuluvate digielemente sisaldavate toodete suhtes kohaldatakse liidu turujärelevalvet ja liidu turule sisenevate toodete kontrollimist käsitlevaid õigusnorme, mis on sätestatud määruses (EL) 2019/1020.

(107) Vastavalt määrusele (EL) 2019/1020 teeb turujärelevalveasutus turujärelevalvet selle liikmesriigi territooriumil, mis on ta määranud. Käesolev määrus ei tohiks takistada liikmesriike valimast, millised pädevad asutused turujärelevalve ülesandeid täitma hakkavad. Iga liikmesriik peaks määrama ühe või mitu oma territooriumil tegutsevat turujärelevalveasutust. Liikmesriikidel peaks olema võimalik turujärelevalveasutuseks määrata olemasoleva või uue asutuse, kaasa arvatud direktiivi (EL) 2022/2555 artikli 8 kohaselt määratud või asutatud pädeva asutuse, määruse (EL) 2019/881 artikli 58 kohaselt määratud riikliku küberturvalisuse sertifitseerimise asutuse või direktiivi 2014/53/EL kohaselt määratud turujärelevalveasutuse. Ettevõtjad peaksid tegema turujärelevalveasutuste ja muude pädevate asutustega täielikku koostööd. Iga liikmesriik peaks teavitama komisjoni ja teisi liikmesriike oma turujärelevalveasutustest ja iga kõnealuse asutuse pädevusvaldkondadest ning tagama käesoleva määrusega seotud turujärelevalve ülesannete täitmiseks vajalikud ressursid ja oskused. Vastavalt määruse (EL) 2019/1020 artikli 10 lõigetele 2 ja 3 peaks iga liikmesriik määrama ühtse kontaktasutuse, mis vastutab muu hulgas turujärelevalveasutuste kooskõlastatud seisukoha esindamise ning eri liikmesriikide turujärelevalveasutuste vahelise koostöö toetamise eest.

(108) Käesoleva määruse ühetaoliseks kohaldamiseks tuleks luua spetsiaalne digielemente sisaldavate toodete küberkerksuse halduskoostöörühm (ADCO) vastavalt määruse (EL) 2019/1020 artikli 30 lõikele 2. ADCO peaks koosnema määratud turujärelevalveasutuste esindajatest ning vajaduse korral ühtsete kontaktasutuste esindajatest. Komisjon peaks toetama ja soodustama turujärelevalveasutuste vahelist koostööd määruse (EL) 2019/1020 artikli 29 alusel loodud liidu toodetele vastavuse võrgustikus, millesse kuuluvad iga liikmesriigi esindajad, kaasa arvatud iga selle määruse artiklis 10 osutatud ühtse kontaktasutuse esindaja ja soovi korral riiklik ekspert, ADCOde esimehed ning komisjoni esindajad. Komisjon peaks osalema liidu toodete nõuetele vastavuse võrgustiku, selle allrühmade ja ADCO koosolekutel. Samuti peaks ta ADCOt abistama tehnilist ja logistilist tuge pakkuva täitevsekretariaadi kaudu. ADCO võib kutsuda osalema ka sõltumatuid eksperte ja teha koostööd teiste, näiteks direktiivi 2014/53/EL alusel loodud ADCOdega.

(109) Turujärelevalveasutused peaksid käesoleva määruse alusel loodud ADCO kaudu tegema tihedat koostööd ja neil peaks olema võimalik töötada välja juhenddokumente, et hõlbustada turujärelevalvet riiklikul tasandil, näiteks töötades välja parimad tavad ja näitajad, et tulemuslikult kontrollida digielemente sisaldavate toodete vastavust käesolevale määrusele.

(110) Õigeaegsete, proportsionaalsete ja tulemuslike meetmete tagamiseks seoses digielemente sisaldavate toodetega, mis kujutavad endast olulist küberriski, tuleks kehtestada liidu kaitsemenetlus, mille raames teavitatakse huvitatud isikuid meetmetest, mida kavatsetakse selliste toodete suhtes võtta. See peaks võimaldama ka turujärelevalveasutustel koostöös asjaomaste ettevõtjatega vajaduse korral varem reageerida. Kui liikmesriigid ja komisjon nõustuvad liikmesriigi võetud meetmete põhjendustega, siis ei peaks komisjon rohkem sekkuma, välja arvatud juhul, kui mittevastavus on põhjendatav puudustega harmoneeritud standardis.

(111) Teatavatel juhtudel võib käesoleva määruse nõuetele vastav digielemente sisaldav toode siiski kujutada olulist küberriski või olla risk isikute tervise ja ohutuse, põhiõiguste kaitseks mõeldud liidu või riigisisesest õigusest tulenevate kohustuste täitmise, direktiivi (EL) 2022/2555 artikli 3 lõikes 1 osutatud elutähtsate üksuste poolt elektroonilise infosüsteemi abil osutatavate teenuste kättesaadavuse, autentsuse, tervikluse või konfidentsiaalsuse või avalike huvide kaitse muude aspektide jaoks. Seepärast on vaja kehtestada õigusnormid, mis tagaksid selliste riskide maandamise. Seetõttu peaksid turujärelevalveasutused võtma meetmeid, mis kohustaksid ettevõtjaid tagama, et toode ei kujuta endast enam kõnealust riski, selle tagasi võtma või turult kõrvaldama, olenevalt sellest, millise riskiga on tegu. Niipea kui turujärelevalveasutus piirab sellisel moel digielemente sisaldava toote vaba liikumist või keelab selle, peab liikmesriik ajutistest meetmetest viivitamata teatama komisjonile ja teistele liikmesriikidele ning esitama otsuse põhjused ja põhjenduse. Kui turujärelevalveasutus võtab endast riski kujutavate digielemente sisaldavate toodete suhtes selliseid meetmeid, peaks komisjon viivitamata alustama konsultatsioone liikmesriikide ja asjaomase ettevõtja või asjaomaste ettevõtjatega ning riiklikku meedet hindama. Kõnealuse hindamise tulemuste põhjal peaks komisjon otsustama, kas riiklik meede on põhjendatud või mitte. Komisjon peaks adresseerima oma otsuse kõikidele liikmesriikidele ning edastama selle viivitamata neile ja asjaomasele ettevõtjale või asjaomastele ettevõtjatele. Kui meedet peetakse põhjendatuks, peakskomisjonil olema võimalik kaaluda ka võimalust võtta vastu ettepanekud asjakohase liidu õiguse läbivaatamiseks.

(112) Kui tegemist on digielemente sisaldavate toodetega, mis kujutavad endast olulist küberriski, ja kui on alust uskuda, et need tooted ei vasta käesolevale määrusele, või kui tegemist on toodetega, mis vastavad käesolevale määrusele, kuid kujutavad endast muid olulisi riske, näiteks riski inimeste tervisele või ohutusele, liidu või riigisisesest õigusest tulenevate kohustuste täitmisele, mille eesmärk on kaitsta põhiõigusi või direktiivi (EL) 2022/2555 artikli 3 lõikes 1 osutatud elutähtsate üksuste poolt elektroonilise infosüsteemi abil osutatavate teenuste kättesaadavusele, autentsusele, terviklusele või konfidentsiaalsusele, peaks komisjonil olema võimalik taotleda, et ENISA teeks hindamise. Selle hindamise põhjal peaks komisjonil olema võimalik võtta rakendusaktidega vastu liidu tasandi parandusmeetmeid või piiravaid meetmeid, sealhulgas nõuda asjaomaste digielemente sisaldavate toodete turult kõrvaldamist või tagasinõudmist mõistliku aja jooksul, mis vastab riski laadile. Komisjonil peaks olema võimalik sellist sekkumist kasutada üksnes erandlike asjaolude korral, mis õigustavad viivitamatut sekkumist siseturu nõuetekohase toimimise säilitamiseks, ning seda üksnes juhul, kui turujärelevalveasutused ei ole võtnud olukorra parandamiseks tulemuslikke meetmeid. Sellised erandlikud asjaolud võivad olla hädaolukorrad, kus näiteks tootja on nõuetele mittevastava digielemente sisaldava toote mitmes liikmesriigis laialdaselt kättesaadavaks teinud, direktiivi (EL) 2022/2555 kohaldamisalasse kuuluvad üksused kasutavad neid ka võtmetähtsusega sektorites, samas kui toodetel on teadaolevad nõrkused, mida kuritahtlikud isikud ära kasutavad ja mille parandamiseks ei paku tootja paiku. Sellistes hädaolukordades peaks komisjonil olema võimalik sekkuda ainult erandlike asjaolude kestel ja juhul, kui käesoleva määruse rikkumine või ilmnenud olulised riskid püsivad.

(113) Kui on märke, et käesolevat määrust ei täideta mitmes liikmesriigis, peaks turujärelevalveasutustel olema võimalik võtta ette ühismeetmeid koos teiste asutustega, et kontrollida vastavust ja teha kindlaks digielemente sisaldavate toodete küberriskid.

(114) Samaaegsed koordineeritud kontrollimeetmed (edaspidi „lauskontrollid“) on turujärelevalveasutuste konkreetsed normide täitmise tagamise meetmed, mis võivad aidata tooteohutust veelgi parandada. Lauskontrolle tuleks eelkõige teha juhul, kui turusuundumused, tarbijate kaebused või muud andmed viitavad sellele, et teatavad digielemente sisaldavate toodete kategooriad põhjustavad sageli küberriske. Lisaks peaksid turujärelevalveasutused lauskontrollitavate tootekategooriate kindlaksmääramisel võtma arvesse ka mittetehniliste riskiteguritega seotud asjaolusid. Selleks peaks turujärelevalveasutustel olema võimalik võtta arvesse direktiivi (EL) 2022/2555 artikli 22 kohaselt tehtud liidu tasandi kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamiste tulemusi, sealhulgas mittetehniliste riskiteguritega seotud asjaolusid. ENISA peaks esitama turujärelevalveasutustele ettepanekud digielemente sisaldavate toodete kategooriate kohta, mille suhtes võiks korraldada lauskontrolle, tuginedes muu hulgas nõrkuste ja intsidentide kohta saadud teadetele.

(115) Arvestades ENISA eksperditeadmisi ja volitusi, peaks tal olema võimalik toetada käesoleva määruse rakendamise protsessi. Eeskätt peaks ENISA saama teha ettepanekuid ühismeetmete kohta, mida turujärelevalveasutused võiksid võtta, tuginedes märkidele või teabele selle kohta, et digielemente sisaldavad tooted ei pruugi mitmes liikmesriigis olla vastavuses käesoleva määrusega, või määrata kindlaks tootekategooriaid, mille suhtes tuleks korraldada lauskontrolle. Erandlike asjaolude korral peaks ENISA saama komisjoni taotlusel korraldada selliste digielemente sisaldavate toodete hindamisi, mis kujutavad endast olulist küberriski, kui siseturu nõuetekohase toimimise säilitamiseks on vaja sekkuda viivitamata.

(116) Käesoleva määrusega antakse ENISA-le teatavad ülesanded, mis nõuavad asjakohaseid eksperditeadmisi ja inimressursse, et ENISA saaks neid ülesandeid tulemuslikult täita. Komisjon teeb liidu üldeelarve projekti ettevalmistamisel ettepaneku ENISA ametikohtade loetelu jaoks vajalike eelarvevahendite kohta vastavalt määruse (EL) 2019/881 artiklis 29 sätestatud menetlusele. Selle protsessi käigus võtab komisjon arvesse ENISA koguressursse, mis võimaldavad tal täita oma ülesandeid, sealhulgas neid, mis on ENISA-le käesoleva määruse kohaselt antud.

(117) Tagamaks, et õigusraamistikku saab vajaduse korral kohandada, peaks komisjonil olema õigus võtta kooskõlas Euroopa Liidu toimimise lepingu artikliga 290 vastu delegeeritud õigusakte seoses digielemente sisaldavate oluliste toodete loetelu ajakohastamise ja lisasse kandmisega. Komisjonile tuleks anda õigus võtta kooskõlas nimetatud artikliga vastu delegeeritud õigusakte, et teha kindlaks digielemente sisaldavad tooted, mille suhtes kohaldatakse muid liidu õigusnorme, millega saavutatakse samal tasemel kaitse kui käesoleva määrusega, ning täpsustada, kas oleks vaja piiranguid või erandeid käesoleva määruse kohaldamisalast ning, kui see on asjakohane, siis ka kõnealuse piirangu ulatus. Õigus võtta kooskõlas nimetatud artikliga vastu delegeeritud õigusakte tuleks komisjonile anda ka selleks, et vajaduse korral lubada Euroopa küberturvalisuse sertifitseerimise kava kohaselt sertifitseerida käesoleva määruse lisas esitatud digielemente sisaldavaid kriitilise tähtsusega tooteid, et ajakohastada digielemente sisaldavate kriitilise tähtsusega toodete loetelu käesolevas määruses sätestatud kriitilisuse kriteeriumide alusel ning et määrata kindlaks määruse (EL) 2019/881 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavad, mida saab kasutada selleks, et tõendada vastavust käesoleva määruse lisas sätestatud olulistele küberturvalisuse nõuetele või nende osadele. Samuti peaks komisjonil olema õigus võtta vastu delegeeritud õigusakte, et määrata kindlaks minimaalne toe kestus konkreetsete tootekategooriate puhul, kui turujärelevalve andmed osutavad toe ebapiisavale kestusele, ning määrata kindlaks küberturvalisusega seotud põhjenduste kohaldamise tingimused seoses aktiivselt ärakasutatavaid nõrkusi käsitlevate teadete edastamise edasilükkamisega.

Lisaks peaks komisjonil olema õigus võtta vastu delegeeritud õigusakte, et kehtestada vabatahtlikud turvalisuse tõendamise programmid, et hinnata vaba ja avatud lähtekoodiga tarkvaraks kvalifitseeruvate digielemente sisaldavate toodete vastavust kõigile või teatavatele olulistele küberturvalisuse nõuetele või muudele käesolevas määruses sätestatud kohustustele, samuti määrata kindlaks ELi vastavusdeklaratsiooni minimaalne sisu ja täiendada elemente, mis peavad olema tehnilises dokumentatsioonis. On eriti oluline, et komisjon viiks ettevalmistava töö käigus läbi asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil, ja et kõnealused konsultatsioonid toimuksid kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes[30] sätestatud põhimõtetega. Eelkõige selleks, et tagada delegeeritud õigusaktide ettevalmistamises võrdne osalemine, saavad Euroopa Parlament ja nõukogu kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel on pidev juurdepääs komisjoni eksperdirühmade koosolekutele, millel arutatakse delegeeritud õigusaktide ettevalmistamist. Käesolevas määruses osutatud õigus võtta vastu delegeeritud õigusakte tuleks komisjonile anda viieks aastaks alates … [käesoleva määruse jõustumise kuupäev]. Komisjon peaks esitama delegeeritud volituste kohta aruande hiljemalt üheksa kuud enne selle viieaastase tähtaja möödumist. Volituste delegeerimist tuleks pikendada automaatselt samaks ajavahemikuks, välja arvatud juhul, kui Euroopa Parlament või nõukogu esitab selle suhtes vastuväite hiljemalt kolm kuud enne iga ajavahemiku lõppemist.

---

30 ELT L 123, 12.5.2016, lk 1.

(118) Selleks et tagada käesoleva määruse rakendamise ühetaolised tingimused, tuleks komisjonile anda rakendamisvolitused, et täpsustada käesoleva määruse lisas sätestatud digielemente sisaldavate oluliste toodete kategooriate tehniline kirjeldus, täpsustada tarkvaramaterjalide loetelu vorm ja elemendid, veelgi täpsustada, milline peab olema tootja poolt digielemente sisaldavate toodete turvalisust mõjutavate aktiivselt ärakasutatavate nõrkuste ja tõsiste intsidentide kohta ENISA-le esitatava teabe vorming ja teatamise kord, kehtestada ühtsed spetsifikatsioonid, mis hõlmavad tehnilisi nõudeid, mis võimaldavad täita käesoleva määruse lisas sätestatud olulisi küberturvalisuse nõudeid, määrata kindlaks tehnilised nõuded märgistusele, piktogrammidele või muudele märgistele, mis on seotud digielemente sisaldavate toodete turvalisusega, nende toe kestuse ja mehhanismid nende kasutuse edendamiseks ning üldsuse teadlikkuse suurendamiseks digielemente sisaldavate toodete turvalisuse kohta, määrata kindlaks mikro- ja väikeettevõtjate vajadusi arvestava lihtsustatud tehnilise dokumentatsiooni vormi ning otsustada liidu tasandi parandusmeetmete või piiravate meetmete üle erandlikel asjaoludel, mis õigustavad viivitamatut sekkumist siseturu nõuetekohase toimimise säilitamiseks. Neid volitusi tuleks teostada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011[31].

(119) Turujärelevalveasutuste usaldusliku ja konstruktiivse koostöö tagamiseks liidu ja riikide tasandil peaksid kõik käeoleva määruse kohaldamises osalejad austama oma ülesannete täitmise käigus saadud teabe ja andmete konfidentsiaalsust.

---

[31] 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. ELI: http://data.europa.eu/eli/reg/2011/182/oj?locale=et).

(120) Et tagada käesolevas määruses sätestatud kohustuste tulemuslik täitmine, peaks igal turujärelevalveasutusel olema õigus määrata haldustrahve või taotleda nende määramist. Seepärast tuleks kehtestada käesolevas määruses sätestatud kohustuste täitmata jätmise eest riigisises õiguses sätestatavate haldustrahvide maksimummäärad. Igal üksikjuhul haldustrahvi suuruse üle otsustades tuleks arvesse võtta kõiki konkreetse olukorra asjakohaseid aspekte ja vähemalt neid asjaolusid, mis on käesolevas määruses sõnaselgelt sätestatud, sealhulgas seda, kas tootja on mikroettevõtja, väike või keskmise suurusega ettevõtja, kaasa arvatud idufirma, ning kas samad või muud turujärelevalveasutused on sama ettevõtja suhtes juba kohaldanud haldustrahve samalaadse rikkumise eest. Sellised asjaolud võivad olla kas raskendavad, kui sama ettevõtja rikkumine jätkub mõne muu liikmesriigi territooriumil kui see, kus haldustrahvi on juba kohaldatud, või leevendavad, kui tagatakse, et mõne teise turujärelevalveasutuse poolt samale ettevõtjale või sama liiki rikkumise puhul kaalutava muu haldustrahvi korral tuleks koos muude asjakohaste konkreetsete asjaoludega juba arvesse võtta ka teistes liikmesriikides määratud karistust ja selle suurust. Kõigil sellistel juhtudel peaks kumulatiivse haldustrahvi puhul, mida mitme liikmesriigi turujärelevalveasutused võivad samale ettevõtjale sama liiki rikkumise eest kohaldada, olema tagatud proportsionaalsuse põhimõtte järgimine. Arvestades, et haldustrahve ei kohaldata mikro- või väikeettevõtjate suhtes, kui nad ei pea kinni 24-tunnisest tähtajast, mille jooksul tuleb saata eelhoiatuse teavitus aktiivselt ärakasutatavatest nõrkustest või tõsistest intsidentidest, mis mõjutavad digielemente sisaldava toote turvalisust, ega avatud lähtekoodiga tarkvara korraldajate suhtes käesoleva määruse mis tahes rikkumise korral, ning võttes arvesse põhimõtet, et karistused peaksid olema mõjusad, proportsionaalsed ja hoiatavad, ei tohiks liikmesriigid nende üksuste suhtes kehtestada muud liiki rahatrahve.

(121) Kui haldustrahv määratakse isikule, kes ei ole ettevõtja, peaks pädev asutus sobiva trahvisumma määramisel arvesse võtma üldist sissetulekutaset selles liikmesriigis ja isiku majanduslikku olukorda. See, kas ja mil määral tuleks kohaldada trahve avaliku sektori asutustele, peaks olema liikmesriikide otsustada.

(122) Liikmesriigid peaksid riikide olusid arvesse võttes uurima võimalust kasutada käesolevas määruses sätestatud karistustest saadavat tulu või sellega samaväärset rahalist summat küberturvalisuse poliitika toetamiseks ja küberturvalisuse taseme tõstmiseks liidus, muu hulgas suurendades kvalifitseeritud küberturvalisuse spetsialistide arvu, tõhustades mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate suutlikkuse suurendamist ning parandades üldsuse teadlikkust küberohtudest.

(123) Oma suhetes kolmandate riikidega püüab liit edendada reguleeritud toodete rahvusvahelist kaubandust. Kaubavahetuse hõlbustamiseks võib vastavushindamise ja reguleeritud toodete suhtes kohaldada mitmesuguseid meetmeid, sealhulgas mitmeid õigusakte, näiteks kahepoolset (valitsustevahelist) vastastikuse tunnustamise lepingut. Vastastikuse tunnustamise lepingud sõlmitakse liidu ja selliste kolmandate riikide vahel, kus on tehniline areng võrreldaval tasemel ja kelle lähenemisviis vastavushindamisele on samalaadne. Kõnealused lepingud põhinevad selliste sertifikaatide, vastavusmärgiste ja testimisaruannete vastastikusel aktsepteerimisel, mille ühe poole vastavushindamisasutused on väljastanud kooskõlas teise poole õigusaktidega. Praegu kehtivad vastastikuse tunnustamise lepingud mitme kolmanda riigiga. Need lepingud on sõlmitud mitmes konkreetses valdkonnas, mis võivad eri kolmandates riikides erineda. Mõistes, et digielemente sisaldavate toodete tarneahelad on ülemaailmsed, võib liit sõlmida käesoleva määrusega reguleeritud toodete puhul vastavushindamist käsitlevaid vastastikuse tunnustamise lepinguid vastavalt ELi toimimise lepingu artiklile 218, et kaubavahetust veelgi hõlbustada. Et tugevdada küberkerksust kogu maailmas, on oluline ka koostöö partneriteks olevate kolmandate riikidega, sest pikas perspektiivis aitab see tugevdada küberturvalisuse raamistikku nii liidus kui ka väljaspool seda.

(124) Tarbijatel peaks olema õigus kasutada oma õigusi seoses käesoleva määruse alusel ettevõtjatele pandud kohustustega esindushagide kaudu vastavalt Euroopa Parlamendi ja nõukogu direktiivile (EL) 2020/1828[32]. Selleks tuleks käesolevas määruses sätestada, et direktiivi (EL) 2020/1828 kohaldatakse esindushagide suhtes, mis käsitlevad käesoleva määruse rikkumisi, mis kahjustavad või võivad kahjustada tarbijate kollektiivseid huve. Seetõttu tuleks kõnealuse direktiivi I lisa vastavalt muuta. Liikmesriikide ülesanne on tagada, et need muudatused kajastuksid ülevõtmismeetmetes, mis on vastu võetud kooskõlas kõnealuse direktiiviga, kuigi asjaomaste riigisiseste ülevõtmismeetmete vastuvõtmine ei ole tingimus, millest sõltuks kõnealuse direktiivi kohaldamine nende esindushagide suhtes. Kõnealuse direktiivi kohaldamine esindushagide suhtes, mis on esitatud ettevõtjate vastu seoses käesoleva määruse sätete rikkumisega, mis kahjustab või võib kahjustada tarbijate kollektiivseid huve, peaks algama … [36 kuud alates käesoleva määruse jõustumise kuupäevast].

(125) Komisjon peaks asjaomaste sidusrühmadega konsulteerides käesoleva määruse sätted regulaarselt hindama ja läbi vaatama, eelkõige selleks, et teha kindlaks, kas neid on vaja muuta seoses ühiskondlike, poliitiliste, tehnoloogiliste ja turutingimuste muutumisega. Käesolev määrus hõlbustab määruse (EL) 2022/2554 ja direktiivi (EL) 2022/2555 kohaldamisalasse kuuluvate digielemente sisaldavaid tooteid kasutavate üksuste tarneahela turvalisuse kohustuste täitmist. Komisjon peaks perioodilise läbivaatamise käigus hindama liidu küberturvalisuse raamistiku kogumõju.

---

[32] Euroopa Parlamendi ja nõukogu 25. novembri 2020. aasta direktiiv (EL) 2020/1828, mis käsitleb tarbijate kollektiivsete huvide kaitsmise esindushagisid ja millega tunnistatakse kehtetuks direktiiv 2009/22/EÜ (ELT L 409, 4.12.2020, lk 1).

(126) Ettevõtjatele tuleks anda piisavalt aega käesolevas määruses sätestatud nõuetega kohanemiseks. Käesolevat määrust tuleks kohaldada alates … [36 kuud pärast käesoleva määruse jõustumise kuupäeva], välja arvatud digelemente sisaldavate toodete turvalisust mõjutavaid aktiivselt ärakasutatavaid nõrkusi ja tõsiseid intsidente käsitlevate teatamiskohustuste osas, mida tuleks kohaldada alates … [21 kuud pärast käesoleva määruse jõustumise kuupäeva], ja vastavushindamisasutustest teatamist käsitlevate sätete osas, mida tuleks kohaldada alates … [18 kuud pärast käesoleva määruse jõustumise kuupäeva].

(127) Oluline on toetada mikroettevõtjaid ning väikeseid ja keskmise suurusega ettevõtjaid, sealhulgas idufirmasid, käesoleva määruse rakendamisel ning minimeerida rakendamisega seotud riske, mis tulenevad teadmiste ja oskusteabe puudumisest turul, samuti selleks, et hõlbustada tootjatel täita käesolevas määruses sätestatud kohustusi. Programm „Digitaalne Euroopa“ ja muud asjakohased liidu programmid pakuvad rahalist ja tehnilist tuge, mis võimaldab neil ettevõtjatel aidata kaasa liidu majanduse kasvule ja küberturvalisuse ühise taseme tugevdamisele liidus. Euroopa küberturvalisuse pädevuskeskus ja riiklikud koordineerimiskeskused ning komisjoni ja liikmesriikide poolt liidu või riigi tasandil loodud Euroopa digitaalse innovatsiooni keskused võiksid samuti toetada ettevõtjaid ja avaliku sektori organisatsioone ning aidata kaasa käesoleva määruse rakendamisele. Nad võiksid oma ülesannete ja pädevuse piires pakkuda mikroettevõtjatele ning väikestele ja keskmise suurusega ettevõtjatele tehnilist ja teaduslikku tuge, näiteks testimiseks ja kolmandate isikute poolseks vastavushindamiseks. Samuti võiksid nad edendada vahendite kasutuselevõttu, et hõlbustada käesoleva määruse rakendamist.

(128) Lisaks peaksid liikmesriigid kaaluma täiendavaid meetmeid, eesmärgiga pakkuda mikroettevõtjatele ning väikestele ja keskmise suurusega ettevõtjatele suuniseid ja toetust, näiteks regulatiivliivakastide ja kommunikatsiooniks mõeldud sihtotstarbeliste kanalite loomise kaudu. Küberturvalisuse taseme tõstmiseks liidus võivad liikmesriigid kaaluda ka toetuse andmist digielemente sisaldavate toodetega seotud küberturvalisuse alase suutlikkuse ja oskuste arendamiseks, ettevõtjate, eelkõige mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate küberkerksuse parandamiseks ning üldsuse teadlikkuse suurendamiseks digielemente sisaldavate toodete küberturvalisusest.

(129) Kuna käesoleva määruse eesmärki ei suuda liikmesriigid piisavalt saavutada, küll aga saab seda meetme ulatuse 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.

(130) Euroopa Andmekaitseinspektoriga konsulteeriti kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725[33] artikli 42 lõikega 1 ning ta esitas arvamuse 9. novembril 2022[34],

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

---

[33] 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).

[34] ELT C 452, 29.11.2022, lk 23.

I peatükk
Üldsätted

Artikkel 1

Reguleerimisese

Käesoleva määrusega nähakse ette:

a) õigusnormid, mis reguleerivad digielemente sisaldavate toodete turul kättesaadavaks tegemist, et tagada selliste toodete küberturvalisus;

b) digielemente sisaldavate toodete projekteerimise, arendamise ja tootmise olulised küberturvalisuse nõuded ning kohustused, mida ettevõtjad peavad selliste toodete puhul seoses küberturvalisusega täitma;

c) selliste protsesside olulised küberturvalisuse nõuded, mille tootjad on kehtestanud nõrkuste käsitlemiseks, et tagada digielemente sisaldavate toodete küberturvalisus toodete kogu eeldatava kasutamise ajal, ning ettevõtjate kohustused seoses nende protsessidega;

d) õigusnormid turujärelevalve, sealhulgas seire ning käesolevas artiklis osutatud õigusnormide ja nõuete täitmise tagamise kohta.

Artikkel 2

Kohaldamisala

1. Käesolevat määrust kohaldatakse turul kättesaadavaks tehtud digielemente sisaldavate toodete suhtes, mille sihtotstarve või mõistlikult prognoositav kasutamine hõlmab otsest või kaudset loogilist või füüsilist ühendust seadme või võrguga andmeside eesmärgil.

2. Käesolevat määrust ei kohaldata digielemente sisaldavate toodete suhtes, mille suhtes kohaldatakse järgmisi liidu õigusakte:

   a) määrus (EL) 2017/745;

   b) määrus (EL) 2017/746;

   c) määrus (EL) 2019/2144.

3. Käesolevat määrust ei kohaldata digielemente sisaldavate toodete suhtes, mis on sertifitseeritud vastavalt määrusele (EL) 2018/1139.

4. Käesolevat määrust ei kohaldata seadmete suhtes, mis kuuluvad Euroopa Parlamendi ja nõukogu direktiivi 2014/90/EL[35] kohaldamisalasse.

---

[35] Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta direktiiv 2014/90/EL, milles käsitletakse laevavarustust ja millega tunnistatakse kehtetuks nõukogu direktiiv 96/98/EÜ (ELT L 257, 28.8.2014, lk 146).

5. Käesoleva määruse kohaldamist digielemente sisaldavate toodete suhtes, mis kuuluvad ka muude selliste liidu õigusnormide kohaldamisalasse, millega on kehtestatud nõuded, mis käsitlevad kõiki I lisas sätestatud oluliste küberturvalisuse nõuetega hõlmatud riske või mõnda neist, võib piirata või selle välistada, kui:

   a) piiramine või välistamine on kooskõlas nende toodete suhtes kohaldatava üldise õigusraamistikuga ning

   b) valdkondlike normidega saavutatakse samasugune või kõrgem kaitsetase kui käesoleva määrusega.

   Komisjonil on õigus võtta kooskõlas artikliga 61 vastu delegeeritud õigusakte, et täiendada käesolevat määrust ja täpsustada asjakohasel juhul, kas selline piiramine või välistamine on vajalik, milliseid tooteid ja õigusnorme see puudutab ning milline on piirangu ulatus.

6. Käesolevat määrust ei kohaldata varuosade suhtes, mis tehakse turul kättesaadavaks digielemente sisaldavate toodete identsete komponentide asendamiseks ja mis on toodetud samade spetsifikatsioonide kohaselt kui komponendid, mille asendamiseks need on ette nähtud.

7. Käesolevat määrust ei kohaldata digielemente sisaldavate toodete suhtes, mis on välja töötatud või mida on muudetud üksnes riikliku julgeoleku või riigikaitse otstarbel, ega toodete suhtes, mis on spetsiaalselt projekteeritud salastatud teabe töötlemiseks.

8. Käesolevas määruses sätestatud kohustused ei hõlma sellise teabe edastamist, mille avalikustamine oleks vastuolus liikmesriikide oluliste riikliku julgeoleku, avaliku julgeoleku või riigikaitse huvidega.

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „digielemente sisaldav toode“ – tarkvara- või riistvaratoode ja selle andmete kaugtöötluslahendused, kaasa arvatud tarkvara- ja riistvarakomponendid, mis lastakse turule eraldi;

2) „andmete kaugtöötlus“ – andmetöötlus, mis toimub distantsilt ja mille jaoks tootja on projekteerinud ja välja töötanud tarkvara või mille jaoks on selline tarkvara projekteeritud ja välja töötatud tootja vastutusel ning mille puudumine ei laseks digielemente sisaldaval tootel täita üht oma funktsiooni;

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

4) „tarkvara“ – elektroonilise infosüsteemi osa, mis koosneb arvutikoodist;

5) „riistvara“ – füüsiline elektrooniline infosüsteem või selle osa, mis suudab digitaalandmeid töödelda, talletada või edastada;

6) „komponent“ – tarkvara või riistvara, mis on ette nähtud integreerimiseks elektroonilisse infosüsteemi;

7) „elektrooniline infosüsteem“ – süsteem, sealhulgas elektri- või elektroonikaseade, mis suudab töödelda, talletada või edastada digitaalandmeid;

8) „loogiline ühendus“ – tarkvaraliidese kaudu teostatav andmesideühenduse virtuaalesitus;

9) „füüsiline ühendus“ – elektrooniliste infosüsteemide või komponentidevaheline ühendus, mis realiseeritakse füüsiliste vahenditega, muu hulgas elektrilise, optilise või mehaanilise liidese, traadi või raadiolainete kaudu;

10) „kaudne ühendus“ – selline ühendus seadme või võrguga, mis ei toimu otse, vaid sellise seadme või võrguga otse ühendatava suurema süsteemi raames;

11) „lõppseade“ – seade, mis on võrku ühendatud ja toimib selle võrgu sisendpunktina;

12) „ettevõtja“ – tootja, volitatud esindaja, importija, turustaja või muu füüsiline või juriidiline isik, kes peab kooskõlas käesoleva määrusega täitma kohustusi, mis on seotud digielemente sisaldava toote tootmisega või digielemente sisaldava toote turul kättesaadavaks tegemisega;

13) „tootja“ – füüsiline või juriidiline isik, kes arendab või toodab digielemente sisaldavat toodet või kes laseb digielemente sisaldavat toodet projekteerida, arendada või toota ja turustab seda tasu eest, tulu teenimise eesmärgil või tasuta oma nime või kaubamärgi all;

14) „avatud lähtekoodiga tarkvara korraldaja“ – juriidiline isik, kes ei ole tootja ja kelle eesmärk on süstemaatiliselt ja püsivalt toetada selliste teatavate digielemente sisaldavate toodete arendamist, mis kvalifitseeruvad vabaks ja avatud lähtekoodiga tarkvaraks ning on ette nähtud kaubandustegevuseks, ning kes tagab nende toodete elujõulisuse;

15) „volitatud esindaja“ – liidus asuv füüsiline või juriidiline isik, kes on saanud tootjalt kirjaliku volituse tegutseda tema nimel seoses kindlaksmääratud ülesannetega;

16) „importija“ – liidus asuv füüsiline või juriidiline isik, kes laseb turule väljaspool liitu asuva füüsilise või juriidilise isiku nime või kaubamärki kandva digielemente sisaldava toote;

17) „turustaja“ – tarneahelas osalev füüsiline või juriidiline isik, kes ei ole tootja ega importija ja kes teeb digielemente sisaldava toote liidu turul kättesaadavaks ilma toote omadusi mõjutamata;

18) „tarbija“ – füüsiline isik, kes tegutseb eesmärgil, mis ei ole seotud tema kaubandus-, majandus-, ametialase või kutsetegevusega;

19) „mikro-, väikesed ja keskmise suurusega ettevõtjad“ – komisjoni soovituse 2003/361/EÜ lisas määratletud mikro-, väikesed ja keskmise suurusega ettevõtjad;

20) „toe kestus“ – ajavahemik, mille ajal tootja peab tagama digielemente sisaldava toote nõrkuste tulemusliku käsitlemise kooskõlas I lisa II osas sätestatud oluliste küberturvalisuse nõuetega;

21) „turule laskmine“ – digielemente sisaldava toote esmakordne liidu turul kättesaadavaks tegemine;

22) „turul kättesaadavaks tegemine“ – kaubandustegevuse käigus digielemente sisaldava toote tasu eest või tasuta tarnimine liidu turule kas turustamiseks või kasutamiseks;

23) „sihtotstarve“ – kasutamine, kaasa arvatud kasutamise konkreetne kontekst ja tingimused, mille jaoks tootja on digielemente sisaldava toote kasutusjuhendis, reklaam- või müügimaterjalides või avaldustes ning tehnilises dokumentatsioonis esitatud teabe kohaselt ette näinud;

24) „mõistlikult prognoositav kasutamine“ – kasutamine, mis ei toimu ilmtingimata tootja poolt kasutusjuhendis, reklaam- või müügimaterjalides või avaldustes ning tehnilises dokumentatsioonis ette nähtud sihtotstarbel, kuid mis võib tõenäoliselt tuleneda mõistlikult prognoositavast inimkäitumisest või tehnilisest toimingust või interaktsioonist;

25) „mõistlikult prognoositav väärkasutamine“ – digielemente sisaldava toote kasutamine viisil, mis ei ole kooskõlas selle sihtotstarbega, kuid mis võib tuleneda mõistlikult prognoositavast inimkäitumisest või interaktsioonist muude süsteemidega;

26) „teavitav asutus“ – riigi ametiasutus, kes vastutab vastavushindamisasutuste hindamise, määramise ja neist teada andmise ning nende järelevalve jaoks vajalike menetluste väljatöötamise ja läbiviimise eest;

27) „vastavushindamine“ – protsess, mille käigus kontrollitakse, kas I lisas sätestatud olulised küberturvalisuse nõuded on täidetud;

28) „vastavushindamisasutus“ – määruse (EÜ) nr 765/2008 artikli 2 punktis 13 määratletud vastavushindamisasutus;

29) „teada antud asutus“ – artikli 43 ja liidu asjakohaste ühtlustamisõigusaktide kohaselt määratud vastavushindamisasutus;

30) „oluline muudatus“ – digielemente sisaldavas tootes pärast selle turule laskmist tehtud muudatus, mis mõjutab digielemente sisaldava toote vastavust I lisa I osas sätestatud olulistele nõuetele või mille tõttu muutub sihtotstarve, mida silmas pidades on digielemente sisaldavat toodet hinnatud;

31) „CE-vastavusmärgis“ – märgis, millega tootja annab teada, et digielemente sisaldav toode ja tootja rakendatud protsessid vastavad I lisas ja kohaldatavates liidu ühtlustamisõigusaktides sätestatud märgise paigaldamist käsitlevatele olulistele küberturvalisuse nõuetele;

32) „liidu ühtlustamisõigusaktid“ – määruse (EL) 2019/1020 I lisas loetletud liidu õigusaktid ja muud liidu õigusaktid, millega ühtlustatakse nende toodete turustamise tingimusi, mille suhtes nimetatud määrust kohaldatakse;

33) „turujärelevalveasutus“ – määruse (EL) 2019/1020 artikli 3 punktis 4 määratletud turujärelevalveasutus;

34) „rahvusvaheline standard“ – määruse (EL) nr 1025/2012 artikli 2 punkti 1 alapunktis a määratletud rahvusvaheline standard;

35) „Euroopa standard“ – määruse (EL) nr 1025/2012 artikli 2 punkti 1 alapunktis b määratletud Euroopa standard;

36) „harmoneeritud standard“ – määruse (EL) nr 1025/2012 artikli 2 punkti 1 alapunktis c määratletud harmoneeritud standard;

37) „küberrisk“ – intsidendist tingitud kahju või häire võimalus, mida väljendatakse sellise kahju või häire ulatust ja intsidendi esinemise tõenäosust kajastava kombineeritud näitajana;

38) „oluline küberrisk“ – küberrisk, mille tehniliste omaduste põhjal võib eeldada suurt tõenäosust sellise intsidendi tekkeks, mis võib põhjustada tõsist negatiivset mõju, muu hulgas olulist varalist või mittevaralist kahju või häiret;

39) „tarkvara koostenimekiri“ – ametlik kirje, milles esitatakse digielemente sisaldava toote tarkvaraelementides sisalduvate komponentide üksikasjad ja tarneahela seosed;

40) „nõrkus“ – digielemente sisaldava toote nõrkus, tundlikkus või viga, mida küberohu tekitaja võib ära kasutada;

41) „ärakasutatav nõrkus“ – nõrkus, mida vastaspool võib praktilistes käitamistingimustes tulemuslikult ära kasutada;

42) „aktiivselt ärakasutatav nõrkus“ – nõrkus, mille kohta on usaldusväärseid tõendeid, et kuritahtlik isik on seda süsteemi omaniku loata süsteemis ära kasutanud;

43) „intsident“ – direktiivi (EL) 2022/2555 artikli 6 punktis 6 määratletud intsident;

44) „digielemente sisaldava toote turvalisust mõjutav intsident“ – intsident, mis mõjutab või võib mõjutada negatiivselt digielemente sisaldava toote võimet kaitsta andmete või funktsioonide kättesaadavust, autentsust, terviklust või konfidentsiaalsust;

45) „intsidendioht“ – direktiivi (EL) 2022/2555 artikli 6 punktis 5 määratletud intsidendioht;

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

47) „isikuandmed“ – määruse (EL) 2016/679 artikli 4 punktis 1 määratletud isikuandmed;

48) „vaba ja avatud lähtekoodiga tarkvara“ – tarkvara, mille lähtekoodi jagatakse avalikult ja mis tehakse kättesaadavaks vaba ja avatud lähtekoodi litsentsi alusel, mis annab kõik õigused teha see vabalt kättesaadavaks, kasutatavaks, muudetavaks ja turustatavaks;

49) „tagasivõtmine“ – määruse (EL) 2019/1020 artikli 3 punktis 22 määratletud tagasivõtmine;

50) „turult kõrvaldamine“ – määruse (EL) 2019/1020 artikli 3 punktis 23 määratletud turult kõrvaldamine;

51) „koordinaatoriks määratud CSIRT“ – direktiivi (EL) 2022/2555 artikli 12 lõike 1 kohaselt koordinaatoriks määratud CSIRT.

Artikkel 4

Vaba liikumine

1. Liikmesriigid ei takista käesoleva määrusega hõlmatud küsimustes käesoleva määruse nõuetele vastavate digielemente sisaldavate toodete turul kättesaadavaks tegemist.

2. Liikmesriigid ei takista käesolevale määrusele mittevastavate digielemente sisaldavate toodete, sealhulgas selle prototüüpide esitlemist ega kasutamist messidel, näitustel ja esitlustel või muudel samalaadsetel üritustel, kui toodet esitletakse nähtava sildiga, millel on selgelt märgitud, et see ei vasta käesolevale määrusele ning seda ei tehta turul kättesaadavaks enne, kui see sellele vastab.

3. Liikmesriigid ei takista käesolevale määrusele mittevastava poolelioleva tarkvara turul kättesaadavaks tegemist, kui tarkvara tehakse kättesaadavaks üksnes testimiseks vajaliku piiratud aja jooksul ning tootel nähtaval sildil on selgelt märgitud, et tarkvara ei vasta käesolevale määrusele ega ole turul kättesaadav muul eesmärgil kui testimiseks.

4. Lõiget 3 ei kohaldata ohutusseadiste suhtes, millele on osutatud muudes liidu ühtlustamisõigusaktides kui käesolev määrus.

Artikkel 5

Digielemente sisaldavate toodete hankimine ja kasutamine

1. Käesoleva määrusega ei takistata liikmesriike kehtestamast digielemente sisaldavate toodete suhtes täiendavaid küberturvalisuse nõudeid nende toodete hankimiseks või kasutamiseks teatavatel eesmärkidel, sealhulgas juhul, kui neid tooteid hangitakse või kasutatakse riikliku julgeoleku või riigikaitse eesmärgil, tingimusel, et need nõuded on kooskõlas liidu õiguses sätestatud liikmesriikide kohustustega ning on nende eesmärkide saavutamiseks vajalikud ja proportsionaalsed.

2. Ilma et see piiraks direktiivide 2014/24/EL ja 2014/25/EL kohaldamist, tagavad liikmesriigid käesoleva määruse kohaldamisalasse kuuluvate digielemente sisaldavate toodete hankimisel, et hankemenetluses võetakse arvesse vastavust käesoleva määruse I lisas sätestatud olulistele küberturvalisuse nõuetele, sealhulgas tootja suutlikkust nõrkusi tulemuslikult käsitleda.

Artikkel 6

Digielemente sisaldavate toodete suhtes kehtivad nõuded

Digielemente sisaldavad tooted tehakse turul kättesaadavaks üksnes juhul, kui:

a) need vastavad I lisa I osas sätestatud olulistele küberturvalisuse nõuetele, tingimusel et nad on nõuetekohaselt paigaldatud ja hooldatud, neid kasutatakse sihtotstarbeliselt või tingimustes, mida võib mõistlikult prognoosida, ja neile on paigaldatud vajalikud turvauuendused, kui see on kohaldatav, ning

b) tootja rakendatud protsessid vastavad I lisa II osas sätestatud olulistele küberturvalisuse nõuetele.

Artikkel 7

Digielemente sisaldavad olulised tooted

1. Digielemente sisaldavaid tooteid, millel on mõne III lisas sätestatud tootekategooria põhifunktsioon, käsitatakse digielemente sisaldavate oluliste toodetena ning nende suhtes kohaldatakse artikli 32 lõigetes 2 ja 3 osutatud vastavushindamismenetlusi. Kui tootesse integreeritakse digielemente sisaldav toode, millel on mõne III lisas sätestatud tootekategooria põhifunktsioon, ei tähenda see iseenesest, et selle toote suhtes tuleb kohaldada artikli 32 lõigetes 2 ja 3 osutatud vastavushindamismenetlusi.

2. Käesoleva artikli lõikes 1 osutatud digielemente sisaldavate toodete kategooriad, mis on jaotatud I ja II klassi vastavalt III lisale, vastavad vähemalt ühele järgmistest kriteeriumidest:

a) digielemente sisaldav toode täidab peamiselt funktsioone, mis on kriitilise tähtsusega muude toodete, võrkude või teenuste küberturvalisuse seisukohast, sealhulgas autentimise ja juurdepääsu, sissetungitõrje ja -tuvastuse, lõppseadme turvalisuse või võrgu kaitsmise tagamine;

b) digielemente sisaldav toode täidab funktsiooni, millega kaasneb märkimisväärne kahjuliku mõju risk seoses selle intensiivsuse ja võimega häirida, kontrollida või kahjustada suurt hulka muid tooteid või kasutajate tervist, turvalisust või ohutust otsese manipuleerimise teel, näiteks kesksüsteemi funktsiooni, sealhulgas võrguhaldus, konfiguratsiooni kontroll, virtualiseerimine või isikuandmete töötlemine.

3. Komisjonil on õigus võtta kooskõlas artikliga 61 vastu delegeeritud õigusakte, et muuta III lisa ning lisada digielemente sisaldavate toodete kategooriate mõlema klassi loetellu uus kategooria ja see määratleda, viia kategooriaid üle ühest klassist teise või jätta olemasolev kategooria sellest loetelust välja. III lisas sätestatud loetelu muutmise vajadust hinnates võtab komisjon arvesse küberturvalisusega seotud funktsioone või digielemente sisaldavast tootest tuleneva küberriski funktsiooni ja taset, nagu on sätestatud käesoleva artikli lõikes 2 osutatud kriteeriumides.

Käesoleva lõike esimeses lõigus osutatud delegeeritud õigusaktidega nähakse asjakohasel juhul ette vähemalt 12-kuuline üleminekuperiood, enne kui hakatakse kohaldama artikli 32 lõigetes 2 ja 3 osutatud asjakohaseid vastavushindamismenetlusi, eelkõige juhul, kui III lisas sätestatud I või II klassi lisatakse uus digielemente sisaldavate oluliste toodete kategooria või kui mõni kategooria viiakse I klassist üle II klassi, välja arvatud juhul, kui lühem üleminekuperiood on põhjendatud tungiva kiireloomulisuse tõttu.

4. Komisjon võtab hiljemalt … [12 kuud pärast käesoleva määruse jõustumise kuupäeva] vastu rakendusakti, milles määratakse kindlaks III lisas sätestatud I ja II klassi digielemente sisaldavate toodete kategooriate tehniline kirjeldus ning IV lisas sätestatud digielemente sisaldavate toodete kategooriate tehniline kirjeldus. Nimetatud rakendusakt võetakse vastu kooskõlas artikli 62 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 8

Digielemente sisaldavad kriitilise tähtsusega tooted

1. Komisjonil on õigus võtta kooskõlas artikliga 61 vastu delegeeritud õigusakte, et täiendada käesolevat määrust ja määrata kindlaks, milliste digielemente sisaldavate toodete puhul, millel on mõne käesoleva määruse IV lisas sätestatud tootekategooria põhifunktsioon, on määruse (EL) 2019/881 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava alusel nõutav vähemalt märkimisväärsele usaldusväärsuse tasemele osutav Euroopa küberturvalisuse sertifikaat, et tõendada vastavust käesoleva määruse I lisas sätestatud olulistele küberturvalisuse nõuetele või osale neist, kui neid digielemente sisaldavate toodete kategooriaid hõlmav Euroopa küberturvalisuse sertifitseerimise kava on vastu võetud määruse (EL) 2019/881 kohaselt ja see on tootjatele kättesaadav. Kõnealustes delegeeritud õigusaktides määratakse kindlaks nõutav usaldusväärsuse tase, mis on proportsionaalne digielemente sisaldava toodetega seotud küberriski tasemega ning mille puhul võetakse arvesse nende sihtotstarvet, sealhulgas direktiivi (EL) 2022/2555 artikli 3 lõikes 1 osutatud elutähtsate üksuste kriitilise tähtsusega sõltuvust nendest.

   Enne kõnealuste delegeeritud õigusaktide vastuvõtmist hindab komisjon kavandatud meetmete võimalikku turumõju ja konsulteerib asjaomaste sidusrühmadega, sealhulgas määruse (EL) 2019/881 kohaselt moodustatud Euroopa küberturvalisuse sertifitseerimise rühmaga. Hindamisel võetakse arvesse liikmesriikide valmisolekut ja suutlikkust asjakohase Euroopa küberturvalisuse sertifitseerimise kava rakendamiseks. Kui käesoleva lõike esimeses lõigus osutatud delegeeritud õigusakte ei ole vastu võetud, kohaldatakse digielemente sisaldavate toodete suhtes, millel on mõne IV lisas sätestatud tootekategooria põhifunktsioon, artikli 32 lõikes 3 osutatud vastavushindamismenetlusi.

Esimeses lõigus osutatud delegeeritud õigusaktides nähakse nende kohaldamiseks ette vähemalt kuuekuuline üleminekuperiood, välja arvatud juhul, kui lühem üleminekuperiood on põhjendatud tungiva kiireloomulisuse tõttu.

2. Komisjonil on õigus võtta kooskõlas artikliga 61 vastu delegeeritud õigusakte, et muuta IV lisa ja lisada või jätta välja digielemente sisaldavate kriitilise tähtsusega toodete kategooriaid. Digielemente sisaldavate kriitilise tähtsusega toodete kategooriate ja nõutava usaldusväärsuse taseme kindlaksmääramisel kooskõlas käesoleva artikli lõikega 1 võtab komisjon arvesse artikli 7 lõikes 2 osutatud kriteeriume ja tagab, et digielemente sisaldavate toodete kategooriad vastavad vähemalt ühele järgmistest kriteeriumidest:

a) direktiivi (EL) 2022/2555 artiklis 3 osutatud elutähtsad üksustel on kriitilise tähtsusega sõltuvus asjakohasesse kategooriasse kuuluvatest digielemente sisaldavatest toodetest;

b) asjakohase kategooria digielemente sisaldavate toodetega seotud intsidendid ja ärakasutatavad nõrkused võivad põhjustada tõsiseid häireid kriitilise tähtsusega tarneahelates kogu siseturul.

Enne delegeeritud õigusaktide vastuvõtmist viib komisjon läbi lõikes 1 osutatud liiki hindamise.

Esimeses lõigus osutatud delegeeritud õigusaktides nähakse ette vähemalt kuuekuuline üleminekuperiood, välja arvatud juhul, kui lühem üleminekuperiood on põhjendatud tungiva kiireloomulisuse tõttu.

Artikkel 9

Sidusrühmadega konsulteerimine

1. Käesoleva määruse rakendamise meetmete ettevalmistamisel konsulteerib komisjon asjaomaste sidusrühmadega, näiteks asjaomaste liikmesriikide ametiasutuste, erasektori ettevõtjate, sealhulgas mikro- ning väikeste ja keskmise suurusega ettevõtjate, avatud lähtekoodiga tarkvara kogukonna, tarbijaühenduste, akadeemiliste ringkondade, asjaomaste liidu asutuste ja organite ning liidu tasandil loodud eksperdirühmadega, ning võtab arvesse nende seisukohti. Eelkõige konsulteerib komisjon asjakohasel juhul struktureeritud viisil kõnealuste sidusrühmadega ja küsib nende arvamust järgmistel juhtudel:

   a) artiklis 26 osutatud suuniste koostamisel;

   b) III lisas sätestatud tootekategooriate tehniliste kirjelduste koostamisel kooskõlas artikli 7 lõikega 4, hinnates vajadust tootekategooriate loetelu võimaliku ajakohastamise järele vastavalt artikli 7 lõikele 3 ja artikli 8 lõikele 2, või viies läbi artikli 8 lõikes 1 osutatud võimaliku turumõju hindamise, ilma et see piiraks artikli 61 kohaldamist;

   c) käesoleva määruse hindamiseks ja läbivaatamiseks ettevalmistuste tegemisel.

2. Komisjon korraldab korrapäraselt,vähemalt kord aastas konsultatsioone ja teabeüritusi, et koguda lõikes 1 osutatud sidusrühmade seisukohti käesoleva määruse rakendamise kohta.

Artikkel 10

Oskuste parandamine küberkerkses digikeskkonnas

Käesoleva määruse kohaldamisel ja selleks, et reageerida spetsialistide vajadustele käesoleva määruse rakendamise toetamiseks, edendavad liikmesriigid asjakohasel juhul komisjoni, küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse ja ENISA toetusel, järgides täielikult liikmesriikide kohustusi hariduse valdkonnas, meetmeid ja strateegiaid, mille eesmärk on:

a) arendada küberturvalisuse alaseid oskusi ning luua korralduslikud ja tehnoloogilised vahendid, et tagada kvalifitseeritud spetsialistide piisav kättesaadavus turujärelevalveasutuste ja vastavushindamisasutuste tegevuse toetamiseks;

b) suurendada koostööd erasektori, ettevõtjate (sealhulgas tootjate töötajate ümber- või täiendusõppe kaudu), tarbijate, koolitajate ning haldusasutuste vahel, suurendades seeläbi noorte võimalusi asuda tööle küberturvalisuse sektoris.

Artikkel 11

Üldine tooteohutus

Erandina määruse (EL) 2023/988 artikli 2 lõike 1 kolmanda lõigu punktist b kohaldatakse digielemente sisaldavate toodete suhtes seoses aspektide ja riskide või riskikategooriatega, mida käesolev määrus ei hõlma, kõnealuse määruse III peatüki 1. jagu ning V ja VII ning IX–XI peatükki, kui nende toodete suhtes ei kohaldata määruse (EL) 2023/988 artikli 3 punktis 27 määratletud muudes liidu ühtlustamisõigusaktides sätestatud spetsiifilisi ohutusnõudeid.

Artikkel 12

Suure riskiga tehisintellektisüsteemid

1. Ilma et see piiraks määruse (EL) 2024/1689 artiklis 15 sätestatud täpsust ja stabiilsust käsitlevate nõuete kohaldamist, loetakse digielemente sisaldavad tooted, mis kuuluvad käesoleva määruse kohaldamisalasse ja mis on liigitatud kõnealuse määruse artikli 6 kohaselt suure riskiga tehisintellektisüsteemideks, kõnealuse määruse artiklis 15 sätestatud küberturvalisuse nõuetele vastavaks, kui:

   a) kõnealused tooted vastavad I lisa I osas sätestatud olulistele küberturvalisuse nõuetele;

b) tootja rakendatud protsessid vastavad I lisa II osas sätestatud olulistele küberturvalisuse nõuetele ning

c) määruse (EL) 2024/1689 artikli [artikkel 15] kohaselt nõutava küberturvalisuse kaitse taseme saavutamist tõendab käesoleva määruse alusel välja antud ELi vastavusdeklaratsioon.

2. Käesoleva artikli lõikes 1 osutatud digielemente sisaldavate toodete ja küberturvalisuse nõuete suhtes kohaldatakse määruse (EL) 2024/1689 artiklis 43 ette nähtud vastavushindamismenetlust. Teada antud asutused, kelle pädevuses on kontrollida suure riskiga tehisintellektisüsteemide vastavust määrusele (EL) 2024/1689, on sellise hindamise käigus ühtlasi pädevad kontrollima, kas käesoleva määruse kohaldamisalasse kuuluvad suure riskiga tehisintellektisüsteemid vastavad käesoleva määruse I lisa nõuetele, tingimusel et nende teada antud asutuste vastavust käesoleva määruse artikli 39 nõuetele on hinnatud määruse (EL) 2024/1689 kohase teavitamise korra raames.

3. Erandina käesoleva artikli lõikest 2 kohaldatakse käesoleva määruse III lisas loetletud digielemente sisaldavate oluliste toodete suhtes, millele kohaldatakse käesoleva määruse artikli 32 lõike 2 punktides a ja b ning artikli 32 lõikes 3 osutatud vastavushindamismenetlusi, ning käesoleva määruse IV lisas loetletud digielemente sisaldavate kriitilise tähtsusega toodete suhtes, mille suhtes on kooskõlas käesoleva määruse artikli 8 lõikega 1 nõutav Euroopa küberturvalisuse sertifikaat või millele selle puudumisel kohaldatakse käesoleva määruse artikli 32 lõikes 3 osutatud vastavushindamismenetlusi ning mis on vastavalt määruse (EL) 2024/1689 artiklile 6 liigitatud suure riskiga tehisintellektisüsteemideks ja mille suhtes kohaldatakse määruse (EL) 2024/1689 IV lisas osutatud sisekontrollil põhinevat vastavushindamismenetlust, käesolevas määruses sätestatud vastavushindamismenetlusi, kui tegemist on käesoleva määruse oluliste küberturvalisuse nõuetega.

4. Käesoleva artikli lõikes 1 osutatud digielemente sisaldavate toodete tootjad võivad osaleda määruse (EL) 2024/1689 artiklis 57 osutatud tehisintellekti regulatiivliivakastides.

II peatükk
Ettevõtjate kohustused ning vaba ja avatud lähtekoodiga tarkvara käsitlevad normid

Artikkel 13

Tootjate kohustused

1. Tootja tagab digielemente sisaldava toote turule laskmisel, et see on projekteeritud, arendatud ja toodetud vastavalt I lisa I osas sätestatud olulistele küberturvalisuse nõuetele.

2. Lõikes 1 sätestatud kohustuse täitmiseks hindab tootja digielemente sisaldava tootega seotud küberriske ja võtab hindamise tulemusi arvesse digielemente sisaldava toote kavandamis-, projekteerimis-, arendus-, tootmis-, tarne- ja hooldusetapis, et minimeerida küberriske, ennetada intsidente ja minimeerida nende mõju, sealhulgas seoses kasutajate tervise ja ohutusega.

3. Küberriskide hindamine dokumenteeritakse ja seda ajakohastatakse asjakohasel juhul toe kestuse ajal, mis määratakse kindlaks kooskõlas käesoleva artikli lõikega 8. Küberriskide hindamine hõlmab vähemalt küberriskide analüüsi, mille aluseks on digielemente sisaldava toote sihtotstarve ja mõistlikult prognoositav kasutamine, aga ka kasutustingimused, näiteks kasutuskeskkond või kaitstavad varad, võttes arvesse toote eeldatavat kasutusaega. Küberriskide hindamisel märgitakse, kas ja millisel viisil kohaldatakse asjakohase digielemente sisaldava toote suhtes I lisa I osa punktis 2 sätestatud turvanõudeid ning kuidas neid nõudeid rakendatakse, arvestades küberriskide hindamises esitatud teavet. Samuti märgitakse, kuidas tootja kohaldab I lisa I osa punkti 1 ja I lisa II osas sätestatud nõrkuste käsitlemise nõudeid.

4. Digielemente sisaldava toote turule laskmisel lisab tootja käesoleva artikli lõikes 3 osutatud küberriskide hindamise artikli 31 ja VII lisa kohaselt nõutavasse tehnilisse dokumentatsiooni. Artiklis 12 osutatud digielemente sisaldavate toodete puhul, mille suhtes kohaldatakse ka muid liidu õigusakte, võib küberriskide hindamine olla osa nende liidu õigusaktidega nõutavast riskihindamisest. Kui digielemente sisaldava toote suhtes ei ole teatavad olulised küberturvalisuse nõuded kohaldatavad, lisab tootja kõnealusesse tehnilisse dokumentatsiooni selge põhjenduse.

5. Lõikes 1 sätestatud kohustuse täitmiseks peab tootja täitma kolmandatelt isikutelt hangitud komponentide integreerimisel hoolsuskohustust, et need komponendid ei ohustaks digielemente sisaldava toote küberturvalisust, kaasa arvatud juhul, kui integreeritakse vaba ja avatud lähtekoodiga tarkvara komponente, mida ei ole kaubandustegevuse käigus turul kättesaadavaks tehtud.

6. Digielemente sisaldavasse tootesse integreeritud komponendi, sealhulgas avatud lähtekoodiga komponendi nõrkuse avastamisel teatab tootja sellest komponenti tootvale või hooldavale isikule või üksusele ning tegeleb nõrkusega ja kõrvaldab selle kooskõlas I lisa II osas sätestatud nõrkuste käsitlemise nõuetega. Kui tootja on komponendi nõrkusega tegelemiseks välja töötanud tarkvara või riistvara muudatuse, jagab ta asjakohast koodi või dokumentatsiooni komponenti tootva või hooldava isiku või üksusega, tehes seda asjakohasel juhul masinloetavas vormingus.

7. Tootja dokumenteerib süstemaatiliselt ning toote olemuse ja küberriskidega proportsionaalsel viisil digielemente sisaldava toote asjakohased küberturvalisuse aspektid, sealhulgas nõrkused, millest ta on teada saanud, ja kolmandatelt isikutelt saadud asjakohase teabe, ning ajakohastab toote küberriskide hindamist, kui see on kohaldatav.

8. Tootja tagab digielemente sisaldava toote turule laskmisel ja toe kestuse ajal, et kõnealuse toote, sealhulgas selle komponentide nõrkusi käsitletakse tulemuslikult ja kooskõlas I lisa II osas sätestatud oluliste küberturvalisuse nõuetega.

Tootja määrab toe kestuse kindlaks nii, et see kajastaks ajavahemikku, mil toodet eeldatavasti kasutatakse, võttes eelkõige arvesse kasutajate mõistlikke ootusi, toote olemust, sealhulgas selle sihtotstarvet, ning asjakohaseid liidu õigusnorme, millega määratakse kindlaks digielemente sisaldavate toodete kasutusiga. Toe kestuse kindlaksmääramisel võivad tootjad võtta arvesse ka teiste tootjate poolt turule lastud sarnase funktsiooniga digielemente sisaldavate toodete toe kestust, kasutuskeskkonna kättesaadavust, põhifunktsioone täitvate ja kolmandatelt isikutelt hangitud integreeritud komponentide toe kestust ning artikli 52 lõike 15 kohaselt loodud spetsiaalse halduskoostöörühma (ADCO rühm) ja komisjoni antud asjakohaseid suuniseid. Toe kestuse kindlaksmääramisel arvessevõetavaid asjaolusid kaalutakse viisil, mis tagab proportsionaalsuse.

Ilma et see piiraks teise lõigu kohaldamist, on toe kestus vähemalt viis aastat. Kui digielemente sisaldavat toodet kasutatakse eeldatavasti vähem kui viis aastat, vastab toe kestus eeldatavale kasutusajale.

Võttes arvesse artikli 52 lõikes 16 osutatud ADCO rühma soovitusi, võib komisjon võtta kooskõlas artikliga 61 vastu delegeeritud õigusakte, et täiendada käesolevat määrust ja määrata kindlaks minimaalne toe kestus spetsiifiliste tootekategooriate puhul, kui turujärelevalve andmete kohaselt on toe kestus ebapiisav.

Tootja lisab VII lisas sätestatud tehnilisse dokumentatsiooni teabe, mida võeti arvesse digielemente sisaldava toote toe kestuse kindlaksmääramisel.

Tootjal peavad olema kehtestatud asjakohased põhimõtted ja kord, sealhulgas I lisa II osa punktis 5 osutatud nõrkuste koordineeritud avalikustamise põhimõtted, et käsitleda ja kõrvaldada digielemente sisaldava toote võimalikke sisemiste või väliste allikate teatatud nõrkusi.

9. Tootja tagab, et kõik I lisa II osa punktis 8 osutatud turvauuendused, mis on kasutajatele toe kestuse ajal kättesaadavaks tehtud, jäävad pärast nende väljastamist kättesaadavaks vähemalt kümme aastat või ülejäänud toe kestuse ajal, olenevalt sellest, kumb on pikem.

10. Kui tootja on turule lasknud tarkvaratoote hilisemad oluliselt muudetud versioonid, võib ta tagada vastavuse I lisa II osa punktis 2 sätestatud olulisele küberturvalisuse nõudele ainult selle versiooni puhul, mille tootja viimati turule laskis, kui varem turule lastud versioonide kasutajatel on tasuta juurdepääs viimasele turule lastud versioonile ja neile ei teki lisakulusid seoses riist- ja tarkvarakeskkonna kohandamisega, kus nad toote algversiooni kasutavad.

11. Tootja võib pidada avalikke tarkvaraarhiive, et kasutajatel oleks parem juurdepääs varasematele versioonidele. Sellistel juhtudel teavitatakse kasutajaid selgelt ja kergesti kättesaadaval viisil riskidest, mis kaasnevad sellise tarkvara kasutamisega, millele tuge ei pakuta.

12. Enne digielemente sisaldava toote turule laskmist koostab tootja artiklis 31 osutatud tehnilise dokumentatsiooni.

    Tootja teeb või laseb teha artiklis 32 osutatud vajalikud vastavushindamismenetlused.

    Kui vastavushindamismenetluse käigus tõendatakse, et digielemente sisaldav toode vastab I lisa I osas sätestatud olulistele küberturvalisuse nõuetele ja tootja rakendatud protsessid vastavad I lisa II osas sätestatud olulistele küberturvalisuse nõuetele, koostab tootja artikli 28 kohase ELi vastavusdeklaratsiooni ja kinnitab tootele artikli 30 kohaselt CE-vastavusmärgise.

13. Tootja hoiab tehnilist dokumentatsiooni ja ELi vastavusdeklaratsiooni turujärelevalveasutustele esitamiseks alles vähemalt kümme aastat alates digielemente sisaldava toote turule laskmisest või toe kestuse ajal, olenevalt sellest, kumb on pikem.

14. Tootja tagab, et on kehtestatud kord, mille kohaselt seeriatoodanguna toodetav digielemente sisaldav toode vastab ka hilisemas etapis käesoleva määruse nõuetele. Tootja võtab nõuetekohaselt arvesse muudatusi arendus- ja tootmisprotsessis või digielemente sisaldava toote konstruktsioonis või omadustes ning muudatusi harmoneeritud standardites, Euroopa küberturvalisuse sertifitseerimise kavades või artiklis 27 osutatud ühtses spetsifikatsioonis, mille alusel digielemente sisaldava toote vastavust nõuetele deklareeritakse või kontrollitakse.

15. Tootja tagab, et tema digielemente sisaldavale tootele on kantud tüübi-, partii- või seerianumber või muu märge, mille alusel saab toodet tuvastada, või kui see ei ole võimalik, siis tagab, et see teave esitatakse pakendil või digielemente sisaldava tootega kaasas olevas dokumendis.

16. Tootja märgib digielemente sisaldavale tootele, selle pakendile või sellega kaasas olevasse dokumenti oma nime, registreeritud kaubanime või registreeritud kaubamärgi ja postiaadressi, e-posti aadressi või muud digitaalsed kontaktandmed, ja kui see on kohaldatav, veebisaidi, mille kaudu tootjaga saab ühendust võtta. See teave peab olema esitatud ka II lisas esitatud kasutajale mõeldud teabes ja juhistes. Kontaktandmed esitatakse kasutajale ja turujärelevalveasutustele kergesti arusaadavas keeles.

17. Käesoleva määruse kohaldamisel määrab tootja ühtse kontaktpunkti, mis võimaldab kasutajal temaga otse ja kiiresti suhelda, sealhulgas selleks, et hõlbustada digielemente sisaldava toote nõrkustest teatamist.

    Tootja tagab, et ühtne kontaktpunkt on kasutajatele kergesti tuvastatav. Ta lisab II lisas sätestatud kasutajale mõeldud teabesse ja juhistesse ka ühtse kontaktpunkti andmed.

    Ühtne kontaktpunkt võimaldab kasutajal valida tema eelistatud sidevahendid ega piira selliseid vahendeid automatiseeritud vahenditega.

18. Tootja tagab, et digielemente sisaldava tootega on kaasas II lisas sätestatud kasutajale mõeldud teave ja juhised paberil või elektrooniliselt. See teave ja juhised esitatakse kasutajale ja turujärelevalveasutustele kergesti arusaadavas keeles. Nii juhised kui ka teave peavad olema selged, arusaadavad, loogilised ja loetavad. Need peavad võimaldama digielemente sisaldavat toodet turvaliselt paigaldada, käitada ja kasutada. Tootja hoiab II lisas sätestatud kasutajale mõeldud teavet ja juhiseid kasutajale ja turujärelevalveasutustele kättesaadavana vähemalt kümme aastat alates digielemente sisaldava toote turule laskmisest või toe kestuse ajal, olenevalt sellest, kumb on pikem. Kui teave ja juhised esitatakse veebis, tagab tootja, et need on juurdepääsetavad, kasutusmugavad ja veebis kättesaadavad vähemalt kümme aastat pärast digielemente sisaldava toote turule laskmist või toe kestuse ajal, olenevalt sellest, kumb on pikem.

19. Tootja tagab, et lõikes 8 osutatud toe kestuse lõppkuupäev, sealhulgas vähemalt kuu ja aasta, on ostu ajal, ja kohaldataval juhul digielemente sisaldaval tootel, selle pakendil või digivahendite abil, selgelt ja arusaadavalt kindlaks määratud ning kergesti kättesaadav.

    Kui see on digielemente sisaldava toote olemust arvestades tehniliselt teostatav, kuvab tootja kasutajale teate selle kohta, et tema digielemente sisaldava toote toe kestus on lõppenud.

20. Tootja annab digielemente sisaldava tootega kaasa ELi vastavusdeklaratsiooni koopia või lihtsustatud ELi vastavusdeklaratsiooni. Kui esitatakse lihtsustatud ELi vastavusdeklaratsioon, sisaldab see täpset veebiaadressi, kus on ELi vastavusdeklaratsiooni täistekst.

21. Alates digielemente sisaldava toote turule laskmisest ja toe kestuse ajal võtavad tootjad, kes teavad või kellel on põhjust uskuda, et digielemente sisaldav toode või tootja rakendatud protsessid ei vasta I lisas sätestatud olulistele küberturvalisuse nõuetele, viivitamata parandusmeetmed, mis on vajalikud, et viia digielemente sisaldav toode või tootja protsessid nõuetega vastavusse või asjakohasel juhul toode turult kõrvaldada või tagasi võtta.

22. Turujärelevalveasutuse põhjendatud taotluse korral esitab tootja kõnealusele asutusele sellele kergesti arusaadavas keeles kas paberil või elektrooniliselt kogu teabe ja dokumentatsiooni, mida on vaja digielemente sisaldava toote ning tootja rakendatud protsesside vastavuse tõendamiseks I lisas sätestatud olulistele küberturvalisuse nõuetele. Kui kõnealune asutus seda taotleb, teeb tootja temaga koostööd kõigi meetme korral, mis on võetud tema poolt turule lastud digielemente sisaldavast tootest tulenevate küberriskide kõrvaldamiseks.

23. Tootja, kes lõpetab tegevuse ja ei ole seetõttu võimeline järgima käesolevat määrust, teatab enne tegevuse lõpetamise jõustumist tegevuse eelseisvast lõpetamisest asjaomastele turujärelevalveasutustele ning kättesaadavate vahendite ja võimaluste piires ka asjakohaste turule lastud digielemente sisaldavate toodete kasutajatele.

24. Komisjon võib rakendusaktidega, võttes arvesse Euroopa ja rahvusvahelisi standardeid ning parimaid tavasid, täpsustada I lisa II osa punktis 1 osutatud tarkvara koostenimekirja vormi ja elemente. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 62 lõikes 2 osutatud kontrollimenetlusega.

25. Selleks et hinnata liikmesriikide ja kogu liidu sõltuvust tarkvarakomponentidest ning eelkõige vabaks ja avatud lähtekoodiga tarkvaraks liigitatavatest komponentidest, võib ADCO rühm otsustada teha teatavate digielemente sisaldavate toodete kategooriate kohta kogu liitu hõlmava sõltuvuse hindamise. Selleks võivad turujärelevalveasutused nõuda selliste kategooriate digielemente sisaldavate toodete tootjatelt, et nad esitaksid I lisa II osa punktis 1 osutatud asjakohased tarkvara koostenimekirjad. Kõnealuse teabe põhjal võivad turujärelevalveasutused esitada ADCO rühmale anonüümitud koondteabe tarkvarast sõltumise kohta. ADCO rühm esitab sõltuvuse hindamise tulemuste aruande direktiivi (EL) 2022/2555 artikli 14 kohaselt loodud koostöörühmale.

Artikkel 14

Tootjate teatamiskohustused

1. Tootja teavitab kõigist digielemente sisaldava toote aktiivselt ärakasutatavatest nõrkustest, millest ta on teada saanud, samal ajal vastavalt käesoleva artikli lõikele 7 koordinaatoriks määratud CSIRTi ja ENISAt. Tootja teavitab igast aktiivselt ärakasutatavast nõrkusest artikli 16 kohaselt loodud ühtse teatamisplatvormi kaudu.

2. Lõikes 1 osutatud teavitamise eesmärgil esitab tootja:

   a) põhjendamatu viivituseta, ent igal juhul 24 tunni jooksul alates sellest, kui tootja sai aktiivselt ärakasutatavast nõrkusest teada, eelhoiatuse teavituse, milles märgib kohaldataval juhul liikmesriigid, kus tootja teada tema digielemente sisaldav toode on kättesaadavaks tehtud;

b) juhul, kui asjakohast teavet ei ole juba esitatud, põhjendamatu viivituseta, ent igal juhul 72 tunni jooksul alates sellest, kui tootja sai aktiivselt ärakasutatavast nõrkusest teada, nõrkuste teavituse, milles esitatakse kättesaadav üldteave asjakohase digielemente sisaldava toote, ärakasutamise üldise olemuse ja asjakohase nõrkuse, võetud parandus- või leevendusmeetmete ning nende parandus- või leevendusmeetmete kohta, mida kasutajad saavad võtta; teavituses märgitakse kohaldataval juhul ka see, kui tundlikuks tootja esitatud teavet peab;

c) juhul, kui asjakohast teavet ei ole juba esitatud, hiljemalt 14 päeva pärast parandus- või leevendusmeetme kättesaadavaks tegemist lõpparuande, mis sisaldab vähemalt järgmist:

   i) nõrkuse, sealhulgas selle raskusastme ja mõju kirjeldus;

   ii) teave kõigi kuritahtlike isikute kohta, kes on nõrkust ära kasutanud või kasutavad, kui see teave on kättesaadav;

   iii) üksikasjad turvauuenduste ja muude parandusmeetmete kohta, mis on nõrkuse kõrvaldamiseks kättesaadavaks tehtud.

3. Tootja teavitab kõigist digielemente sisaldava toote turvalisust mõjutavatest tõsistest intsidentidest, millest ta on saanud teada, samal ajal vastavalt käesoleva artikli lõikele 7 koordinaatoriks määratud CSIRTi ja ENISAt. Tootja teavitab igast intsidendist artikli 16 kohaselt loodud ühtse teatamisplatvormi kaudu.

4. Lõikes 3 osutatud teavitamise eesmärgil esitab tootja:

a) põhjendamatu viivituseta, ent igal juhul 24 tunni jooksul alates sellest, kui tootja sai digielemente sisaldava toote turvalisust mõjutavast tõsisest intsidendist teada, eelhoiatuse teavituse, milles märgib muu hulgas vähemalt teabe selle kohta, kas intsidendi on kahtluste kohaselt põhjustanud ebaseaduslik või kuritahtlik tegevus, ning kohaldataval juhul ka liikmesriigid, kus tootja teada tema digielemente sisaldav toode on kättesaadavaks tehtud;

b) juhul, kui asjakohast teavet ei ole juba esitatud, põhjendamatu viivituseta, ent igal juhul 72 tunni jooksul alates sellest, kui tootja sai intsidendist teada, intsidendi teavituse, milles esitatakse kättesaadav üldteave intsidendi olemuse kohta, intsidendi esialgne hinnang, võetud parandus- või leevendusmeetmed ning teave parandus- või leevendusmeetmete kohta, mida kasutajad saavad võtta; teavituses märgitakse kohaldataval juhul ka see, kui tundlikuks tootja esitatud teavet peab;

c) juhul, kui asjakohast teavet ei ole juba esitatud, ühe kuu jooksul pärast punktis b osutatud intsidendi teavituse esitamist lõpparuande, mis sisaldab vähemalt järgmist:

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

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

iii) kohaldatud ja kohaldamisel olevad leevendusmeetmed.

5. Lõike 3 kohaldamisel loetakse digielemente sisaldava toote turvalisust mõjutav intsident tõsiseks, kui:

a) see mõjutab või võib mõjutada negatiivselt digielemente sisaldava toote võimet kaitsta tundlike või oluliste andmete või funktsioonide kättesaadavust, autentsust, terviklust või konfidentsiaalsust või

b) sellega on kaasnenud või võib kaasneda ründekoodi sisestamine digielemente sisaldavasse tootesse või digielemente sisaldava toote kasutaja võrgu- ja infosüsteemidesse või ründekoodi käivitamine nendes.

6. Vajaduse korral võib koordinaatoriks määratud CSIRT, kes algselt teavituse saab, nõuda, et tootja esitaks vahearuande aktiivselt ärakasutatava nõrkuse või digielemente sisaldava toote turvalisust mõjutava tõsise intsidendi seisu kohta.

7. Käesoleva artikli lõigetes 1 ja 3 osutatud teavitused esitatakse artiklis 16 osutatud ühtse teatamisplatvormi kaudu, kasutades ühte artikli 16 lõikes 1 osutatud teavitusahela lõpp-punkti. Teavitus esitatakse selle liikmesriigi koordinaatoriks määratud CSIRTi teavitusahela lõpp-punkti kaudu, kus on liidus tootja peamine tegevuskoht, ja teavitus on samal ajal kättesaadav ka ENISA-le.

Käesoleva määruse kohaldamisel käsitatakse tootja peamise tegevuskohana liidus liikmesriiki, kus tema digielemente sisaldava toote küberturvalisusega seotud otsused valdavalt tehakse. Kui sellist liikmesriiki ei ole võimalik kindlaks määrata, käsitatakse peamise tegevuskohana seda liikmesriiki, kus on asjaomase tootja kõige suurema arvu töötajatega tegevuskoht liidus.

Kui tootjal ei ole liidus peamist tegevuskohta, esitab ta lõigetes 1 ja 3 osutatud teavitused selle liikmesriigi koordinaatoriks määratud CSIRTi teavitusahela lõpp-punkti kaudu, mis määratakse kindlaks vastavalt järgmisele järjestusele ja tootjale kättesaadavale teabele:

a) liikmesriik, kus asub volitatud esindaja, kes tegutseb tootja nimel suurima arvu digielemente sisaldavate toodete puhul;

b) liikmesriik, kus asub importija, kes laseb turule kõige rohkem selle tootja digielemente sisaldavaid tooteid;

c) liikmesriik, kus asub turustaja, kes on teinud turul kättesaadavaks kõige rohkem selle tootja digielemente sisaldavaid tooteid;

d) liikmesriik, kus asub kõige rohkem selle tootja digielemente sisaldavate toodete kasutajaid.

Seoses kolmanda lõigu punktiga d võib tootja esitada samale koordinaatoriks määratud CSIRTile, keda ta esimesena teavitas, teavitused ka kõigi järgmiste aktiivselt ärakasutatavate nõrkuste või digielemente sisaldava toote turvalisust mõjutavate tõsiste intsidentide kohta.

8. Kui tootja on saanud teada aktiivselt ärakasutatavast nõrkusest või tõsisest intsidendist, mis mõjutab digielemente sisaldava toote turvalisust, teavitab ta asjakohasel juhul struktureeritud kergesti automaattöödeldavas masinloetavas vormingus digielemente sisaldava toote kasutajaid, keda see mõjutab, ja asjakohasel juhul kõiki kasutajaid kõnealusest nõrkusest või intsidendist ning vajaduse korral riskimaandamis- ja parandusmeetmetest, mida kasutajad saavad võtta selle nõrkuse või intsidendi mõju leevendamiseks. Kui tootja ei teavita digielemente sisaldava toote kasutajaid piisavalt kiiresti, võivad koordinaatoriks määratud CSIRTid, keda nõrkusest või intsidendist teavitati, edastada kasutajatele seda teavet, kui seda peetakse proportsionaalseks ja vajalikuks kõnealuse nõrkuse või intsidendi mõju ennetamiseks või leevendamiseks.

9. Hiljemalt … [12 kuud pärast käesoleva määruse jõustumise kuupäeva] võtab komisjon kooskõlas käesoleva määruse artikliga 61 vastu delegeeritud õigusaktid, et täiendada käesolevat määrust ja määrata kindlaks tingimused küberturvalisusega seotud aluste kohaldamiseks seoses teavituste edastamise edasilükkamisega, nagu on osutatud käesoleva määruse artikli 16 lõikes 2. Komisjon teeb delegeeritud õigusakti eelnõu väljatöötamisel koostööd direktiivi (EL) 2022/2555 artikli 15 kohaselt loodud CSIRTide võrgustiku ja ENISAga.

10. Komisjon võib rakendusaktidega täpsustada käesolevas artiklis ning artiklites 15 ja 16 osutatud teavituste vormingut ja esitamise korda. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 62 lõikes 2 osutatud kontrollimenetlusega. Komisjon teeb nende rakendusaktide eelnõude väljatöötamisel koostööd CSIRTide võrgustiku ja ENISAga.

Artikkel 15

Vabatahtlik teatamine

1. Tootjad ning muud füüsilised või juriidilised isikud võivad koordinaatoriks määratud CSIRTi või ENISAt vabatahtlikult teavitada digielemente sisaldava toote nõrkustest ja küberohtudest, mis võivad digielemente sisaldava toote riskiprofiili mõjutada.

2. Tootjad ning muud füüsilised või juriidilised isikud võivad koordinaatoriks määratud CSIRTi või ENISAt vabatahtlikult teavitada digielemente sisaldava toote turvalisust mõjutavast intsidendist ja intsidendiohust, mis oleks võinud sellise intsidendi põhjustada.

3. Koordinaatoriks määratud CSIRT või ENISA menetleb käesoleva artikli lõigetes 1 ja 2 osutatud teavitusi artiklis 16 sätestatud korra kohaselt.

   Koordinaatoriks määratud CSIRT võib kohustuslike teavituste menetlemise seada vabatahtlike teavituste menetlemisest tähtsamale kohale.

4. Kui füüsiline või juriidiline isik, kes ei ole tootja, teavitab kooskõlas lõikega 1 või 2 aktiivselt ärakasutatavast nõrkusest või digielemente sisaldava toote turvalisust mõjutavast tõsisest intsidendist, teavitab koordinaatoriks määratud CSIRT sellest põhjendamatu viivituseta tootjat.

5. Koordinaatoriks määratud CSIRT ja ENISA tagavad teavitava füüsilise või juriidilise isiku esitatud teabe konfidentsiaalsuse ja asjakohase kaitse. Ilma et see piiraks kuritegude ennetamist, uurimist, avastamist ja nende eest vastutusele võtmist, ei kaasne vabatahtliku teatamisega teavitavale füüsilisele või juriidilisele isikule lisakohustusi, mida tal ei oleks olnud, kui ta ei oleks teavitust esitanud.

Artikkel 16

Ühtse teatamisplatvormi loomine

1. Artikli 14 lõigetes 1 ja 3 ning artikli 15 lõigetes 1 ja 2 osutatud teavituste jaoks ning tootjate teatamiskohustuste lihtsustamiseks loob ENISA ühtse teatamisplatvormi. Ühtse teatamisplatvormi igapäevast tegevust haldab ja seda hoiab töökorras ENISA. Ühtse teatamisplatvormi ülesehitus võimaldab liikmesriikidel ja ENISA-l võtta kasutusele oma teavitusahela lõpp-punktid.

2. Pärast teavituse saamist edastab algselt teavituse saanud koordinaatoriks määratud CSIRT teavituse viivitamata ühtse teatamisplatvormi kaudu koordinaatoriteks määratud CSIRTidele, kelle territooriumil tootja teavituse kohaselt digielemente sisaldav toode on kättesaadavaks tehtud.

Erandlikel asjaoludel ja eelkõige tootja taotlusel ning võttes arvesse esitatud teabe tundlikkuse taset, nagu tootja on käesoleva määruse artikli 14 lõike 2 punkti a kohaselt märkinud, võib teavituse edastamist küberturvalisusega seotud põhjendatud alustel rangelt vajaliku ajavahemiku võrra edasi lükata, sealhulgas juhul, kui nõrkuse suhtes kohaldatakse nõrkuste koordineeritud avalikustamise menetlust, nagu on osutatud direktiivi (EL) 2022/2555 artikli 12 lõikes 1. Kui CSIRT otsustab teavituse edastamise edasi lükata, teatab ta otsusest viivitamata ENISA-le ning annab teada nii edasilükkamise põhjuse kui ka selle, millal ta teavituse edastab vastavalt käesolevas lõikes sätestatud edastamiskorrale. ENISA võib toetada CSIRTi küberturvalisusega seotud aluste kohaldamisel seoses teavituse edastamise edasilükkamisega.

Eelkõige on väga erandlikud asjaolud, kui tootja märgib artikli 14 lõike 2 punktis b osutatud teavituses järgmist:

a) kuritahtlik osaleja on teavitatud nõrkust aktiivselt ära kasutanud ja kättesaadava teabe kohaselt ei ole seda ära kasutatud üheski teises liikmesriigis kui selle koordinaatoriks määratud CSIRTi liikmesriik, keda tootja on nõrkusest teavitanud;

b) teavitatud nõrkust käsitleva teabe viivitamatu edastamisega antaks tõenäoliselt teavet, mille avalikustamine oleks vastuolus selle liikmesriigi oluliste huvidega; või

c) teavitatud nõrkus kujutab endast otsest suurt küberriski, mis tuleneb teabe edastamisest.

ENISA-le tehakse samal ajal kättesaadavaks ainult teave selle kohta, et tootja on esitanud teavituse, toote üldteave, teave ärakasutamise üldise laadi kohta ja teave selle kohta, et kohaldatud on turvalisusega seotud aluseid, kuni asjaomastele CSIRTidele ja ENISA-le on edastatud teavituse täisversioon. Kui ENISA leiab selle teabe põhjal, et esineb süsteemne risk, mis mõjutab turvalisust siseturul, soovitab ta teavituse saanud CSIRTil edastada teavituse täisversiooni teistele koordinaatoriteks määratud CSIRTidele ja ENISA-le endale.

3. Pärast teavituse saamist digielemente sisaldava toote aktiivselt ärakasutatava nõrkuse või digielemente sisaldava toote turvalisust mõjutava tõsise intsidendi kohta esitavad koordinaatoriteks määratud CSIRTid oma liikmesriigi turujärelevalveasutustele teavituse teabe, mida turujärelevalveasutused vajavad käesolevast määrusest tulenevate kohustuste täitmiseks.

4. ENISA võtab asjakohaseid ja proportsionaalseid tehnilisi, tegevuslikke ja korralduslikke meetmeid, et juhtida riske, mis ohustavad ühtse teatamisplatvormi turvalisust ning ühtse teatamisplatvormi kaudu esitatud või edastatud teavet. Ta teavitab CSIRTide võrgustikku ja komisjoni põhjendamatu viivituseta igast turvaintsidendist, mis mõjutab ühtset teatamisplatvormi.

5. ENISA töötab koostöös CSIRTide võrgustikuga välja tehnilised spetsifikatsioonid tehniliste, tegevuslike ja korralduslike meetmete kohta, mis on seotud lõikes 1 osutatud ühtse teatamisplatvormi loomise, hoolduse ja turvalise toimimisega, sealhulgas vähemalt ühtse teatamisplatvormi loomise, toimimise ja hoolduse turbemeetmed, samuti teavitusahela lõpp-punktidega, mille võtavad kasutusele riigi tasandil koordinaatoriteks määratud CSIRTid ja liidu tasandil ENISA, sealhulgas menetluslikud aspektid, millega tagatakse, et kui teavitatud nõrkuse suhtes parandus- või leevendusmeetmed puuduvad, jagatakse teavet selle nõrkuse kohta kooskõlas rangete turvaprotokollidega ja teadmisvajaduse alusel, ning rakendab neid spetsifikatsioone.

6. Kui koordinaatoriks määratud CSIRTile on direktiivi (EL) 2022/2555 artikli 12 lõikes 1 osutatud nõrkuste koordineeritud avalikustamise menetluse raames teatatud aktiivselt ärakasutatavast nõrkusest, võib algselt teavituse saanud koordinaatoriks määratud CSIRT lükata asjakohase teavituse ühtse teatamisplatvormi kaudu edastamise küberturvalisusega seotud põhjendatud alustel edasi ajavahemiku võrra, mis ei ole pikem kui rangelt vajalik, ja seni, kuni asjaomased nõrkuste koordineeritud avalikustamise osalised on andnud avalikustamiseks nõusoleku. See nõue ei takista tootjaid teavitamast sellisest nõrkusest vabatahtlikult käesolevas artiklis sätestatud korras.

Artikkel 17

Muud teatamisega seotud normid

1. ENISA võib edastada kooskõlas direktiivi (EL) 2022/2555 artikliga 16 loodud Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikule (EU-CyCLONe) käesoleva määruse artikli 14 lõigete 1 ja 3 ning artikli 15 lõigete 1 ja 2 kohaselt teavitatud teabe, kui selline teave on asjakohane tegevustasandil ulatuslike küberintsidentide ja kriiside kooskõlastatud juhtimiseks. Sellise asjakohasuse kindlakstegemiseks võib ENISA võtta arvesse CSIRTide võrgustiku tehtud tehnilisi analüüse, kui need on olemas.

2. Kui üldsuse teavitamine on vajalik digielemente sisaldava toote turvalisust mõjutava tõsise intsidendi ennetamiseks või leevendamiseks või poolelioleva intsidendi käsitlemiseks või kui intsidendi avalikustamine on muul viisil avalikes huvides, võib asjaomase liikmesriigi koordinaatoriks määratud CSIRT pärast asjaomase tootjaga konsulteerimist ja asjakohasel juhul koostöös ENISAga üldsusele intsidendist teada anda või nõuda, et tootja seda teeks.

3. ENISA koostab käesoleva määruse artikli 14 lõigete 1 ja 3 ning artikli 15 lõigete 1 ja 2 kohaselt saadud teavituste põhjal iga 24 kuu tagant tehnilise aruande digielemente sisaldavate toodete küberriskidega seotud uute suundumuste kohta ja esitab selle direktiivi (EL) 2022/2555 artikli 14 kohaselt loodud koostöörühmale. Esimene aruanne esitatakse 24 kuu jooksul pärast artikli 14 lõigetes 1 ja 3 sätestatud kohustuste kohaldamise algust. ENISA lisab oma tehnilistes aruannetes sisalduva asjakohase teabe oma direktiivi (EL) 2022/2555 artikli 18 kohaselt esitatavasse aruandesse, mis käsitleb küberturvalisuse olukorda liidus.

4. Pelgalt teavitamise tõttu artikli 14 lõigete 1 ja 3 või artikli 15 lõigete 1 ja 2 kohaselt ei kaasne teavituse esitavale füüsilisele või juriidilisele isikule suuremat vastutust.

5. Kui turvauuendus või muu parandus- või leevendusmeede on kättesaadav, lisab ENISA kokkuleppel asjaomase digielemente sisaldava toote tootjaga käesoleva määruse artikli 14 lõike 1 või artikli 15 lõike 1 kohaselt teavitatud ja üldsusele teadaoleva nõrkuse direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasi.

6. Koordinaatoriks määratud CSIRTid pakuvad tootjatele, eelkõige mikro-, väike- või keskmise suurusega ettevõtjaks liigituvatele tootjatele seoses artikli 14 kohaste teatamiskohustustega kasutajatuge.

Artikkel 18

Volitatud esindajad

1. Tootja võib kirjaliku volituse alusel määrata volitatud esindaja.

2. Artikli 13 lõikest 1 kuni lõikeni 11, lõike 12 esimese lõiguni ja lõikes 14 sätestatud kohustused ei kuulu volitatud esindaja ülesannete hulka.

3. Volitatud esindaja täidab ülesandeid tootjalt saadud volituste piires. Volitatud esindaja esitab volituse koopia nõudmise korral turujärelevalveasutusele. Volitus võimaldab volitatud esindajal teha vähemalt järgmist:

a) hoida artiklis 28 osutatud ELi vastavusdeklaratsiooni ja artiklis 31 osutatud tehnilist dokumentatsiooni turujärelevalveasutustele esitamiseks alles vähemalt kümme aastat alates digielemente sisaldava toote turule laskmisest või toe kestuse ajal, olenevalt sellest, kumb on pikem;

b) esitada turujärelevalveasutuse põhjendatud taotluse korral talle kogu teave ja dokumentatsioon digielemente sisaldava toote nõuetele vastavuse tõendamiseks;

c) teha turujärelevalveasutustega nende taotluse korral koostööd seoses meetmetega, mis on võetud sellisest digielemente sisaldavast tootest tulenevate riskide kõrvaldamiseks, mida volitatud esindaja volitused hõlmavad.

Artikkel 19

Importijate kohustused

1. Importijad lasevad turule üksnes selliseid digielemente sisaldavaid tooteid, mis vastavad I lisa I osas sätestatud olulistele küberturvalisuse nõuetele ja mille tootja rakendatud protsessid vastavad I lisa II osas sätestatud olulistele küberturvalisuse nõuetele.

2. Enne digielemente sisaldava toote turule laskmist peab importija tagama, et:

   a) tootja on läbi viinud artiklis 32 osutatud asjakohased vastavushindamismenetlused;

   b) tootja on koostanud tehnilise dokumentatsiooni;

   c) digielemente sisaldaval tootel on artiklis 30 osutatud CE-märgis ja sellega on kaasas artikli 13 lõikes 20 osutatud ELi vastavusdeklaratsioon ning II lisas sätestatud kasutajale mõeldud teave ja juhised, mis on kasutajatele ja turujärelevalveasutustele kergesti arusaadavas keeles;

   d) tootja on täitnud artikli 13 lõigetes 15, 16 ja 19 sätestatud nõuded.

   Käesoleva lõike kohaldamisel peab importija suutma esitada vajalikud dokumendid, mis tõendavad käesolevas artiklis sätestatud nõuete täitmist.

3. Kui importija arvab või tal on põhjust uskuda, et digielemente sisaldav toode või tootja rakendatud protsessid ei vasta käesolevale määrusele, ei lase importija toodet turule enne, kui toode või tootja rakendatud protsessid on viidud käesoleva määrusega vastavusse. Lisaks teavitab importija tootjat ja turujärelevalveasutusi, kui digielemente sisaldav toode kujutab endast olulist küberriski.

   Kui importijal on põhjust uskuda, et digielemente sisaldav toode võib mittetehnilisi riskitegureid arvestades põhjustada olulist küberriski, teavitab importija sellest turujärelevalveasutusi. Sellise teabe saamisel järgivad turujärelevalveasutused artikli 54 lõikes 2 osutatud menetlusi.

4. Importija märgib digielemente sisaldavale tootele, selle pakendile või sellega kaasas olevasse dokumenti oma nime, registreeritud kaubanime või registreeritud kaubamärgi, postiaadressi, e-posti aadressi või muud digitaalsed kontaktandmed, ja kui see on kohaldatav, veebisaidi, mille kaudu importijaga saab ühendust võtta. Kontaktandmed esitatakse kasutajale ja turujärelevalveasutustele kergesti arusaadavas keeles.

5. Kui importija teab või tal on põhjust uskuda, et digielemente sisaldav toode, mille ta on turule lasknud, ei vasta käesolevale määrusele, võtab ta viivitamata vajalikud parandusmeetmed, et tagada digielemente sisaldava toote viimine käesoleva määrusega vastavusse või asjakohasel juhul kõrvaldada see turult või võtta see tagasi.

   Digielemente sisaldava toote nõrkusest teada saamisel teavitavad importijad tootjat sellest nõrkusest põhjendamatu viivituseta. Kui digielemente sisaldav toode põhjustab olulist küberriski, teatab importija sellest viivitamata nende liikmesriikide turujärelevalveasutustele, kus ta digielemente sisaldava toote turul kättesaadavaks on teinud, esitades eelkõige andmed mittevastavuse ja võetud parandusmeetmete kohta.

6. Importija hoiab ELi vastavusdeklaratsiooni koopiat turujärelevalveasutustele esitamiseks alles vähemalt kümme aastat alates digielemente sisaldava toote turule laskmisest või toe kestuse ajal, olenevalt sellest, kumb on pikem, ja tagab, et tehniline dokumentatsioon on kõnealustele asutustele taotluse alusel kättesaadav.

7. Turujärelevalveasutuse põhjendatud taotluse korral esitab importija kõnealusele asutusele sellele kergesti arusaadavas keeles kas paberil või elektrooniliselt kogu teabe ja dokumentatsiooni, mida on vaja digielemente sisaldava toote I lisa I osas sätestatud olulistele küberturvalisuse nõuetele vastavuse tõendamiseks, ning tootja rakendatud protsesside I lisa II osas sätestatud olulistele küberturvalisuse nõuetele vastavuse tõendamiseks. Kui kõnealune asutus seda taotleb, teeb importija temaga koostööd kõigi meetme korral, mis on võetud tema poolt turule lastud digielemente sisaldavast tootest tulenevate küberriskide kõrvaldamiseks.

8. Kui digielemente sisaldava toote importija saab teada, et selle toote tootja on lõpetanud oma tegevuse ega suuda seetõttu täita käesolevas määruses sätestatud kohustusi, teatab importija sellest olukorrast asjaomastele turujärelevalveasutustele ning kättesaadavate vahendite ja võimaluste piires ka turule lastud digielemente sisaldavate toodete kasutajatele.

Artikkel 20

Turustajate kohustused

1. Digielemente sisaldavat toodet turul kättesaadavaks tehes peab turustaja vajaliku hoolikusega järgima käesolevas määruses sätestatud nõudeid.

2. Enne digielemente sisaldava toote turul kättesaadavaks tegemist kontrollib turustaja, et:

a) digielemente sisaldaval tootel on CE-vastavusmärgis;

b) tootja ja importija on täitnud artikli 13 lõigetes 15, 16, 18, 19 ja 20 ning artikli 19 lõikes 4 esitatud kohustused ning edastanud turustajale kõik vajalikud dokumendid.

3. Turustaja, kes arvab või kellel on tema käsutuses oleva teabe alusel põhjust uskuda, et digielemente sisaldav toode või tootja rakendatud protsessid ei vasta I lisas sätestatud olulistele küberturvalisuse nõuetele, ei tee digielemente sisaldavat toodet turul kättesaadavaks enne, kui see toode või tootja rakendatud protsessid on viidud vastavusse käesoleva määrusega. Kui digielemente sisaldav toode kujutab endast olulist küberriski, teatab turustaja sellest põhjendamatu viivituseta tootjale ja turujärelevalveasutustele.

4. Turustaja, kes teab või kellel on tema käsutuses oleva teabe alusel põhjust uskuda, et tema poolt turul kättesaadavaks tehtud digielemente sisaldav toode või tootja rakendatud protsessid ei ole kooskõlas käesoleva määrusega, veendub, et kõnealuse digielemente sisaldava toote või tootja rakendatud protsesside vastavusse viimiseks vajalikud parandusmeetmed on võetud, või kõrvaldab toote vajaduse korral turult või võtab tagasi.

Digielemente sisaldava toote nõrkusest teada saamisel teavitab turustaja tootjat põhjendamatu viivituseta kõnealusest nõrkusest. Kui digielemente sisaldav toode põhjustab olulist küberriski, teatab turustaja sellest viivitamata nende liikmesriikide turujärelevalveasutustele, kus ta digielemente sisaldava toote turul kättesaadavaks tegi, esitades eelkõige andmed nõuetele mittevastavuse ja võetud parandusmeetmete kohta.

5. Turujärelevalveasutuse põhjendatud taotluse korral esitab turustaja kõnealusele asutusele kergesti arusaadavas keeles kas paberil või elektrooniliselt kogu teabe ja dokumentatsiooni, mida on vaja digielemente sisaldava toote ja tootja rakendatud protsesside käesolevale direktiivile vastavuse tõendamiseks. Kui kõnealune asutus seda taotleb, teeb ta sellega koostööd kõigi meetmete korral, mis on võetud tema poolt turul kättesaadavaks tehtud digielemente sisaldavast tootest tulenevate küberriskide kõrvaldamiseks.

6. Kui digielemente sisaldava toote turustaja saab tema käsutuses oleva teabe põhjal teada, et selle toote tootja on lõpetanud tegevuse ega suuda seetõttu täita käesolevas määruses sätestatud kohustusi, teatab turustaja sellest olukorrast põhjendamatu viivituseta asjaomastele turujärelevalveasutustele ning kättesaadavate vahendite ja võimaluste piires ka turule lastud digielemente sisaldavate toodete kasutajatele.

Artikkel 21

Juhtumid, mil importijad ja turustajad täidavad tootjate kohustusi

Kui importija või turustaja laseb digielemente sisaldava toote turule oma nime või kaubamärgi all või muudab oluliselt juba turule lastud digielemente sisaldavat toodet, loetakse see importija või tarnija käesoleva määruse kohaldamisel tootjaks ja tema suhtes kohaldatakse artikleid 13 ja 14.

Artikkel 22

Muud juhtumid, mil kohaldatakse tootjate kohustusi

1. Käesoleva määruse kohaldamisel käsitatakse tootjana füüsilist või juriidilist isikut, kes ei ole tootja, importija ega turustaja, kes muudab oluliselt digielemente sisaldavat toodet ja teeb selle toote turul kättesaadavaks.

2. Käesoleva artikli lõikes 1 osutatud isiku suhtes kohaldatakse artiklites 13 ja 14 sätestatud kohustusi digielemente sisaldava toote selles osas, mida on oluliselt muudetud, või juhul kui oluline muudatus mõjutab digielemente sisaldava toote kui terviku küberturvalisust, kogu toote ulatuses.

Artikkel 23

Ettevõtjate identifitseerimine

1. Ettevõtjad esitavad turujärelevalveasutusele taotluse alusel järgmise teabe:

   a) iga sellise ettevõtja nimi ja aadress, kes on neile digielemente sisaldava toote tarninud;

   b) iga sellise ettevõtja nimi ja aadress, kellele nad on digielemente sisaldava toote tarninud, kui see on kättesaadav.

2. Ettevõtjad peavad hoidma lõikes 1 osutatud teabe esitamiseks alles kümme aastat alates sellest, kui neile digielemente sisaldav toode tarniti või kui nad ise digielemente sisaldava toote tarnisid.

Artikkel 24

Avatud lähtekoodiga tarkvara korraldaja kohustused

1. Avatud lähtekoodiga tarkvara korraldajad koostavad küberturvalisuse põhimõtted ja dokumenteerivad neid kontrollitavalt, selleks et edendada digielemente sisaldava turvalise toote väljatöötamist ja nõrkuste tulemuslikku käsitlemist selle toote arendajate poolt. Kõnealuste põhimõtetega edendatakse ka artiklis 15 sätestatud vabatahtlikku nõrkustest teatamist selle toote arendajate poolt ning võetakse arvesse avatud lähtekoodiga tarkvara korraldamise eripära ning selle suhtes kohaldatavat õiguslikku ja organisatsioonilist korda. Need põhimõtted peavad eelkõige hõlmama nõrkuste dokumenteerimise, nendega tegelemise ja nende kõrvaldamisega seotud aspekte ning edendama avastatud nõrkusi käsitleva teabe jagamist avatud lähtekoodi kogukonnas.

2. Avatud lähtekoodiga tarkvara korraldajad teevad turujärelevalveasutustega nende taotluse korral koostööd, et leevendada küberriske, mis tulenevad digielemente sisaldavast vabaks ja avatud lähtekoodiga tarkvaraks kvalifitseeruvast tootest.

   Turujärelevalveasutuse põhjendatud taotluse korral esitavad avatud lähtekoodiga tarkvara korraldajad kõnealusele asutusele kergesti arusaadavas keeles kas paberil või elektrooniliselt lõikes 1 osutatud dokumendid.

3. Artikli 14 lõikes 1 sätestatud kohustusi kohaldatakse avatud lähtekoodiga tarkvara korraldajate suhtes niivõrd, kuivõrd nad on seotud digielemente sisaldavate toodete arendamisega. Artikli 14 lõigetes 3 ja 8 sätestatud kohustusi kohaldatakse avatud lähtekoodiga tarkvara korraldajate suhtes niivõrd, kuivõrd digielemente sisaldavate toodete turvalisust mõjutavad tõsised intsidendid avaldavad mõju võrgu- ja infosüsteemidele, mida avatud lähtekoodiga tarkvara korraldajad selliste toodete arendamiseks pakuvad.

Artikkel 25

Vaba ja avatud lähtekoodiga tarkvara turvalisuse tõendamine

Selleks et hõlbustada artikli 13 lõikes 5 sätestatud hoolsuskohustuse täitmist, eelkõige tootjate puhul, kes integreerivad oma digielemente sisaldavatesse toodetesse vaba ja avatud lähtekoodiga tarkvara komponente, on komisjonil õigus võtta kooskõlas artikliga 61 vastu delegeeritud õigusakte käesoleva määruse täiendamiseks, kehtestades vabatahtlikud turvalisuse tõendamise programmid, mis võimaldavad vaba ja avatud lähtekoodiga tarkvaraks kvalifitseeruvate digielemente sisaldavate toodete arendajatel või kasutajatel ning muudel kolmandatel isikutel hinnata selliste toodete vastavust kõigile või teatavatele olulistele küberturvalisuse nõuetele või muudele käesolevas määruses sätestatud kohustustele.

Artikkel 26

Suunised

1. Rakendamise hõlbustamiseks ja selle järjepidevuse tagamiseks avaldab komisjon suunised, et aidata ettevõtjatel käesolevat määrust kohaldada, pöörates erilist tähelepanu nõuete täitmise lihtsustamisele mikro- ning väikeste ja keskmise suurusega ettevõtjate jaoks.

2. Kui komisjon kavatseb anda välja lõikes 1 osutatud suuniseid, käsitleb ta vähemalt järgmisi aspekte:

   a) käesoleva määruse kohaldamisala, pöörates erilist tähelepanu andmete kaugtöötluslahendustele ning vaba ja avatud lähtekoodiga tarkvarale;

   b) toe kestuse kohaldamine digielemente sisaldavate toodete teatavate kategooriate suhtes;

   c) suunised käesoleva määruse kohaldamisalasse kuuluvatele tootjatele, kelle suhtes kohaldatakse ka muid liidu ühtlustamisõigusakte kui käesolev määrus või muid seotud liidu õigusakte;

   d) olulise muudatuse mõiste.

   Komisjon peab ka kergesti kättesaadavat loetelu käesoleva määruse kohaselt vastu võetud delegeeritud õigusaktidest ja rakendusaktidest.

3. Käesoleva artikli kohaste suuniste ettevalmistamisel konsulteerib komisjon asjaomaste sidusrühmaga.

III PEATÜKK

Digielemente sisaldava toote vastavus nõuetele

Artikkel 27

Nõuetele vastavuse eeldamine

1. Digielemente sisaldavad tooted ja tootja rakendatud protsessid, mis on vastavuses selliste harmoneeritud standardite või nende osadega, mille viited on avaldatud *Euroopa Liidu Teatajas*, eeldatakse olevat vastavuses I lisas sätestatud oluliste küberturvalisuse nõuetega, mida nimetatud standardid või nende osad käsitlevad.

   Kooskõlas määruse (EL) nr 1025/2012 artikli 10 lõikega 1 esitab komisjon ühele või mitmele Euroopa standardiorganisatsioonile taotluse koostada käesoleva määruse I lisas sätestatud oluliste küberturvalisuse nõuete kohta harmoneeritud standardid. Komisjon püüab käesoleva määrusega seotud standardimistaotluste ettevalmistamisel võtta arvesse olemasolevaid või väljatöötamisel olevaid Euroopa ja rahvusvahelisi küberturvalisuse standardeid, et lihtsustada harmoneeritud standardite väljatöötamist kooskõlas määrusega (EL) nr 1025/2012.

2. Komisjon võib võtta vastu rakendusakte, millega kehtestatakse ühtsed spetsifikatsioonid, mis hõlmavad tehnilisi nõudeid, mille abil on võimalik tagada käesoleva määruse kohaldamisalasse kuuluvate digielemente sisaldavate toodete vastavus I lisas sätestatud olulistele küberturvalisuse nõuetele.

Kõnealused rakendusaktid võetakse vastu üksnes juhul, kui on täidetud järgmised tingimused:

a) komisjon on määruse (EL) nr 1025/2012 artikli 10 lõike 1 kohaselt esitanud ühele või mitmele Euroopa standardiorganisatsioonile taotluse koostada I lisas sätestatud oluliste küberturvalisuse nõuete kohta harmoneeritud standard ning:

i) taotlust ei ole vastu võetud;

ii) kõnealust taotlust käsitlevaid harmoneeritud standardeid ei esitatud määruse (EL) nr 1025/2012 artikli 10 lõikes 1 sätestatud tähtaja jooksul või

iii) harmoneeritud standardid ei vasta taotlusele ning

b) *Euroopa Liidu Teatajas* ei ole avaldatud ühtegi määruse (EL) nr 1025/2012 kohast viidet harmoneeritud standarditele, mis kataks I lisas sätestatud asjakohaseid olulisi küberturvalisuse nõudeid, ning mõistliku aja jooksul ei ole sellist viidet kavas avaldada.

Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 62 lõikes 2 osutatud kontrollimenetlusega.

3. Enne käesoleva artikli lõikes 2 osutatud rakendusakti eelnõu koostamist teavitab komisjon määruse (EL) nr 1025/2012 artiklis 22 osutatud komiteed sellest, et tema hinnangul on käesoleva artikli lõikes 2 osutatud tingimused täidetud.

4. Lõikes 2 osutatud rakendusakti eelnõu ettevalmistamisel võtab komisjon arvesse asjaomaste asutuste seisukohti ning konsulteerib nõuetekohaselt kõigi asjaomaste sidusrühmadega.

5. Eeldatakse, et digielemente sisaldavad tooted ja tootja rakendatud protsessid, mis on vastavuses käesoleva artikli lõikes 2 osutatud rakendusaktide või nende osadega kehtestatud ühtsete spetsifikatsioonidega, on vastavuses I lisas sätestatud oluliste küberturvalisuse nõuete või nende osadega, mida nimetatud ühtsed spetsifikatsioonid käsitlevad.

6. Kui Euroopa standardiorganisatsioon võtab harmoneeritud standardi vastu ja esitab selle komisjonile, et avaldada selle viide *Euroopa Liidu Teatajas*, annab komisjon harmoneeritud standardile kooskõlas määrusega (EL) nr 1025/2012 hinnangu. Kui harmoneeritud standardi viide avaldatakse *Euroopa Liidu Teatajas*, tunnistab komisjon kehtetuks lõikes 2 osutatud rakendusaktid või nende osad, mis katavad samu olulisi küberturvalisuse nõudeid mis see harmoneeritud standard.

7. Kui liikmesriik on seisukohal, et ühtsed spetsifikatsioonid ei vasta täielikult I lisas sätestatud olulistele küberturvalisuse nõuetele, teatab ta sellest komisjonile ning esitab üksikasjaliku selgituse. Komisjon annab üksikasjalikule selgitusele hinnangu ja võib rakendusakti, millega kõnealused ühtsed spetsifikatsioonid kehtestatakse, asjakohasel juhul muuta.

8. Eeldatakse, et digielemente sisaldavad tooted ja tootja rakendatud protsessid, mille kohta on määruse (EL) 2019/881 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava alusel välja antud ELi vastavusdeklaratsioon või sertifikaat, on vastavuses I lisas sätestatud oluliste küberturvalisuse nõuetega, kui ELi vastavusdeklaratsioon või Euroopa küberturvalisuse sertifikaat või nende osad hõlmavad neid nõudeid.

9. Komisjonil on õigus võtta kooskõlas käesoleva määruse artikliga 61 vastu delegeeritud õigusakte käesoleva määruse täiendamiseks, et määratleda määruse (EL) 2019/881 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavad, mille alusel tõendada digielemente sisaldavate toodete vastavust I lisas sätestatud olulistele küberturvalisuse nõuetele või nende osadele. Selliste kavade alusel vähemalt märkimisväärsel usaldusväärsuse tasemel välja antud Euroopa küberturvalisuse sertifikaat vabastab tootja ühtlasi kolmanda isiku tehtava vastavushindamise kohustusest kõnealuste nõuete osas, nagu on sätestatud käesoleva määruse artikli 32 lõike 2 punktides a ja b ning artikli 32 lõike 3 punktides a ja b.

Artikkel 28

ELi vastavusdeklaratsioon

1. Tootja koostab artikli 13 lõike 12 kohaselt ELi vastavusdeklaratsiooni ning kinnitab, et I lisas sätestatud kohaldatavate oluliste küberturvalisuse nõuete täitmine on tõendatud.

2. ELi vastavusdeklaratsioon peab vastama V lisas sätestatud näidisele ning sisaldama VIII lisa asjakohastes vastavushindamismenetlustes kindlaks määratud elemente. Sellist deklaratsiooni tuleb asjakohasel juhul ajakohastada. See tõlgitakse keeltesse, mida nõuab liikmesriik, kus digielemente sisaldav toode turule lastakse või turul kättesaadavaks tehakse.

Artikli 13 lõikes 20 osutatud lihtsustatud ELi vastavusdeklaratsioon peab vastama VI lisas sätestatud näidisele. See tõlgitakse keeltesse, mida nõuab liikmesriik, kus digielemente sisaldav toode turule lastakse või turul kättesaadavaks tehakse.

3. Kui digielemente sisaldava toote suhtes kohaldatakse rohkem kui üht liidu õigusakti, millega nõutakse ELi vastavusdeklaratsiooni, siis koostatakse kõigi nende liidu õigusaktide kohta üks ühine ELi vastavusdeklaratsioon. Kõnealuses deklaratsioonis nimetatakse asjaomased liidu õigusaktid, sealhulgas avaldamisviited.

4. ELi vastavusdeklaratsiooni koostamisega võtab tootja endale vastutuse digielemente sisaldava toote nõuetele vastavuse eest.

5. Komisjonil on õigus võtta kooskõlas artikliga 61 vastu delegeeritud õigusakte, millega täiendatakse käesolevat määrust, lisades V lisas sätestatud ELi vastavusdeklaratsioonis minimaalselt esitatavate andmete loetellu elemente, et võtta arvesse tehnika arengut.

Artikkel 29

CE-vastavusmärgise üldpõhimõtted

CE-vastavusmärgise suhtes kohaldatakse määruse (EÜ) nr 765/2008 artiklis 30 sätestatud üldpõhimõtteid.

Artikkel 30

CE-vastavusmärgise kinnitamise nõuded ja tingimused

1. CE-vastavusmärgis kinnitatakse digielemente sisaldavale tootele nii, et see on nähtav, loetav ja kustumatu. Kui nii ei ole digielemente sisaldava toote laadi tõttu võimalik või otstarbekas märgist kinnitada, pannakse see digielemente sisaldava toote pakendile ja tootega kaasasolevale artiklis 28 osutatud ELi vastavusdeklaratsioonile. Tarkvaraliste digielemente sisaldavate toodete puhul pannakse CE-vastavusmärgis kas artiklis 28 osutatud ELi vastavusdeklaratsioonile või tarkvaratoote juurde kuuluvale veebisaidile. Viimasel juhul peab veebisaidi asjakohane osa olema tarbijatele hõlpsalt ja otseselt ligipääsetav.

2. Digielemente sisaldavale tootele kinnitatava CE-vastavusmärgise kõrgus võib toote omadustest tulenevalt olla alla 5 mm, tingimusel et märgis on nähtav ja loetav.

3. CE-vastavusmärgis kinnitatakse digielemente sisaldavale tootele enne selle turule laskmist. Lisaks võib märgisele järgneda piktogramm või muu märgis, mis osutab erilisele küberriskile või kasutusviisile, millele on osutatud lõike 6 kohastes rakendusaktides.

4. CE-vastavusmärgisele järgneb teada antud asutuse identifitseerimisnumber, kui kõnealune asutus on kaasatud artiklis 32 osutatud täielikul kvaliteedi tagamisel põhinevasse (põhineb moodulil H) vastavushindamismenetlusse.

   Teada antud asutuse identifitseerimisnumbri kinnitab kas asutus ise või tema juhiste järgi tootja või tootja volitatud esindaja.

5. Liikmesriigid tuginevad olemasolevatele mehhanismidele, et tagada CE-vastavusmärgise kasutamise korra nõuetekohane rakendamine, ja võtavad märgise vale kasutamise korral asjakohaseid meetmeid. Kui digielemente sisaldavate toodete suhtes kohaldatakse muid liidu ühtlustamisõigusakte kui käesolev määrus, milles nähakse samuti ette CE-vastavusmärgise kinnitamine, näitab CE-vastavusmärgis, et tooted vastavad ka nende muudes liidu ühtlustamisõigusaktides sätestatud nõuetele.

6. Komisjon võib rakendusaktidega kehtestada tehnilised spetsifikatsioonid märgistusele, piktogrammidele või muudele märgistele, mis on seotud digielemente sisaldavate toodete turvalisusega, nende toe kestuse ja mehhanismid nende kasutuse edendamiseks ning üldsuse teadlikkuse suurendamiseks digielemente sisaldavate toodete turvalisuse kohta. Rakendusaktide eelnõude ettevalmistamisel konsulteerib komisjon asjaomaste sidusrühmadega ja ADCO rühmaga, kui see on artikli 52 lõike 15 kohaselt juba loodud. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 62 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 31

Tehniline dokumentatsioon

1. Tehniline dokumentatsioon peab sisaldama kõiki asjakohaseid andmeid või üksikasju vahendite kohta, mida tootja on kasutanud selleks, et tagada digielemente sisaldavate toodete ja tootja rakendatud protsesside vastavus I lisas sätestatud olulistele küberturvalisuse nõuetele. Dokumentatsioon peab sisaldama vähemalt VII lisas esitatud elemente.

2. Tehniline dokumentatsioon koostatakse enne digielemente sisaldava toote turule laskmist ja seda ajakohastatakse asjakohasel juhul pidevalt, vähemalt toe kestuse vältel.

3. Artiklis 12 osutatud digielemente sisaldavate toodete puhul, mille suhtes kohaldatakse ka muid liidu õigusakte, millega nähakse ette tehniline dokumentatsioon, koostatakse üksainus tehniline dokumentatsioon, mis sisaldab VII lisas osutatud teavet ja kõnealuste liidu õigusaktidega nõutavat teavet.

4. Vastavushindamismenetlusega seotud tehniline dokumentatsioon ja kirjavahetus on selle liikmesriigi ametlikus keeles, kus teada antud asutus asub, või mõnes muus sellele asutusele vastuvõetavas keeles.

5. Komisjonil on õigus võtta kooskõlas artikliga 61 vastu delegeeritud õigusakte, et täiendada käesolevat määrust elementidega, mis lisatakse VII lisas sätestatud tehnilisse dokumentatsiooni, et võtta arvesse tehnika arengut ja käesoleva määruse rakendamisprotsessis toimunut. Selleks püüab komisjon tagada mikro-, väikeste ja keskmise suurusega ettevõtjatele proportsionaalse halduskoormuse.

Artikkel 31

Digielemente sisaldavate toodete vastavushindamismenetlused

1. Selleks et teha kindlaks digielemente sisaldava toote ja tootja rakendatud protsesside vastavus I lisas sätestatud olulistele küberturvalisuse nõuetele, teeb tootja vastavushindamise. Tootja tõendab vastavust olulistele küberturvalisuse nõuetele, kohaldades mis tahes järgmistest menetlustest:

   a) VIII lisas sätestatud sisekontrollimenetlus (põhineb moodulil A);

   b) VIII lisas sätestatud ELi tüübihindamismenetlus (põhineb moodulil B), millele järgneb VIII lisas sätestatud tootmise sisekontrollil põhinev ELi tüübivastavuse hindamine (põhineb moodulil C);

c) VIII lisas sätestatud täielikul kvaliteedi tagamisel põhinev vastavuse hindamine (põhineb moodulil H) või

d) kui see on kättesaadav ja kohaldatav, siis artikli 27 lõike 9 kohane Euroopa küberturvalisuse sertifitseerimise kava.

2. Kui tootja hindab III lisa kohaselt I klassi kuuluva digielemente sisaldava olulise toote ja tootja rakendatud protsesside vastavust I lisas sätestatud olulistele küberturvalisuse nõuetele ning ta ei ole või on ainult osaliselt kohaldanud harmoneeritud standardeid, ühtseid spetsifikatsioone või artiklis 27 osutatud märkimisväärse usaldusväärsuse tasemega Euroopa küberturvalisuse sertifitseerimise kavasid või kui sellised harmoneeritud standardid, ühtsed spetsifikatsioonid või Euroopa küberturvalisuse sertifitseerimise kavad puuduvad, siis kohaldatakse asjaomase digielemente sisaldava toote ja tootja rakendatud protsesside suhtes mis tahes järgmistest menetlustest seoses nende oluliste küberturvalisuse nõuetega:

a) VIII lisas sätestatud ELi tüübihindamismenetlus (põhineb moodulil B), millele järgneb VIII lisas sätestatud tootmise sisekontrollil põhinev tüübivastavuse hindamine (põhineb moodulil C), või

b) VIII lisas sätestatud täielikul kvaliteedi tagamisel põhinev vastavuse hindamine (põhineb moodulil H).

3. Kui toode on III lisa kohaselt II klassi kuuluv digielemente sisaldav oluline toode, tõendab tootja vastavust I lisas sätestatud olulistele küberturvalisuse nõuetele, kasutades mis tahes järgmistest menetlustest:

   a) VIII lisas sätestatud ELi tüübihindamismenetlus (põhineb moodulil B), millele järgneb VIII lisas sätestatud tootmise sisekontrollil põhinev tüübivastavuse hindamine (põhineb moodulil C);

   b) VIII lisas sätestatud täielikul kvaliteedi tagamisel põhinev vastavuse hindamine (põhineb moodulil H) või

   c) kui see on kättesaadav ja kohaldatav, käesoleva määruse artikli 27 lõike 9 kohane Euroopa küberturvalisuse sertifitseerimise kava vähemalt märkimisväärsel usaldusväärsuse tasemel vastavalt määrusele (EL) 2019/881.

4. IV lisas loetletud digielemente sisaldava kriitilise tähtsusega toote puhul tõendatakse vastavust I lisas sätestatud olulistele küberturvalisuse nõuetele, kasutades ühte järgmistest menetlustest:

   a) artikli 8 lõike 1 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava või

   b) kui artikli 8 lõike 1 tingimused ei ole täidetud, siis mõni käesoleva artikli lõikes 3 osutatud menetlustest.

5. III lisas sätestatud kategooriatesse kuuluvate vaba ja avatud lähtekoodiga tarkvaraks kvalifitseeruvate digielemente sisaldavate toodete tootjad peavad suutma tõendada vastavust I lisas sätestatud olulistele küberturvalisuse nõuetele, kohaldades üht käesoleva artikli lõikes 1 osutatud menetlustest, tingimusel et nende toodete turule laskmise ajal tehakse üldsusele kättesaadavaks artiklis 31 osutatud tehniline dokumentatsioon.

6. Vastavushindamismenetluste tasude kehtestamisel võetakse arvesse mikro-, väikeste ja keskmise suurusega ettevõtjate, sealhulgas idufirmade konkreetseid huve ja vajadusi ning neid tasusid vähendatakse proportsionaalselt nende konkreetsete huvide ja vajadustega.

Artikkel 33

Mikro-, väikeste ja keskmise suurusega ettevõtjate, sealhulgas idufirmade tugimeetmed

1. Liikmesriigid võtavad vajaduse korral järgmisi mikro- ja väikeettevõtjate vajadustele kohandatud meetmeid:

   a) korraldavad konkreetset teadlikkuse suurendamise ja koolitustegevust käesoleva määruse kohaldamise kohta;

b) seavad sisse sihtotstarbelised kanalid kommunikatsiooniks mikro- ja väikeettevõtjatega ning asjakohasel juhul kohalike avaliku sektori asutustega, et anda nõu ja vastata päringutele käesoleva määruse rakendamise kohta;

c) toetavad testimis- ja vastavushindamise toiminguid, sealhulgas asjakohasel juhul Euroopa küberturvalisuse pädevuskeskuse toel.

2. Liikmesriigid võivad asjakohasel juhul luua küberkerksuse regulatiivliivakastid. Sellised regulatiivliivakastid toimivad digielemente sisaldavate uuenduslike toodete kontrollitud testkeskkonnana, mis aitab kaasa nende toodete väljatöötamisele, projekteerimisele, valideerimisele ja testimisele käesoleva määruse nõuete täitmise eesmärgil piiratud aja jooksul enne turule laskmist. Komisjon ja asjakohasel juhul ENISA võivad pakkuda tehnilist tuge, nõu ja vahendeid regulatiivliivakastide loomiseks ja tegevuses hoidmiseks. Regulatiivliivakastid luuakse turujärelevalveasutuste otsese järelevalve ja juhendamise all ning nende toel. Liikmesriigid teavitavad komisjoni ja teisi turujärelevalveasutusi ADCO rühma kaudu regulatiivliivakasti loomisest. Regulatiivliivakastid ei mõjuta pädevate asutuste järelevalve- ja parandusvolitusi. Liikmesriigid tagavad regulatiivliivakastidele avatud, õiglase ja läbipaistva juurdepääsu ning hõlbustavad eelkõige mikro- ja väikeettevõtjate, sealhulgas idufirmade juurdepääsu.

3. Komisjon annab kooskõlas artikliga 26 mikro-, väikestele ja keskmise suurusega ettevõtjatele suuniseid käesoleva määruse rakendamiseks.

4. Komisjon annab teada, millist rahalist toetust on võimalik saada olemasolevate liidu programmide õigusraamistikus, eelkõige selleks, et vähendada mikro- ja väikeettevõtjate finantskoormust.

5. Mikro- ja väikeettevõtjad võivad esitada kõik VII lisas määratletud tehnilise dokumentatsiooni elemendid lihtsustatud vormis. Selleks määrab komisjon rakendusaktidega kindlaks mikro- ja väikeettevõtjate vajadusi arvestava lihtsustatud tehnilise dokumentatsiooni vormi, milles nähakse ka ette VII lisas sätestatud elementide esitamise viis. Kui mikro- või väikeettevõtja otsustab esitada VII lisas sätestatud teabe lihtsustatud korras, kasutab ta käesolevas lõikes osutatud vormi. Teada antud asutused peavad seda vormi vastavushindamise tegemisel arvestama.

   Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 62 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 34

Vastastikuse tunnustamise lepingud

Liit võib kooskõlas ELi toimimise lepingu artikliga 218 sõlmida rahvusvahelise kaubanduse edendamiseks ja lihtsustamiseks vastastikuse tunnustamise lepinguid kolmandate riikidega, võttes arvesse kolmanda riigi tehnilise arengu taset ja vastavushindamise põhimõtteid.

IV peatükk
Vastavushindamisasutustest teatamine

Artikkel 35

Teatamine

1. Liikmesriigid teatavad komisjonile ja teistele liikmesriikidele, missugused asutused on volitatud tegema käesoleva määruse alusel vastavushindamisi.

2. Liikmesriigid püüavad tagada hiljemalt … [24 kuud pärast käesoleva määruse jõustumise kuupäeva], et liidus on vastavushindamiste tegemiseks piisav arv teada antud asutusi, et hoida ära kitsaskohad ja takistused turule sisenemisel.

Artikkel 36

Teavitavad asutused

1. Iga liikmesriik määrab teavitava asutuse, kes vastutab vastavushindamisasutuste hindamise, määramise ja nendest teatamise ning nende järelevalveks vajalike menetluste kasutuselevõtmise ja rakendamise eest, sealhulgas artikli 41 järgimise eest.

2. Liikmesriigid võivad otsustada, et lõikes 1 osutatud hindamist ja järelevalvet teeb määruse (EÜ) nr 765/2008 tähenduses ja sellega kooskõlas riiklik akrediteerimisasutus.

3. Kui teavitav asutus delegeerib või teeb käesoleva artikli lõikes 1 osutatud hindamise, teatamise või järelevalve muul viisil ülesandeks asutusele, mis ei ole valitsusasutus, siis peab see asutus olema juriidiline isik ja järgima mutatis mutandis artiklit 37. Lisaks peab sel asutusel olema kord oma tegevusest tulenevate kohustuste katmiseks.

4. Teavitav asutus vastutab täielikult lõikes 3 osutatud asutuse täidetavate ülesannete eest.

Artikkel 37

Nõuded teavitava asutuse kohta

1. Teavitav asutus määratakse nii, et ei tekiks huvide konflikti vastavushindamisasutustega.

2. Teavitava asutuse tööd korraldatakse ja see toimub nii, et on tagatud tema tegevuse objektiivsus ja erapooletus.

3. Teavitava asutuse töö korraldatakse nii, et kõiki vastavushindamisasutusest teatamisega seotud otsuseid teevad sellised pädevad isikud, kes ei ole teinud hindamist.

4. Teavitav asutus ei paku ega osuta neid teenuseid, mida osutavad vastavushindamisasutused, ega ärieesmärgiga või konkureerivaid nõustamisteenuseid.

5. Teavitav asutus tagab saadud teabe konfidentsiaalsuse.

6. Teavitaval asutusel peab tööülesannete nõuetekohaseks täitmiseks olema piisav arv pädevaid töötajaid.

Artikkel 38

Teavitavate asutuste kohta teatamise kohustus

1. Liikmesriigid annavad komisjonile teada vastavushindamisasutuste hindamiseks ja nendest teatamiseks ning teada antud asutuste järelevalveks läbiviidud menetlustest ning nendes menetlustes tehtud muudatustest.

2. Komisjon teeb lõikes 1 osutatud teabe avalikult kättesaadavaks.

Artikkel 39

Nõuded seoses teada antud asutustega

1. Teada andmise eesmärgil peab vastavushindamisasutus vastama lõigete 2–12 nõuetele.

2. Vastavushindamisasutus peab olema asutatud riigisisese õiguse kohaselt ning olema juriidiline isik.

3. Vastavushindamisasutus peab olema kolmandast isikust asutus, mis on sõltumatu organisatsioonist või digielemente sisaldavast tootest, mida ta hindab.

   Asutust, mis kuulub ettevõtjate ühendusse või kutseliitu, mis esindab ettevõtjaid, kes on seotud hinnatavate digielemente sisaldavate toodete projekteerimise, arendamise, tootmise, tarnimise, monteerimise, kasutamise või hooldamisega, võib käsitada sellise kolmandast isikust asutusena tingimusel, et on tõendatud selle sõltumatus ja huvide konflikti puudumine.

4. Vastavushindamisasutus, selle kõrgem juhtkond ja ükski vastavushindamisülesannete täitmise eest vastutav töötaja ei tohi olla hinnatava digielemente sisaldava toote projekteerija, arendaja, tootja, tarnija, importija, turustaja, paigaldaja, ostja, omanik, kasutaja, hooldaja ega ühegi nimetatud isiku esindaja. See ei välista vastavushindamisasutuse tegevuseks vajalike hinnatavate toodete kasutamist või selliste toodete kasutamist isiklikul otstarbel.

Vastavushindamisasutus, selle kõrgem juhtkond ja vastavushindamisülesannete täitmise eest vastutavad töötajad ei tohi olla otseselt seotud nende poolt hinnatavate digielemente sisaldavate toodete projekteerimise, arendamise, tootmise, impordi, turustamise, turundamise, paigaldamise, kasutamise või hooldamisega ega esindada nimetatud tegevustega seotud osalist. Nad ei tohi osaleda üheski tegevuses, mis võib olla vastuolus tehtavate otsuste sõltumatusega või ausameelsusega vastavushindamistoimingutes, mille tegemiseks neist on teada antud. See kehtib eelkõige nõustamisteenuste kohta.

Vastavushindamisasutus tagab, et tema tütarettevõtjate või alltöövõtjate tegevus ei mõjuta vastavushindamistoimingute konfidentsiaalsust, objektiivsust ega erapooletust.

5. Vastavushindamisasutus ja selle töötajad teevad vastavushindamistoiminguid suurima erialase kohusetunde ja konkreetses valdkonnas nõutava tehnilise pädevusega, laskmata end mõjutada mis tahes surveavaldustel ja ahvatlustel (eelkõige rahalistel), millel võib olla mõju nende otsustele või vastavushindamise tulemustele, eriti isikute või isikute rühmade poolt, kes on huvitatud nimetatud toimingute tulemustest.

6. Vastavushindamisasutus peab olema võimeline tegema kõiki VIII lisas nimetatud vastavushindamistoiminguid, millega seoses on temast teada antud, olenemata sellest, kas vastavushindamisasutus täidab neid ülesandeid ise või täidetakse neid tema nimel ja tema vastutusel.

   Vastavushindamisasutusel peavad iga vastavushindamismenetluse ja iga digielemente sisaldava toote tüübi jaoks, millega seoses on temast teada antud, alati olema:

   a) tehniliste teadmistega töötajad, kellel on vastavushindamisülesannete tegemiseks piisavad ja asjakohased kogemused;

   b) menetluste kirjeldused, mille kohaselt vastavushindamist tuleb teha ning mis tagavad läbipaistvuse ja võimaluse neid menetlusi korrata; asjakohased tegevuspõhimõtted ja kord vahe tegemiseks teada antud asutusena tehtavate ja muude tegevuste vahel;

c) menetlused selliste toimingute tegemiseks, milles võetakse asjakohaselt arvesse ettevõtja suurust, tegevusvaldkonda, struktuuri, käsitletava tootetehnoloogia keerukusastet ning seda, kas tegemist on mass- või seeriatootmisega.

Vastavushindamisasutusel peavad olema vajalikud vahendid vastavushindamistoimingute nõuetekohase teostamisega seotud tehniliste ja haldusülesannete täitmiseks ning juurdepääs vajalikule varustusele ja vahenditele.

7. Vastavushindamisülesannete täitmise eest vastutavad töötajad peavad:

a) omama head tehnilist ja kutsealast ettevalmistust kõigi vastavushindamistoimingute tegemiseks, millega seoses on asjaomasest vastavushindamisasutusest teada antud;

b) omama piisavaid teadmisi tehtavate hindamiste nõuete kohta ja ettenähtud volitusi nende hindamiste tegemiseks;

c) tundma ja mõistma I lisas sätestatud olulisi küberturvalisuse nõudeid, kohaldatavaid harmoneeritud standardeid ja ühtseid spetsifikatsioone ning liidu ühtlustamisõigusaktide ja nende rakendusaktide asjakohaseid sätteid;

d) oskama koostada sertifikaate, protokolle ja aruandeid, mis tõendavad vastavushindamise tegemist.

8. Tagatakse vastavushindamisasutuste, nende kõrgema juhtkonna ja hindamise eest vastutavate töötajate erapooletus.

Vastavushindamisasutuse kõrgema juhtkonna ja hindamise eest vastutavate töötajate tasu suurus ei tohi sõltuda tehtud vastavushindamiste hulgast ega nende hindamiste tulemustest.

9. Kui vastutus ei kuulu riigisisese õiguse alusel liikmesriigile või kui liikmesriik ise ei ole vastavushindamise eest otseselt vastutav, siis võtab vastavushindamisasutus endale vastutuskindlustuse.

10. Vastavushindamisasutuse töötajad hoiavad ametisaladust kogu teabe kohta, mis on saadud VIII lisa või selle rakendamiseks kehtestatud riigisisese õiguse sätte kohaste toimingute käigus, välja arvatud teabevahetus selle liikmesriigi turujärelevalveasutustega, kus asutus tegutseb. Tagada tuleb omandiõiguste kaitse. Vastavushindamisasutus rakendab dokumenteeritud menetlusi, mis tagavad vastavuse käesoleva lõikega.

11. Vastavushindamisasutus võtab osa asjakohastest standardimistegevustest ja artikli 51 alusel loodud teada antud asutuste koordineerimisrühma tegevusest või tagab, et tema hindamise eest vastutavaid töötajaid on sellest teavitatud ning kohaldab nimetatud rühma töö tulemusel koostatud haldusotsuseid ja -dokumente üldiste suunistena.

12. Vastavushindamisasutus tegutseb vastavalt sidusatele, õiglastele, proportsionaalsetele ja mõistlikele tingimustele, vältides ettevõtjate liigset koormamist, eelkõige võttes tasude puhul arvesse mikro-, väikeste ja keskmise suurusega ettevõtjate huve.

Artikkel 40

Nõuetele vastavuse eeldamine teada antud asutuste korral

Kui vastavushindamisasutus tõendab, et ta vastab sellistes asjakohastes harmoneeritud standardites või nende osades sätestatud kriteeriumidele, mille viited on avaldatud *Euroopa Liidu Teatajas*, siis eeldatakse, et ta vastab artikli 39 nõuetele, kui kohaldatavad harmoneeritud standardid hõlmavad neid nõudeid.

Artikkel 41

Teada antud asutuste tütarettevõtjad ja alltöövõtjad

1. Kui teada antud asutus kasutab vastavushindamisega seotud ülesannete täitmiseks alltöövõtjat või tütarettevõtjat, siis tagab ta, et alltöövõtja või tütarettevõtja vastab artiklis 39 sätestatud nõuetele, ning teatab sellest teavitavale asutusele.

2. Teada antud asutus vastutab täielikult ülesannete eest, mida täidavad tema alltöövõtjad ja tütarettevõtjad, olenemata nende asukohast.

3. Alltöövõtjat või tütarettevõtjat võib kasutada ainult tootja nõusolekul.

4. Teada antud asutus hoiab teavitavale asutusele esitamiseks alles dokumente alltöövõtja või tütarettevõtja kvalifikatsiooni hindamise kohta ja nende poolt käesoleva määruse kohaselt tehtud tööde kohta.

Artikkel 42

Teada andmise taotlus

1. Vastavushindamisasutus esitab teada andmise taotluse oma asukohaks oleva liikmesriigi teavitavale asutusele.

2. Taotlusega koos esitatakse vastavushindamistoimingute, vastavushindamismenetluse või -menetluste ja digielemente sisaldava toote või toodete kirjeldus, millega tegelemist asutus oma pädevusena taotleb, ning riikliku akrediteerimisasutuse väljastatud akrediteerimistunnistus, kui see on olemas, mis tõendab, et vastavushindamisasutus vastab artikli 39 nõuetele.

3. Kui vastavushindamisasutus ei saa akrediteerimistunnistust esitada, esitab ta teavitavale asutusele kõik dokumentaalsed tõendid, mida on vaja, et kontrollida, kinnitada ja regulaarselt jälgida tema vastavust artiklis 39 esitatud nõuetele.

Artikkel 43

Teada andmise kord

1. Teavitav asutus annab teada ainult nendest vastavushindamisasutustest, mis vastavad artiklis 39 esitatud nõuetele.

2. Teavitav asutus teavitab komisjoni ja teisi liikmesriike teada antud ja määratud organisatsioonide uue teabesüsteemi kaudu, mille on välja töötanud ja mida haldab komisjon.

3. Teavitus sisaldab täielikku ülevaadet vastavushindamistoimingutest, vastavushindamismoodulist või -moodulitest ja digielemente sisaldavast tootest või toodetest ning asjakohast pädevuse kinnitust.

4. Kui teavitus ei põhine artikli 42 lõikes 2 osutatud akrediteerimistunnistusel, siis esitab teavitav asutus komisjonile ja teistele liikmesriikidele dokumentaalsed tõendid, mis kinnitavad vastavushindamisasutuse pädevust ja kehtivat korda, millega tagatakse asutuse regulaarne järelevalve ja selle jätkuv vastavus artikli 39 nõuetele.

5. Asjaomane asutus võib teada antud asutuse toiminguid teha üksnes juhul, kui komisjon või teised liikmesriigid ei esita vastuväiteid kahe nädala jooksul pärast teavituse saamist, kui teavitamine põhines akrediteerimistunnistusel, või kahe kuu jooksul pärast teavituse saamist, kui akrediteerimist ei kasutatud.

   Ainult sellist asutust peetakse käesoleva määruse kohaldamisel teada antud asutuseks.

6. Komisjoni ja teisi liikmesriike teavitatakse kõigist edaspidistest asjakohastest muudatustest nimetatud teavituses.

Artikkel 44

Teada antud asutuste identifitseerimisnumbrid ja loetelud

1. Komisjon määrab teada antud asutusele identifitseerimisnumbri.

   Ta määrab üheainsa identifitseerimisnumbri, isegi kui asutusest antakse teada mitme liidu õigusakti alusel.

2. Komisjon teeb üldsusele kättesaadavaks käesoleva määruse alusel teada antud asutuste loetelu, mis sisaldab asutustele antud identifitseerimisnumbreid ja toiminguid, millega seoses neist on teada antud.

   Komisjon tagab loetelu ajakohastamise.

Artikkel 45

Teavituse muudatused

1. Kui teavitav asutus on kindlaks teinud või talle on teatatud, et teada antud asutus ei vasta enam artikli 39 nõuetele või ei ole täitnud ettenähtud kohustusi, siis kitsendab teavitav asutus teavitust, peatab teavituse või tühistab selle, lähtudes sellest, kui suur on nõuetele mittevastavus või kohustuste täitmata jätmine. Ta teatab sellest viivitamata komisjonile ja teistele liikmesriikidele.

2. Kui teavitust kitsendatakse või kui selle kehtivus peatatakse või tühistatakse või kui teada antud asutus on lõpetanud tegevuse, siis on teavitava liikmesriigi ülesanne tagada, et selle asutuse dokumente menetleb mõni teine teada antud asutus või et need oleksid taotluse korral kättesaadavad teavitavale asutusele turujärelevalveasutustele.

Artikkel 46

Teada antud asutuse pädevuse vaidlustamine

1. Komisjon uurib iga juhtumit, mil tal tekib kahtlus, või kui tema tähelepanu juhitakse kahtlusele seoses teada antud asutuse pädevusega täita või jätkuvalt täita talle esitatud nõudeid ja talle pandud kohustusi.

2. Komisjoni taotluse korral esitab teavitav liikmesriik talle kogu teabe selle kohta, mille alusel konkreetsest asutusest teada anti, või mis näitab, et see asutus on endiselt pädev.

3. Komisjon tagab, et kogu tundlikku teavet, mis uurimise käigus saadi, käsitletakse konfidentsiaalsena.

4. Kui komisjon teeb kindlaks, et teada antud asutus ei täida või enam ei täida temast teada andmise aluseks olevaid nõudeid, teavitab ta sellest teavitavat liikmesriiki ja nõuab temalt vajalike parandusmeetmete võtmist, sealhulgas vajaduse korral teada andmise tühistamist.

Artikkel 47

Teada antud asutuse tegevuskohustused

1. Teada antud asutus teeb vastavushindamist kooskõlas artiklis 32 ja VIII lisas esitatud vastavushindamismenetlustega.

2. Vastavushindamisi tehakse proportsionaalsel viisil, vältides ettevõtjate liigset koormamist. Vastavushindamisasutus võtab oma tegevuse käigus asjakohaselt arvesse ettevõtja suurust, eelkõige mikro- ning väikeste ja keskmise suurusega ettevõtjate puhul, tegevusvaldkonda, struktuuri, keerukusastet ning digielemente sisaldavate toodete ja kõnealuse tehnoloogia küberriski taset ning seda, kas tegemist on mass- või seeriatootmisega.

3. Seejuures arvestab teada antud asutus, millist rangust ja kaitset on vaja, et digielemente sisaldav toode vastaks käesoleva määruse nõuetele.

4. Kui teada antud asutus leiab, et tootja ei ole kinni pidanud I lisas või vastavates harmoneeritud standardites või artikli 27 kohastes ühtsetes spetsifikatsioonides sätestatud nõuetest, nõuab ta kõnealuselt tootjalt nõuetekohaste parandusmeetmete võtmist ja ei väljasta vastavussertifikaati.

5. Kui pärast sertifikaadi väljastamist avastab teada antud asutus nõuetele vastavuse jälgimisel, et digielemente sisaldav toode ei vasta enam käesoleva määruse nõuetele, nõuab ta tootjalt asjakohaste parandusmeetmete võtmist ja vajaduse korral peatab sertifikaadi või tunnistab selle kehtetuks.

6. Kui parandusmeetmeid ei võeta või neil ei ole soovitud tulemust, siis teada antud asutus vastavalt vajadusele kas kitsendab asjaomast sertifikaati või peatab sertifikaadi või tunnistab selle kehtetuks.

Artikkel 48

Teada antud asutuste otsuste vaidlustamine

Liikmesriigid tagavad, et teada antud asutuste otsuste vaidlustamiseks on olemas asjakohane menetlus.

Artikkel 49

Teada antud asutuse teabekohustus

1. Teada antud asutus annab teavitavale asutusele teada järgmisest:

   a) kõik juhtumid, kui sertifikaat jäetakse andmata, seda kitsendatakse, see peatatakse või tunnistatakse kehtetuks;

   b) teavitamise valdkonda ja tingimusi mõjutavad asjaolud;

c) kõik turujärelevalveasutustelt saadud teabetaotlused vastavushindamistoimingute kohta;

d) (taotluse korral) vastavushindamistoimingud, mida teada antud asutus on teavitusvaldkonnas teinud, ja muu tegevus, sealhulgas piiriülene tegevus ja alltöövõtt.

2. Teada antud asutused esitavad teistele käesoleva määruse alusel teada antud samalaadsete vastavushindamistoimingute ja samade digielemente sisaldavate toodetega tegelevatele asutustele asjakohase teabe negatiivsete ja taotluse korral ka positiivsete vastavushindamistulemuste kohta.

Artikkel 50

Kogemuste vahetamine

Komisjon korraldab kogemuste vahetamise liikmesriikides teavituspoliitika eest vastutavate ametiasutuste vahel.

Artikkel 51

Teada antud asutuste tegevuse koordineerimine

1. Komisjon tagab teada antud asutuste vahel sobiva koordineerimise ja koostöö, mida ettenähtud viisil korraldab teada antud asutuste valdkonnaülene rühm.

2. Liikmesriigid tagavad oma teada antud asutuste osalemise nimetatud rühma töös otseselt või määratud esindajate vahendusel.

V peatükk

Turujärelevalve ja täitmise tagamine

Artikkel 52

Digielemente sisaldavate toodete turujärelevalve ja kontroll liidu turul

1. Käesoleva määruse kohaldamisalasse kuuluvate digielemente sisaldavate toodete suhtes kohaldatakse määrust (EL) 2019/1020.

2. Käesoleva määruse tulemuslikuks kohaldamiseks määrab iga liikmesriik ühe või mitu turujärelevalveasutust. Liikmesriigid võivad määrata käesoleva määruse kohaseks turujärelevalveasutuseks olemasoleva või uue asutuse.

3. Käesoleva artikli lõike 2 kohaselt määratud turujärelevalveasutused vastutavad ka turujärelevalvetoimingute tegemise eest seoses artiklis 24 sätestatud avatud lähtekoodiga tarkvara korraldajate kohustustega. Kui turujärelevalveasutus leiab, et avatud lähtekoodiga tarkvara korraldaja ei täida kõnealuses artiklis sätestatud kohustusi, nõuab ta avatud lähtekoodiga tarkvara korraldajalt kõigi asjakohaste parandusmeetmete võtmise tagamist. Avatud lähtekoodiga tarkvara korraldajad tagavad, et nende käesolevast määrusest tulenevate kohustuste täitmiseks võetakse kõik asjakohased parandusmeetmed.

4. Vajaduse korral teevad turujärelevalveasutused koostööd määruse (EL) 2019/881 artikli 58 kohaselt määratud riiklike küberturvalisuse sertifitseerimise asutustega ja vahetavad korrapäraselt teavet. Käesoleva määruse artikli 14 kohaste teatamiskohustuste täitmise järelevalvel teevad määratud turujärelevalveasutused koostööd ja vahetavad korrapäraselt teavet koordinaatoriks määratud CSIRTide ja ENISAga.

5. Turujärelevalveasutused võivad taotleda koordinaatoriks määratud CSIRTilt või ENISA-lt tehnilist nõu küsimustes, mis on seotud käesoleva määruse rakendamise ja täitmise tagamisega. Artikli 54 kohase uurimise tegemisel võivad turujärelevalveasutused taotleda koordinaatoriks määratud CSIRTilt või ENISA-lt analüüsi tegemist digielemente sisaldavate toodete vastavuse hindamise toetamiseks.

6. Vajaduse korral teevad turujärelevalveasutused koostööd teiste turujärelevalveasutustega, kes on määratud käesolevast määrusest erinevate liidu ühtlustamisõigusaktide alusel muude toodete jaoks, ning vahetavad korrapäraselt teavet.

7. Turujärelevalveasutused teevad vajaduse korral koostööd liidu andmekaitseõiguse üle järelevalvet tegevate asutustega. Selline koostöö hõlmab nende asutuste teavitamist kõigist järeldustest, mis on nende pädevuste jaoks asjakohased, sealhulgas lõike 10 kohaste suuniste ja nõuannete andmisel, kui sellised suunised ja nõuanded on seotud isikuandmete töötlemisega.

   Liidu andmekaitseõiguse üle järelevalvet tegevatel asutustel on õigus taotleda ja juurde pääseda käesoleva määruse alusel loodud või säilitatavatele dokumentidele, kui juurdepääs nendele dokumentidele on vajalik nende ülesannete täitmiseks. Nad teavitavad asjaomase liikmesriigi määratud turujärelevalveasutusi igast sellisest taotlusest.

8. Liikmesriigid tagavad, et määratud turujärelevalveasutustel on käesolevast määrusest tulenevate ülesannete täitmiseks piisavad rahalised ja tehnilised vahendid, sh asjakohasel juhul töötlemise automatiseerimise vahendid, ja vajalike küberturbeoskustega inimressursid.

9. Komisjon julgustab ja hõlbustab määratud turujärelevalveasutuste vahelist kogemuste vahetamist.

10. Turujärelevalveasutused võivad komisjoni ja asjakohasel juhul CSIRTide ja ENISA toetusel anda ettevõtjatele suuniseid ja nõu käesoleva määruse rakendamise kohta.

11. Turujärelevalveasutused teavitavad tarbijaid kooskõlas määruse (EL) 2019/1020 artikliga 11 sellest, kuhu esitada kaebusi, mis võivad osutada mittevastavusele käesoleva määruse nõuetele, ning annavad tarbijatele teavet selle kohta, kus ja kuidas on võimalik kasutada mehhanisme, et hõlbustada digielemente sisaldavaid tooteid mõjutada võivatest nõrkustest, intsidentidest ja küberohtudest teatamist.

12. Turujärelevalveasutused hõlbustavad vajaduse korral koostööd asjaomaste sidusrühmadega, sealhulgas teadus-, uurimis- ja tarbijaorganisatsioonidega.

13. Turujärelevalveasutused esitavad komisjonile iga-aastasi aruandeid asjakohaste turujärelevalvetoimingute tulemuste kohta. Määratud turujärelevalveasutused esitavad komisjonile ja asjaomastele riiklikele konkurentsiasutustele viivitamata kogu turujärelevalvetoimingute käigus kindlaks tehtud teabe, mis võib pakkuda huvi liidu konkurentsiõiguse kohaldamise seisukohast.

14. Käesoleva määruse kohaldamisalasse kuuluvate digielemente sisaldavate toodete puhul, mis on määruse (EL) 2024/1689 artikli 6 kohaselt liigitatud suure riskiga tehisintellektisüsteemideks, on määruse (EL) 2024/1689kohaselt määratud turujärelevalveasutused need asutused, kes vastutavad käesoleva määrusega nõutava turujärelevalve eest. Määruse (EL) 2024/1689 kohaselt määratud turujärelevalveasutused teevad asjakohasel juhul koostööd käesoleva määruse kohaselt määratud turujärelevalveasutustega ning käesoleva määruse artikli 14 kohaste teatamiskohustuste täitmise järelevalve puhul koordinaatoriks määratud CSIRTide ja ENISAga. Määruse (EL) 2024/1689 kohaselt määratud turujärelevalveasutused teavitavad käesoleva määruse kohaselt määratud turujärelevalveasutusi eelkõige järeldustest, mis on asjakohased nende käesoleva määruse rakendamisega seotud ülesannete täitmiseks.

15. Käesoleva määruse ühetaoliseks kohaldamiseks luuakse ADCO rühm vastavalt määruse (EL) 2019/1020 artikli 30 lõikele 2. ADCO rühm koosneb määratud turujärelevalveasutuste esindajatest ning asjakohasel juhul ühtsete kontaktasutuste esindajatest. ADCO rühm käsitleb ka konkreetseid küsimusi, mis on seotud turujärelevalvetoimingutega seoses avatud lähtekoodiga tarkvara korraldajatele pandud kohustustega.

16. Turujärelevalveasutused jälgivad, kuidas tootjad on oma digielemente sisaldavate toodete toe kestuse kindlaksmääramisel kohaldanud artikli 13 lõikes 8 osutatud kriteeriume.

ADCO rühm avaldab avalikult kättesaadaval ja kasutajasõbralikul moel asjakohase statistika digielemente sisaldavate toodete kategooriate kohta, sealhulgas toe keskmise kestuse, mille tootja on kindlaks määranud vastavalt artikli 13 lõikele 8, ning annab suuniseid, mis sisaldavad toe soovituslikku kestust digielemente sisaldavate toodete kategooriate jaoks.

Kui andmed osutavad digielemente sisaldavate toodete teatavate kategooriate toe ebapiisavale kestusele, võib ADCO rühm anda turujärelevalveasutustele soovitusi keskenduda oma tegevuses sellistele digielemente sisaldavate toodete kategooriatele.

Artikkel 53

Juurdepääs andmetele ja dokumentatsioonile

Kui see on vajalik, et hinnata digielemente sisaldavate toodete ja tootjate rakendatud protsesside vastavust I lisas sätestatud olulistele küberturvalisuse nõuetele, antakse turujärelevalveasutustele põhjendatud taotluse korral juurdepääs neile kergesti arusaadavas keeles esitatud andmetele, mida on vaja selliste toodete projekteerimise, arendamise, tootmise ja nõrkuste käsitlemise hindamiseks, sealhulgas asjaomase ettevõtja sisedokumentidele.

Artikkel 54

Olulist küberriski põhjustava digielemente sisaldava toote riikliku tasandi menetlus

1. Kui liikmesriigi turujärelevalveasutusel on piisavalt põhjust arvata, et digielemente sisaldav toode, sh selle nõrkuste käsitlemine, põhjustab olulist küberriski, korraldab ta viivitamata ning asjakohasel juhul koostöös asjaomase CSIRTiga asjaomase digielemente sisaldava toote hindamise, et selgitada välja, kas toode vastab käesolevas määruses sätestatud nõuetele. Asjaomased ettevõtjad teevad turujärelevalveasutustega sel eesmärgil vajaduse korral koostööd.

Kui turujärelevalveasutus leiab hindamise tegemisel, et digielemente sisaldav toode ei vasta käesoleva määruse nõuetele, nõuab ta viivitamata, et asjaomane ettevõtja kas võtaks kõik vajalikud parandusmeetmed digielemente sisaldava toote vastavusse viimiseks nende nõuetega või kõrvaldaks selle turult või võtaks selle tagasi turujärelevalveasutuse poolt määratud mõistliku aja jooksul, mis vastab küberriski laadile.

Turujärelevalveasutus teatab sellest asjakohasele teada antud asutusele. Parandusmeetmete suhtes kehtib määruse (EL) 2019/1020 artikkel 18.

2. Käesoleva artikli lõikes 1 osutatud küberriski olulisuse kindlaksmääramisel võtavad turujärelevalveasutused arvesse ka mittetehnilisi riskitegureid, eelkõige neid, mis on tehtud kindlaks direktiivi (EL) 2022/2555 artikli 22 kohaselt tehtud liidu tasandi kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamise tulemusel. Kui turujärelevalveasutusel on piisavalt põhjust arvata, et digielemente sisaldav toode kujutab endast mittetehnilisi riskitegureid arvestades olulist küberriski, teavitab ta sellest direktiivi (EL) 2022/2555 artikli 8 kohaselt määratud või asutatud pädevaid asutusi ning teeb vajaduse korral nende asutustega koostööd.

3. Kui turujärelevalveasutus on seisukohal, et mittevastavus ei piirdu üksnes nende liikmesriigiga, siis teavitab ta komisjoni ja teisi liikmesriike hindamise tulemustest ja meetmetest, mille võtmist ta on ettevõtjalt nõudnud.

4. Ettevõtja tagab, et kõik vajalikud parandusmeetmed võetakse kõigi asjakohaste digielemente sisaldavate toodete korral, mille ta on liidu turul kättesaadavaks teinud.

5. Kui ettevõtja ei võta lõike 1 teises lõigus osutatud aja jooksul piisavaid parandusmeetmeid, siis rakendab turujärelevalveasutus kõiki asjakohaseid ajutisi meetmeid, et kõnealuse digielemente sisaldava toote kättesaadavaks tegemine siseturul keelata või seda piirata, digielemente sisaldav toode turult kõrvaldada või see tagasi võtta.

   Turujärelevalveasutus teavitab komisjoni ja teisi liikmesriike nimetatud meetmetest viivitamata.

6. Lõikes 5 osutatud teave hõlmab kõiki kättesaadavaid andmeid: eelkõige nõuetele mittevastava digielemente sisaldava toote identifitseerimisandmed, selle digielemente sisaldava toote päritolu, väidetava mittevastavuse ja kaasneva riski laad, liikmesriigis võetud meetmete laad ja kestus ning asjaomase ettevõtja esitatud seisukohad. Turujärelevalveasutus näitab eelkõige, kas mittevastavus on seotud mõnega järgmistest põhjustest:

   a) digielemente sisaldav toode või tootja rakendatud protsessid ei vasta I lisas sätestatud olulistele küberturvalisuse nõuetele;

   b) puudused artiklis 27 osutatud harmoneeritud standardites, Euroopa küberturvalisuse sertifitseerimise kavades või ühtsetes spetsifikatsioonides.

7. Teiste liikmesriikide turujärelevalveasutused, kes ei ole menetluse algatajad, teatavad viivitamata komisjonile ja teistele liikmesriikidele nende võetud meetmetest ja mis tahes muust nende käsutuses olevast asjaomase digielemente sisaldava toote mittevastavusega seotud teabest ning kui nad ei ole teada antud riigisisese meetmega nõus, siis ka oma vastuväidetest.

8. Kui kolme kuu jooksul alates käesoleva artikli lõikes 5 osutatud teate kättesaamisest ei ole teised liikmesriigid ega komisjon esitanud vastuväiteid liikmesriigi ajutise meetme suhtes, loetakse meede põhjendatuks. See ei piira asjaomase ettevõtja määruse (EL) 2019/1020 artikli 18 kohaseid menetlusõigusi.

9. Kõigi liikmesriikide turujärelevalveasutused tagavad, et asjaomase digielemente sisaldava toote suhtes võetakse viivitamata asjakohaseid piiravaid meetmeid, näiteks kõrvaldatakse toode liikmesriigi turult.

Artikkel 55

Liidu kaitsemeetmete menetlus

1. Kui kolme kuu jooksul alates artikli 54 lõikes 5 osutatud teate kättesaamisest esitab mõni liikmesriik teise liikmesriigi võetud meetmele vastuväiteid või kui komisjon arvab, et meede on liidu õigusega vastuolus, siis algatab komisjon liikmesriigi meetme hindamiseks viivitamata konsulteerimise asjaomase liikmesriigiga ja asjaomase ettevõtja või asjaomaste ettevõtjatega. Selle hindamise tulemuste põhjal otsustab komisjon üheksa kuu jooksul alates artikli 54 lõikes 5 osutatud teate saamisest, kas riiklik meede on põhjendatud või mitte, ning teatab selle otsuse asjaomasele liikmesriigile.

2. Kui liikmesriigi meede loetakse põhjendatuks, siis võtavad kõik liikmesriigid vajalikke meetmeid, et tagada nõuetele mittevastava digielemente sisaldava toote kõrvaldamine oma turult, ja teatavad sellest komisjonile. Kui riiklikku meedet peetakse põhjendamatuks, tunnistab asjaomane liikmesriik selle kehtetuks.

3. Kui liikmesriigi meede loetakse põhjendatuks ja digielemente sisaldava toote nõuetele mittevastavus loetakse tulenevat puudustest harmoneeritud standardites, kohaldab komisjon määruse (EL) nr 1025/2012 artikliga 11 ettenähtud menetlust.

4. Kui riiklik meede loetakse põhjendatuks ja digielemente sisaldava toote mittevastavus loetakse tulenevat puudustest artiklis 27 osutatud Euroopa küberturvalisuse sertifitseerimise kavas, kaalub komisjon, kas muuta vastavalt artikli 27 lõikele 9 vastu võetud delegeeritud õigusakti, milles on sätestatud kõnealusele sertifitseerimiskavale vastavuse eeldus, või tunnistada see kehtetuks.

5. Kui riiklik meede loetakse põhjendatuks ja digielemente sisaldava toote mittevastavus loetakse tulenevat puudustest artiklis 27 osutatud ühtsetes spetsifikatsioonides, kaalub komisjon, kas muuta ühtseid spetsifikatsioone käsitlevat artikli 27 lõike 2 kohaselt vastu võetud rakendusakti või tunnistada see kehtetuks.

Artikkel 56

Olulist küberriski põhjustava digielemente sisaldava toote liidu tasandi menetlus

1. Kui komisjonil on piisavalt põhjust arvata, muu hulgas ENISA-lt saadud teabe põhjal, et olulise küberriskiga digielemente sisaldav toode ei vasta käesolevas määruses sätestatud nõuetele, teavitab ta asjaomaseid turujärelevalveasutusi. Kui turujärelevalveasutused hindavad seda digielemente sisaldavat toodet, mis võib kujutada endast olulist küberriski seoses käesolevas määruses sätestatud nõuetele vastavusega, kohaldatakse artiklites 54 ja 55 osutatud menetlusi.

2. Kui komisjonil on piisavalt põhjust arvata, et digielemente sisaldav toode kujutab endast mittetehnilisi riskitegureid arvestades olulist küberriski, teavitab ta sellest asjaomast turujärelevalveasutust ja asjakohasel juhul direktiivi (EL) 2022/2555 artikli 8 kohaselt määratud või asutatud pädevaid asutusi ning teeb vajaduse korral nende asutustega koostööd. Komisjon võtab arvesse ka tuvastatud riskide tähtsust digielemente sisaldava toote seisukohalt, pidades silmas oma ülesandeid, mis on seotud direktiivi (EL) 2022/2555 artiklis 22 sätestatud liidu tasandi kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamistega, ning konsulteerib vajaduse korral direktiivi (EL) 2022/2555 artikli 14 kohaselt loodud koostöörühma ja ENISAga.

3. Asjaoludel, mis õigustavad viivitamatut sekkumist siseturu nõuetekohase toimimise jätkumiseks, ning kui komisjonil on piisavalt põhjust arvata, et lõikes 1 osutatud digielemente sisaldav toode ei vasta endiselt käesoleva määruse nõuetele ja asjaomased turujärelevalveasutused ei ole võtnud tulemuslikke meetmeid, teeb komisjon vastavushindamise ning võib paluda ENISA-l teha hindamist toetava analüüsi. Komisjon teavitab sellest asjaomaseid turujärelevalveasutusi. Asjaomased ettevõtjad teevad ENISAga vajalikul viisil koostööd.

4. Lõikes 3 osutatud hinnangu põhjal võib komisjon otsustada, et liidu tasandil on vaja võtta parandusmeede või piirav meede. Selleks konsulteerib komisjon viivitamata asjaomaste liikmesriikidega ja asjaomase ettevõtja või asjaomaste ettevõtjatega.

5. Käesoleva artikli lõikes 4 osutatud konsulteerimise põhjal võib komisjon võtta vastu rakendusakte, et näha ette liidu tasandi parandusmeetmed või piiravad meetmed, sealhulgas nõuda asjaomaste digielemente sisaldavate toodete turult kõrvaldamist või tagasivõtmist mõistliku aja jooksul, mis vastab riski laadile. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 62 lõikes 2 osutatud kontrollimenetlusega.

6. Komisjon teavitab lõikes 5 osutatud rakendusaktidest viivitamata asjaomast ettevõtjat või asjaomaseid ettevõtjaid. Liikmesriigid rakendavad neid rakendusakte viivitamata ja teatavad sellest komisjonile.

7. Lõikeid 3–6 kohaldatakse komisjoni sekkumist õigustanud erakorralise olukorra ajal, eeldusel et asjaomast digielemente sisaldavat toodet ei ole viidud vastavusse käesoleva määrusega.

Artikkel 57

Nõuetele vastavad digielemente sisaldavad tooted, mis kujutavad endast olulist küberriski

1. Liikmesriigi turujärelevalveasutus nõuab, et ettevõtja võtaks kõik asjakohased meetmed, kui ta leiab pärast artikli 54 kohast hindamist, et kuigi digielemente sisaldav toode ja tootja rakendatud protsessid on käesoleva määrusega kooskõlas, kujutavad need endast olulist küberriski ning ühtlasi riski järgmisele:

   a) inimeste tervisele või ohutusele;

   b) põhiõiguste kaitseks ette nähtud liidu või riigisisesest õigusest tulenevate kohustuste täitmisele;

c) direktiivi (EL) 2022/2555 artikli 3 lõikes 1 osutatud elutähtsate üksuste poolt elektroonilise infosüsteemi kaudu pakutavate teenuste kättesaadavusele, autentsusele, terviklusele või konfidentsiaalsusele või

d) muudele avaliku huvi kaitse aspektidele.

Esimeses lõigus osutatud meetmed võivad sisaldada meetmeid tagamaks, et asjaomase digielemente sisaldava toote ja tootja rakendatud protsessidega ei kaasne turul kättesaadavaks tegemisel enam asjaomaseid riske, asjaomase digielemente sisaldava toote turult kõrvaldamist või selle tagasivõtmist, ning need meetmed peavad vastama kõnealuste riskide laadile.

2. Tootja või muud asjaomased ettevõtjad tagavad, et parandusmeetmeid võetakse kõigi asjaomaste digielemente sisaldavate toodete suhtes, mille nad on liidu turul kättesaadavaks teinud, lõikes 1 osutatud liikmesriigi turujärelevalveasutuse kehtestatud tähtaja jooksul.

3. Liikmesriik teavitab komisjoni ja teisi liikmesriike viivitamata lõike 1 kohaselt võetud meetmetest. Kõnealune teave peab sisaldama kõiki teadaolevaid üksikasju, eelkõige asjaomaste digielemente sisaldavate toodete tuvastamiseks vajalikke andmeid, kõnealuste digielemente sisaldavate toodete päritolu ja tarneahelat, kaasneva riski laadi ning liikmesriigis võetud meetmete laadi ja kestust.

4. Komisjon alustab viivitamata konsultatsioone liikmesriikidega ja asjaomase ettevõtjaga ning hindab võetud riiklikke meetmeid. Selle hindamise tulemuste põhjal otsustab komisjon, kas meede on põhjendatud või ei ole, ning teeb vajaduse korral ettepaneku sobivate meetmete kohta.

5. Komisjon adresseerib lõikes 4 osutatud otsuse liikmesriikidele.

6. Kui komisjonil on piisavalt põhjust arvata, muu hulgas ENISA-lt saadud teabe põhjal, et digielemente sisaldava tootega, mis küll vastab käesoleva määruse nõuetele, kaasnevad käesoleva artikli lõikes 1 osutatud riskid, teavitab ta sellest asjaomast turujärelevalveasutust või asjaomaseid turujärelevalveasutusi ning võib paluda tal/neil teha hindamise ja järgida artiklis 54 ning käesoleva artikli lõigetes 1, 2 ja 3 osutatud menetlusi.

7. Asjaoludel, mis õigustavad viivitamatut sekkumist siseturu nõuetekohase toimimise jätkumiseks ja kui komisjonil on piisavalt põhjust arvata, et lõikes 6 osutatud digielemente sisaldav toode kujutab endast jätkuvalt lõikes 1 osutatud riske ja asjaomased riiklikud turujärelevalveasutused ei ole võtnud tulemuslikke meetmeid, hindab komisjon kõnealusest digielemente sisaldavast tootest tulenevaid riske ning võib paluda ENISA-l esitada analüüsi, et kõnealust hinnangut toetada, ja teavitab sellest asjaomaseid turujärelevalveasutusi. Asjaomased ettevõtjad teevad ENISAga vajalikul viisil koostööd.

8. Lõikes 7 osutatud hinnangu põhjal võib komisjon teha kindlaks, et liidu tasandil on vaja võtta parandusmeede või piirav meede. Selleks konsulteerib komisjon viivitamata asjaomaste liikmesriikidega ja asjaomas(t)e ettevõtja(te)ga.

9. Käesoleva artikli lõikes 8 osutatud konsulteerimise põhjal võib komisjon võtta vastu rakendusakte, et teha otsus liidu tasandi parandusmeetmete või piiravate meetmete kohta, sealhulgas nõuda asjaomaste digielemente sisaldavate toodete turult kõrvaldamist või tagasivõtmist mõistliku aja jooksul, mis vastab riski laadile. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 62 lõikes 2 osutatud kontrollimenetlusega.

10. Komisjon edastab lõikes 9 osutatud rakendusaktid viivitamata asjaomas(t)ele ettevõtja(te)le. Liikmesriigid rakendavad neid rakendusakte viivitamata ja teavitavad sellest komisjoni.

11. Lõikeid 6–10 kohaldatakse komisjoni sekkumist õigustanud erakorralise olukorra ajal ja seni, kuni asjaomane digielemente sisaldav toode kujutab endast jätkuvalt lõikes 1 osutatud riske.

Artikkel 58

Vormiline nõuetele mittevastavus

1. Kui mõne liikmesriigi turujärelevalveasutus on avastanud ühe järgmistest asjaoludest, nõuab ta, et asjaomane tootja lõpetaks asjaomase nõuetele mittevastavuse:

   a) CE-vastavusmärgise kinnitamisel ei ole järgitud artiklite 29 ja 30 nõudeid;

   b) CE-vastavusmärgist ei ole kinnitatud;

   c) ELi vastavusdeklaratsiooni ei ole koostatud;

   d) ELi vastavusdeklaratsioon ei ole koostatud nõuetekohaselt;

e) vastavushindamises osaleva teada antud asutuse identifitseerimisnumbrit ei ole kinnitatud, kui see on asjakohane;

f) tehniline dokumentatsioon ei ole kättesaadav või ei ole täielik.

2. Kui lõikes 1 osutatud nõuetele mittevastavust ei kõrvaldata, võtab asjaomane liikmesriik kõik vajalikud meetmed digielemente sisaldava toote turul kättesaadavaks tegemise piiramiseks või keelamiseks või tagab toote turult tagasivõtmise või kõrvaldamise.

Artikkel 59

Turujärelevalveasutuste ühismeetmed

1. Turujärelevalveasutused võivad leppida teiste asjaomaste asutustega kokku ühismeetmetes, mille eesmärk on tagada küberturvalisus ja tarbijate kaitse seoses konkreetsete turule lastud või turul kättesaadavaks tehtud digielemente sisaldavate toodetega, eelkõige digielemente sisaldavate toodetega, millega sageli kaasnevad küberriskid.

2. Komisjon või ENISA teeb ettepaneku ühismeetmete kohta, mida turujärelevalveasutused võtavad käesoleva määruse nõuete täitmise kontrollimiseks, võttes aluseks andmed või teabe selle kohta, et käesoleva määruse kohaldamisalasse kuuluvad digielemente sisaldavad tooted tõenäoliselt ei vasta mitmes liikmesriigis käesolevas määruses sätestatud nõuetele.

3. Turujärelevalveasutused ja asjakohasel juhul komisjon tagavad, et ühismeetmete kokkulepe ei põhjusta ettevõtjate vahelist ebaausat konkurentsi ega kahjusta kokkuleppe osaliste objektiivsust, sõltumatust ja erapooletust.

4. Turujärelevalveasutus võib mis tahes uurimise käigus võetud ühismeetmete tulemusel saadud teavet kasutada.

5. Asjaomane turujärelevalveasutus ja asjakohasel juhul komisjon teevad ühismeetmete kokkuleppe, sealhulgas selle osaliste nimed, üldsusele kättesaadavaks.

Artikkel 60

Lauskontrollid

1. Turujärelevalveasutused võtavad teatavate digielemente sisaldavate toodete või nende kategooriate suhtes samaaegseid koordineeritud kontrollimeetmeid (lauskontrollid), et kontrollida nende vastavust käesolevale määrusele või avastada määruse rikkumisi. Need lauskontrollid võivad hõlmata variisikuna soetatud digielemente sisaldavate toodete kontrollimist.

2. Kui asjaomased turujärelevalveasutused ei ole kokku leppinud teisiti, koordineerib lauskontrolle komisjon. Lauskontrolli koordinaator teeb asjakohasel juhul koondtulemused üldsusele kättesaadavaks.

3. Kui ENISA määrab oma ülesannete täitmisel, sealhulgas artikli 11 lõigete 1 ja 3 kohaselt saadud teavituste põhjal kindlaks digielemente sisaldavate toodete kategooriad, mille puhul võib korraldada lauskontrolle, esitab ta lauskontrolli ettepaneku käesoleva artikli lõikes 2 osutatud koordinaatorile, et turujärelevalveasutused selle läbi vaataksid.

4. Lauskontrolle tehes võivad asjaomased turujärelevalveasutused kasutada artiklites 52–58 sätestatud uurimisõigusi ja kõiki muid neile riigisisese õigusega antud õigusi.

5. Turujärelevalveasutused võivad kutsuda lauskontrollidel osalema komisjoni ametnikke ja teisi komisjoni volitatud isikuid.

VI peatükk
Delegeeritud volitused ja komiteemenetlus

Artikkel 61

Delegeeritud volituste rakendamine

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

2. Artikli 2 lõike 5 teises lõigus, artikli 7 lõikes 3, artikli 8 lõigetes 1 ja 2, artikli 13 lõike 8 neljandas lõigus, artikli 14 lõikes 9, artiklis 25, artikli 27 lõikes 9, artikli 28 lõikes 5 ja artikli 31 lõikes 5 osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile viieks aastaks alates … [käesoleva määruse jõustumise kuupäev]. Komisjon esitab delegeeritud volituste kohta aruande hiljemalt üheksa kuud enne viieaastase tähtaja möödumist. Volituste delegeerimist pikendatakse 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 2 lõike 5 teises lõigus, artikli 7 lõikes 3, artikli 8 lõigetes 1 ja 2, artikli 13 lõike 8 neljandas lõigus, artikli 14 lõikes 9, artiklis 25, artikli 27 lõikes 9, artikli 28 lõikes 5 ja artikli 31 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 nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.

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

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

6. Artikli 2 lõike 5 teise lõigu, artikli 7 lõike 3, artikli 8 lõigete 1 ja 2, artikli 13 lõike 8 neljanda lõigu, artikli 14 lõike 9, artikli 25, artikli 27 lõike 9, artikli 28 lõike 5 ja artikli 31 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 vastuväidet või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväidet. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kahe kuu võrra.

Artikkel 62

Komiteemenetlus

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

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

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

VII peatükk
Konfidentsiaalsus ja karistused

Artikkel 63

Konfidentsiaalsus

1. Kõik käesoleva määruse kohaldamises osalejad austavad oma ülesannete täitmisel ja tegevuse käigus saadud teabe ja andmete konfidentsiaalsust, et kaitsta eeskätt järgmist:

   a) intellektuaalomandiõigused ning füüsilise või juriidilise isiku konfidentsiaalne äriteave või ärisaladused, kaasa arvatud lähtekood, välja arvatud juhtudel, millele on viidatud Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/943[36] artiklis 5;

   b) käesoleva määruse tulemuslik rakendamine, eelkõige inspekteerimise, uurimise ja auditite eesmärgil;

   c) avaliku ja riigi julgeolekuga seotud huvid;

   d) kriminaal- või haldusmenetluste usaldusväärsus.

[36] Euroopa Parlamendi ja nõukogu 8. juuni 2016. aasta direktiiv (EL) 2016/943, milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset (ELT L 157, 15.6.2016, lk 1).

2. Ilma et see piiraks lõike 1 kohaldamist, ei avaldata turujärelevalveasutuste vahel ning turujärelevalveasutuste ja komisjoni vahel konfidentsiaalsena vahetatud teavet enne, kui selleks on andnud nõusoleku turujärelevalveasutus, kust teave pärineb.

3. Lõiked 1 ja 2 ei mõjuta komisjoni, liikmesriikide ja teada antud asutuste õigust ja kohustust vahetada teavet ja edastada hoiatusi ega asjaomaste isikute kohustust anda teavet liikmesriikide kriminaalõiguse alusel.

4. Komisjon ja liikmesriigid võivad vajaduse korral vahetada tundlikku teavet nende kolmandate riikide asutustega, kellega nad on sõlminud kahe- või mitmepoolsed konfidentsiaalsuse kokkulepped, mis tagavad piisava kaitsetaseme.

Artikkel 64

Karistused

1. Liikmesriigid kehtestavad käesoleva määruse rikkumise korral kohaldatavad karistusnormid ja võtavad kõik vajalikud meetmed nende rakendamise tagamiseks. Kehtestatud karistused peavad olema mõjusad, proportsionaalsed ja hoiatavad. Liikmesriigid teavitavad komisjoni viivitamata nimetatud normidest ja meetmetest ning teavitavad teda viivitamata nende hilisematest muudatustest.

2. Kui toode ei vasta I lisas sätestatud olulistele küberturvalisuse nõuetele ning artiklites 13 ja 14 nimetatud kohustustele, kohaldatakse haldustrahvi kuni 15 000 000 eurot või, kui rikkuja on ettevõtja, kuni 2,5 % tema eelmise majandusaasta ülemaailmsest kogukäibest, olenevalt sellest, kumb on suurem.

3. Artiklites 18–23, artiklis 28, artikli 30 lõigetes 1–4, artikli 31 lõigetes 1–4, artikli 32 lõigetes 1, 2 ja 3, artikli 33 lõikes 5 ning artiklites 39, 41, 47, 49 ja 53 sätestatud kohustuste täitmatajätmise korral kohaldatakse haldustrahvi kuni 10 000 000 eurot või, kui rikkuja on ettevõtja, kuni 2 % tema eelmise majandusaasta ülemaailmsest kogukäibest, olenevalt sellest, kumb on suurem.

4. Kui teada antud asutustele ja turujärelevalveasutustele on taotluse peale esitatud vale, ebatäielikku või eksitavat teavet, kohaldatakse haldustrahvi kuni 5 000 000 eurot või, kui rikkuja on ettevõtja, kuni 1 % tema eelmise majandusaasta ülemaailmsest kogukäibest, olenevalt sellest, kumb on suurem.

5. Igal konkreetsel juhul kohaldatava haldustrahvi suuruse üle otsustamisel võetakse arvesse konkreetse olukorra kõiki asjaomaseid asjaolusid ning pööratakse asjakohast tähelepanu järgmisele:

   a) rikkumise olemus, raskusaste ja kestus ning selle tagajärjed;

   b) kas samad või muud turujärelevalveasutused on juba kohaldanud sama ettevõtja suhtes sarnase rikkumise eest haldustrahve;

   c) rikkumise toime pannud ettevõtja suurus, eelkõige mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate, sealhulgas idufirmade puhul, ja turuosa.

6. Haldustrahve kohaldavad turujärelevalveasutused teavitavad sellest kohaldamisest teiste liikmesriikide turujärelevalveasutusi määruse (EL) 2019/1020 artiklis 34 osutatud info- ja teavitussüsteemi kaudu.

7. Iga liikmesriik kehtestab õigusnormid selle kohta, kas ja millisel määral võib haldustrahve määrata selles liikmesriigis asuvatele avaliku sektori asutustele ja organitele.

8. Olenevalt liikmesriikide õigussüsteemidest võib haldustrahve käsitlevaid õigusnorme kohaldada selliselt, et trahve määravad riigi pädevad kohtud või muud asutused vastavalt neis liikmesriikides riiklikul tasandil kehtestatud pädevustele. Selliste õigusnormide kohaldamisel neis liikmesriikides on samaväärne mõju.

9. Haldustrahve võib sõltuvalt iga üksikjuhtumi asjaoludest määrata lisaks muudele parandusmeetmetele või piiravatele meetmetele, mida turujärelevalveasutused sama rikkumise eest kohaldavad.

10. Erandina lõigetest 3–9 ei kohaldata nendes lõigetes osutatud haldustrahve:

a) mikro- või väikeettevõtjaks liigituvate tootjate suhtes seoses artikli 14 lõike 2 punktis a või artikli 14 lõike 4 punktis a osutatud tähtajast kinni pidamata jätmisega;

b) käesoleva määruse rikkumise korral avatud lähtekoodiga tarkvara korraldajate poolt.

Artikkel 65

Esindushagid

Esindushagide suhtes, mis on esitatud seoses ettevõtjapoolse käesoleva määruse sätete rikkumisega, mis kahjustab või võib kahjustada tarbijate kollektiivseid huve, kohaldatakse direktiivi (EL) 2020/1828.

VIII peatükk
Ülemineku- ja lõppsätted

Artikkel 66

Määruse (EL) 2019/1020 muutmine

Määruse (EL) 2019/1020 I lisasse lisatakse järgmine punkt:

„XX[+] [Euroopa Parlamendi ja nõukogu määrus (EL) 2024/…*[++]].

---

* Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, 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 …, ELI: …).“

[+] ELT: palun sisestada teksti määruse (EL) 2019/1020 I lisas esitatud loendi järgmine järjestikune number.

[++] ELT: palun sisestada teksti dokumendis PE-CONS 100/23 (2022/0272(COD)) sisalduva määruse number ning esitada joonealuses märkuses kõnealuse määruse number, kuupäev, pealkiri ja ELT avaldamisviide.

Artikkel 67

Direktiivi (EL) 2020/1828 muutmine

Direktiivi (EL) 2020/1828 I lisasse lisatakse järgmine punkt:

„XX[+] [Euroopa Parlamendi ja nõukogu määrus (EL) 2024/…*[++]].

_____

* Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, 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 …, ELI: …).“

[+] ELT: palun sisestada teksti määruse (EL) 2019/1020 I lisas esitatud loendi järgmine järjestikune number.

[++] ELT: palun sisestada teksti dokumendis PE-CONS 100/23 (2022/0272(COD)) sisalduva määruse number ning esitada joonealuses märkuses kõnealuse määruse number, kuupäev, pealkiri ja ELT avaldamisviide.

Artikkel 68

Määruse (EL) nr 168/2013 muutmine

Euroopa Parlamendi ja nõukogu määruse (EL) nr 168/2013[37] II lisa muudetakse järgmiselt.

C1 osa tabelisse lisatakse järgmine kanne:

”

XX[+]	18	sõiduki kaitsmine küberrünnete eest		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

“.

[37] Euroopa Parlamendi ja nõukogu 15. jaanuari 2013. aasta määrus (EL) nr 168/2013 kahe-, kolme- ja neljarattaliste sõidukite kinnituse ja turujärelevalve kohta (ELT L 60, 2.3.2013, lk 52).

[+] ELT: palun sisestada teksti määruse (EL) 168/2013 II lisas pealkirja C1 all järgmine järjestikune number.

Artikkel 69

Üleminekusätted

1. ELi tüübihindamissertifikaadid ja tüübikinnitusotsused, mis on välja antud seoses küberturvalisuse nõuetega digielemente sisaldavatele toodetele, mille suhtes kohaldatakse muid liidu ühtlustamisõigusakte kui käesolevat määrust, kehtivad kuni … [42 kuud alates käesoleva määruse jõustumise kuupäevast], välja arvatud juhul, kui need aeguvad enne seda kuupäeva või kui sellistes muudes liidu ühtlustamisõigusaktides on sätestatud teisiti; sel juhul jäävad need kehtima kõnealuste õigusaktide kohaselt.

2. Digielemente sisaldavate toodete suhtes, mis on turule lastud enne … [36 kuud alates käesoleva määruse jõustumise kuupäevast], kohaldatakse käesolevas määruses sätestatud nõudeid üksnes juhul, kui alates nimetatud kuupäevast on neid tooteid oluliselt muudetud.

3. Erandina käesoleva artikli lõikest 2 kohaldatakse artiklis 14 sätestatud kohustusi kõigi käesoleva määruse kohaldamisalasse kuuluvate digielemente sisaldavate toodete suhtes, mis on turule lastud enne … [36 kuud alates käesoleva määruse jõustumise kuupäevast].

Artikkel 70

Hindamine ja läbivaatamine

1. Hiljemalt … [72 kuud alates käesoleva määruse jõustumise kuupäevast] ja seejärel iga nelja aasta tagant esitab komisjon Euroopa Parlamendile ja nõukogule aruande käesoleva määruse hindamise ja läbivaatamise kohta. Kõnealused aruanded avalikustatakse.

2. Hiljemalt … [45 kuud alates käesoleva määruse jõustumise kuupäevast] esitab komisjon pärast ENISA ja CSIRTide võrgustikuga konsulteerimist Euroopa Parlamendile ja nõukogule aruande, milles hinnatakse artiklis 16 sätestatud ühtse teatamisplatvormi tulemuslikkust ning koordinaatoriteks määratud CSIRTide poolt artikli 16 lõikes 2 osutatud küberturvalisusega seotud aluste kohaldamise mõju ühtse teatamisplatvormi tulemuslikkusele seoses saadud teavituste piisavalt kiire edastamisega teistele asjaomastele CSIRTidele.

Artikkel 71

Jõustumine ja kohaldamine

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

2. Käesolevat määrust kohaldatakse alates … [36 kuud alates käesoleva määruse jõustumise kuupäevast].

   Artiklit 14 kohaldatakse siiski alates … [21 kuud alates käesoleva määruse jõustumise kuupäevast] ja IV peatükki (artiklid 35–51) kohaldatakse alates … [18 kuud alates käesoleva määruse jõustumise kuupäevast].

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

…,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

I LISA

OLULISED KÜBERTURVALISUSE NÕUDED

I osa Küberturvalisuse nõuded digielemente sisaldavate toodete omaduste kohta

1) Digielemente sisaldavaid tooteid tuleb projekteerida, arendada ja toota sellisel viisil, et need tagaksid riskidest lähtuvalt asjakohase küberturvalisuse taseme.

2) Artikli 13 lõikes 2 osutatud küberriskide hindamise alusel ja kui see on asjakohane, peavad digielemente sisaldavad tooted:

   a) olema tehtud turul kättesaadavaks ilma teadaolevate ärakasutatavate nõrkusteta;

   b) olema tehtud turul kättesaadavaks vaikimisi turvalise konfiguratsiooniga, juhul kui tootja ja ärikasutaja ei ole seoses digielemente sisaldava kohandatud tootega kokku leppinud teisiti; muu hulgas peab saama toote lähtestada algsesse olekusse;

   c) tagama, et nõrkustega saab tegeleda turvauuenduste abil, sealhulgas asjakohasel juhul automaatsete turvauuenduste abil, mis paigaldatakse asjakohase aja jooksul ja mis on aktiveeritud vaikesättena ning millel on selge ja kergesti kasutatav loobumismehhanism, teatades kasutajatele kättesaadavatest uuendustest, ning võimalus neid ajutiselt edasi lükata;

d) tagama asjakohaste kontrollimehhanismide (sealhulgas, aga mitte ainult, autentimis-, identimis- või juurdepääsu haldamise süsteemide) abil kaitse loata juurdepääsu eest ning teatama võimalikust loata juurdepääsust;

e) kaitsma talletatud, edastatavate või muul moel töödeldavate andmete (isikuandmed või muud andmed) konfidentsiaalsust, näiteks krüpteerides asjaomased andmed tipptasemel mehhanismidega nende jõudeoleku või edastamise ajal ja kasutades muid tehnilisi vahendeid;

f) kaitsma talletatud, edastatavate või muul moel töödeldavate andmete (isikuandmed või muud andmed), käskude, programmide ja konfiguratsioonide terviklust mistahes manipuleerimise või muutmise eest, milleks kasutaja ei ole luba andnud, ja teatama rikkumistest;

g) töötlema üksnes selliseid andmeid (isikuandmed või muud andmed), mis on piisavad, asjakohased ja piirduvad sellega, mis on vajalik seoses digielemente sisaldava toote sihtotstarbega (andmete minimeerimine);

h) kaitsma oluliste ja põhifunktsioonide kättesaadavust, seda ka pärast intsidenti, sealhulgas ummistusrünnete vastu suunatud vastupidavus- ja leevendusmeetmetega;

i) minimeerima toodete endi või ühendatud seadmete kahjulikku mõju muude seadmete või võrkude pakutavate teenuste kättesaadavusele;

j) olema projekteeritud, arendatud ja toodetud selliselt, et ründepinnad, sh välisliidesed, oleksid võimalikult piiratud;

k) olema projekteeritud, arendatud ja toodetud selliselt, et vähendada intsidendi mõju, kasutades asjakohaseid mehhanisme ja meetodeid ärakasutamise mõjude leevendamiseks;

l) andma turvalisusega seotud teavet, registreerides ja seirates asjaomaseid sisetoiminguid, sh juurdepääsu andmetele, teenustele või funktsioonidele või nende muutmist, koos loobumismehhanismiga kasutajate jaoks;

m) pakkuma kasutajatele võimalust kõik andmed ja seaded turvaliselt ja lihtsasti alaliselt eemaldada, ning juhul, kui selliseid andmeid saab edastada muudele toodetele või süsteemidele, tagama, et seda tehakse turvaliselt.

II osa Nõrkuste käsitlemise nõuded

Digielemente sisaldavate toodete tootjad peavad:

1) tegema kindlaks ja dokumenteerima digielemente sisaldavate toodete nõrkused ja komponendid, koostades muu hulgas tarkvara koostenimekirja, mis on üldkasutatavas ja masinloetavas vormingus ning milles käsitletakse vähemalt toodete kõrgema taseme sõltuvusi;

2) tegelema viivitamata digielemente sisaldavaid tooteid ähvardavate riskidega seotud nõrkustega ja need kõrvaldama, pakkudes muu hulgas turvauuendusi; kui see on tehniliselt teostatav, tuleb uusi turvauuendusi pakkuda funktsiooniuuendustest eraldi;

3) tegema digielemente sisaldava toote turvalisuse kohta mõjusaid ja korrapäraseid teste ja läbivaatamisi;

4) jagama pärast turvauuenduse kättesaadavaks tegemist teavet parandatud nõrkuste kohta ja avalikustama selle üldsusele, sh nõrkuste kirjelduse, teabe, mille põhjal kasutaja saab kindlaks teha, milliseid digielemente sisaldavaid tooteid need mõjutasid, nõrkuste mõju, raskusastme ning selge ja juurdepääsetava teabe, mis aitaks kasutajatel nõrkused kõrvaldada; igakülgselt põhjendatud juhtudel, kui tootjad leiavad, et avaldamisest tulenevad turvariskid kaaluvad üles turvalisusega seotud kasu, võivad nad parandatud nõrkust käsitleva teabe avalikustamise edasi lükata, kuni kasutajatele on antud võimalus asjaomast paika kasutada;

5) kehtestama nõrkuste koordineeritud avalikustamise põhimõtted ja tagama nende täitmise;

6) võtma meetmeid, et hõlbustada teabe jagamist oma digielemente sisaldava toote ja selles tootes sisalduvate kolmandate isikute komponentide võimalike nõrkuste kohta, sh esitama kontaktaadressi, kuhu teatada digielemente sisaldavas tootes avastatud nõrkustest;

7) nägema ette digielemente sisaldavate toodete uuenduste turvalise levitamise mehhanismid, et tagada nõrkuste õigeaegne ja turvauuenduste puhul asjakohasel juhul automaatne kõrvaldamine või leevendamine;

8) tagama, et kui kindlakstehtud turvaprobleemide lahendamiseks on olemas turvauuendused, levitatakse neid viivitamata ja juhul, kui tootja ja ärikasutaja ei ole seoses digielemente sisaldava kohandatud tootega kokku leppinud teisiti, tasuta koos nõuandvate sõnumitega, milles antakse kasutajatele asjakohast teavet muu hulgas meetmete kohta, mida võib võtta.

II LISA

KASUTAJALE MÕELDUD TEAVE JA JUHISED

Digielemente sisaldava tootega peab kaasas olema vähemalt järgmine teave:

1. tootja nimi, registreeritud kaubanimi või registreeritud kaubamärk ning postiaadress, e-posti aadress või muud digitaalsed kontaktandmed, ja kui see on olemas, veebisait, mille kaudu saab tootjaga ühendust võtta;

2. ühtne kontaktpunkt, kuhu võib saata ja kus võetakse vastu teavet digielemente sisaldava toote nõrkuste kohta ning kust võib leida tootja nõrkuste koordineeritud avalikustamise põhimõtted;

3. nimi ja tüüp ning mis tahes lisateave, mille põhjal saab digielemente sisaldava toote kordumatult tuvastada;

4. digielemente sisaldava toote sihtotstarve, sh tootja poolt ette nähtud turvakeskkond, ning toote olulised funktsioonid ja teave turvaomaduste kohta;

5. kõik teadaolevad või prognoositavad asjaolud, mis on seotud digielemente sisaldava toote kasutamisega vastavalt selle sihtotstarbele või mõistlikult prognoositava väärkasutamise tingimustes, mis võivad põhjustada olulisi küberriske;

6. kui see on asjakohane, siis internetiaadress, kus saab juurde pääseda ELi vastavusdeklaratsioonile;

7. see, millist liiki tehnilist turvatuge tootja pakub, ja toe kestuse, mille jooksul võivad kasutajad eeldada, et nõrkustega tegeletakse ja neile pakutakse turvauuendusi, lõppkuupäev;

8. üksikasjalikud juhised või internetiaadress, mis viitab sellistele üksikasjalikele juhistele ja teabele selle kohta:

   a) millised on vajalikud meetmed toote esmasel kasutuselevõtmisel ja toote kasutusea jooksul, et tagada digielemente sisaldava toote turvaline kasutamine;

   b) kuidas digielemente sisaldava toote muutmine võib mõjutada andmete turvalisust;

   c) kuidas saab paigaldada turvalisuse seisukohast olulisi uuendusi;

   d) kuidas digielemente sisaldav toode turvaliselt kasutusest kõrvaldada, sh teave selle kohta, kuidas kasutaja andmed turvaliselt eemaldada;

   e) kuidas saab I lisa I osa punktis c nõutud turvauuenduste automaatset paigaldamist võimaldava vaikesätte välja lülitada;

   f) kui digielemente sisaldav toode on ette nähtud integreerimiseks muudesse digielemente sisaldavatesse toodetesse, siis teave, mis on vajalik integreerija jaoks, et järgida I lisas sätestatud olulisi küberturvalisuse nõudeid ja VII lisas sätestatud dokumenteerimisnõudeid;

9. kui tootja otsustab teha tarkvara koostenimekirja kasutajale kättesaadavaks, siis teave selle kohta, kust on võimalik tarkvara koostenimekirjale juurde pääseda.

III LISA

DIGIELEMENTE SISALDAVAD OLULISED TOOTED

I klass

1. Identiteedihalduse süsteemide ja eelisjuurdepääsu haldamise tarkvara ja riistvara, sh autentimis- ja juurdepääsu kontrolli lugerid, kaasa arvatud biomeetriliste andmete lugerid

2. Autonoomsed ja sisseehitatud veebibrauserid

3. Paroolihaldurid

4. Tarkvara, mis otsib pahavara, kõrvaldab selle või paneb karantiini

5. Digielemente sisaldavad tooted, millel on virtuaalse privaatvõrgu (VPN) funktsioon

6. Võrguhalduse süsteemid

7. Turvateabe ja -sündmuste haldamise (SIEM) süsteemid

8. Buutimishaldurid

9. Avaliku võtme taristu ja digisertifikaatide väljaandmise tarkvara

10. Füüsilised ja virtuaalsed võrguliidesed

11. Operatsioonisüsteemid

12. Ruuterid, internetiühenduse jaoks mõeldud modemid ja kommutaatorid

13. Turvafunktsioonidega mikroprotsessorid

14. Turvafunktsioonidega mikrokontrollerid

15. Turvafunktsioonidega rakendusspetsiifilised integraallülitused (ASIC) ja programmeeritavad ventiilimaatriksid (FPGA)

16. Nutikodu üldotstarbelised virtuaalassistendid

17. Turvafunktsioonidega nutikodu tooted, sh arukad ukselukud, turvakaamerad, beebimonitorisüsteemid ja häiresüsteemid

18. Euroopa Parlamendi ja nõukogu direktiiviga 2009/48/EÜ[1] hõlmatud internetiühendusega mänguasjad, millel on interaktiivsed sotsiaalfunktsioonid (nt rääkimine või filmimine) või millel on asukoha jälgimise funktsioonid

19. Inimkehal kantavad või inimkehale paigutatavad isiklikud kantavad tooted, millel on terviseseire (nt jälgimise) eesmärk ja mille suhtes ei kohaldata määrust (EL) 2017/745 või määrust (EL) 2017/746, või isiklikud kantavad tooted, mis on ette nähtud kasutamiseks laste poolt ja lastel.

II klass

1. Hüperviisorid ja konteinerite käigusüsteemid, mis toetavad operatsioonisüsteemide ja samalaadsete keskkondade virtualiseeritud käitamist

2. Tulemüürid, sissetungi tuvastamise ja ennetamise süsteemid

3. Muukimiskindlad mikroprotsessorid

4. Muukimiskindlad mikrokontrollerid.

---

[1] Euroopa Parlamendi ja nõukogu 18. juuni 2009. aasta direktiiv 2009/48/EÜ mänguasjade ohutuse kohta (ELT L 170, 30.6.2009, lk 1).

IV LISA

DIGIELEMENTE SISALDAVAD KRIITILISE TÄHTSUSEGA TOOTED

1. Turvalaegastega riistvaraseadmed

2. Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/944[1] artikli 2 punktis 23 määratletud nutiarvestisüsteemide nutiarvestite lüüsid ja muud seadmed kõrgema turvalisuse tagamiseks, sh turvaliseks krüptotöötluseks

3. Kiipkaardid või sarnased seadmed, sh turvaelemendid.

---

[1] Euroopa Parlamendi ja nõukogu 5. juuni 2019. aasta direktiiv (EL) 2019/944 elektrienergia siseturu ühiste normide kohta ja millega muudetakse direktiivi 2012/27/EL (ELT L 158, 14.6.2019, lk 125).

V LISA

ELi VASTAVUSDEKLARATSIOON

Artiklis 28 osutatud ELi vastavusdeklaratsioon peab sisaldama kogu järgmist teavet.

1. Nimi ja tüüp ning mis tahes lisateave, mille põhjal saab digielemente sisaldava toote kordumatult tuvastada

2. Tootja või tema volitatud esindaja nimi ja aadress

3. Märge, et ELi vastavusdeklaratsioon on väljastatud üksnes pakkuja vastutusel

4. Deklareeritav toode (digielemente sisaldava toote identifitseerimine, mis võimaldab toodet jälgida, millega võib olla kaasas ka foto, kui see on asjakohane)

5. Kinnitus, et eelkirjeldatud deklareeritav toode on kooskõlas asjaomaste liidu ühtlustamisõigusaktidega

6. Viited kasutatud asjaomastele harmoneeritud standarditele või muule ühtsele spetsifikatsioonile või küberturvalisuse sertifitseerimisele, millele vastavust deklareeritakse

7. Kui see on asjakohane, siis teada antud asutuse nimi ja number, vastavushindamismenetluse kirjeldus ja väljastatud sertifikaadi tunnusnumber

8. Lisateave:

Allkirjastanud (kes ja kelle nimel): ……

(väljaandmise koht ja kuupäev)

(nimi, ametinimetus) (allkiri):

VI LISA

LIHTSUSTATUD ELi VASTAVUSDEKLARATSIOON

Artikli 13 lõikes 20 osutatud lihtsustatud ELi vastavusdeklaratsioon esitatakse järgmisel kujul.

Käesolevaga kinnitab [tootja nimi], et [digielemente sisaldava toote tüübi nimetus] tüüpi digielemente sisaldav toode vastab Euroopa Parlamendi ja nõukogu määruse (EL) …/…[1] nõuetele.

ELi vastavusdeklaratsiooni täistekst on kättesaadav järgmisel internetiaadressil:

---

[1] ELT: palun sisestada teksti dokumendis PE-CONS nr/AA (2022/0272(COD)) sisalduva määruse number.

VII LISA

TEHNILISE DOKUMENTATSIOONI SISU

Artiklis 31 osutatud tehniline dokumentatsioon peab sisaldama asjaomase digielemente sisaldava toote kohta vähemalt järgmist teavet:

1. digielemente sisaldava toote üldine kirjeldus, sealhulgas:

   a) selle sihtotstarve;

   b) tarkvara versioonid, mis mõjutavad seadme vastavust olulistele küberturvalisuse nõuetele;

   c) kui digielemente sisaldav toode on riistvaratoode, siis fotod või illustratsioonid, mis kujutavad toote väliseid tunnuseid, märgistust ja sisemist struktuuri;

   d) II lisas sätestatud kasutajatele mõeldud teave ja juhised;

2. digielemente sisaldava toote projekteerimise, arendamise ja tootmise ning nõrkuste käsitlemise protsesside kirjeldus, sealhulgas:

   a) vajalik teave digielemente sisaldava toote projekteerimise ja arendamise kohta, sh, kui see on asjakohane, joonised ja skeemid ja süsteemi arhitektuuri kirjeldus, mis selgitavad, kuidas tarkvarakomponendid üksteisele tuginevad või üksteisele sisendit annavad ja kuidas need on üldisesse töötlemisse integreeritud;

b) vajalik teave ja spetsifikatsioonid tootja kehtestatud nõrkuste käsitlemise protsesside kohta, sh tarkvara koostenimekiri, nõrkuste koordineeritud avalikustamise põhimõtted, tõendid selle kohta, et on esitatud kontaktaadress, millele nõrkustest teatada, ja uuenduste turvaliseks levitamiseks valitud tehniliste lahenduste kirjeldus;

c) vajalik teave ja spetsifikatsioonid digielemente sisaldava toote tootmise ja seire protsesside ning nende protsesside valideerimise kohta;

3. käesoleva määruse artikli 13 kohane hinnang küberriskidele, mille tõrjumiseks digielemente sisaldav toode on projekteeritud, arendatud, toodetud, tarnitud ja hooldatud, nagu on sätestatud artiklis 13, sealhulgas see, kuidas on kohaldatavad I lisa I osas sätestatud olulised küberturvalisuse nõuded;

4. asjakohane teave, mida võeti artikli 13 lõike 8 kohaselt arvesse digielemente sisaldava toote toe kestuse kindlaksmääramisel;

5. loetelu täielikult või osaliselt kohaldatavatest harmoneeritud standarditest, mille viitenumbrid on avaldatud *Euroopa Liidu Teatajas*, käesoleva määruse artiklis 27 sätestatud ühtsetest spetsifikatsioonidest või määruse (EL) 2019/881 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavadest vastavalt käesoleva määruse artikli 27 lõikele 8, ning kui kõnealuseid harmoneeritud standardeid, ühtseid spetsifikatsioone või Euroopa küberturvalisuse sertifitseerimise kavasid ei ole kohaldatud, siis nende lahenduste kirjeldused, mis on vastu võetud, et järgida I lisa I ja II osas sätestatud olulisi küberturvalisuse nõudeid, sealhulgas muude kohaldatud asjakohaste tehniliste spetsifikatsioonide loetelu. Osaliselt kohaldatud harmoneeritud standardite, ühtsete spetsifikatsioonide või Euroopa küberturvalisuse sertifitseerimise kavade puhul täpsustatakse tehnilises dokumentatsioonis osad, mida on kohaldatud;

6. aruanded testide kohta, mis on tehtud, et kontrollida digielemente sisaldava toote ja nõrkuste käsitlemise protsesside vastavust I lisa I ja II osas sätestatud kohaldatavatele olulistele küberturvalisuse nõuetele;

7. ELi vastavusdeklaratsiooni koopia;

8. kui see on asjakohane, tarkvara koostenimekiri turujärelevalveasutuse põhjendatud taotluse korral, kui see on vajalik, et kõnealune asutus saaks kontrollida vastavust I lisas sätestatud olulistele küberturvalisuse nõuetele.

VIII LISA

VASTAVUSHINDAMISMENETLUSED

I osa Sisekontrollil põhinev vastavushindamine (põhineb moodulil A)

1. Sisekontroll on vastavushindamismenetlus, mille puhul tootja täidab käesoleva osa punktides 2, 3 ja 4 sätestatud kohustusi ning tagab ja kinnitab oma ainuvastutusel, et digielemente sisaldavad tooted vastavad kõigile I lisa I osas sätestatud olulistele küberturvalisuse nõuetele ning tootja vastab I lisa II osas sätestatud olulistele küberturvalisuse nõuetele.

2. Tootja koostab VII lisas kirjeldatud tehnilise dokumentatsiooni.

3. Digielemente sisaldavate toodete projekteerimine, arendamine, tootmine ja nõrkuste käsitlemine

   Tootja võtab kõik vajalikud meetmed, et toodete projekteerimise, arendamise, tootmise ja nõrkuste käsitlemise protsessid ja nende seire tagaksid valmistatud või väljatöötatud digielemente sisaldava toote ja tootja kehtestatud protsesside vastavuse I lisa I ja II osas sätestatud olulistele küberturvalisuse nõuetele.

4. Vastavusmärgis ja vastavusdeklaratsioon

4.1. Tootja kinnitab CE-vastavusmärgise igale digielemente sisaldavale tootele, mis vastab käesoleva määruse kohaselt sätestatud nõuetele.

4.2. Tootja koostab iga digielemente sisaldava toote kohta kirjaliku ELi vastavusdeklaratsiooni vastavalt artiklile 28 ja säilitab seda koos tehnilise dokumentatsiooniga riiklike ametiasutuste jaoks kättesaadavana kümne aasta jooksul pärast digielemente sisaldava toote turule laskmist või toe kestuse ajal, olenevalt sellest, kumb on pikem. ELi vastavusdeklaratsioonis märgitakse ära digielemente sisaldav toode, mille kohta deklaratsioon on koostatud. ELi vastavusdeklaratsiooni koopia tehakse asjaomaste ametiasutuste nõudmisel neile kättesaadavaks.

5. Volitatud esindajad

Punktis 4 sätestatud tootja kohustusi võib tootja nimel ja vastutusel täita tema volitatud esindaja, kui asjakohased kohustused on volituses täpsustatud.

II osa ELi tüübihindamine (põhineb moodulil B)

1. Eli tüübihindamine on vastavushindamismenetluse osa, mille käigus teada antud asutus hindab digielemente sisaldava toote tehnilist projekti ja arendust ja tootja kehtestatud nõrkuste käsitlemise protsesse ning kinnitab, et digielemente sisaldav toode vastab I lisa I osas sätestatud olulistele küberturvalisuse nõuetele ja tootja vastab I lisa II osas sätestatud olulistele küberturvalisuse nõuetele.

2. ELi tüübihindamiseks hinnatakse digielemente sisaldava toote tehnilise projekti ja arenduse vastavust, kontrollides tehnilist dokumentatsiooni ja punktis 3 osutatud täiendavaid tõendeid koos toote ühe või mitme kriitilise tähtsusega osa näidiste hindamisega (toote- ja konstruktsioonitüübi kombinatsioon).

3. Tootja esitab ELi tüübihindamise taotluse ühele enda valitud teada antud asutusele.

   Taotlus sisaldab järgmist:

   3.1 tootja nimi ja aadress ning kui taotluse on esitanud volitatud esindaja, siis ka tema nimi ja aadress;

3.2 kirjalik kinnitus selle kohta, et sama taotlust ei ole esitatud ühelegi teisele teada antud asutusele;

3.3 tehniline dokumentatsioon, mille põhjal saab hinnata digielemente sisaldava toote vastavust I lisa I osas sätestatud kohaldatavatele olulistele nõuetele ja tootja nõrkuste käsitlemise protsesside vastavust I lisa II osas sätestatule, ning ühtlasi peab see sisaldama piisavat analüüsi ja hinnangut riskide kohta. Tehnilises dokumentatsioonis määratakse kindlaks kohaldatavad nõuded ja käsitletakse digielemente sisaldava toote projekteerimist, tootmist ja tööpõhimõtet hindamiseks vajalikul määral. Tehniline dokumentatsioon sisaldab, kui see on asjakohane, vähemalt VII lisas sätestatud elemente;

3.4 tõendusmaterjal tehnilise projekti ja arenduslahenduste ning nõrkuste käsitlemise protsesside piisavuse kohta. Tõendusmaterjalis tuleb nimetada kõik kasutatud dokumendid, eelkõige juhul, kui asjaomaseid harmoneeritud standardeid või tehnilisi spetsifikatsioone ei ole täielikult kohaldatud. Vajaduse korral sisaldab tõendusmaterjal tootja asjakohases laboris või tootja nimel ja tema vastutusel mõnes teises testimislaboris tehtud testide tulemusi.

4. Teada antud asutus teeb järgmist:

4.1. vaatab läbi tehnilise dokumentatsiooni ja tõendusmaterjali, et hinnata digielemente sisaldava toote tehnilise projekti ja arenduse vastavust I lisa I osas sätestatud olulistele küberturvalisuse nõuetele ning tootja kehtestatud nõrkuste käsitlemise protsesside vastavust I lisa II osas sätestatud olulistele küberturvalisuse nõuetele;

4.2. kontrollib, kas näidised on välja töötatud või valmistatud vastavalt tehnilisele dokumentatsioonile, ja teeb kindlaks nii need elemendid, mis on projekteeritud ja arendatud vastavalt asjaomaste harmoneeritud standardite või tehniliste spetsifikatsioonide kohaldatavatele sätetele, kui ka elemendid, mille projekteerimisel ja arendamisel ei ole nende standardite asjaomaseid sätteid kohaldatud;

4.3. teeb või laseb teha asjaomased kontrollid ja testid, et selgitada välja, kas juhtudel, kui tootja on otsustanud kohaldada I lisas sätestatud nõuete jaoks asjaomastes harmoneeritud standardites või tehnilistes spetsifikatsioonides esitatud lahendusi, on neid kohaldatud korrektselt;

4.4. teeb või laseb teha asjaomased kontrollid ja testid, et selgitada välja, kas juhtudel, kui I lisas sätestatud nõuete jaoks ei ole asjaomastes harmoneeritud standardites või tehnilistes spetsifikatsioonides esitatud lahendusi kohaldatud, vastavad tootja kasutatud lahendused asjaomastele küberturvalisuse olulistele nõuetele;

4.5. lepib tootjaga kokku kontrollide ja vajalike testide sooritamise koha.

5. Teada antud asutus koostab hindamisaruande, kuhu on märgitud vastavalt punktile 4 ellu viidud tegevused ja nende tulemused. Ilma et see piiraks teada antud asutuse kohustusi teavitavate asutuste ees, avalikustab teada antud asutus nimetatud aruande sisu kas täielikult või osaliselt ainult tootja loal.

6. Kui tüüp ja nõrkuste käsitlemise protsessid vastavad I lisas sätestatud olulistele küberturvalisuse nõuetele, väljastab teada antud asutus tootjale ELi tüübihindamissertifikaadi. Sertifikaat sisaldab tootja nime ja aadressi, kontrollide põhjal tehtud järeldusi, kehtivustingimusi (kui on) ja vajalikke andmeid kinnitatud tüübi ja nõrkuste käsitlemise protsesside identifitseerimiseks. Sertifikaadile võib olla lisatud üks või mitu lisa.

Sertifikaat ja selle lisad sisaldavad kogu asjaomast teavet, mis võimaldab hinnata valmistatud või väljatöötatud digielemente sisaldavate toodete vastavust kontrollitud tüübile ja nõrkuste käsitlemise protsessidele ning teha vajaduse korral kasutuskontrolli.

Kui tüüp ja nõrkuste käsitlemise protsessid ei vasta I lisas sätestatud kohaldatavatele olulistele küberturvalisuse nõuetele, keeldub teada antud asutus ELi tüübihindamissertifikaadi väljaandmisest ning teavitab sellest taotlejat, põhjendades keeldumist üksikasjalikult.

7. Teada antud asutus hoiab ennast kursis üldtunnustatud tehnika taseme muutustega, mis annavad märku sellest, et kinnitatud tüüp ja nõrkuste käsitlemise protsessid ei pruugi enam vastata käesoleva määruse I lisas sätestatud kohaldatavatele olulistele küberturvalisuse nõuetele, ning otsustab, kas sellised muutused nõuavad edasist uurimist. Kui uuringud on vajalikud, teavitab teada antud asutus sellest tootjat.

Tootja teavitab ELi tüübihindamissertifikaadiga seotud tehnilist dokumentatsiooni hoidvat teada antud asutust kõigist kinnitatud tüübi ja nõrkuste käsitlemise protsesside muudatustest, mis võivad mõjutada vastavust I lisas sätestatud olulistele küberturvalisuse nõuetele või sertifikaadi kehtivustingimusi. Sellised muudatused tuleb täiendavalt heaks kiita ja vormistada esialgse ELi tüübihindamissertifikaadi lisana.

8. Teada antud asutus teeb korrapäraselt auditeid tagamaks, et I lisa II osas sätestatud nõrkuste käsitlemise protsesse rakendatakse nõuetekohaselt.

9. Iga teada antud asutus teavitab oma teavitavaid asutusi enda väljastatud või tühistatud ELi tüübihindamissertifikaatidest ja nende lisadest ning teeb teavitavatele asutustele regulaarselt või nende taotluse korral kättesaadavaks nimekirja sertifikaatidest ja nende lisadest, mille andmisest keelduti, mis peatati või mida muul viisil piirati.

   Iga teada antud asutus teavitab teisi teada antud asutusi ELi tüübihindamissertifikaatidest ja nende lisadest, mille andmisest ta on keeldunud, mille ta on tühistanud, peatanud või mida ta on muul viisil piiranud, ning taotluse korral ka enda väljastatud sertifikaatidest ja nende lisadest.

   Komisjon, liikmesriigid ja teised teada antud asutused võivad taotluse korral saada ELi tüübihindamissertifikaadi ja kõigi selle lisade koopia. Komisjon ja liikmesriigid võivad taotluse korral saada tehnilise dokumentatsiooni ja teada antud asutuse tehtud kontrollide tulemuste koopia. Teada antud asutus hoiab ELi tüübihindamissertifikaadi ning selle lisade ja täienduste koopia ning tootja esitatud dokumentatsiooni sisaldava tehnilise toimiku alles kuni nimetatud sertifikaadi kehtivusaja lõpuni.

10. Tootja hoiab ELi tüübihindamissertifikaadi ning selle lisade ja täienduste koopia koos tehnilise dokumentatsiooniga riiklike ametiasutuste jaoks kättesaadavana kümne aasta jooksul pärast digielemente sisaldava toote turule laskmist või toe kestuse ajal, olenevalt sellest, kumb on pikem.

11. Tootja volitatud esindaja võib esitada punktis 3 osutatud taotluse ning täita punktides 7 ja 10 sätestatud kohustusi, kui asjakohased kohustused on volituses täpsustatud.

III osa Tootmise sisekontrollil põhinev tüübivastavus (põhineb moodulil C)

1. Tootmise sisekontrollil põhinev tüübivastavus on vastavushindamismenetluse osa, mille puhul tootja täidab käesoleva osa punktides 2 ja 3 sätestatud kohustusi ning tagab ja kinnitab, et asjaomased digielemente sisaldavad tooted vastavad ELi tüübihindamissertifikaadis kirjeldatud tüübile ja I lisa I osas sätestatud olulistele küberturvalisuse nõuetele ning tootja vastab I lisa II osas sätestatud olulistele küberturvalisuse nõuetele.

2. Tootmine

Tootja võtab kõik vajalikud meetmed, et tootmine ja selle järelevalve tagaksid valmistatud digielemente sisaldava toote vastavuse ELi tüübihindamissertifikaadis kirjeldatud kinnitatud tüübile ja I lisa I osas sätestatud olulistele küberturvalisuse nõuetele, ning tagab, et tootja vastab I lisa II osas sätestatud olulistele küberturvalisuse nõuetele.

3. Vastavusmärgis ja vastavusdeklaratsioon

3.1. Tootja kinnitab CE-vastavusmärgise igale digielemente sisaldavale tootele, mis vastab ELi tüübihindamissertifikaadis kirjeldatud tüübile ja õigusaktis sätestatud nõuetele.

3.2. Tootja koostab iga tootemudeli kohta kirjaliku vastavusdeklaratsiooni ja säilitab seda riiklike ametiasutuste jaoks kättesaadavana kümne aasta jooksul pärast digielemente sisaldava toote turule laskmist või toe kestuse ajal, olenevalt sellest, kumb on pikem. Vastavusdeklaratsioonis määratletakse toote mudel, mille kohta see koostati. Vastavusdeklaratsiooni koopia tehakse asjaomaste ametiasutuste nõudmisel neile kättesaadavaks.

4. Volitatud esindaja

Punktis 3 sätestatud tootja kohustusi võib tootja nimel ja vastutusel täita tema volitatud esindaja, kui asjakohased kohustused on volituses täpsustatud.

IV osa Täielikul kvaliteedi tagamisel põhinev vastavus (põhineb moodulil H)

1. Täielikul kvaliteedi tagamisel põhinev vastavus on vastavushindamismenetlus, mille puhul tootja täidab käesoleva osa punktides 2 ja 5 sätestatud kohustusi ning tagab ja kinnitab oma ainuvastutusel, et asjaomased digielemente sisaldavad tooted või tootekategooriad vastavad I lisa I osas sätestatud olulistele küberturvalisuse nõuetele ning tootja kehtestatud nõrkuste käsitlemise protsessid vastavad I lisa II osas sätestatud nõuetele.

2. Digielemente sisaldavate toodete projekteerimine, arendamine, tootmine ja nõrkuste käsitlemine

Tootja kasutab asjaomaste digielemente sisaldavate toodete projekteerimiseks, arendamiseks ja lõpptoodangu kontrollimiseks ja katsetamiseks ning nõrkuste käsitlemiseks punktis 3 nimetatud heakskiidetud kvaliteedisüsteemi, säilitab selle toimivuse kogu toe kestuse jooksul, ning tema suhtes kohaldatakse punktis 4 nimetatud järelevalvet.

3. Kvaliteedisüsteem

3.1. Tootja esitab taotluse kvaliteedisüsteemi hindamiseks asjakohaste digielemente sisaldavate toodete puhul enda valitud teada antud asutusele.

Taotlus sisaldab järgmist:

– tootja nimi ja aadress ning kui taotluse on esitanud volitatud esindaja, siis ka tema nimi ja aadress;

– tehniline dokumentatsioon iga sellise digielemente sisaldavate toodete kategooria ühe mudeli kohta, mida kavatsetakse valmistada või välja töötada. Tehniline dokumentatsioon sisaldab, kui see on asjakohane, vähemalt VII lisas sätestatud elemente;

– kvaliteedisüsteemi käsitlev dokumentatsioon ning

– kirjalik kinnitus selle kohta, et sama taotlust ei ole esitatud ühelegi teisele teada antud asutusele.

3.2. Kvaliteedisüsteem tagab digielemente sisaldavate toodete vastavuse I lisa I osas sätestatud olulistele küberturvalisuse nõuetele ning tootja kehtestatud nõrkuste käsitlemise protsesside vastavuse I lisa II osas sätestatud nõuetele.

Kõik tootja poolt vastu võetud elemendid, nõuded ja sätted tuleb süstemaatiliselt ja korrektselt dokumenteerida kirjalike tegevuspõhimõtete, menetluste ja juhistena. Kvaliteedisüsteemi dokumentatsioon peab võimaldama kvaliteedikavade, -plaanide, -käsiraamatute ja -aruannete ühtset tõlgendamist.

Eelkõige peab see sisaldama piisavat kirjeldust järgmise kohta:

– kvaliteedieesmärgid ja organisatsiooniline struktuur ning juhtkonna kohustused ja volitused seoses projekteerimise, arendamise, tootekvaliteedi ja nõrkuste käsitlemisega;

– tehnilise projekti ja arenduse kirjeldused, sealhulgas kohaldatavad standardid, ning kui asjaomaseid harmoneeritud standardeid või tehnilisi spetsifikatsioone ei kohaldata täies ulatuses, vahendid, millega tagatakse, et digielemente sisaldavate toodete suhtes kohaldatavad I lisa I osas sätestatud olulised küberturvalisuse nõuded täidetakse;

– menetluste kirjeldused, sealhulgas kohaldatavad standardid, ning kui asjaomaseid harmoneeritud standardeid või tehnilisi spetsifikatsioone ei kohaldata täies ulatuses, vahendid, millega tagatakse, et tootjate suhtes kohaldatavad I lisa II osas sätestatud olulised küberturvalisuse nõuded täidetakse;

– projekteerimise ja arendamise järelevalve- ja kontrollimeetodid, asjaomasesse digielemente sisaldavate toodete kategooriasse kuuluvate toodete projekteerimisel ja arendamisel kasutatavad protsessid ja süstemaatilised meetmed;

– kasutatavad tootmise, kvaliteedikontrolli ja kvaliteedi tagamise meetodid, protsessid ja süstemaatilised meetmed;

– enne tootmist, selle vältel ja pärast seda tehtavad kontrollimised ja testid ning nende sagedus;

– kvaliteediandmestikud, näiteks kontrolliaruanded ning testimis- ja kalibreerimisandmed ja asjaomaste töötajate kvalifikatsiooni käsitlevad aruanded;

– vahendid, mis võimaldavad jälgida toote nõutud projekteerimis- ja tootekvaliteedi saavutamist ja kvaliteedisüsteemi tulemuslikku toimimist.

3.3. Teada antud asutus hindab kvaliteedisüsteemi, et teha kindlaks, kas see vastab punktis 3.2 osutatud nõuetele.

Teada antud asutus peab nõuetele vastavaks neid kvaliteedisüsteemi elemente, mis vastavad riikliku standardi kirjeldustele, mille puhul rakendatakse asjaomast harmoneeritud standardit või tehnilist spetsifikatsiooni.

Lisaks kvaliteedisüsteemialastele kogemustele peab auditirühmas olema vähemalt üks liige, kellel on asjaomase valdkonna ja tootetehnoloogia hindamise kogemus ning kes tunneb käesoleva määruses sätestatud nõudeid. Auditi käigus tehakse kontrollkäik tootja valdustesse, kui sellised valdused on olemas. Auditirühm vaatab läbi punkti 3.1 teises taandes osutatud tehnilise dokumentatsiooni, et kontrollida, kas tootja suudab kindlaks teha käesoleva määruse sätestatud nõuded ja teostada vajalikke kontrolle, et tagada digielemente sisaldava toote vastavus nimetatud nõuetele.

Otsusest teatatakse tootjale või tema volitatud esindajale.

Teade sisaldab auditi põhjal tehtud järeldusi ning põhjendatud hindamisotsust.

3.4. Tootja kohustub täitma heakskiidetud kvaliteedisüsteemist tulenevaid kohustusi ja hoidma süsteemi asjakohase ja tõhusana.

3.5. Tootja teatab kvaliteedisüsteemi kinnitanud teada antud asutusele kvaliteedisüsteemi mis tahes kavandatud muudatusest.

Teada antud asutus hindab kavandatavaid muudatusi ja otsustab, kas muudetud kvaliteedisüsteem vastab punktis 3.2 osutatud nõuetele või on vaja uut hindamist.

Teada antud asutus teavitab oma otsusest tootjat. Teavitus sisaldab hindamise järeldusi ning põhjendatud hindamisotsust.

4. Järelevalve, mille eest vastutab teada antud asutus

4.1. Järelevalve eesmärk on tagada, et tootja täidab heakskiidetud kvaliteedisüsteemist tulenevaid kohustusi nõuetekohaselt.

4.2. Tootja võimaldab teada antud asutusele hindamiseks juurdepääsu projekteerimis-, arendamis-, tootmis-, kontrollimis- ja testimiskohtadele ning laoruumidele ja esitab talle kogu vajaliku teabe, eelkõige:

– kvaliteedisüsteemi dokumentatsiooni;

– kvaliteedisüsteemi projekteerimist käsitlevas osas ette nähtud kvaliteediandmestikud, nagu analüüsitulemused, arvutused ja testid;

– kvaliteedisüsteemi tootmist käsitlevas osas ettenähtud kvaliteediandmestikud, nagu kontrolliaruanded ning testimis- ja kalibreerimisandmed ja asjaomaste töötajate kvalifikatsiooni käsitlevad aruanded.

4.3. Teada antud asutus teostab korrapäraselt auditeid tagamaks, et tootja säilitab ja rakendab kvaliteedisüsteemi, ja esitab tootjale selle kohta auditiaruande.

5. Vastavusmärgis ja vastavusdeklaratsioon

5.1. Tootja kinnitab igale digielemente sisaldavale tootele, mis vastab käesoleva määruse I lisa I osas sätestatud nõuetele, CE-vastavusmärgise ja punktis 3.1osutatud teada antud asutuse vastutusel selle asutuse identifitseerimisnumbri.

5.2. Tootja koostab iga tootemudeli kohta kirjaliku vastavusdeklaratsiooni ja säilitab seda riiklike ametiasutuste jaoks kättesaadavana kümne aasta jooksul pärast digielemente sisaldava toote turule laskmist või toe kestuse ajal, olenevalt sellest, kumb on pikem. Vastavusdeklaratsioonis määratletakse toote mudel, mille kohta see koostati.

Vastavusdeklaratsiooni koopia tehakse asjaomaste ametiasutuste nõudmisel neile kättesaadavaks.

6. Tootja säilitab riiklike ametiasutuste jaoks kättesaadavana vähemalt kümne aasta jooksul pärast digielemente sisaldava toote turule laskmist või toe kestuse ajal, olenevalt sellest, kumb on pikem:

6.1 punktis 3.1 osutatud tehnilise dokumentatsiooni;

6.2 punktis 3.1 osutatud kvaliteedisüsteemi käsitleva dokumentatsiooni;

6.3 punktis 3.5 osutatud muudatuse heakskiidetud kujul;

6.4 punktides 3.5 ja 4.3 osutatud teada antud asutuse otsused ja aruanded.

7. Iga teada antud asutus teatab oma teavitavatele asutustele kvaliteedisüsteemidele antud heakskiitudest või heakskiidu tühistamistest ja teeb oma teavitavatele asutustele perioodiliselt või nende taotlusel kättesaadavaks nimekirja juhtumitest, mil kvaliteedisüsteemi heakskiitmisest keelduti, heakskiit peatati või heakskiitu muul viisil piirati.

Iga teada antud asutus teatab teistele teada antud asutustele juhtumitest, mil ta keeldus kvaliteedisüsteemi heakskiitmisest, peatas heakskiidu või tühistas selle, ning taotluse korral ka kvaliteedisüsteemidele tema poolt antud heakskiitudest.

8. Volitatud esindaja

Punktides 3.1, 3.5, 5 ja 6 sätestatud tootja kohustusi võib täita tema nimel ja vastutusel tema volitatud esindaja, kui asjakohased kohustused on volituses täpsustatud.

Selle õigusakti kohta on tehtud avaldus, mis on leitav [ELT lisab viite: OJ C, XXX, XX.XX.2024, lk XX] ning järgmiselt lingilt: [ELT: palun lisada avalduse link].