Euroopa Liidu
Nõukogu

Brüssel, 16. september 2022
(OR. en)

12429/22

Institutsioonidevaheline dokument:
2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

ETTEPANEK

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	15. september 2022
Saaja:	Nõukogu peasekretariaat
Komisjoni dok nr:	COM(2022) 454 final
Teema:	Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrust (EL) 2019/1020

Käesolevaga edastatakse delegatsioonidele dokument COM(2022) 454 final.

Lisatud: COM(2022) 454 final

EUROOPA
KOMISJON

Brüssel, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrust (EL) 2019/1020

(EMPs kohaldatav tekst)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

SELETUSKIRI

1. ETTEPANEKU TAUST

• Ettepaneku põhjused ja eesmärgid

Üha enam tabavad riist- ja tarkvaratooteid edukad küberründed; nende tõttu suurenes küberkuritegevuse hinnanguline ülemaailmne kulu 2021. aastaks 5,5 triljoni euroni aastas. Neid tooteid mõjutavad kaks põhiprobleemi, mis suurendavad kasutajate ja ühiskonna kulusid: 1) küberturvalisuse madal tase, mida kajastavad levinud nõrkused ning ebapiisavad ja ebajärjekindlad turvauuendused nende kõrvaldamiseks, ning 2) kasutajate ebapiisav arusaamine ja juurdepääs teabele, mis takistab neil valida piisavate küberturvalisuse omadustega tooteid või kasutada neid turvalisel viisil. Võrgustatud keskkonnas võib ühe tootega seotud küberintsident mõjutada tervet organisatsiooni või kogu tarneahelat ning selle mõju võib sageli minutite jooksul laieneda üle siseturu piiride. See võib põhjustada olulisi häireid majandustegevuses ja ühiskonnaelus või muutuda isegi eluohtlikuks.

Digielemente sisaldavate toodete küberturvalisusel on tugev piiriülene mõõde, kuna ühes riigis toodetud tooteid kasutatakse sageli kogu siseturul. Lisaks levivad algselt üht üksust või liikmesriiki mõjutanud intsidendid sageli minutite jooksul üle kogu siseturu.

Kuigi teatavate digielemente sisaldavate toodete suhtes kohaldatakse kehtivaid siseturgu käsitlevaid õigusakte, ei ole enamik riist- ja tarkvaratooteid praegu hõlmatud ühegi ELi õigusaktiga, mis käsitleks nende küberturvalisust. Eelkõige ei käsitleta praeguses ELi õigusraamistikus sisseehitamata tarkvara küberturvalisust, vaatamata sellele, et küberrünnete sihtmärgiks võetakse üha enam just nende toodete nõrkused, põhjustades märkimisväärseid ühiskondlikke ja majanduslikke kulusid. Leidub palju näiteid märkimisväärsete küberrünnete kohta, mis olid tingitud toodete ebaoptimaalsest turvalisusest, näiteks WannaCry lunavarauss, mille puhul kasutati ära Windowsi nõrkust ning mis mõjutas 2017. aastal 200 000 arvutit 150 riigis ja tekitas miljardite USA dollarite suuruse kahju; Kaseya VSA tarneahela rünne, mille käigus kasutati Kaseya võrguhaldustarkvara, et rünnata enam kui 1 000 ettevõtet, ja mis sundis üht supermarketiketti sulgema Rootsis kõik oma 500 kauplust, või paljud pangarakenduste häkkimise intsidendid, mille eesmärk oli varastada pahaaimamatute tarbijate raha.

Siseturu nõuetekohase toimimise tagamiseks määrati kindlaks kaks põhieesmärki: 1) luua tingimused digielemente sisaldavate turvaliste toodete arendamiseks, tagades, et turule lastakse vähemate nõrkustega riist- ja tarkvaratooted, ning tagada, et tootjad suhtuvad turvalisusesse tõsiselt toote kogu elutsükli jooksul, ning 2) luua tingimused, mis võimaldavad kasutajatel digielemente sisaldavate toodete valimisel ja kasutamisel küberturvalisust arvesse võtta. Seati neli erieesmärki: i) tagada, et tootjad parandavad digielemente sisaldavate toodete turvalisust alates projekteerimis- ja arendamisetapist ning kogu elutsükli jooksul; ii) tagada sidus küberturvalisuse raamistik, mis hõlbustab riist- ja tarkvaratootjatel nõuete täitmist; iii) suurendada digielemente sisaldavate toodete turvaomaduste läbipaistvust ning iv) võimaldada ettevõtjatel ja tarbijatel digielemente sisaldavaid tooteid turvaliselt kasutada.

Küberturvalisuse tugev piiriülene olemus ja selliste intsidentide kasvav arv, millel on piiriülene ning muudele sektoritele ja toodetele ülekanduv mõju, tähendavad, et liikmesriigid üksi ei suuda eesmärke tulemuslikult saavutada. Võttes arvesse digielemente sisaldavate toodete turgude ülemaailmset olemust, seistakse liikmesriikide territooriumil samade digielemente sisaldavate toodete puhul silmitsi samade riskidega. Kujunev killustunud

raamistik, mis koosneb potentsiaalselt lahknevatest siseriiklikest õigusnormidest, võib takistada digielemente sisaldavate toodete avatud ja konkurentsivõimelise ühtse turu toimimist. Seega on vaja ELi tasandi ühismeetmeid, et suurendada kasutajate usaldust ja digielemente sisaldavate ELi toodete populaarsust. Need tooksid kasu ka siseturule, tagades õiguskindluse ja luues võrdsed võimalused digielemente sisaldavate toodete müüjatele, nagu on rõhutatud ka Euroopa tuleviku konverentsi lõpparuandes, milles on esitatud kodanike üleskutse suurendada ELi rolli küberohtude vastu võitlemisel.

- **Koostoime poliitikavaldkonnas praegu kehtivate õigusnormidega**

ELi raamistik koosneb mitmest horisontaalsest õigusaktist, mis käsitlevad küberturvalisusega seotud teatavaid aspekte eri vaatenurkadest (tooted, teenused, kriisiohje ja kuriteod). 2013. aastal jõustus direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid[1] ning millega ühtlustatakse kriminaliseerimist ja karistusi mitme infosüsteemide vastu suunatud kuriteo puhul. 2016. aasta augustis jõustus esimese kogu ELi hõlmava küberturvalisust käsitleva õigusaktina direktiiv (EL) 2016/1148 võrgu- ja infosüsteemide turvalisuse kohta (küberturvalisuse direktiiv)[2]. Selle läbivaatamine, mille tulemusel võetakse vastu direktiiv [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)], tõstab ELi ühist ambitsioonitaset. 2019. aastal jõustus ELi küberturvalisuse määrus,[3] mille eesmärk on suurendada IKT-toodete, -teenuste ja -protsesside turvalisust vabatahtliku Euroopa küberturvalisuse sertifitseerimise raamistiku kehtestamisega[4].

Kogu tarneahela küberturvalisus on tagatud ainult siis, kui on tagatud kõigi selle komponentide küberturvalisus. Eespool nimetatud ELi õigusaktides on selles osas siiski märkimisväärseid lünki, kuna need ei sisalda kohustuslikke nõudeid digielemente sisaldavate toodete turvalisuse kohta.

Kavandatav kübervastupidavusvõime määrus käsitleb turule lastavaid digielemente sisaldavaid tooteid, aga direktiivi [direktiiv XXX/XXX (küberturvalisuse 2. direktiiv)] eesmärk on tagada elutähtsate ja oluliste üksuste osutatavate teenuste küberturvalisuse kõrge tase. Direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] kohaselt peavad

---

1 Euroopa Parlamendi ja nõukogu 12. augusti 2013. aasta direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK (ELT L 218, 14.8.2013, lk 8–14).

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

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 Küberturvalisuse määrus võimaldab välja töötada spetsiaalsed sertifitseerimiskavad. Iga kava sisaldab viiteid asjakohastele standarditele või kavas kindlaks määratud tehnilisele kirjeldusele või muudele küberturvalisuse nõuetele. Küberturvalisuse sertifitseerimise väljatöötamise otsus on riskipõhine.

liikmesriigid tagama, et selle kohaldamisalasse kuuluvad elutähtsad ja olulised üksused, nagu tervishoiu- või pilveteenuse osutajad ja avaliku halduse üksused, võtavad asjakohaseid ja proportsionaalseid tehnilisi, operatiivseid ja korralduslikke küberturvalisuse meetmeid. See hõlmab muu hulgas nõuet tagada võrgu- ja infosüsteemide hankimise, arendamise ja hooldamise turvalisus, sealhulgas nõrkuste käitlemine ja avalikustamine. Direktiivis [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] nõutakse, et komisjon võtaks 21 kuu jooksul pärast direktiivi jõustumist vastu rakendusaktid, milles sätestatakse kõnealuste meetmete tehnilised ja metoodilised nõuded, mida peavad järgima teatavat liiki üksused, näiteks pilvandmetöötlusteenuse osutajad. Kõigi muude üksuste puhul võib komisjon võtta vastu rakendusakti, milles sätestatakse tehnilised ja metoodilised nõuded ning valdkondlikud nõuded. Selle raamistikuga tagatakse, et kübervastupidavusvõime määruse oluliste küberturvalisuse nõuetega sarnaseid tehnilisi kirjeldusi ja meetmeid rakendatakse ka teenusena pakutava tarkvara (teenustarkvara) projekteerimisel, arendamisel ja selle nõrkuste käitlemisel. See võiks näiteks tagada küberturvalisuse kõrge taseme digitaalsete tervise infosüsteemide puhul, sealhulgas juhul, kui neid pakutakse teenustarkvarana (SaaS) või kui need on välja töötatud tervishoiuasutustes (asutusesiseselt) kooskõlas kavandatava [ühtse Euroopa terviseandmeruumi määrusega].

- **Koostoime muude liidu tegevuspõhimõtetega**

Nagu on märgitud teatises „Euroopa digituleviku kujundamine“,[5] on väga oluline, et EL kasutaks ära kõik digiajastu hüved ning tugevdaks oma tööstust ja innovatsioonisuutlikkust ohututes ja eetilistes piirides. Euroopa andmestrateegias on sätestatud andmeid kasutava ühiskonna eeltingimusena neli sammast – andmekaitse, põhiõigused, ohutus ja küberturvalisus.

Ka digielementide võimalusega toodete suhtes kohaldatav praegune ELi raamistik[6] hõlmab mitut õigusakti, sealhulgas konkreetseid tooteid käsitlevaid ELi õigusakte, mis hõlmavad ohutusega seotud aspekte, ja tootevastutust käsitlevaid üldisi õigusakte. Ettepanek on kooskõlas kehtiva toodetega seotud ELi õigusraamistikuga ning hiljutiste seadusandlike ettepanekutega, nagu komisjoni ettepanek võtta vastu määrus [tehisintellekti käsitlev määrus][7].

Kavandatud määrust kohaldataks kõigi komisjoni delegeeritud määruse (EL) 2022/30 kohaldamisalasse kuuluvate raadioseadmete suhtes. Lisaks hõlmavad käesolevas määruses sätestatud nõuded kõiki direktiivi 2014/53/EL artikli 3 lõike 3 punktides d, e ja f osutatud oluliste nõuete elemente, sealhulgas peamisi elemente, mis on sätestatud nimetatud delegeeritud määruse alusel vastu võetud [komisjoni rakendusotsuses XXX/2022 Euroopa standardiorganisatsioonidele esitatava standardimistaotluse kohta]. Õigusliku kattuvuse vältimiseks nähakse ette, et komisjon tunnistab delegeeritud määruse kehtetuks või muudab

---

[5] Komisjoni 19. veebruari 2020. aasta teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Euroopa digituleviku kujundamine“ (COM(2020) 67 final).

[6] Peamiselt uut õigusraamistikku käsitlevad õigusaktid.

[7] 21. aprilli 2021. aasta ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte (COM(2021) 206 final).

seda seoses kavandatava määrusega hõlmatud raadioseadmetega, et alates kavandatava määruse kohaldatavaks muutumisest kohaldataks seda nende suhtes.

Töö dubleerimise vältimiseks nähakse ette, et harmoneeritud standardite ettevalmistamisel ja väljatöötamisel käesoleva määruse rakendamise hõlbustamiseks võtavad komisjon ja Euroopa standardiorganisatsioonid arvesse standardimistööd, mis on tehtud vastavalt komisjoni rakendusotsusele C(2022) 5637, mis käsitleb standardimistaotlust seoses raadioseadmete direktiivi kohase delegeeritud määrusega (EL) 2022/30.

2. ÕIGUSLIK ALUS, SUBSIDIAARSUS JA PROPORTSIONAALSUS

• Õiguslik alus

Ettepaneku õiguslik alus on Euroopa Liidu toimimise lepingu (edaspidi „ELi toimimise leping“) artikkel 114, milles on ette nähtud meetmete võtmine, et tagada siseturu loomine ja toimimine. Ettepaneku eesmärk on ühtlustada digielemente sisaldavate toodete suhtes kehtivad küberturvalisuse nõuded kõigis liikmesriikides ja kõrvaldada kaupade vaba liikumise takistused.

ELi toimimise lepingu artiklit 114 võib kasutada õigusliku alusena, et vältida selliste takistuste tulenemist liikmesriikide õigusaktide ja lähenemisviiside erinevustest seoses sellega, kuidas õiguskindlusetust ja lünki kehtivates õigusraamistikes kõrvaldatakse[8]. Lisaks on Euroopa Kohus tunnistanud, et erinevate tehniliste nõuete kohaldamine võib olla piisav alus ELi toimimise lepingu artikli 114 kohaldamiseks[9].

Praegune ELi õigusraamistik, mida kohaldatakse digielemente sisaldavate toodete suhtes, põhineb ELi toimimise lepingu artiklil 114 ja koosneb mitmest õigusaktist, mis käsitlevad muu hulgas konkreetseid tooteid ja ohutusega seotud aspekte või mis on üldised tootevastutust käsitlevad õigusaktid. See hõlmab siiski ainult teatavaid aspekte seoses materiaalsete digitaaltoodete ja vajaduse korral neisse toodetesse sisseehitatud tarkvara küberturvalisusega. Riigi tasandil on liikmesriigid hakanud võtma riiklikke meetmeid, millega nõutakse, et digitaaltoodete müüjad parandaksid nende küberturvalisust[10]. Samal ajal on digitaaltoodete küberturvalisusel eriti tugev piiriülene mõõde, kuna ühes riigis toodetud tooteid kasutavad sageli organisatsioonid ja tarbijad kogu siseturul. Intsidendid, mis algselt puudutavad ühte üksust või liikmesriiki, levivad sageli minutite jooksul muudesse organisatsioonidesse ja sektoritesse ning mitmesse liikmesriiki.

---

[8] Kohtuotsus, Euroopa Kohus (suurkoda), 3. detsember 2019, Tšehhi Vabariik *vs*. Euroopa Parlament ja Euroopa Liidu Nõukogu, C-482/17, punkt 35.

[9] Kohtuotsus, Euroopa Kohus (suurkoda), 2. mai 2006, Suurbritannia ja Põhja-Iiri Ühendkuningriik *vs*. Euroopa Parlament ja Euroopa Liidu Nõukogu, C-217/04, punktid 62–63.

[10] Näiteks 2019. aastal lõi Soome esemevõrguseadmete, näiteks nutitelerite, nutitelefonide ja mänguasjade märgistamise süsteemi, mis põhineb ETSI standarditel. Saksamaa võttis hiljuti kasutusele lairibaruuterite, nutitelerite, kaamerate, kõlarite, mänguasjade ning puhastus- ja aiarobotite tarbijaturvalisuse märgise.

ELi ja liikmesriikide tasandil seni vastu võetud eri õigusaktides ja algatustes käsitletakse tuvastatud probleeme vaid osaliselt ja need võivad tekitada siseturul õigusaktide killustatust, suurendades õiguskindlusetust nii nende toodete müüjate kui ka kasutajate jaoks ning tekitades ettevõtjatele tarbetut lisakoormust vajaduse tõttu täita sarnaste tooteliikide puhul erinevaid nõudeid.

Kavandatud määrusega ühtlustataks ja lihtsustataks ELi regulatiivset keskkonda digielemente sisaldavate toodete suhtes kehtivate küberturvalisuse nõuetega ning välditaks eri õigusaktidest tulenevaid kattuvaid nõudeid. Sellega suurendataks kogu liidus ettevõtjate ja kasutajate õiguskindlust ning ühtlustataks paremini Euroopa ühtset turgu, luues soodsamad tingimused ettevõtjatele, kes soovivad ELi turule siseneda.

- **Subsidiaarsus (ainupädevusse mittekuuluva valdkonna puhul)**

Küberturvalisuse tugev piiriülene olemus üldiselt ning selliste riskide ja intsidentide kasvav arv, millel on piiriülene ning muudele sektoritele ja toodetele ülekanduv mõju, tähendavad, et liikmesriigid üksi ei suuda kõnealuse sekkumise eesmärke tulemuslikult saavutada. Riikide lähenemisviisid probleemide lahendamisel ja eelkõige lähenemisviisid, millega kehtestatakse kohustuslikud nõuded, tekitavad täiendavat õiguskindlusetust ja õiguslikke tõkkeid. Ettevõtetel võib sujuv laienemine teistesse liikmesriikidesse olla takistatud, mistõttu kasutajad jäävad ilma nende toodete hüvedest.

Seepärast on vaja ELi tasandi ühismeetmeid, et suurendada kasutajate usaldust ja seega digielemente sisaldavate ELi toodete populaarsust. Need tooksid kasu ka digitaalsele ühtsele turule ja siseturule üldiselt, tagades õiguskindluse ning luues võrdsed võimalused digielemente sisaldavate toodete tootjatele.

Nõukogu 23. mai 2022. aasta järeldustes Euroopa Liidu kübervaldkonna riskiseisundi parandamise kohta kutsutakse komisjoni üles tegema 2022. aasta lõpuks ettepanek ühtsete küberturvalisuse nõuete kohta, mis kehtivad ühendatud seadmete suhtes.

- **Proportsionaalsus**

Mis puudutab kavandatud määruse proportsionaalsust, siis kaalutud poliitikavariantide meetmed ei läheks kaugemale sellest, mis on vajalik üld- ja erieesmärkide saavutamiseks, ega põhjustaks ebaproportsionaalseid kulusid. Täpsemalt tagataks kaalutava sekkumisega, et digielemente sisaldavad tooted on kaitstud kogu nende elutsükli jooksul ja proportsionaalselt asjaomaste riskidega, kehtestades selleks sihipärased ja tehnoloogianeutraalsed nõuded, mis jäävad mõistlikuks ja vastavad üldiselt asjaomaste üksuste huvidele.

Ettepanekus esitatud olulised küberturvalisuse nõuded põhinevad laialdaselt kasutatavatel standarditel ning järgnevas standardimisprotsessis võetakse arvesse toodete tehnilisi eripärasid. See tähendab, et kui see on konkreetset riskitaset arvestades vajalik, kohandatakse turvameetmeid. Lisaks nähtaks kavandatud horisontaalsete eeskirjadega ette üksnes kriitilise tähtsusega toodete hindamine kolmanda isiku poolt. See hõlmaks vaid väikest osa digielemente sisaldavate toodete turust. Mõju VKEdele sõltuks nende tegutsemisest nende konkreetsete tootekategooriate turul.

Seoses vastavushindamise kulude proportsionaalsusega võtavad kolmandate isikute poolseid hindamisi ellu viivad teavitatud asutused oma tasude kehtestamisel arvesse ettevõtja suurust. Samuti nähakse rakendamise ettevalmistamiseks ette mõistlik 24-kuuline üleminekuperiood, mis annab asjaomastele turgudele aega valmistuda, ning samal ajal määratakse kindlaks

teadus- ja arendustegevusse tehtavate investeeringute selge suund. Kõik ettevõtjate kantavad nõuete täitmisega seotud kulud oleksid väiksemad kui kasu, mida toob digielemente sisaldavate toodete suurem turvalisus ja lõppkokkuvõttes kasutajate suurem usaldus nende toodete vastu.

- **Vahendi valik**

Regulatiivne sekkumine tähendaks määruse, mitte direktiivi vastuvõtmist. See tuleneb asjaolust, et seda liiki tooteid käsitlevatest õigusaktidest oleks määrus tuvastatud probleemide lahendamisel tulemuslikum ja vastaks sõnastatud eesmärkidele, kuna tegemist on sekkumisega, millest sõltub väga laia tootekategooria siseturule laskmine. Direktiivi ülevõtmise protsess võib sellise sekkumise puhul jätta riigi tasandil liiga palju kaalutlusruumi, mis võib põhjustada teatavate oluliste küberturvalisuse nõuete ebaühtlust, õiguskindlusetust, edasist killustatust või isegi diskrimineerivaid piiriüleseid olukordi, eriti kui võtta arvesse asjaolu, et hõlmatud tooted võivad olla mitmeotstarbelised ning et tootjad võivad toota selliseid mitmesse kategooriasse kuuluvaid tooteid.

3. JÄRELHINDAMISE, SIDUSRÜHMADEGA KONSULTEERIMISE JA MÕJU HINDAMISE TULEMUSED

- **Konsulteerimine sidusrühmadega**

Komisjon on konsulteerinud paljude sidusrühmadega. Liikmesriike ja sidusrühmi kutsuti osalema avalikul konsultatsioonil ning küsitlustes ja seminaridel osana uuringust, mille korraldas komisjoni mõjuhinnangu ettevalmistamise tööd toetav konsortsium, kuhu kuulusid Wavestone, Euroopa Poliitikauuringute Keskus (CEPS) ja ICF. Konsulteeritud sidusrühmade hulka kuulusid riiklikud turujärelevalveasutused, küberturvalisuse valdkonnas tegutsevad liidu asutused, riist- ja tarkvara tootjad, riist- ja tarkvara importijad ja turustajad, kutseorganisatsioonid, tarbijaorganisatsioonid ja digielemente sisaldavate toodete kasutajad ning kodanikud, teadlased ja akadeemilised ringkonnad, teavitatud asutused ja akrediteerimisasutused ning küberturvalisuse valdkonna spetsialistid.

Konsultatsioonid hõlmasid alljärgnevat:

- ICFi, Wavestone'i, Carsa ja CEPSi moodustatud konsortsiumi esimene uuring, mis avaldati 2021. aasta detsembris[11]. Uuringu käigus tehti kindlaks mitu turutõrget ja hinnati võimalikke regulatiivseid sekkumisi;

- avalik konsultatsioon, mille sihtrühma kuulusid kodanikud, sidusrühmad ja küberturvalisuse eksperdid. Esitati 176 vastust. Need aitasid kaasa erinevate arvamuste ja kogemuste kogumisele kõigilt sidusrühmadelt;

- komisjoni kübervastupidavusvõime määruse ettevalmistavat tööd toetava uuringu raames korraldatud seminarid tõid kõigist 27 liikmesriigist kokku ligikaudu 100 mitmesuguste sidusrühmade esindajat;

---

[11] „Study on the need of Cybersecurity requirements for ICT products", nr 2020–0715, uuringu lõpparuanne, kättesaadav aadressil https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

- korraldati intervjuud ekspertidega, et saada parem arusaam digielemente sisaldavate toodetega seotud praegustest küberturvalisuse probleemidest ja arutada poliitikavariante võimaliku regulatiivse sekkumise jaoks;

- peeti kahepoolseid arutelusid riiklike küberturvalisuse asutuste, erasektori ja tarbijaorganisatsioonidega;

- tegeleti peamiste VKEdest sidusrühmade sihipärase teavitamisega.

- **Eksperdiarvamuste kogumine ja kasutamine**

Konsultatsioonide eesmärk oli saada teavet viie peamise hindamiskriteeriumi kohta, mis põhinevad ELi parema õigusloome suunistel (tulemuslikkus, tõhusus, asjakohasus, sidusus, ELi lisaväärtus), ning võimalike tulevikuvariantide võimaliku mõju kohta. Töövõtja ei ole mitte ainult pöördunud sidusrühmade poole, keda kavandatav määrus otseselt mõjutaks, vaid on konsulteerinud ka paljude küberturvalisuse valdkonna ekspertidega.

- **Mõjuhinnang**

Komisjon korraldas käesoleva ettepaneku mõju hindamise, mille vaatas läbi komisjoni õiguskontrollikomitee. Õiguskontrollikomiteega toimus 6. juulil 2022 koosolek ja sellele järgnes positiivne arvamus. Mõjuhinnangut kohandati, et võtta arvesse õiguskontrollikomitee soovitusi ja märkusi.

Komisjon uuris erinevaid poliitikavariante ettepaneku üldeesmärgi saavutamiseks:

- pehme õiguse lähenemisviis ja vabatahtlikud meetmed (1. variant): selle variandi puhul puuduks kohustuslik regulatiivne sekkumine. Selle asemel annaks komisjon välja teatisi, suuniseid, soovitusi ja võimalikke tegevusjuhendeid, et soodustada vabatahtlike meetmete võtmist. ELi horisontaalsete eeskirjade puudumise kompenseerimiseks jätkataks vabatahtlike või kohustuslike riiklike kavade väljatöötamist;

- sihipärane regulatiivne sekkumine digielemente sisaldavate materiaalsete toodete ja vastava sisseehitatud tarkvara küberturvalisuse valdkonnas (2. variant): see variant hõlmaks sihipärast tootepõhist regulatiivset sekkumist, mis piirduks küberturvalisuse nõuete lisamise ja/või muutmisega juba kehtivates õigusaktides või uute õigusaktide vastuvõtmisega uute riskide ilmnemise korral, sealhulgas võib-olla ka sisseehitamata tarkvara puhul.

3. ja 4. variant hõlmavad eri ulatusega horisontaalset regulatiivset sekkumist, mis suures osas põhineb uuel õigusraamistikul. Selles raamistikus sätestatakse olulised nõuded, mis peavad olema täidetud teatavate toodete siseturule laskmiseks. Uues õigusraamistikus on üldjuhul ette nähtud ka vastavushindamine, mille tootja korraldab selleks, et tõendada tootega seotud kindlaksmääratud nõuete täitmist:

- kombineeritud lähenemisviis, sealhulgas horisontaalsed kohustuslikud eeskirjad digielemente sisaldavate materiaalsete toodete ja vastava sisseehitatud tarkvara küberturvalisuse kohta ning järkjärguline lähenemisviis sisseehitamata tarkvara puhul (3. variant): see variant hõlmaks määrust, millega kehtestatakse kõigi digielemente sisaldavate materiaalsete toodete ja nendesse sisseehitatud tarkvara suhtes horisontaalsed küberturvalisuse nõuded,

mis peavad olema täidetud nende toodete turule laskmiseks, ning see hõlmaks kahte allvarianti koos kohustusliku kolmanda isiku poolse hindamisega ja ilma selleta (3i ja 3ii). Sisseehitamata tarkvara ei oleks reguleeritud;

- horisontaalne regulatiivne sekkumine, millega kehtestatakse küberturvalisuse nõuded laiale hulgale materiaalsetele ja immateriaalsetele digielemente sisaldavatele toodetele, sealhulgas sisseehitamata tarkvarale (4. variant): see variant sarnaneb 3. variandiga, kui kohaldamisala välja arvata. 4. variandi puhul hõlmaks võimaliku määruse kohaldamisala sisseehitamata tarkvara (on kaks allvarianti, mis hõlmavad üksnes kriitilise tähtsusega (4a) või kogu tarkvara (4b)). Mõlema allvariandi puhul kaalutakse samu vastavushindamisega seotud variante nagu 3. variandi puhul.

4. variant (allvariantidega, mis hõlmavad kogu tarkvara ja kriitilise tähtsusega toodete kohustuslikku kolmanda isiku poolset hindamist) osutus eelistatud variandiks, tuginedes tulemuslikkuse hindamisele erieesmärkide ja kulutõhususe alusel. See variant tagaks konkreetsete horisontaalsete küberturvalisuse nõuete kehtestamise kõigi siseturule lastavate või seal kättesaadavaks tehtavate digielemente sisaldavate toodete suhtes ning oleks ainus variant, mis hõlmab kogu digitaalset tarneahelat. Selline regulatiivne sekkumine hõlmaks ka sisseehitamata tarkvara, millel on sageli nõrku kohti, ning tagaks seega sidusa lähenemisviisi kõigi digielemente sisaldavate toodete puhul, kusjuures vastutus oleks eri ettevõtjate vahel selgelt jaotatud.

See poliitikavariant loob ka lisaväärtust, hõlmates hoolsuskohustuse ja kogu elutsükli aspekte pärast digielemente sisaldavate toodete turule laskmist, et tagada muu hulgas asjakohase teabe andmine turvalisusealase toe kohta ja turvauuenduste tegemine. See poliitikavariant täiendaks ühtlasi kõige tõhusamalt võrgu- ja infoturbe raamistiku hiljutist läbivaatamist, tagades eeltingimused tarneahela turvalisuse suurendamiseks.

Eelistatud variant tooks eri sidusrühmadele märkimisväärset kasu. Ettevõtjate jaoks hoiaks see ära digielemente sisaldavate toodete suhtes kohaldatavate turvaeeskirjade lahknevuse ja vähendaks asjaomaste küberturvalisuse õigusaktide nõuete täitmisega seotud kulusid. See vähendaks küberintsidentide arvu, intsidentide käsitlemise kulusid ja mainekahju. Algatus võib kogu ELis vähendada ettevõtjaid mõjutavate intsidentidega seotud kulusid hinnanguliselt 180–290 miljardi euro võrra aastas. See tooks kaasa käibe suurenemise, kuna nõudlus digielemente sisaldavate toodete järele suureneks. See parandaks ettevõtjate ülemaailmset mainet, mis tooks kaasa nõudluse suurenemise ka väljaspool ELi. Kasutajate jaoks suurendaks eelistatud variant turvaomaduste läbipaistvust ja hõlbustaks digielemente sisaldavate toodete kasutamist. Tarbijad ja kodanikud saaksid kasu ka oma põhiõiguste (nagu eraelu puutumatus ja andmekaitse) paremast kaitsest.

Kui avalikul konsultatsioonil osalejatel paluti hinnata poliitikameetmete tõhusust, nõustusid nad, et kõige tõhusam meede oleks 4. variant (4,08 punkti skaalal 1–5). Osalejate hulka kuulusid tarbijaorganisatsioonid (5,00), end kasutajatena määratlenud osalejad (4,22), teavitatud asutused (4,17), turujärelevalveasutused (5,00) ja digielemente sisaldavate toodete tootjad (3,85), sealhulgas väikesed ja keskmise suurusega tootjad (4,05).

- **Õigusnormide toimivus ja lihtsustamine**

Käesolevas ettepanekus sätestatakse nõuded, mida kohaldatakse tark- ja riistvara tootmise suhtes. Vaja on tagada õiguskindlus ja vältida siseturul toodetega seotud küberturvalisuse

nõuete edasist killustumist; seda vajadust on tõendanud eri sidusrühmade laialdane toetus horisontaalsele sekkumisele. Ettepanekuga vähendatakse tootjatele mitme tooteohutust käsitleva õigusaktiga pandud regulatiivset koormust. Uue õigusraamistikuga vastavusse viimine tähendab sekkumise ja selle nõuete täitmise tagamise paremat toimimist. Ettepanekuga lihtsustatakse kaitsemeetmete menetluse protsessi, kaasates tootjad ja liikmesriigid enne komisjoni teavitamist. Suur osa ettepaneku kohaldamisalasse kuuluvatest tootjatest on uue õigusraamistiku toimimisega juba kursis, mis aitab kaasa selle mõistmisele ja rakendamisele. Tarbijate ja ettevõtjate seisukohast suurendab ettepanek usaldust digielemente sisaldavate toodete vastu.

- **Põhiõigused**

Kõik poliitikavariandid peaksid teataval määral tõhustama selliste põhiõiguste ja -vabaduste kaitset nagu eraelu puutumatus, isikuandmete kaitse, ettevõtlusvabadus ning vara või inimväärikuse ja isikupuutumatuse kaitse. Sellega seoses oleks kõige tulemuslikum eelkõige eelistatud 4. poliitikavariant, mis hõlmab horisontaalset regulatiivset sekkumist ja millel on lai poliitiline ulatus, kuna see aitab tõenäolisemalt vähendada intsidentide, sealhulgas isikuandmetega seotud rikkumiste arvu ja raskusastet. Samuti suurendaks see õiguskindlust ja looks ettevõtjatele võrdsed tingimused, suurendaks kasutajate usaldust ja digielemente sisaldavate ELi toodete üldist populaarsust, kaitstes seeläbi vara ja parandades ettevõtjate äritegevuse tingimusi.

Horisontaalsed küberturvalisuse nõuded aitaksid kaasa isikuandmete turvalisuse tagamisele, kaitstes digielemente sisaldavates toodetes sisalduva teabe konfidentsiaalsust, terviklikkust ja kättesaadavust. Nende nõuete täitmine hõlbustab isikuandmete kaitse üldmääruse (EL) 2016/679[12] kohase isikuandmete töötlemise turvalisuse nõude täitmist. Ettepanekuga parandataks läbipaistvust ja kasutajate teavitamist, sealhulgas nende kasutajate puhul, kellel võib olla vähem küberturvalisusealaseid oskusi. Kasutajaid teavitataks paremini ka digielemente sisaldavate toodete riskidest, võimalustest ja piirangutest ning see annaks neile paremad võimalused võtta vajalikke ennetus- ja leevendusmeetmeid jääkriskide vähendamiseks.

4. MÕJU EELARVELE

Euroopa Liidu Küberturvalisuse Ametile (ENISA) käesoleva määrusega antud ülesannete täitmiseks peab ENISA paigutama vahendid ümber ligikaudu 4,5 täistööajale taandatud töötaja ulatuses. Komisjon peaks nägema ette 7 täistööajale taandatud töötajat, et täita oma käesolevast määrusest tulenevaid kohustusi seoses nõuete täitmise tagamisega.

Üksikasjalik ülevaade kaasnevatest kuludest on esitatud käesoleva ettepanekuga seotud finantsselgituses.

[12] 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).

5. MUU TEAVE

• Rakenduskavad ning järelevalve, hindamise ja aruandluse kord

Komisjon jälgib nende uute sätete rakendamist, kohaldamist ja järgimist, et hinnata nende tulemuslikkust. Määruses nähakse ette, et komisjon vaatab selle läbi ja hindab seda ning esitab selle kohta avaliku aruande Euroopa Parlamendile ja nõukogule 36 kuud pärast kohaldamise alguskuupäeva ning seejärel iga nelja aasta tagant.

• Ettepaneku sätete üksikasjalik selgitus

Üldsätted (I peatükk)

Käesolevas kavandatavas määruses sätestatakse a) õigusnormid, mis reguleerivad digielemente sisaldavate toodete turule laskmist, et tagada selliste toodete küberturvalisus; b) digielemente sisaldavate toodete projekteerimise, arendamise ja tootmise olulised nõuded ning kohustused, mida ettevõtjad peavad selliste toodete puhul seoses küberturvalisusega täitma; c) selliste protsesside olulised nõuded, mille tootjad on kehtestanud nõrkuste käitlemiseks, et tagada digielemente sisaldavate toodete küberturvalisus kogu toote elutsükli vältel, ning ettevõtjate kohustused seoses nende protsessidega; d) õigusnormide turujärelevalve ja eespool nimetatud õigusnormide ja nõuete täitmise tagamise kohta.

Kavandatud määrust kohaldatakse kõigi digielemente sisaldavate toodete suhtes, mille kavandatud ja mõistlikult prognoositav kasutamine hõlmab otsest või kaudset loogilist või füüsilist andmeühendust seadme või võrguga.

Kavandatud määrust ei kohaldata selliste digielemente sisaldavate toodete suhtes, mis kuuluvad määruse (EL) 2017/745 [inimestel kasutatavad meditsiiniseadmed ja selliste seadmete abiseadmed] ja määruse (EL) 2017/746 [inimestel kasutatavad *in vitro* diagnostikameditsiiniseadmed ja selliste seadmete abiseadmed] kohaldamisalasse, kuna mõlemad määrused käsitlevad nõudeid seadmete kohta, sealhulgas tarkvara kohta, ja tootjate üldisi kohustusi, mis hõlmavad toodete kogu olelusringi, ning vastavushindamismenetlusi. Käesolevat määrust ei kohaldata digielemente sisaldavate toodete suhtes, mis on sertifitseeritud vastavalt määrusele (EL) 2018/1139 [tsiviillennundusohutuse ühtlaselt kõrge tase], ega toodete suhtes, mille suhtes kohaldatakse määrust (EL) 2019/2144 [mis käsitleb mootorsõidukite ja nende haagiste ning mootorsõidukite jaoks ette nähtud süsteemide, osade ja eraldi seadmestike tüübikinnituse nõudeid].

Digielemente sisaldavate kriitilise tähtsusega toodete suhtes kohaldatakse konkreetseid vastavushindamismenetlusi ning need jaotatakse III lisa kohaselt I ja II klassi vastavalt nende küberriski tasemele, kusjuures II klass kajastab suuremat riski. Digielemente sisaldavat toodet peetakse kriitilise tähtsusega tooteks ja see lisatakse seega III lisasse selle digielemente sisaldava toote võimalike küberturvalisuse nõrkuste mõju põhjal. Küberriski kindlakstegemisel võetakse muu hulgas arvesse digielemente sisaldava toote küberturvalisusega seotud funktsionaalsust ja kavandatud kasutamist tundlikes keskkondades, näiteks tööstuskeskkonnas.

Komisjonil on ühtlasi õigus võtta käesoleva määruse täiendamiseks vastu delegeeritud õigusakte, millega määratakse kindlaks digielemente sisaldavate ülikriitilise tähtsusega toodete kategooriad, mille puhul tootjad peavad saama Euroopa küberturvalisuse

sertifitseerimise kava alusel Euroopa küberturvalisuse sertifikaadi, et tõendada vastavust I lisas sätestatud olulistele nõuetele või nende osadele. Selliste digielemente sisaldavate ülikriitilise tähtsusega toodete kategooriate kindlaksmääramisel võtab komisjon arvesse digielemente sisaldavate toodete kategooriaga seotud küberriski taset, pidades silmas üht või mitut kriteeriumi, mida võetakse arvesse digielemente sisaldavate kriitilise tähtsusega toodete loetlemisel III lisas, ning hinnangut selle kohta, kas selle kategooria tooteid kasutavad või neile tuginevad direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv) lisas [I lisa] osutatud liiki elutähtsad üksused või kas neil toodetel on potentsiaalne tulevane tähtsus nende üksuste tegevuse jaoks või kas need on olulised digielemente sisaldavate toodete tarneahela kui terviku vastupidavusvõime tagamiseks häirivate sündmuste korral.

Ettevõtjate kohustused (II peatükk)

Ettepanek sisaldab tootjate, importijate ja turustajate kohustusi, mis põhinevad otsuses nr 768/2008/EÜ ette nähtud erisätetel. Oluliste küberturvalisuse nõuete ja kohustustega nähakse kõigi digielemente sisaldavate toodete puhul ette, et need tehakse turul kättesaadavaks üksnes juhul, kui need nõuetekohase tarnimise ja õige paigaldamise, hooldamise ning sihtotstarbelise või mõistlikult prognoositavatel tingimustel kasutamise korral on vastavuses käesolevas määruses sätestatud oluliste küberturvalisuse nõuetega.

Oluliste nõuete ja kohustustega nähtaks ette, et tootjad peavad võtma digielemente sisaldavate toodete projekteerimisel, arendamisel ja tootmisel arvesse küberturvalisust, täitma oma toodete projekteerimisel ja arendamisel hoolsuskohustust seoses turvaaspektidega, tagama läbipaistvuse küberturvalisuse aspektide puhul, mis tuleb klientidele teatavaks teha, tagama proportsionaalsel viisil turvalisusealase toe (uuendused) ning täitma nõrkuste käitlemise nõudeid.

Ettevõtjatele alates tootjatest kuni turustajate ja importijateni kehtestataks seoses digielemente sisaldavate toodete turule laskmisega piisavad kohustused, võttes arvesse nende ettevõtjate rolli ja kohustusi tarneahelas.

Digielemente sisaldava toote vastavus (III peatükk)

Digielemente sisaldav toode, mis on vastavuses harmoneeritud standardite või nende osadega, mille viited on avaldatud *Euroopa Liidu Teatajas*, eeldatakse olevat vastavuses käesolevas kavandatud määruses sätestatud oluliste nõuetega. Kui harmoneeritud standardid puuduvad või on ebapiisavad või kui standardimismenetluses esineb põhjendamatuid viivitusi või kui Euroopa standardiorganisatsioonid ei ole komisjoni taotlust vastu võtnud, võib komisjon võtta rakendusaktidega vastu ühtsed kirjeldused.

Lisaks eeldatakse, et digielemente sisaldavad tooted, mis on sertifitseeritud või mille kohta on välja antud ELi vastavusdeklaratsioon või sertifikaat määruse (EL) 2019/881 kohase Euroopa küberturvalisuse sertifitseerimise kava alusel ja mille kohta komisjon on rakendusaktiga täpsustanud, et ta saab eeldada vastavust käesolevale määrusele, vastavad käesoleva määruse olulistele nõuetele või nende osadele, niivõrd kui ELi vastavusdeklaratsioon või küberturvalisuse sertifikaat või nende osad hõlmavad neid nõudeid.

Et vältida tootjate põhjendamatut halduskoormust, peaks komisjon ühtlasi vajaduse korral täpsustama, kas sellise Euroopa küberturvalisuse sertifitseerimise kava alusel välja antud küberturvalisuse sertifikaat kaotab tootjate kohustuse tagada kolmanda isiku poolne vastavushindamine, mis on käesoleva määruse asjaomaste nõuetega ette nähtud.

Tootja peab viima ellu digielemente sisaldava toote vastavushindamise ja nõrkuste käitlemise protsessid, mille ta on kehtestanud I lisas sätestatud olulistele nõuetele vastavuse tõendamiseks, järgides ühte VI lisas sätestatud menetlustest. I ja II klassi kuuluvate kriitilise tähtsusega toodete tootjad peavad kasutama nõuetele vastavuse tagamiseks asjaomaseid vajalikke mooduleid. II klassi kuuluvate kriitilise tähtsusega toodete tootjad peavad oma vastavushindamisse kaasama kolmanda isiku.

Vastavushindamisasutustest teavitamine (IV peatükk)

Teavitatud asutuste nõuetekohane toimimine on äärmiselt oluline, et tagada küberturvalisuse kõrge tase ja kõigi huvitatud isikute usaldus uue lähenemisviisi süsteemi vastu. Seepärast sätestatakse ettepanekus kooskõlas otsusega nr 768/2008/EÜ nõuded vastavushindamisasutuste (teavitatud asutused) eest vastutavatele liikmesriikide ametiasutustele. Sellega jäetakse teavitatud asutuste määramise ja järelevalve lõplik kohustus liikmesriikidele. Liikmesriigid määravad teavitava asutuse, kes vastutab vastavushindamisasutuste hindamiseks ja nendest teavitamiseks ning teavitatud asutuste järelevalveks vajalike menetluste kehtestamise ja rakendamise eest.

Turujärelevalve ja täitmise tagamine (V peatükk)

Kooskõlas määrusega (EL) 2019/1020 teevad riiklikud turujärelevalveasutused turujärelevalvet asjaomase liikmesriigi territooriumil. Liikmesriigid võivad otsustada määrata turujärelevalveasutuseks mis tahes olemasoleva või uue asutuse, sealhulgas direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] artiklis [artikkel X] osutatud määratud riiklikud pädevad asutused või määruse (EL) 2019/881 artiklis 58 osutatud määratud riiklikud küberturvalisuse sertifitseerimise asutused. Ettevõtjatel palutakse teha turujärelevalveasutuste ja muude pädevate asutustega täielikku koostööd.

Delegeeritud volitused ja komiteemenetlused (VI peatükk)

Tagamaks, et õigusraamistikku saab vajaduse korral kohandada, on komisjonil õigus võtta kooskõlas ELi toimimise lepingu artikliga 290 vastu delegeeritud õigusakte, et ajakohastada I ja II klassi kuuluvate kriitilise tähtsusega toodete loetelu ja täpsustada nende toodete määratlusi; täpsustada, kas vajalik on piirang või väljajätmine selliste digielemente sisaldavate toodete puhul, mis on hõlmatud muude liidu õigusnormidega, milles kehtestatud nõuetega saavutatakse samasugune kaitsetase nagu käesoleva määrusega; kehtestada kohustus sertifitseerida teatavad digielemente sisaldavad ülikriitilise tähtsusega tooted käesolevas määruses sätestatud kriteeriumide alusel; määrata kindlaks ELi vastavusdeklaratsiooni minimaalne sisu ja täiendada tehnilises dokumentatsioonis esitatavaid elemente.

Komisjonil on ühtlasi õigus võtta vastu rakendusakte, et: määrata kindlaks aruandekohustuste ja tarkvaramaterjalide loetelu vorm või elemendid; määrata kindlaks Euroopa küberturvalisuse sertifitseerimise kavad, mida saab kasutada käesolevas määruses sätestatud olulistele nõuetele või nende osadele vastavuse tõendamiseks; võtta vastu ühtsed kirjeldused; kehtestada CE-vastavusmärgise kinnitamise tehnilised kirjeldused; võtta erandlikel asjaoludel, mis õigustavad viivitamatut sekkumist, liidu tasandil parandus- või piiravaid meetmeid, et säilitada siseturu hea toimimine.

Konfidentsiaalsus ja karistused (VII peatükk)

Kõik käesolevat määrust kohaldavad osalised austavad oma ülesannete täitmise ja tegevuse käigus saadud teabe ja andmete konfidentsiaalsust.

Et tagada käesolevas määruses sätestatud kohustuste tõhus täitmine, peaks igal turujärelevalveasutusel olema õigus määrata haldustrahve või taotleda nende määramist. Samamoodi kehtestatakse käesolevas määruses nende haldustrahvide ülemmäärad, mis tuleks siseriiklikes õigusaktides sätestada käesolevas määruses sätestatud kohustuste täitmata jätmise eest.

Ülemineku- ja lõppsätted (VIII peatükk)

Et anda tootjatele, teavitatud asutustele ja liikmesriikidele aega uute nõuetega kohanemiseks, hakatakse kavandatud määrust kohaldama [24 kuud] pärast selle jõustumist, välja arvatud tootjate aruandekohustus, mida hakatakse kohaldama [12 kuud] pärast jõustumise kuupäeva.

2022/0272 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrust (EL) 2019/1020

(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 riikide parlamentidele,

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

võttes arvesse Regioonide Komitee arvamust[2],

toimides seadusandliku tavamenetluse kohaselt

ning arvestades järgmist:

(1) Siseturu toimimist on vaja parandada ning selleks tuleb kehtestada ühtne õigusraamistik, 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.

---

1 ELT C ..., ..., lk …

2 ELT C ..., ..., lk …

Ühtlasi on selle eesmärk luua tingimused, et kasutajad saaksid digielemente sisaldavaid tooteid valides ja kasutades võtta arvesse küberturvalisust.

(3) Praegu kehtivad asjakohased liidu õigusaktid sisaldavad mitut horisontaalsete normide kogumit, mis käsitlevad küberturvalisusega seotud teatavaid aspekte eri vaatenurkadest, sealhulgas digitaalse tarneahela turvalisuse parandamise meetmed. Küberturvalisust käsitlevad kehtivad liidu õigusaktid, sealhulgas [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] ja Euroopa Parlamendi ja nõukogu määrus (EL) 2019/881,[3] ei reguleeri siiski otseselt digielemente sisaldavate toodete turvalisuse kohustuslikke nõudeid.

(4) Kehtivaid liidu õigusakte 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 ettevõtjate jaoks tarbetu koormuse täita samalaadsete toodete puhul paljusid eri nõudeid. Selliste toodete küberturvalisusel on eriti tugev piiriülene aspekt, sest ühes riigis valmistatud tooteid kasutavad organisatsioonid ja tarbijad sageli kõikjal siseturul. See tähendab, et kõnealust valdkonda on vaja reguleerida liidu tasandil. Liidu õiguslikku keskkonna ühtlustamiseks tuleks kehtestada digielemente sisaldavate toodete küberturvalisuse nõuded. Ühtlasi tuleks kogu liidus tagada ettevõtjate ja kasutajate jaoks kindlustunne ning ühtne turg tuleks paremini ühtlustada, luues liidu turule siseneda soovivate ettevõtjate jaoks paremini toimivad tingimused.

(5) Liidu tasandil on mitmetes programmilistes ja poliitilistes dokumentides, näiteks ELi küberturvalisuse strateegias digikümnendi jaoks,[4] nõukogu 2. detsembri 2020. aasta ja 23. mai 2022. aasta järeldustes ning Euroopa Parlamendi 10. juuni 2021. aasta resolutsioonis,[5] esitatud üleskutse kehtestada digitaalsete või ühendatud toodete jaoks liidu küberturvalisuse erinõuded, kusjuures maailmas on mitu riiki selle probleemi lahendamiseks omal algatusel juba meetmeid võtnud. Euroopa tuleviku konverentsi lõpparuandes soovisid kodanikud ELi rolli tugevdamist küberohtudega võitlemisel[6].

---

[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] JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/ET/ALL/?uri=JOIN:2020:18:FIN.

[5] 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_ET.html.

[6] „Euroopa tuleviku konverents – aruanne konverentsi lõpptulemuste kohta“, mai 2022, 28. ettepanek, punkt 2. Konverents toimus aprillist 2021 kuni maini 2022. See oli ainulaadne kodanike juhitud aruteludemokraatia üritus, mis toimus üleeuroopalisel tasandil ja hõlmas

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

(7) 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 ühendatavad tooted projekteeritakse ja neid arendatakse kooskõlas käesolevas määruses sätestatud oluliste nõuetega. See käib nii nende toodete kohta, mida saab ühendada füüsiliselt riistvaralise liidese kaudu, kui ka neid, mis ühendatakse loogiliselt, näiteks võrgupesa, toru, faili, rakendusliidese või muud liiki tarkvaraliidese kaudu. Küberturvalisuse ohud võivad enne teatava sihtmärgini jõudmist levida mitmesuguste digielemente sisaldavate toodete kaudu, näiteks mitmest nõrkuse ärakasutamisest tekitatud ahelas, ja seepärast peaksid tootjad tagama ka selliste toodete küberturvalisuse, mis on teiste seadmete või võrkudega ühendatud üksnes kaudselt.

(8) Kui kehtestatakse küberturvalisuse nõuded digielemente sisaldavate toodete turule laskmise jaoks, paraneb nende toodete küberturvalisus nii tarbijate kui ka ettevõtjate jaoks. See hõlmab ka haavatavatele tarbijatele mõeldud digielemente sisaldavate toodete, näiteks mänguasjade ja beebimonitoride turule laskmise nõudeid.

(9) Käesoleva määrusega tagatakse digielemente sisaldavate toodete küberturvalisuse kõrge tase. Määrusega ei reguleerita selliseid teenuseid nagu teenusena pakutav tarkvara (SaaS), välja arvatud digielemente sisaldava tootega seotud kaugandmetöötluslahendused, s.o igasugune distantsilt toimuv andmevahetus, mille jaoks on tarkvara projekteerinud ja välja töötanud asjaomase toote tootja või mille jaoks on selline tarkvara projekteeritud ja välja töötatud selle tootja vastutusel ning mille puudumine ei laseks sellisel digielemente sisaldaval tootel täita üht oma funktsioonidest. [Direktiiviga XXX/XXXX (küberturvalisuse 2. direktiiv)] on kehtestatud küberturvalisuse ja intsidentidest teatamise nõuded elutähtsate ja oluliste üksuste, näiteks elutähtsa taristu jaoks, et suurendada nende osutatavate teenuste vastupidavusvõimet. [Direktiivi XXX/XXXX (küberturvalisuse 2. direktiiv)] kohaldatakse pilvteenuste ja pilvteenuse mudelite suhtes (näiteks SaaS). Selle direktiivi kohaldamisalasse kuuluvad kõik liidus pilvteenuseid osutavad üksused, mis vastavad keskmise suurusega ettevõtjatele kehtestatud künnisele või ületavad selle.

(10) Et mitte takistada innovatsiooni ja teadusuuringuid, ei peaks käesoleva määruse kohaldamisalasse kuuluma vaba ja avatud lähtekoodiga tarkvara, mida arendatakse või pakutakse väljaspool äritegevust. Eeskätt puudutab see tarkvara, kaasa arvatud selle lähtekoodi ja muudetud versioone, mida jagatakse avalikult ja mis on vabalt kättesaadav, kasutatav, muudetav ja edasi levitatav. Tarkvara puhul ei pruugi äritegevust iseloomustada üksnes toote eest hinna küsimine, vaid ka tehniliste tugiteenuste eest hinna küsimine, tarkvaraplatvormi pakkumine, mille kaudu tootja

---

tuhandeid Euroopa kodanikke, samuti poliitilisi osalejaid, sotsiaalpartnereid, kodanikuühiskonna esindajaid ja peamisi sidusrühmi.

teenib raha muude teenuste eest, või isikuandmete kasutamine muul otstarbel kui üksnes tarkvara turvalisuse, ühilduvuse või koostalitlusvõime parandamiseks.

(11) Turvaline internet on elutähtsa taristu ja ühiskonna kui terviku toimimiseks hädavajalik. [Direktiivi XXX/XXXX (küberturvalisuse 2. direktiiv)] eesmärk on tagada elutähtsate ja oluliste üksuste, sealhulgas avatud interneti tuumteenuseid toetavate ning internetiühendust ja internetiteenuseid tagavate 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 XXX/XXXX (küberturvalisuse 2. direktiiv)] tulenevaid tarneahela nõudeid, tagades, et nende teenuste osutamiseks kasutatavate digielemente sisaldavate toodete väljatöötamine toimub turvalisel viisil ning neil on juurdepääs selliste toodete õigeaegsetele turvauuendustele.

(12) Euroopa Parlamendi ja nõukogu määrusega (EL) 2017/745[7] on kehtestatud õigusnormid meditsiiniseadmete kohta ning Euroopa Parlamendi ja nõukogu määrusega (EL) 2017/746[8] *in vitro* diagnostikameditsiiniseadmete kohta. Mõlemas määruses on käsitletud küberriske ja järgitud lähenemisviise, mida puudutatakse ka käesolevas määruses. Konkreetsemalt on määruses (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 nende määruste I lisa kõiki asjaomaseid olulisi nõudeid[9]. Seega ei peaks digielemente sisaldavad tooted, mille suhtes kohaldatakse üht neist määrustest, kuuluma käesoleva määruse kohaldamisalasse.

---

[7] 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).

[8] 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).

[9] MDCG 2019-16, mille on kinnitanud määruse (EL) 2017/745 artikliga 103 loodud meditsiiniseadmete koordineerimisrühm.

(13) Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/2144[10] 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 kasutuseaga seotud küberriskide jaoks kooskõlas kohaldatavate ÜRO eeskirjadega tehniliste kirjelduste ja küberturvalisuse kohta[11] ning millega on ette nähtud konkreetsed vastavushindamismenetlused. 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, seadmete, sealhulgas tarkvara lennukõlblikkuse oluliste nõuete raamistik, milles võetakse arvesse kohustust kaitsta infoturvaohtude eest. Seega ei kehti käesolevas määruses sätestatud olulised nõuded ja vastavushindamismenetlused digielemente sisaldavate toodete suhtes, mille suhtes kohaldatakse määrust (EL) 2019/2144, ja määruse (EL) 2018/1139 kohaselt sertifitseeritud toodete suhtes. Määruse (EL) 2018/1139 kohane sertifitseerimismenetlus tagab usaldusväärsuse taseme, mille poole käesoleva määrusega püüeldakse.

(14) 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 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 käesoleva määruse I lisas sätestatud oluliste

---

[10] 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).

[11] Ühinenud Rahvaste Organisatsiooni (ÜRO) eeskiri nr 155: ühtsed sätted, mis käsitlevad sõidukite tüübikinnitust seoses küberturvalisuse ja küberturvalisuse haldamise süsteemiga [2021/387].

[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).

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 kaitse samasugune tase, nagu on ette nähtud käesoleva määrusega. Komisjonil on õigus võtta käesoleva määruse muutmiseks vastu delegeeritud õigusakte ning määrata kindlaks sellised tooted ja normid. Kehtivate liidu õigusaktide kohta, mille suhtes tuleks kohaldada sellist piirangut või välistust, esitatakse käesolevas määruses konkreetsed sätted, et selgitada määruse suhet kõnealuste liidu õigusaktidega.

(15) Delegeeritud määruses (EL) 2022/30 on sätestatud, et teatavate raadioseadmete suhtes kohaldatakse direktiivi 2014/53/EL artikli 3 lõike 3 punktis d (võrgu kahjustamine ja võrgu ressursside kuritarvitamine), punktis e (isikuandmed ja eraelu puutumatus) ja punktis f (pettused) sätestatud olulisi nõudeid. [Komisjoni rakendusotsuses XXX/2022 Euroopa standardiorganisatsioonidele esitatud standardimistaotluse kohta] on sätestatud nõuded konkreetsete standardite väljatöötamise kohta, et veelgi täpsustada, kuidas neid kolme olulist nõuet tuleks käsitleda. Käesolevas määruses sätestatud olulised nõuded sisaldavad kõiki direktiivi 2014/53/EL artikli 3 lõike 3 punktides d, e ja f osutatud oluliste nõuete elemente. Peale selle on käesolevas määruses sätestatud olulised 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 komisjoni rakendusotsusega C(2022) 5637 standardimistaotluse kohta seoses raadioseadmete direktiivi delegeeritud määrusega 2022/30, et valmistada ette ja töötada välja käesoleva määruse rakendamist hõlbustavad harmoneeritud standardid.

(16) Direktiiv 85/374/EMÜ[13] 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.

(17) Käesolev määrus ei tohiks piirata Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679[14] kohaldamist, sealhulgas sätteid selliste andmekaitse sertifitseerimismehhanismide ning andmekaitsepitserite ja -märgiste kasutuselevõtuks, mille abil saab tõendada, et vastutavate töötlejate ja volitatud töötlejate isikuandmete töötlemise toimingud vastavad kõnealusele määrusele.

---

[13] Nõukogu 25. juuli 1985. aasta direktiiv 85/374/EMÜ liikmesriikide tootevastutust käsitlevate õigus- ja haldusnormide ühtlustamise kohta (EÜT L 210, 7.8.1985).

[14] 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).

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 nimetatud riiklikud turujärelevalveasutused tegema koostööd liidu andmekaitseõiguse järelevalvega tegelevate asutustega. Liidu andmekaitseõiguse järelevalvega tegelevatel asutustel peaks samuti olema juurdepääs oma ülesannete täitmiseks vajalikule teabele.

(18) Kui artiklis [määruse (EL) nr 910/2014 artikli 6a lõige 2, nagu seda on muudetud ettepanekuga määruse kohta, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega] osutatud Euroopa digiidentiteeditasku väljastaja tooted kuuluvad käesoleva määruse kohaldamisalasse, peaksid nad täitma nii käesoleva määrusega ettenähtud olulisi horisontaalseid nõudeid kui ka artikliga [määruse (EL) nr 910/2014 artikkel 6a, nagu seda on muudetud ettepanekuga määruse kohta, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega] ettenähtud spetsiifilisi turvanõudeid. Nõuete täitmise hõlbustamiseks peaks digiidentiteeditasku väljastaja saama tõendada Euroopa digiidentiteeditasku vastavust kummaski õigusaktis sätestatud nõuetele sedasi, et laseb oma tooted sertifitseerida määruse (EL) 2019/881 alusel loodud sellise Euroopa küberturvalisuse sertifitseerimise kava kohaselt, mille kohta komisjon on rakendusaktiga näinud ette käesolevale määrusele vastavuse eelduse, kuivõrd sertifikaat või selle osad hõlmavad neid nõudeid.

(19) Teatavaid käesolevas määruses sätestatud ülesandeid peaks täitma ENISA kooskõlas määruse (EL) 2019/881 artikli 3 lõikega 2. Esmajoones peaks ENISA saama tootjatelt teateid digielemente sisaldavates toodetes esinevate aktiivselt ärakasutatavate nõrkuste kohta, aga ka intsidentide kohta, mis mõjutavad nende toodete turvalisust. ENISA peaks need teated edastama ka asjaomastele küberturbe intsidentide lahendamise üksustele (CSIRTidele) või liikmesriikide direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] artikli [artikkel X] kohaselt määratud asjaomastele ühtsetele kontaktpunktidele ning teavitama asjaomaseid turujärelevalveasutusi teatatud nõrkusest. ENISA peaks kogutud teabe põhjal koostama iga kahe aasta järel tehnilise aruande küberriskide värskete suundumuste kohta digielemente sisaldavates toodetes ning esitama selle direktiivis [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] osutatud koostöörühmale. Arvestades ENISA eksperditeadmisi ja volitusi, peaks ENISA ühtlasi saama toetada käesoleva määruse rakendamise protsessi. Eeskätt peaks ta 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 üheaegseid koordineeritud kontrollimeetmeid. Erandlike asjaolude korral peaks ENISA saama komisjoni taotlusel korraldada selliste digielemente sisaldavate toodete hindamisi, mis kujutavad endast

olulist küberriski, kui siseturu hea toimimise säilitamiseks on vaja sekkuda viivitamata.

(20) Digielemente sisaldavatel toodetel peaks olema CE-vastavusmärgis, mis näitab 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.

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

(22) Tagamaks et digielemente sisaldavad tooted ei põhjusta turule laskmisel inimestele ja organisatsioonidele küberriske, tuleks selliste toodete jaoks kehtestada olulised nõuded. Kui hiljem muudetakse toodet füüsiliste või digitaalsete vahenditega, mida tootja ette ei näinud ja mis võib tähendada, et toode ei vasta enam asjakohastele olulistele nõuetele, tuleks seda pidada oluliseks muutmiseks. Näiteks tarkvarauuendused või -parandused võib ühildada hooldustöödega, eeldusel et need ei muuda juba turule lastud toodet viisil, mis mõjutaks vastavust kohaldatavatele nõuetele või muudaks kavandatud kasutamist, millest lähtuvalt on toodet hinnatud. Nagu füüsilise parandamise või muutmise korral, tuleks digielemente sisaldavat toodet käsitada tarkvara muutmise tõttu oluliselt muudetud tootena, kui tarkvarauuendusega muudetakse toote algselt kavandatud funktsioone, liiki või tööd ning selliseid muudatusi ei olnud esialgses riskihindamises ette nähtud või kui tarkvarauuenduse tõttu on ohu laad muutunud või riskitase tõusnud.

(23) Liidu ühtlustamisõigusaktidega reguleeritud toodete olulise muutmise laialdaselt juurdunud mõistega kooskõlas on otstarbekas kontrollida digielemente sisaldava toote vastavust ja vajaduse korral teha sellele uus vastavushindamine alati, kui leiab aset oluline muudatus, mis võib mõjutada 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 muudatustest, mis võivad kaasa tuua olulisi muudatusi.

(24) Digielemente sisaldava toote määruses [ökodisaini määrus] määratletud renoveerimine, hooldus ja parandamine ei pruugi põhjustada toote olulist muutmist, näiteks siis, kui kavandatud kasutamist ja funktsioone ei muudeta ja riski taset ei mõjutata. Toote uuendamine tootja poolt võib siiski põhjustada muudatusi toote projektis ja arendamises ning võib seega mõjutada toote kavandatud kasutamist ja vastavust käesolevas määruses sätestatud nõuetele.

(25) Digielemente sisaldavaid tooteid peaks käsitama kriitilise tähtsusega toodetena, kui toote võimalike küberturvalisuse nõrkuste ärakasutamise kahjulik mõju võib olla

tõsine muu hulgas küberturvalisusega seotud funktsioonide või kavandatud kasutamise tõttu. Turvalisusprobleemide leviku tarneahelas võivad kaasa tuua eeskätt selliste digielemente sisaldavate toodete nõrkused, mille funktsioonid on seotud küberturvalisusega (näiteks turvalised elemendid). Küberintsidendi mõju tõsidus võib suureneda ka siis, kui võetakse arvesse toote kavandatud kasutamist, näiteks tööstuskeskkonnas või seoses direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] [I lisa] lisas osutatud liiki elutähtsa üksusega või kriitilise tähtsusega või tundlike funktsioonide (näiteks isikuandmete töötlemine) täitmise korral.

(26) Digielemente sisaldavate kriitilise tähtsusega toodete suhtes tuleks kohaldada rangemaid vastavushindamismenetlusi, jäädes oma lähenemises siiski proportsionaalseks. Sel otstarbel tuleks digielemente sisaldavad kriitilise tähtsusega tooted jagada kahte klassi, lähtudes nende tootekategooriatega seotud küberriskide tasemest. II klassi tooteid hõlmava võimaliku küberintsidendi kahjulik mõju võib olla suurem kui I klassi tooteid hõlmava intsidendi puhul näiteks johtuvalt toote küberturvalisusega seotud funktsiooni laadist või kavandatud kasutamisest tundlikus keskkonnas ning seetõttu tuleks sellise toote suhtes kohaldada rangemat vastavushindamismenetlust.

(27) Käesoleva määruse III lisas osutatud digielemente sisaldavate kriitilise tähtsusega toodete kategooriaid tuleks mõista kui tooteid, mille põhifunktsioon on sellist liiki, mis on loetletud käesoleva määruse III lisas. Näiteks on käesoleva määruse III lisas loetletud tooted, mis on nende põhifunktsiooni järgi määratletud II klassi kuuluvate üldotstarbeliste mikroprotsessoritena. Sellest tulenevalt kohaldatakse üldotstarbeliste mikroprotsessorite suhtes kohustuslikku kolmanda isiku vastavushindamist. See ei kehti aga muude toodete suhtes, millesse võib olla integreeritud üldotstarbeline mikroprotsessor, kuid millele ei ole käesoleva määruse III lisas sõnaselgelt viidatud. Komisjon peaks [12 kuu jooksul pärast käesoleva määruse jõustumist] võtma vastu delegeeritud õigusaktid, et täpsustada III lisas sätestatud I ja II klassi tootekategooriate määratlusi.

(28) Käesolevas määruses käsitletakse küberriske sihipäraselt. Digielemente sisaldavad tooted võivad siiski põhjustada muid ohutusriske, mis ei ole seotud küberturvalisusega. Selliste riskide suhtes tuleks ka edaspidi kohaldada muid asjakohaseid tootealaseid liidu õigusakte. Kui muid liidu ühtlustamisõigusakte ei kohaldata, tuleks nende riskide suhtes kohaldada määrust [üldise tooteohutuse määrus]. Käesoleva määruse sihipärasust arvestades tuleks seega käesoleva määrusega hõlmamata riskide osas erandina määruse [üldise tooteohutuse määrus] artikli 2 lõike 1 kolmanda lõigu punktist b kohaldada digielemente sisaldavate toodete suhtes määruse [üldise tooteohutuse määrus] III peatüki 1. jaotist, V ja VII peatükki ja peatükke IX–XI, kui nende toodete suhtes ei kohaldata muude liidu ühtlustamisõigusaktidega kehtestatud erinõudeid [üldise tooteohutuse määruse artikli 3 punkti 25] tähenduses.

(29) Digielemente sisaldavad tooted, mis on vastavalt määruse[15] [tehisintellektimäärus] artiklile 6 liigitatud suure riskiga tehisintellektisüsteemiks ja mis kuuluvad käesoleva määruse kohaldamisalasse, peaksid vastama käesolevas määruses sätestatud olulistele

---

15 Määrus [tehisintellektimäärus].

nõuetele. Kui sellised suure riskiga tehisintellektisüsteemid vastavad käesolevas määruses sätestatud olulistele nõuetele, tuleks need lugeda määruse [tehisintellektimäärus] artiklis [artikkel 15] sätestatud küberturvalisuse nõuetele vastavaks, kuivõrd käesoleva määruse alusel välja antud ELi vastavusdeklaratsioon või selle osad hõlmavad neid nõudeid. Mis puudutab käesoleva määruse kohaldamisalasse kuuluva ja suure riskiga tehisintellektisüsteemiks liigitatud digielemente sisaldava toote oluliste küberturvalisuse nõuetega seotud vastavushindamismenetlusi, siis tuleks käesoleva määruse vastavate sätet asemel reeglina kohaldada määruse [tehisintellektimäärus] artikli 43 asjaomaseid sätteid. Sellise reegli tagajärjel ei tohiks siiski väheneda käesoleva määruse kohaldamisalasse kuuluvate digielemente sisaldavate kriitilise tähtsusega toodete usaldusväärsuse vajalik tase. Seepärast tuleks erandina sellest reeglist kohaldada suure riskiga tehisintellektisüsteemide suhtes, mis kuuluvad määruse [tehisintellektimäärus] kohaldamisalasse ja kvalifitseeruvad ühtlasi digielemente sisaldavateks kriitilise tähtsusega toodeteks vastavalt käesolevale määrusele ning mille suhtes kohaldatakse määruse [tehisintellektimäärus] VI lisas osutatud sisekontrollil põhinevat vastavushindamismenetlust, käesoleva määruse vastavushindamise sätteid selles osas, mis puudutab käesoleva määruse olulisi nõudeid. Sellisel juhul tuleks kõigis muudes määrusega [tehisintellektimäärus] hõlmatud aspektides kohaldada sätteid, mis käsitlevad [tehisintellektimäärus] VI lisas sätestatud sisekontrollil põhinevat vastavushindamismenetlust.

(30) Määruse [masinamääruse ettepanek] kohaldamisalasse kuuluvad masinavaldkonna tooted, mis on digielemente sisaldavad tooted käesoleva määruse tähenduses ja mille kohta on käesoleva määruse alusel välja antud vastavusdeklaratsioon, tuleks lugeda määruse [masinamääruse ettepanek] [III lisa punktides 1.1.9 ja 1.2.1] sätestatud olulistele tervisekaitse- ja ohutusnõuetele vastavaks rikkumise eest kaitsmise ning juhtimissüsteemide ohutuse ja töökindluse poolest, kui vastavust nendele nõuetele on tõendatud käesoleva määruse alusel välja antud ELi vastavusdeklaratsioonis.

(31) Käesolevas määruses sätestatud olulisi nõudeid täiendab määrus [Euroopa terviseandmeruumi määruse ettepanek]. Määruse [Euroopa terviseandmeruumi määruse ettepanek] kohaldamisalasse kuuluvad digitaalsed tervise infosüsteemid, mis on digielemente sisaldavad tooted käesoleva määruse tähenduses, peaksid seega vastama ka käesolevas määruses sätestatud olulistele nõuetele. Nende tootjad peaksid tõendama vastavust vastavalt määruses [Euroopa terviseandmeruumi määruse ettepanek] nõutule. Nõuete täitmise hõlbustamiseks võivad tootjad koostada ühe tehnilise dokumendi, mis sisaldab mõlema õigusaktiga nõutavaid elemente. Käesolev määrus ei hõlma SaaSi kui sellist ja seega ei kuulu SaaSi litsentsimis- ja tarnemudeli kaudu pakutavad digitaalsed tervise infosüsteemid käesoleva määruse kohaldamisalasse. Samuti ei kuulu käesoleva määruse kohaldamisalasse digitaalsed tervise infosüsteemid, mis on välja töötatud ja mida kasutatakse asutuse sees, sest neid ei lasta turule.

(32) Tagamaks et digielemente sisaldavad tooted on turvalised nii turule laskmise ajal kui ka kogu elutsükli jooksul, tuleb kehtestada nõrkuste käitlemise olulised nõuded ja olulised küberturvalisuse nõuded, mis puudutavad digielemente sisaldavate toodete omadusi. Tootjad peaksid täitma kõiki nõrkuste käitlemisega seotud olulisi nõudeid ja tagama, et nende tooted tarnitakse ilma teadaolevate ärakasutatavate nõrkusteta, ning samas peaksid nad kindlaks tegema, millised muud toote omadustega seotud olulised nõuded on asjaomase tooteliigi puhul asjakohased. Sel otstarbel peaksid tootjad

korraldama digielemente sisaldava tootega seotud küberriskide hindamise, et teha kindlaks asjaomased riskid ja asjaomased olulised nõuded ning kohaldada sobivaid harmoneeritud standardeid või ühtseid kirjeldusi nõuetekohaselt.

(33) Siseturule lastavate digielemente sisaldavate toodete turvalisuse parandamiseks on vaja kehtestada olulised nõuded. Need olulised nõuded ei tohiks piirata direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)][16] [artikliga X] ettenähtud kriitilise tähtsusega tarneahelate ELi koordineeritud riskihindamiste kohaldamist, milles võetakse arvesse nii tehnilisi kui ka vajaduse korral mittetehnilisi riskitegureid, näiteks tarnijate lubamatut mõjutamist kolmanda riigi poolt. Samuti ei tohiks see piirata liikmesriikide õigust kehtestada täiendavaid nõudeid, milles võetakse vastupidavuse kõrge taseme tagamiseks arvesse mittetehnilisi tegureid, kaasa arvatud neid, mis on määratletud soovituses (EL) 2019/534, kogu ELi hõlmavas 5G-võrkude turvalisuse koordineeritud riskihindamise aruandes ja direktiivis [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] osutatud võrgu- ja infoturbe koostöörühma kokkulepitud 5G-küberturvalisuse ELi meetmepaketis.

(34) Tagamaks et riikide CSIRTidele ja direktiivi [direktiiv XX/XXXX (küberturvalisuse 2. direktiiv)] artikli [artikkel X] kohaselt määratud asjaomastele ühtsetele kontaktpunktidele antakse teave, mida need vajavad oma ülesannete täitmiseks ning elutähtsate ja oluliste üksuste küberturvalisuse üldise taseme tõstmiseks, ning tagamaks et turujärelevalveasutused tegutsevad tulemuslikult, peaksid digielemente sisaldavate toodete tootjad teatama ENISA-le nõrkustest, mida aktiivselt ära kasutatakse. Digielemente sisaldavaid tooteid turustatakse enamasti kõikjal siseturul ja seega tuleks digielemente sisaldava toote iga ärakasutatavat nõrkust käsitada ohuna siseturu toimimisele. Tootjad peaksid kaaluma ka parandatud nõrkade kohtade avalikustamist direktiivi [direktiiv XX/XXXX (küberturvalisuse 2. direktiiv)] alusel loodud ja ENISA hallatavas Euroopa nõrkuste andmebaasis või muus avalikult juurdepääsetavas nõrkuste andmebaasis.

(35) Tootjad peaksid ENISA-le teatama ka kõigist intsidentidest, mis mõjutavad digielemente sisaldava toote turvalisust. Olenemata direktiiviga [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] elutähtsate ja oluliste üksuste jaoks ettenähtud intsidentidest teatamise kohustustest on ENISA, direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] artikli [artikkel X] kohaselt määratud ühtsete kontaktpunktide ja turujärelevalveasutuste jaoks ülioluline saada digielemente sisaldavate toodete tootjatelt teavet, mis võimaldaks neil hinnata selliste toodete turvalisust. Tagamaks, et kasutajad saavad nende digielemente sisaldavaid tooteid mõjutavatele 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 riskide seisukohast põhjendatud, pöörduda otse kasutajate poole.

---

[16] Euroopa Parlamendi ja nõukogu [kuupäev] direktiiv XXX,[mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv 2016/1148, (ELT L xx, kuupäev, lk x).

(36) Digielemente sisaldavate toodete tootjad peaksid kehtestama nõrkuste koordineeritud avalikustamise põhimõtted, et üksikisikutel või üksustel oleks lihtsam nõrkustest teatada. Nõrkuste koordineeritud avalikustamise põhimõtetes tuleks kirjeldada struktureeritud protsessi, mille kohaselt turvanõrkusest tootjale teatada nii, et tootja saaks sellised nõrkused diagnoosida ja kõrvaldada enne, kui üksikasjalik teave nõrkuse kohta avalikustatakse kolmandatele isikutele või avalikkusele. Arvestades et teavet laialdaselt kasutatavates digielemente sisaldavate 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 (nn puugipreemia programmid).

(37) Hõlbustamaks nõrkuste analüüsimist peaksid tootjad nimetama ja dokumenteerima digielemente sisaldavate toodete koostisosad ning koostama nn tarkvaramaterjalide loetelu. Tarkvaramaterjalide loetelu 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 riskide jälgi. Tootjate jaoks on eriti oluline tagada, et nende tooted ei sisaldaks kolmandate isikute välja töötatud kaitsetuid komponente.

(38) Et vastavust käesoleva määruse nõuetele oleks lihtsam hinnata, tuleks eeldada vastavust juhul, kui digielemente sisaldav toode on vastavuses harmoneeritud standarditega, milles pannakse käesoleva määruse olulised nõuded üksikasjalike tehniliste kirjelduste vormi ja mis on vastu võetud kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1025/2012[17]. Määrusega (EL) nr 1025/2012 on ette nähtud menetlus vastuväidete esitamiseks harmoneeritud standarditele, kui need standardid ei vasta täielikult käesoleva määruse nõuetele.

(39) Määrusega (EL) 2019/881 on kehtestatud IKT toodete, protsesside ja teenuste Euroopa küberturvalisuse sertifitseerimise vabatahtlik raamistik. Euroopa küberturvalisuse sertifitseerimise kavad võivad hõlmata käesoleva määruse kohaldamisalasse kuuluvaid digielemente sisaldavaid tooteid. Käesolev määrus peaks 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 küberturvalisuse kava alusel, mille komisjon on rakendusaktis ära märkinud, vastavad käesoleva määruse olulistele nõuetele niivõrd, kuivõrd küberturvalisuse sertifikaat või vastavusdeklaratsioon või nende osa hõlmavad neid nõudeid. Käesolevast määrusest lähtuvalt tuleks hinnata, kas digielemente sisaldavate toodete jaoks oleks vaja uut Euroopa küberturvalisuse sertifitseerimise kava. Sellistes tulevastes Euroopa küberturvalisuse sertifitseerimise kavades, mis hõlmavad digielemente sisaldavaid

---

[17] 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).

tooteid, tuleks arvesse võtta käesolevas määruses sätestatud olulisi nõudeid ja hõlbustada käesoleva määruse järgimist. Komisjonil peaks olema õigus rakendusaktidega täpsustada, milliseid Euroopa küberturvalisuse sertifitseerimise kavasid võib kasutada, et tõendada vastavust käesolevas määruses sätestatud olulistele nõuetele. Lisaks peaks komisjon tootjate põhjendamatu halduskoormuse vältimiseks, kui see on asjakohane, täpsustama, kas sellise Euroopa küberturvalisuse sertifitseerimise kava alusel välja antud küberturvalisuse sertifikaat vabastab tootja kolmanda isiku tehtava vastavushindamise kohustusest, mis on käesoleva määrusega vastavate nõuete puhul ette nähtud.

(40) Pärast seda, kui on jõustunud rakendusakt, millega nähakse ette [komisjoni XXX rakendusmäärus (EL) .../... Euroopa ühise kriteeriumidel põhineva küberturvalisuse sertifitseerimise kava kohta] (EUCC), mis puudutab käesoleva määruse kohaldamisalasse kuuluvaid riistvaratooteid, näiteks riistvara turvamooduleid ja mikroprotsessoreid, võib komisjon rakendusaktiga täpsustada, kuidas EUCC võimaldab eeldada vastavust käesoleva määruse I lisas või selle osades viidatud olulistele nõuetele. Lisaks võib sellises rakendusaktis täpsustada, kuidas EUCC alusel välja antud sertifikaat vabastab tootja kolmanda isiku tehtava vastavushindamise kohustusest, mis on vastavate nõuete puhul käesoleva määruse kohaselt nõutav.

(41) Kui harmoneeritud standardeid ei ole vastu võetud või kui harmoneeritud standardites ei käsitleta käesoleva määruse olulisi nõudeid piisavalt, peaks komisjon saama rakendusaktidega vastu võtta ühtsed kirjeldused. Põhjuseks, miks töötada harmoneeritud standarditele tuginemise asemel välja sellised ühtsed kirjeldused, võib olla standardimistaotluse tagasilükkamine mõne Euroopa standardiorganisatsiooni poolt, põhjendamatud viivitused asjakohaste harmoneeritud standardite kehtestamisel või väljatöötatud standardite ebapiisav vastavus käesoleva määruse nõuetele või mõnele komisjoni taotlusele. Et vastavust käesolevas määruses sätestatud olulistele nõuetele oleks lihtsam hinnata, tuleks eeldada vastavust juhul, kui digielemente sisaldav toode on vastavuses ühtsete kirjeldustega, mille komisjon on vastu võtnud käesoleva määruse kohaselt, et esitada nende nõuete üksikasjalikud tehnilised kirjeldused.

(42) Tootjad peaksid koostama ELi vastavusdeklaratsiooni, milles esitatakse käesoleva direktiivi kohaselt nõutav teave digielemente sisaldava toote vastavuse kohta käesoleva direktiivi olulistele nõuetele ja, kui see on asjakohane, muudele asjaomastele liidu ühtlustamisõigusaktidele, mille kohaldamisalasse 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.

(43) 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[18]. 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 käesoleva määruse nõuetele.

(44) Et ettevõtjad saaksid tõendada vastavust käesolevas määruses sätestatud olulistele 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[19] on kehtestatud vastavushindamismenetluste moodulid, arvestades kaasnevaid riske ja vajaliku turvalisuse taset. Sektoritevahelise ühtsuse tagamiseks ja ühekordsetest lahendustest hoidumiseks on vastavushindamismenetlused, mis on piisavad, et kontrollida digielemente sisaldavate toodete vastavust käesolevas määruses sätestatud olulistele nõuetele, loodud nimetatud moodulite põhjal. Vastavushindamismenetlustega tuleks uurida ja kontrollida nii toote kui ka protsessiga seotud nõudeid, mis katavad kogu digielemente sisaldava toote elutsüklit, sh toote kavandamine, projekteerimine, arendamine või tootmine, testimine ja hooldus.

(45) Üldjuhul peaks digielemente sisaldavate toodete vastavushindamise tegema tootja omal vastutusel, järgides otsuse 768/2008/EÜ moodulit A. Tootjale peaks jääma vabadus valida rangem vastavushindamismenetlus, millesse on kaasatud kolmas isik. Kui toode on klassifitseeritud I klassi kriitilise tähtsusega tooteks, on käesolevas määruses sätestatud olulistele nõuetele vastavuse tõendamiseks vaja täiendavat kindlust. Kui tootja soovib teha vastavushindamist omal vastutusel (moodul A), peaks ta kohaldama harmoneeritud standardeid, ühtseid kirjeldusi või määruse (EL) 2019/881 kohaseid küberturvalisuse sertifitseerimise kavasid, mille komisjon on rakendusaktis ära märkinud. Kui tootja selliseid harmoneeritud standardeid, ühtseid kirjeldusi või küberturvalisuse sertifitseerimise kavasid ei kohalda, peaks ta kohaldama vastavushindamist, millesse on kaasatud kolmas isik. 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 kriitilise tähtsusega toodete proportsionaalse ja tulemusliku vastavushindamismenetluse jaoks kõige sobivamaks valitud vastavalt otsuse 768/2008/EÜ moodulitel B+C või H põhinevad vastavushindamismenetlused. Tootja, kes teeb vastavushindamismenetluse koos kolmanda isikuga, võib valida menetluse, mis sobib tema projekteerimis- ja tootmisprotsessiga kõige paremini. Arvestades, et II klassi kriitilise tähtsusega toodeteks liigitatud toodete kasutamisega on seotud veelgi suurem küberrisk, peaks nende vastavushindamisse olema alati kaasatud kolmas isik.

---

[18] 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).

[19] 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).

(46) 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 käesoleva määruse olulistele nõuetele projekteerimise, arendamise ja tootmise etapis, tuleks loetletud toiminguid käsitada tootmisega samaväärse tegevusena.

(47) 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.

(48) Digielemente sisaldavate toodete vastavushindamise kvaliteedi ühtlase taseme tagamiseks on vaja kehtestada nõuded ka teavitavate ametiasutuste kohta ja muude teavitatud 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.

(49) 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.

(50) Vastavushindamisasutused kasutavad vastavushindamise mõne toimingu tegemiseks sageli alltöövõtjaid või tütarettevõtjaid. Turule lastavate digielemente sisaldavate toodete ettenähtud kaitsetaseme tagamiseks on oluline, et vastavushindamisse kaasatud alltöövõtjad ja tütarettevõtjad vastaksid vastavushindamise ülesannete täitmisel samadele nõuetele kui teavitatud asutused.

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

(52) Et teavitatud asutused võivad oma teenuseid pakkuda kogu liidus, peaksid teised liikmesriigid ja komisjon saama võimaluse esitada teavitatud 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 teavitatud asutustena.

(53) Konkurentsivõime tagamiseks on oluline, et teavitatud 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 teavitatud asutuste vahel.

(54) Liidu õigusaktide 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 Euroopa Parlamendi ja nõukogu määruses (EL) 2019/1020[20].

(55) Vastavalt määrusele (EL) 2019/1020 teevad turujärelevalveasutused turujärelevalvet oma liikmesriigi territooriumil. Käesolev määrus ei tohiks takistada liikmesriike valimast, millised pädevad asutused kõnealuseid ülesandeid täitma hakkavad. Iga liikmesriik peaks määrama ühe või mitu oma territooriumil tegutsevat turujärelevalveasutust. Liikmesriigid võivad turujärelevalveasutuseks määrata mis tahes olemasoleva või uue asutuse, kaasa arvatud direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] artiklis [artikkel X] osutatud riigi pädeva asutuse või määruse (EL) 2019/881 artiklis 58 osutatud määratud riikliku küberturvalisuse sertifitseerimise asutuse. 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 järelevalveülesannete 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.

(56) Käesoleva määruse ühetaoliseks kohaldamiseks tuleks luua spetsiaalne halduskoostöörühm vastavalt määruse (EL) 2019/1020 artikli 30 lõikele 2. See halduskoostöörühm peaks koosnema määratud turujärelevalveasutuste esindajatest ning vajaduse korral ühtsete kontaktasutuste esindajatest. Komisjon peaks toetama ja soodustama turujärelevalveasutuste vahelist koostööd määruse (EL) 2019/1020 artikliga 29 loodud liidu toodetele vastavuse võrgustikus, millesse kuuluvad iga liikmesriigi esindajad, kaasa arvatud iga määruse (EL) 2019/1020 artiklis 10 osutatud ühtse kontaktasutuse esindaja ja soovi korral riiklik ekspert, halduskoostöörühmade esimehed ning komisjoni esindajad. Komisjon peaks osalema võrgustiku, selle allrühmade ja vastava halduskoostöörühma koosolekutel. Samuti peaks ta seda halduskoostöörühma abistama tehnilist ja logistilist tuge pakkuva täitevsekretariaadi näol.

(57) Õigeaegsete, proportsionaalsete ja tulemuslike meetmete tagamiseks seoses digielemente sisaldavate toodetega, mis kujutavad endast olulist küberriski, tuleks ette

---

[20] 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).

näha 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.

(58) 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 liikmesriigi õigusest tulenevate kohustuste täitmise, [direktiivi XXX/XXXX (küberturvalisuse 2. direktiiv) I lisas] osutatud liiki elutähtsate üksuste poolt elektroonilise infosüsteemi abil osutatavate teenuste käideldavuse, 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 nõudma või turult kõrvaldama, olenevalt sellest, millise riskiga on tegu. Niipea kui turujärelevalveasutus piirab sellisel moel 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 toodete suhtes selliseid meetmeid, peaks komisjon viivitamata alustama konsultatsioone liikmesriikide ja asjaomas(t)e ettevõtja(te)ga 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 asjaomas(t)ele ettevõtja(te)le. Kui meedet peetakse põhjendatuks, võib komisjon kaaluda ka võimalust võtta vastu ettepanekud liidu vastavate õigusaktide läbivaatamiseks.

(59) 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, põhiõigustele või [direktiivi XXX/XXXX (küberturvalisuse 2. direktiiv) I lisas] osutatud liiki elutähtsate üksuste poolt osutatavatele teenustele, võib komisjon taotleda, et ENISA teeks hindamise. Selle hindamise põhjal võib komisjon võtta rakendusaktidega vastu liidu tasandi parandusmeetmeid või piiravaid meetmeid, sealhulgas nõuda turult kõrvaldamist või tagasinõudmist mõistliku aja jooksul, mis vastab riski laadile. Komisjon võib sellist sekkumist kasutada üksnes erandlike asjaolude korral, mis õigustavad viivitamatut sekkumist siseturu hea toimimise säilitamiseks, ning seda üksnes juhul, kui järelevalveasutused ei ole võtnud olukorra parandamiseks tulemuslikke meetmeid. Sellised erandlikud asjaolud võivad olla hädaolukorrad, kus näiteks tootja on nõuetele mittevastava toote mitmes liikmesriigis laialdaselt kättesaadavaks teinud, [direktiivi XXX/XXXX (küberturvalisuse 2. direktiiv)] kohaldamisalasse kuuluvad üksused kasutavad neid ka võtmetähtsusega sektorites, samas kui toodetel on teadaolevad nõrkused, mida pahatahtlikud isikud ära kasutavad ja mille parandamiseks ei paku tootja paiku. Sellistes hädaolukordades võib komisjon sekkuda ainult erandlike asjaolude kestel ja juhul, kui käesoleva määruse rikkumine või ilmnenud olulised riskid püsivad.

(60) 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.

(61) Samaaegsed koordineeritud kontrollimeetmed („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 tootekategooriad põhjustavad sageli küberriske. ENISA peaks esitama turujärelevalveasutustele ettepanekud tootekategooriate kohta, mille suhtes võiks korraldada lauskontrolle, tuginedes muu hulgas toote nõrkuste ja intsidentide kohta saadud teadetele.

(62) Tagamaks, et õigusraamistikku saab vajaduse korral kohandada, tuleks komisjonile delegeerida õigus võtta vastu õigusakte vastavalt aluslepingu artiklile 290, et ajakohastada III lisas loetletud kriitilise tähtsusega toodete loetelu ja täpsustada nende tootekategooriate määratlusi. Komisjonile tuleks delegeerida õigus võtta kooskõlas nimetatud artikliga vastu 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 õigusakte tuleks komisjonile delegeerida ka selleks, et vajaduse korral lubada sertifitseerida teatavaid digielemente sisaldavaid ülikriitilise tähtsusega tooteid, tuginedes käesolevas määruses sätestatud kriitilise tähtsuse kriteeriumidele, ning selleks, et täpsustada 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[21] sätestatud põhimõtetega. Eelkõige selleks, et tagada võrdne osalemine delegeeritud õigusaktide ettevalmistamises, 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.

(63) Selleks et tagada käesoleva määruse rakendamise ühetaolised tingimused, tuleks komisjonile anda rakendamisvolitused, et: täpsustada tarkvaramaterjalide loetelu vorm ja elemendid, veelgi täpsustada, milline peab olema tootja poolt aktiivselt ärakasutatavate nõrkuste ja intsidentide kohta ENISA-le esitatavas teates sisalduva teabe liik, vorming ja teatamise kord, täpsustada Euroopa küberturvalisuse sertifitseerimise kavad, mis on vastu võetud määruse (EL) 2019/881 kohaselt ja mida saab kasutada, et tõendada vastavust käesoleva määruse I lisas sätestatud olulistele nõuetele või nende osadele, võtta vastu ühiseid kirjeldusi I lisas sätestatud oluliste nõuete kohta, kehtestada piktogrammide või digielemente sisaldavate toodete turvalisusega seotud muude märgiste tehnilisi kirjeldusi ja nende kasutamist

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

edendavaid mehhanisme, otsustada erandlike asjaolude korral, mis õigustavad viivitamatut sekkumist siseturu hea toimimise jätkumiseks, liidu tasandi parandusmeetmete või piiravate meetmete üle. Neid volitusi tuleks teostada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011[22].

(64) 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.

(65) Et tagada käesolevas määruses sätestatud kohustuste tõhus täitmine, peaks igal turujärelevalveasutusel olema õigus määrata haldustrahve või taotleda nende määramist. Seepärast tuleks kehtestada käesolevas määruses sätestatud kohustuste täitmata jätmise eest siseriiklikus 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 teised 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.

(66) 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.

(67) Oma suhetes kolmandate riikidega püüab EL 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 riigi puhul. Lepingud on sõlmitud mitmes konkreetses valdkonnas, mis võivad riigiti erineda. Mõistes, et digielemente sisaldavate toodete tarneahelad on ülemaailmsed, võib liit

[22] 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).

sõlmida käesoleva määrusega reguleeritud toodete puhul vastavushindamist käsitlevaid vastastikuse tunnustamise lepinguid vastavalt ELi toimimise lepingu artiklile 218, et kaubavahetust veelgi hõlbustada. Et tugevdada kübervastupidavust kogu maailmas, on oluline ka koostöö partnerriikidega, sest pikas perspektiivis aitab see tugevdada küberturvalisuse raamistikku nii ELis kui ka väljaspool seda.

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

(69) Ettevõtjatele tuleks anda piisavalt aega käesoleva määruse nõuetega kohanemiseks. Käesolevat määrust tuleks hakata kohaldama [24 kuu jooksul] alates selle jõustumisest, välja arvatud aktiivselt ärakasutatavaid nõrkusi ja intsidente käsitlevate aruandluskohustuste osas, mida tuleks hakata kohaldama [12 kuu jooksul] alates käesoleva määruse jõustumisest.

(70) Liikmesriigid ei suuda käesoleva määruse eesmärki piisavalt saavutada, küll aga saab neid meetme ulatuse tõttu paremini saavutada liidu tasandil, ja seega võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Nimetatud artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärgi saavutamiseks vajalikust kaugemale.

(71) Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725[23] artikli 42 lõikele 1 on konsulteeritud Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse [...],

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese

Käesoleva määrusega nähakse ette:

(a) õigusnormid, mis reguleerivad digielemente sisaldavate toodete turule laskmist, et tagada selliste toodete küberturvalisus;

[23] 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).

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

(c) selliste protsesside olulised nõuded, mille tootjad on kehtestanud nõrkuste käitlemiseks, et tagada digielemente sisaldavate toodete küberturvalisus kogu toote elutsükli vältel, ning ettevõtjate kohustused seoses nende protsessidega;

(d) õigusnormide turujärelevalve ja eespool nimetatud õigusnormide ja nõuete täitmise tagamise kohta.

Artikkel 2

Kohaldamisala

1. Käesolevat määrust kohaldatakse digielemente sisaldavate toodete suhtes, mille kavandatud või mõistlikult prognoositav kasutamine hõlmab otsest või kaudset loogilist või füüsilist andmeühendust mõne seadme või võrguga.

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

   (a) selline piiramine või välistamine on kooskõlas nende toodete suhtes kohaldatava üldise reguleeriva raamistikuga ning

   (b) valdkondlike normidega saavutatakse samasugune kaitsetase kui käesoleva määrusega.

   Komisjonil on õigus võtta vastu delegeeritud õigusakte vastavalt artiklile 50, et muuta käesolevat määrust ning täpsustada, olenevalt asjaoludest, kas selline piiramine või välistamine on vajalik, milliseid tooteid ja õigusnorme see puudutab ja milline on piirangu ulatus.

5. Käesolevat määrust ei kohaldata digielemente sisaldavate toodete suhtes, mis on välja töötatud üksnes riikliku julgeoleku või sõjalisel otstarbel, või toodete suhtes, mis on spetsiaalselt projekteeritud salastatud teabe töötlemiseks.

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

(1) „digielemente sisaldav toode“ – tarkvaraline või riistvaraline toode ja selle kaugandmetöötluslahendused, kaasa arvatud tarkvara- ja riistvarakomponendid, mis lastakse turule eraldi;

(2) „kaugandmetöötlus“ – igasugune 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) „digielemente sisaldav kriitilise tähtsusega toode“ – digielemente sisaldav toode, mis kujutab endast küberriski vastavalt artikli 6 lõikes 2 sätestatud kriteeriumidele ja mille põhifunktsioon on sätestatud III lisas;

(4) „digielemente sisaldav ülikriitilise tähtsusega toode“ – digielemente sisaldav toode, mis kujutab endast küberriski vastavalt artikli 6 lõikes 5 sätestatud kriteeriumidele;

(5) „käidutehnoloogia“ – programmeeritavad digisüsteemid või -seadmed, mis suhtlevad füüsilise keskkonnaga või juhivad seadmeid, mis suhtlevad füüsilise keskkonnaga;

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

(7) „riistvara“ – füüsiline elektrooniline infosüsteem või selle osad, mis suudavad digitaalseid andmeid töödelda, talletada või edastada;

(8) „komponent“ – tarkvara või riistvara, mis on mõeldud elektroonilise infosüsteemi koostisosaks;

(9) „elektrooniline infosüsteem“ – mis tahes süsteem, sealhulgas elektri- või elektroonikaseade, mis suudab digitaalseid andmeid töödelda, talletada või edastada;

(10) „loogiline ühendus“ – tarkvaraliidese kaudu rakendatud andmeühenduse virtuaalne esitus;

(11) „füüsiline ühendus“ – elektrooniliste infosüsteemide või komponentide vaheline ühendus, mis realiseeritakse füüsiliste vahenditega, muu hulgas elektrilise või mehaanilise liidese, traadi või raadiolainete kaudu;

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

(13) „privileeg“ – pääsuõigus, mis antakse konkreetsele kasutajale või programmile turvalisusega seotud toimingute tegemiseks elektroonilises infosüsteemis;

(14) „kõrgendatud privileeg“ – konkreetsele kasutajale või programmile antud pääsuõigus turvalisusega seotud laiendatud toimingute kogumi tegemiseks elektroonilises infosüsteemis, mis võib väärkasutuse või rikkumise korral võimaldada kuritahtlikul isikul saada laialdasema juurdepääsu süsteemi või organisatsiooni ressurssidele;

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

(16) „võrgu- või andmetöötlusressursid“ – andme-, riistvara- või tarkvarafunktsioonid, mis on juurdepääsetavad kas kohapeal või võrgu või muu ühendatud seadme kaudu;

(17) „ettevõtja“ – tootja, volitatud esindaja, importija, turustaja või muu füüsiline või juriidiline isik, kelle suhtes kohaldatakse käesolevas määruses sätestatud kohustusi;

(18) „tootja“ – füüsiline või juriidiline isik, kes arendab või valmistab digielemente sisaldavaid tooteid või kes laseb digielemente sisaldavaid tooteid projekteerida, arendada või toota ja turustab neid tasu eest või tasuta oma nime või kaubamärgi all;

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

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

(21) „turustaja“ – tarneahelas osalev füüsiline või juriidiline isik, välja arvatud tootja või importija, kes teeb digielemente sisaldava toote liidu turul kättesaadavaks ilma selle omadusi mõjutamata;

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

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

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

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

(26) „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;

(27) „teavitav asutus“ – riigi ametiasutus, kes vastutab vastavushindamisasutuste hindamise, määramise ja neist teavitamise ning nende seire jaoks vajalike menetluste väljatöötamise ja läbiviimise eest;

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

(29) „vastavushindamisasutus“ – määruse (EL) nr 765/2008 artikli 2 punktis 13 määratletud asutus;

(30) „teavitatud asutus“ – käesoleva määruse artikli 33 ja liidu muude asjaomaste ühtlustamisõigusaktide kohaselt määratud vastavushindamisasutus;

(31) „oluline muudatus“ – digielemente sisaldavas tootes pärast selle turule laskmist tehtud muudatus, mis mõjutab digielemente sisaldava toote vastavust I lisa punktis 1 sätestatud olulistele nõuetele või mille tulemusena muutub kavandatud kasutamine, mida silmas pidades on digielemente sisaldavat toodet hinnatud;

(32) „CE-vastavusmärgis“ – märgis, millega tootja annab teada, et digielemente sisaldav toode ja tootja kehtestatud protsessid vastavad I lisas ja muudes kohaldatavates toodete turustamise tingimusi ühtlustavates liidu õigusaktides („liidu ühtlustamisõigusaktid“) sätestatud märgise paigaldamist käsitlevatele nõuetele;

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

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

(35) „küberrisk“ – direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] artiklis [artikkel X] määratletud risk;

(36) „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 katkestusi;

(37) „tarkvaramaterjalide loetelu“ – ametlik kirje, milles esitatakse digielemente sisaldava toote tarkvaraelementides sisalduvate komponentide üksikasjad ja tarneahela seosed;

(38) „nõrkus“ – direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] artiklis [artikkel X] määratletud nõrkus;

(39) „aktiivselt ärakasutatav nõrkus“ – nõrkus, mille kohta on usaldusväärseid tõendeid, et keegi on süsteemi omaniku loata käivitanud süsteemis ründekoodi;

(40) „isikuandmed“ – määruse (EL) 2016/679 artikli 4 punktis 1 määratletud andmed.

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 tutvustamist ega kasutamist messidel, näitustel ja esitlustel või muudel samalaadsetel üritustel.

3. Liikmesriigid ei takista käesolevale määrusele mittevastava poolelioleva tarkvara kättesaadavaks tegemist tingimusel, et selline tarkvara tehakse kättesaadavaks üksnes piiratud aja jooksul, mis on vajalik testimiseks, ning et nähtaval sildil on selgelt märgitud, et see tarkvara ei vasta käesolevale määrusele ja see ei ole turul kättesaadav muul eesmärgil kui testimiseks.

Artikkel 5

Digielemente sisaldavate toodete suhtes kehtivad nõuded

Digielemente sisaldavad tooted tehakse turul kättesaadavaks üksnes juhul, kui:

(1) need vastavad I lisa punktis 1 sätestatud olulistele nõuetele, tingimusel et nad on nõuetekohaselt paigaldatud, hooldatud, neid kasutatakse sihtotstarbeliselt või tingimustes, mida võib mõistlikult prognoosida, ja neid ajakohastatakse, kui see on asjakohane, ning

(2) tootja kehtestatud protsessid vastavad I lisa punktis 2 sätestatud olulistele nõuetele.

Artikkel 6

Digielemente sisaldavad kriitilise tähtsusega tooted

1. III lisas loetletud kategooriasse kuuluvaid digielemente sisaldavaid tooteid peetakse digielemente sisaldavateks kriitilise tähtsusega toodeteks. Sellesse kategooriasse kuuluvaks peetakse tooteid, millel on mõne III lisas loetletud kategooria põhifunktsioon. Digielemente sisaldavad kriitilise tähtsusega tooted jagatakse I ja II klassi vastavalt III lisale, lähtudes nende toodetega seotud küberriski tasemest.

2. Komisjonil on õigus võtta kooskõlas artikliga 50 vastu delegeeritud õigusakte, et muuta III lisa ja lisada digielemente sisaldavate kriitilise tähtsusega toodete kategooriate loetellu uusi kategooriaid või kustutada sellest loetelust olemasolevaid kategooriaid. III lisa muutmise vajadust hinnates võtab komisjon arvesse digielemente sisaldavate toodete kategooriaga seotud küberriskide taset. Küberriski taseme kindlaksmääramisel võetakse arvesse üht või mitut järgmist kriteeriumi:

   (a) digielemente sisaldava toote küberturvalisusega seotud funktsioonid ja see, kas digielemente sisaldaval tootel on vähemalt üks järgmistest omadustest:

      (i) see on projekteeritud tööks kõrgendatud privileegidega või privileegide haldamiseks;

      (ii) sellel on otsejuurdepääs või eelisjuurdepääs võrgu- või andmetöötlusressurssidele;

      (iii) see on projekteeritud kontrollima juurdepääsu andmetele või käidutehnoloogiale;

      (iv) see täidab usalduse seisukohast kriitilise tähtsusega funktsiooni, esmajoones turbefunktsioone nagu võrgu juhtimine, lõppseadmete turve ja võrgu kaitsmine;

(b) kavandatud kasutamine tundlikus keskkonnas, sh tööstuskeskkonnas, või direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv) lisas [I lisa] osutatud liiki elutähtsate üksuste poolt:

(c) kavandatud kasutamine kriitilise tähtsusega või tundlike funktsioonide jaoks, näiteks isikuandmete töötlemiseks;

(d) negatiivse mõju võimalik ulatus, eeskätt intensiivsus ja võime mõjutada paljusid isikuid;

(e) see, kui suures ulatuses on digielemente sisaldav toode juba põhjustanud varalist või mittevaralist kahju või katkestusi või tekitanud tõsist muret seoses kahjuliku mõju realiseerumisega.

3. Komisjonil on õigus võtta kooskõlas artikliga 50 vastu delegeeritud õigusakt, et täiendada käesolevat määrust ja täpsustada III lisas sätestatud I ja II klassi tootekategooriate määratlusi. Delegeeritud õigusakt võetakse vastu [12 kuu jooksul alates käesoleva määruse jõustumisest].

4. Digielemente sisaldavate kriitilise tähtsusega toodete suhtes kohaldatakse artikli 24 lõigetes 2 ja 3 osutatud vastavushindamismenetlusi.

5. Komisjonil on õigus võtta kooskõlas artikliga 50 vastu delegeeritud õigusakte, et täiendada käesolevat määrust ja täpsustada digielemente sisaldavate ülikriitilise tähtsusega toodete kategooriaid, mille jaoks peavad tootjad saama Euroopa küberturvalisuse sertifitseerimise kava kohase Euroopa küberturvalisuse sertifikaadi vastavalt määrusele (EL) 2019/881, et tõendada vastavust I lisas või selle osades sätestatud olulistele nõuetele. Digielemente sisaldavate ülikriitilise tähtsusega toodete selliste kategooriate kindlaksmääramisel võtab komisjon arvesse digielemente sisaldavate toodete kategooriaga seotud küberriskide taset, pidades silmas üht või mitut lõikes 2 loetletud kriteeriumi ja arvestades hinnangut sellele, kas:

(a) direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv) lisas [I lisa] osutatud liiki elutähtsad üksused kasutavad selle kategooria tooteid või sõltuvad nendest või kas need tooted võivad tulevikus olla potentsiaalselt olulised selliste üksuste tegevuse jaoks; või

(b) kas selle kategooria tooted on olulised digielemente sisaldavate toodete üldise tarneahela vastupidavuse jaoks katkestuste korral.

Artikkel 7

Üldine tooteohutus

Erandina määruse [üldise tooteohutuse määrus] artikli 2 lõike 1 kolmanda lõigu punktist b, kui digielemente sisaldavate toodete suhtes ei kohaldata muudes liidu ühtlustamisõigusaktides sätestatud erinõudeid [üldise tooteohutuse määruse artikli 3 punkti 25] tähenduses, kohaldatakse nende toodete suhtes määruse [üldise tooteohutuse määrus] III peatüki 1. jagu, V ja VII peatükki ning IX–XI peatükki seoses ohutusriskidega, mida käesolev määrus ei hõlma.

Artikkel 8

Suure riskiga tehisintellektisüsteemid

1. Määruse [tehisintellektimäärus] artikli [artikli 6] kohaselt suure riskiga tehisintellektisüsteemideks liigitatud digielemente sisaldavaid tooteid, mis kuuluvad käesoleva määruse kohaldamisalasse ja vastavad käesoleva määruse I lisa 1. jaos sätestatud olulistele nõuetele ning mille puhul tootja rakendatud protsessid vastavad I lisa 2. jaos sätestatud olulistele nõuetele, loetakse vastavaks määruse [tehisintellektimäärus] artiklis [artikkel 15] sätestatud küberturvalisuse nõuetele, ilma et see piiraks muid kõnealuses artiklis sätestatud täpsuse ja usaldusväärsusega seotud nõudeid, ning niivõrd, kuivõrd nende nõuetega nõutava kaitsetaseme saavutamist tõendab käesoleva määruse alusel välja antud ELi vastavusdeklaratsioon.

2. Lõikes 1 osutatud toodete ja küberturvalisuse nõuete suhtes kohaldatakse asjakohast vastavushindamismenetlust määruse [tehisintellektimäärus] artikli 43 kohaselt. Teavitatud asutustel, kellel on õigus kontrollida suure riskiga tehisintellektisüsteemide vastavust määrusele [tehisintellektimäärus], on sellise hindamise käigus ühtlasi õigus kontrollida, kas käesoleva määruse kohaldamisalasse kuuluvad suure riskiga tehisintellektisüsteemid vastavad käesoleva määruse I lisa nõuetele, tingimusel et nende teavitatud asutuste vastavust käesoleva määruse artikli 29 nõuetele on hinnatud määruse [tehisintellektimäärus] kohase teavitamise korra raames.

3. Erandina lõikest 2 kohaldatakse käesoleva määruse III lisas loetletud digielemente sisaldavate kriitilise tähtsusega toodete suhtes (millele tuleb teha käesoleva määruse artikli 24 lõike 2 punktides a ja b ning artikli 24 lõike 3 punktides a ja b osutatud vastavushindamismenetlused ning mis on ühtlasi liigitatud suure riskiga tehisintellektisüsteemideks vastavalt määruse [tehisintellektimäärus] artiklile [artikkel 6] ja mille suhtes kohaldatakse määruse [tehisintellektimäärus] lisas [VI lisa] osutatud sisekontrollil põhinevat vastavushindamismenetlust) käesoleva määrusega nõutavaid vastavushindamismenetlusi, kui tegemist on käesoleva määruse oluliste nõuetega.

Artikkel 9

Masinavaldkonna tooted

Määruse [masinamääruse ettepanek] kohaldamisalasse kuuluvad masinavaldkonna tooted, mis on käesoleva määruse tähenduses digielemente sisaldavad tooted ja mille kohta on käesoleva määruse alusel välja antud ELi vastavusdeklaratsioon, loetakse määruse [masinamääruse ettepanek] lisas [III lisa punktid 1.1.9 ja 1.2.1] sätestatud olulistele tervisekaitse- ja ohutusnõuetele vastavaks rikkumise eest kaitsmise ning juhtimissüsteemide ohutuse ja töökindluse poolest, kui nendele nõuetele vastava kaitsetaseme saavutamist on tõendatud käesoleva määruse alusel välja antud ELi vastavusdeklaratsioonis.

II PEATÜKK

ETTEVÕTJATE KOHUSTUSED

Artikkel 10

Tootjate kohustused

1. Tootjad tagavad digielemente sisaldava toote turulelaskmisel, et see on projekteeritud, arendatud ja toodetud vastavalt I lisa 1. jaos sätestatud olulistele nõuetele.

2. Lõikes 1 sätestatud kohustuse täitmiseks hindavad tootjad digielemente sisaldava tootega seotud küberriske ja võtavad selle hindamise tulemusi arvesse digielemente sisaldava toote kavandamis-, projekteerimis-, arendus-, tootmis-, tarne- ja hooldusetapis, et minimeerida küberriske, ennetada turvaintsidente ja minimeerida selliste intsidentide mõju, sealhulgas seoses kasutajate tervise ja ohutusega.

3. Digielemente sisaldava toote turulelaskmisel lisab tootja artikli 23 ja V lisa kohasesse tehnilisse dokumentatsiooni küberriskihindamise. Artiklis 8 ja artikli 24 lõikes 4 osutatud digielemente sisaldavate toodete puhul, mille suhtes kohaldatakse ka muid liidu õigusakte, võib küberriskihindamine olla osa nende liidu õigusaktidega nõutavast riskihindamisest. Kui turustatava digielemente sisaldava toote suhtes ei kohaldata teatavaid olulisi nõudeid, lisab tootja kõnealusesse dokumentatsiooni selge põhjenduse.

4. Lõikes 1 sätestatud kohustuse täitmiseks peavad tootjad täitma hoolsuskohustust kolmandatelt isikutelt hangitud komponentide integreerimisel digielemente sisaldavatesse toodetesse. Nad kohustuvad tagama, et sellised komponendid ei ohusta digielemente sisaldava toote turvalisust.

5. Tootja dokumenteerib süstemaatiliselt ja küberriskide olemusega proportsionaalsel viisil, digielemente sisaldava toote asjakohaseid küberturvalisuse aspekte, sealhulgas ilmnenud nõrkusi ja kolmandatelt isikutelt saadud asjakohast teavet, ning ajakohastab vajaduse korral toote riskihindamist.

6. Digielemente sisaldava toote turulelaskmisel ja toote eeldatava kasutusea jooksul või viie aasta jooksul pärast toote turule laskmist, olenevalt sellest, kumb on lühem, tagavad tootjad, et kõnealuse toote nõrkust käsitletakse tulemuslikult ja kooskõlas I lisa punktis 2 sätestatud oluliste nõuetega.

   Tootjal peavad olema asjakohane poliitika ja menetlused, sealhulgas I lisa 2. jao punktis 5 osutatud nõrkuste koordineeritud avalikustamise poliitika, et käsitleda ja parandada digielemente sisaldava toote võimalikke sisemiste või väliste allikate teatatud nõrkusi.

7. Enne digielemente sisaldava toote turule laskmist koostab tootja artiklis 23 osutatud tehnilise dokumentatsiooni.

   Tootja teeb või laseb teha artiklis 24 osutatud vajalikud vastavushindamised.

Kui vastavushindamisel tõendatakse, et digielemente sisaldav toode vastab I lisa 1. jaos sätestatud olulistele nõuetele ja tootja rakendatud protsessid vastavad I lisa 2. jaos sätestatud olulistele nõuetele, siis koostab tootja artikli 20 kohase ELi vastavusdeklaratsiooni ja kinnitab tootele artikli 22 kohaselt CE-vastavusmärgise.

8. Tootja hoiab tehnilist dokumentatsiooni ja vajaduse korral ELi vastavusdeklaratsiooni turujärelevalveasutustele esitamiseks alles kümme aastat alates digielemente sisaldava toote turule laskmisest.

9. Tootja tagab, et on kehtestatud kord, mille kohaselt seeriatoodanguna toodetavad digielemente sisaldavad tooted jäävad ka edaspidi nõuetele vastavaks. Tootja võtab nõuetekohaselt arvesse muudatusi tootearenduses ja tootmisprotsessis või digielemente sisaldava toote konstruktsioonis või omadustes ning muudatusi harmoneeritud standardites, Euroopa küberturvalisuse sertifitseerimise kavades või artiklis 19 osutatud ühtses kirjelduses, mille alusel digielemente sisaldava toote vastavust deklareeritakse või kontrollitakse.

10. Tootja peab tagama, et digielemente sisaldava tootega on kaasas II lisas sätestatud teave ja juhised elektroonilisel või füüsilisel kujul. Teave ja juhised peavad olema kasutajatele kergesti arusaadavas keeles. Nii juhised kui ka teave peavad olema selged, arusaadavad, loogilised ja loetavad. Need peavad võimaldama digielemente sisaldavate toodete turvalist paigaldamist, käitamist ja kasutamist.

11. Tootja annab digielemente sisaldava tootega kaasa ELi vastavusdeklaratsiooni või lisab II lisas sätestatud juhistesse ja teabesse veebiaadressi, kus on ELi vastavusdeklaratsioon.

12. Alates digielemente sisaldava toote turule laskmisest ja toote eeldatava kasutusea jooksul või viie aasta jooksul pärast turule laskmist, olenevalt sellest, kumb on lühem, võtavad tootjad, kes teavad või kellel on põhjust uskuda, et digielemente sisaldav toode või tootja rakendatud protsessid ei vasta I lisas sätestatud olulistele nõuetele, viivitamata parandusmeetmed, mis on vajalikud, et viia digielemente sisaldav toode või tootja protsessid nõuetega vastavusse või toode vajadusel turult kõrvaldada või tagasi nõuda.

13. 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 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.

14. Tootja, kes lõpetab tegevuse ja ei ole seetõttu võimeline täitma käesolevas määruses sätestatud kohustusi, teatab enne tegevuse lõpetamise jõustumist sellest olukorrast asjaomastele turujärelevalveasutustele ning kättesaadavate vahendite ja võimaluste piires ka turule lastud digielemente sisaldavate toodete kasutajatele.

15. Komisjon võib rakendusaktidega täpsustada I lisa 2. jao punktis 1 sätestatud tarkvaramaterjalide loetelu vormi ja elemente. Kõnealuste rakendusaktide vastuvõtmisel järgitakse artikli 51 lõikes 2 osutatud kontrollimenetlust.

Artikkel 11

Tootjate aruandekohustused

1. Tootja teatab ENISA-le põhjendamatu viivituseta ja igal juhul 24 tunni jooksul pärast sellest teada saamist kõigist digielemente sisaldava toote aktiivselt ärakasutatavatest nõrkustest. Teade peab sisaldama üksikasju kõnealuse nõrkuse ja vajaduse korral võetud parandus- või leevendusmeetmete kohta. Pärast teate kättesaamist edastab ENISA selle asjaomase liikmesriigi CSIRTile, kes on vastavalt direktiivi [direktiiv XXX/XXXX (NIS2)] artiklile [artikkel X] määratud nõrkuste koordineeritud avalikustamiseks, ja teavitab turujärelevalveasutust teatatud nõrkusest põhjendamatu viivituseta, välja arvatud küberriskidega seotud põhjendatud juhtudel.

2. Tootja teavitab ENISAt põhjendamatu viivituseta ja igal juhul 24 tunni jooksul pärast teadasaamist kõigist intsidentidest, mis mõjutavad digielemente sisaldava toote turvalisust. ENISA edastab teated direktiivi [direktiiv XXX/XXXX (NIS2)] artikli [artikkel X] kohaselt määratud ühtsele kontaktpunktile asjaomastes liikmesriikides ning teavitab teatatud intsidentidest turujärelevalveasutust põhjendamatu viivituseta, välja arvatud küberriskidega seotud põhjendatud juhtudel. Teade intsidendist sisaldab teavet intsidendi raskusastme ja mõju kohta ning vajaduse korral märget selle kohta, kas tootja kahtlustab, et intsidendi põhjustas ebaseaduslik või kuritahtlik tegevus, või leiab, et sellel on piiriülene mõju.

3. ENISA esitab direktiivi [direktiiv XXX/XXXX (NIS2)] artikliga [artikkel X] loodud Euroopa küberkriisi kontaktasutuste võrgustikule (EU-CyCLONe) lõigete 1 ja 2 kohaselt teatatud teabe, kui selline teave on asjakohane suuremahuliste küberintsidentide ja kriiside kooskõlastatud juhtimiseks operatiivtasandil.

4. Tootja teavitab digielemente sisaldava toote kasutajaid põhjendamatu viivituseta ja pärast teadasaamist intsidendist ja vajaduse korral parandusmeetmetest, mida kasutaja saab intsidendi mõju leevendamiseks võtta.

5. Komisjon võib rakendusaktide vastuvõtmisega täpsustada lõigete 1 ja 2 kohaselt esitatavate teadete teabe liiki, vormingut ning esitamise korda. Kõnealuste rakendusaktide vastuvõtmisel järgitakse artikli 51 lõikes 2 osutatud kontrollimenetlust.

6. ENISA koostab lõigete 1 ja 2 kohaselt saadud teadete põhjal iga kahe aasta tagant tehnilise aruande digielemente sisaldavate toodete küberriskidega seotud uute suundumuste kohta ja esitab selle direktiivi [direktiiv XXX/XXXX (NIS2)] artiklis [artikkel X] osutatud koostöörühmale. Esimene selline aruanne esitatakse 24 kuu jooksul pärast lõigetes 1 ja 2 sätestatud kohustuste kohaldamise algust.

7. Digielemente sisaldavasse tootesse integreeritud komponendi, sealhulgas avatud lähtekoodiga komponendi nõrkuse avastamisel teatavad tootjad sellest komponenti hooldavale isikule või üksusele.

Artikkel 12

Volitatud esindajad

1. Tootja võib kirjaliku volituse alusel määrata volitatud esindaja.

2. Artikli 10 lõikest 1 kuni lõike 7 esimese taandeni ja lõikes 9 sätestatud kohustused ei kuulu volitatud esindaja ülesannete hulka.

3. Volitatud esindaja täidab ülesandeid tootjalt saadud volituste piires. Volitus võimaldab volitatud esindajal teha vähemalt järgmist:

   (a) hoida artiklis 20 osutatud ELi vastavusdeklaratsiooni ja artiklis 23 osutatud tehnilist dokumentatsiooni turujärelevalveasutustele esitamiseks alles kümme aastat alates digielemente sisaldava toote turule laskmisest;

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

   (c) kui turujärelevalveasutused seda taotlevad, teha nendega koostööd mis tahes meetme korral, mis on võetud sellisest digielemente sisaldavast tootest tulenevate riskide kõrvaldamiseks, mida volitatud esindaja volitused hõlmavad.

Artikkel 13

Importijate kohustused

1. Importijad lasevad turule üksnes selliseid digielemente sisaldavaid tooteid, mis vastavad I lisa 1. jaos sätestatud olulistele nõuetele ja mille tootja rakendatud protsessid vastavad I lisa 2. jaos sätestatud olulistele nõuetele.

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

   (a) tootja on läbi viinud artiklis 24 osutatud asjakohased vastavushindamismenetlused;

   (b) tootja on koostanud tehnilise dokumentatsiooni.

   (c) digielemente sisaldav toode kannab artiklis 22 osutatud CE-vastavusmärgist ning sellega on kaasas II lisas sätestatud teave ja juhised.

3. Kui importija arvab või tal on põhjust uskuda, et digielemente sisaldav toode või tootja rakendatud protsessid ei vasta I lisas sätestatud olulistele nõuetele, ei lase importija toodet turule enne, kui see toode või tootja rakendatud protsessid on viidud vastavusse I lisas sätestatud oluliste nõuetega. Lisaks teavitab importija tootjat ja turujärelevalveasutusi, kui digielemente sisaldav toode kujutab endast olulist küberriski.

4. Importija märgib oma nime, registreeritud kaubanime või registreeritud kaubamärgi, postiaadressi ja meiliaadressi digielemente sisaldavale tootele või, kui see ei ole võimalik, digielemente sisaldava toote pakendile või tootega kaasasolevasse dokumenti. Kontaktandmed esitatakse lõppkasutajale ja turujärelevalveasutustele kergesti arusaadavas keeles.

5. Importija tagab, et digielemente sisaldava tootega on kaasas II lisas sätestatud juhised ja teave kasutajatele kergesti arusaadavas keeles.

6. Importija, kes arvab või kellel on põhjust uskuda, et tema poolt turule lastud digielemente sisaldav toode või tootja rakendatud protsessid ei vasta I lisas sätestatud olulistele nõuetele, võtavad kõnealuse digielemente sisaldava toote või tootja rakendatud protsesside I lisas sätestatud oluliste nõuetega vastavusse viimiseks viivitamata vajalikke parandusmeetmeid, vajaduse korral kõrvaldavad selle turult või nõuavad tagasi.

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

7. Importija hoiab ELi vastavusdeklaratsiooni koopiat turujärelevalveasutustele esitamiseks alles kümme aastat alates digielemente sisaldava toote turule laskmisest ja tagab, et tehniline dokumentatsioon on kõnealustele asutustele taotluse alusel kättesaadav.

8. Turujärelevalveasutuse põhjendatud taotluse korral esitavad importijad kõnealusele asutusele sellele kergesti arusaadavas keeles kas paberil või elektrooniliselt kogu teabe ja dokumentatsiooni, mida on vaja digielemente sisaldava toote I lisa 1. jaos sätestatud olulistele nõuetele vastavuse tõendamiseks, ning tootja rakendatud protsesside I lisa 2. jaos sätestatud olulistele nõuetele vastavuse tõendamiseks. 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.

9. Kui digielemente sisaldava toote importija saab teada, et selle toote tootja lõpetas 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 14

Turustajate kohustused

1. Digielemente sisaldavat toodet turul kättesaadavaks tehes peab turustaja vajaliku hoolikusega järgima käesoleva määruse nõudeid.

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

   (a) digielemente sisaldaval tootel on CE-vastavusmärgis;

   (b) tootja on täitnud artikli 10 lõigetes 10 ja 11 ning importija artikli 13 lõikes 4 esitatud kohustused.

3. Turustaja, kes arvab või kellel on põhjust uskuda, et digielemente sisaldav toode või tootja rakendatud protsessid ei vasta I lisas sätestatud olulistele nõuetele, ei tee digielemente sisaldavat toodet turul kättesaadavaks enne, kui see toode või tootja

rakendatud protsessid on viidud vastavusse. Kui digielemente sisaldav toode kujutab endast olulist küberriski, teatab turustaja sellest tootjale ja turujärelevalveasutustele.

4. Turustaja, kes arvab või kellel on põhjust uskuda, et tema poolt turul kättesaadavaks tehtud digielemente sisaldav toode või tootja rakendatud protsessid ei vasta I lisas sätestatud olulistele nõuetele, veendub, et kõnealuse digielemente sisaldava toote või tootja rakendatud protsesside vastavusse viimiseks vajalikud parandusmeetmed on võetud, või kõrvaldab toote vajaduse korral turult või nõuab tagasi.

   Digielemente sisaldava toote nõrkuse tuvastamisel teavitavad turustajad 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 mittevastavuse ja võetud parandusmeetmete kohta.

5. Turujärelevalveasutuse põhjendatud taotluse korral esitab turustaja kõnealusele asutusele sellele kergesti arusaadavas keeles kas paberil või elektrooniliselt kogu teabe ja dokumentatsiooni, mida on vaja digielemente sisaldava toote ja tootja rakendatud protsesside I lisas sätestatud olulistele nõuetele vastavuse tõendamiseks. Kui kõnealune asutus seda taotleb, teevad nad sellega koostööd kõigi meetmete korral, mis on võetud nende poolt turul kättesaadavaks tehtud digielemente sisaldavast tootest tulenevate küberriskide kõrvaldamiseks.

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

Artikkel 15

Juhtumid, millal 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, siis loetakse käesoleva määruse kohaldamisel seda importijat või tarnijat tootjaks ja tema suhtes kehtivad artikli 10 ning artikli 11 lõigete 1, 2, 4 ja 7 kohased tootja kohustused.

Artikkel 16

Muud juhtumid, millal kohaldatakse tootjate kohustusi

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

Selle isiku suhtes kohaldatakse artiklis 10 ning artikli 11 lõigetes 1, 2, 4 ja 7 sätestatud tootja kohustusi toote selles osas, mida on oluliselt muudetud, või, juhul kui oluline muudatus mõjutab digielemente sisaldava toote kui terviku küberturvalisust, kogu toote ulatuses.

Artikkel 17

Ettevõtjate identifitseerimine

1. Ettevõtjad esitavad turujärelevalveasutustele taotluse alusel ja kui teave on kättesaadav, 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;

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

III PEATÜKK

DIGIELEMENTE SISALDAVATE TOODETE VASTAVUS

Artikkel 18

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 oluliste nõuetega, mida nimetatud standardid või nende osad käsitlevad ja mis on sätestatud I lisas.

2. Eeldatakse, et digielemente sisaldavad tooted ja tootja rakendatud protsessid, mis vastavad artiklis 19 osutatud ühtsele kirjeldusele, on vastavuses I lisas sätestatud oluliste nõuetega niivõrd, kuivõrd nimetatud ühtne kirjeldus hõlmab neid nõudeid.

3. Digielemente sisaldavad tooted ja tootja rakendatud protsessidega, mille kohta on määruse (EL) 2019/881 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava alusel välja antud ELi vastavusdeklaratsioon või sertifikaat, nagu nähakse ette lõikes 4, eeldatakse olevat vastavuses I lisas sätestatud oluliste nõuetega, kui ELi vastavusdeklaratsioon või küberturvalisuse sertifikaat või nende osad hõlmavad neid nõudeid.

4. Komisjonil on õigus kehtestada rakendusaktidega määruse (EL) 2019/881 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavad, millega saab tõendada vastavust I lisas sätestatud olulistele nõuetele või nende osadele. Lisaks täpsustab komisjon vajaduse korral, kas selliste kavade alusel välja antud küberturvalisuse sertifikaat vabastab tootja kolmanda isiku tehtava vastavushindamise kohustusest kõnealuste nõuete osas, nagu on sätestatud artikli 24 lõike 2 punktides a ja b ning lõike 3 punktides a ja b. Kõnealuste rakendusaktide vastuvõtmisel järgitakse artikli 51 lõikes 2 osutatud kontrollimenetlust.

Artikkel 19

Ühtne kirjeldus

Kui artiklis 18 osutatud harmoneeritud standardeid ei ole või kui komisjon leiab, et asjaomased harmoneeritud standardid ei ole piisavad käesoleva määruse nõuete või komisjoni standardimistaotluse täitmiseks, või kui standardimismenetluses esineb põhjendamatuid viivitusi või kui Euroopa standardiorganisatsioonid ei ole komisjoni harmoneeritud standardite koostamise taotlust vastu võtnud, on komisjonil õigus võtta rakendusaktidega vastu ühtne kirjeldus I lisas sätestatud oluliste nõuete kohta. Kõnealuste rakendusaktide vastuvõtmisel järgitakse artikli 51 lõikes 2 osutatud kontrollimenetlust.

Artikkel 20

ELi vastavusdeklaratsioon

1. Tootja koostab artikli 10 lõike 7 kohaselt ELi vastavusdeklaratsiooni, milles tuleb kinnitada, et I lisas sätestatud olulised nõuded on täidetud.

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

3. Kui digielemente sisaldava toote suhtes kohaldatakse rohkem kui ühte liidu õigusakti, millega nõutakse ELi vastavusdeklaratsiooni, siis koostatakse kõigi nende liidu õigusaktide kohta ühine ELi vastavusdeklaratsioon. Kõnealuses deklaratsioonis näidatakse ära asjakohased 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 50 vastu delegeeritud õigusakte, millega täiendatakse käesolevat määrust, lisades IV lisas sätestatud ELi vastavusdeklaratsioonis minimaalselt esitatavate andmete loetellu elemente, et võtta arvesse tehnika arengut.

Artikkel 21

CE-vastavusmärgise üldpõhimõtted

Artikli 3 lõikes 32 määratletud CE-vastavusmärgise suhtes kohaldatakse määruse (EÜ) nr 765/2008 artiklis 30 sätestatud üldpõhimõtteid.

Artikkel 22

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 20 osutatud ELi vastavusdeklaratsioonile. Tarkvaraliste digielemente sisaldavate toodete puhul pannakse CE-vastavusmärgis kas artiklis 20 osutatud ELi vastavusdeklaratsioonile või tarkvaratoote juurde kuuluvale veebisaidile.

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 pakendil märgisele järgneda piktogramm või muu märgis, mis osutab erilisele riskile või kasutusviisile, millele on osutatud lõike 6 kohastes rakendusaktides.

4. CE-vastavusmärgisele järgneb teavitatud asutuse identifitseerimisnumber, kui kõnealune asutus on kaasatud artiklis 24 osutatud täielikul kvaliteedi tagamisel põhinevasse (mooduli H põhisesse) vastavushindamismenetlusse.

   Teavitatud 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 õigusakte, mis näevad samuti ette CE-vastavusmärgise kinnitamist, näitab CE-vastavusmärgis, et tooted vastavad ka nende muude õigusaktide nõuetele.

6. Komisjon võib rakendusaktidega kehtestada tehnilised nõuded piktogrammidele või muudele märgistele, mis on seotud digielemente sisaldavate toodete turvalisusega, ja mehhanismid nende kasutuse edendamiseks. Kõnealuste rakendusaktide vastuvõtmisel järgitakse artikli 51 lõikes 2 osutatud kontrollimenetlust.

Artikkel 23

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 nõuetele. Dokumentatsioon peab sisaldama vähemalt V lisas esitatud elemente.

2. Tehniline dokumentatsioon koostatakse enne digielemente sisaldava toote turule laskmist ja seda ajakohastatakse vajaduse korral pidevalt toote eeldatava kasutusea vältel või viie aasta vältel pärast digielemente sisaldava toote turule laskmist, olenevalt sellest, kumb on lühem.

3. Artiklis 8 ja artikli 24 lõikes 4 osutatud digielemente sisaldavate toodete puhul, mille suhtes kohaldatakse ka muid liidu õigusakte, koostatakse üksainus tehniline

dokumentatsioon, mis sisaldab käesoleva määruse V lisas osutatud teavet ja kõnealuste liidu õigusaktidega nõutavat teavet.

4. Vastavushindamismenetlusega seotud tehniline dokumentatsioon ja kirjavahetus koostatakse selle liikmesriigi ametlikus keeles, kus teavitatud asutus on registreeritud, või mõnes muus asutusele vastuvõetavas keeles.

5. Komisjonil on õigus võtta kooskõlas artikliga 50 vastu delegeeritud õigusakte, et täiendada käesolevat määrust elementidega, mis lisatakse V lisas sätestatud tehnilisse dokumentatsiooni, et võtta arvesse tehnika arengut ja käesoleva määruse rakendamisprotsessis toimunut.

Artikkel 24

Digielemente sisaldavate toodete vastavushinamismenetlused

1. Selleks et teha kindlaks digielemente sisaldava toote ja tootja rakendatud protsesside vastavus I lisa olulistele nõuetele, teeb tootja selle vastavushindamise. Tootja või tema volitatud esindaja tõendab vastavust olulistele nõuetele ühega järgmistest menetlustest.

   (a) VI lisas sätestatud (mooduli A põhine) sisekontrollimenetlus või

   (b) VI lisas sätestatud (mooduli B põhine) ELi tüübihindamismenetlus, millele järgneb VI lisas sätestatud tootmise sisekontrollil põhinev (mooduli C põhine) ELi tüübile vastavuse hindamine; või

   (c) VI lisas sätestatud täielikul kvaliteedi tagamisel põhinev vastavushindamine (moodul H).

2. Kui tootja või tema volitatud esindaja hindab III lisa kohaselt I klassi kuuluva digielemente sisaldava kriitilise tähtsusega toote ja tootja rakendatud protsesside vastavust I lisas sätestatud olulistele nõuetele ning ta ei ole või on ainult osaliselt kohaldanud harmoneeritud standardeid, ühtset kirjeldust või Euroopa küberturvalisuse sertifitseerimise kavasid vastavalt artiklile 18 või kui sellised harmoneeritud standardid, ühtne kirjeldus või Euroopa küberturvalisuse sertifitseerimise kavad puuduvad, siis kohaldatakse asjaomase digielemente sisaldava toote ja tootja rakendatud protsesside suhtes üht järgmistest menetlustest seoses nende oluliste nõuetega:

   (a) VI lisas sätestatud (mooduli B põhine) ELi tüübihindamismenetlus, millele järgneb VI lisas sätestatud tootmise sisekontrollil põhinev (mooduli C põhine) ELi tüübile vastavuse hindamine; või

   (b) VI lisas sätestatud täielikul kvaliteedi tagamisel põhinev vastavushindamine (moodul H).

3. Kui toode on III lisa kohaselt II klassi kuuluv digielemente sisaldav kriitilise tähtsusega toode, tõendab tootja või tema volitatud esindaja vastavust I lisas sätestatud olulistele nõuetele, kasutades ühte järgmistest menetlustest:

(a) VI lisas sätestatud (mooduli B põhine) ELi tüübihindamismenetlus, millele järgneb VI lisas sätestatud tootmise sisekontrollil põhinev (mooduli C põhine) ELi tüübile vastavuse hindamine; või

(b) VI lisas sätestatud täielikul kvaliteedi tagamisel põhinev vastavushindamine (moodul H).

4. Määruse [Euroopa terviseandmeruumi määrus] kohaldamisalasse kuuluvate ja digitaalseteks tervise infosüsteemideks liigitatud digielemente sisaldavate toodete tootjad peavad tõendama vastavust käesoleva määruse I lisas sätestatud olulistele nõuetele, kasutades asjakohast vastavushindamismenetlust, nagu on nõutud määruses [Euroopa terviseandmeruumi määruse III peatükk].

5. Vastavushindamismenetluste tasude kehtestamisel võtavad teavitatud asutused arvesse VKEde konkreetseid huve ja vajadusi ning vähendavad tasusid proportsionaalselt nende huvide ja vajadustega.

IV PEATÜKK

VASTAVUSHINDAMISASUTUSTEST TEATAMINE

Artikkel 25

Teatamine

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

Artikkel 26

Teavitavad asutused

1. Liikmesriigid määravad teavitava asutuse, kes vastutab vastavushindamisasutuste hindamiseks ja nendest teatamiseks ning teavitatud asutuste järelevalveks vajalike menetluste kasutuselevõtmise ja rakendamise eest, sealhulgas artikli 31 järgimise eest.

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

Artikkel 27

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 28

Teavitavate asutuste kohta teatamise kohustus

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

2. Komisjon teeb selle teabe avalikkusele kättesaadavaks.

Artikkel 29

Nõuded teavitatud asutuste kohta

1. Teavitamise eesmärgil peab vastavushindamisasutus vastama lõigete 2–12 nõuetele.

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

3. Vastavushindamisasutus peab olema kolmandast isikust asutus, mis on sõltumatu organisatsioonist või 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 selliseks asutuseks pidada tingimusel, et on tõendatud selle sõltumatus ja mis tahes huvide konflikti puudumine.

4. Vastavushindamisasutus, selle kõrgem juhtkond ja vastavushindamisülesannete täitmise eest vastutavad töötajad ei tohi olla hinnatava digielemente sisaldava toote projekteerija, arendaja, tootja, tarnija, 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 toodete projekteerimise, arendamise, tootmise, turustamise, 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 teavitatud. 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 tema otsustele või vastavushindamise tulemustele, eriti isikute või isikute rühmade poolt, kes on huvitatud nimetatud toimingute tulemustest.

6. Vastavushindamisasutus peab olema võimeline tegema kõiki VI lisas nimetatud vastavushindamistoiminguid, millega seoses on temast teavitatud, 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 teavitatud, alati olema:

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

(b) menetluste kirjeldused, mille kohaselt vastavushindamist tehakse ning mis tagavad läbipaistvuse ja võimaluse neid menetlusi korrata; asjakohased tegevuspõhimõtted ja kord vahe tegemiseks teavitatud 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 vastavushindamistoimingutega seotud tehniliste ja haldusülesannete täitmiseks asjakohasel viisil, samuti vajalik varustus või ruumid.

7. Vastavushindamisülesannete täitmise eest vastutavad töötajad peavad:

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

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

(c) oluliste nõuete, kohaldatavate harmoneeritud standardite ning liidu ühtlustamisõigusaktide ja nende rakendusaktide asjakohaste sätete tundmine ja mõistmine;

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

8. Tagatakse vastavushindamisasutuste, nende juhtkonna ja hindamistöötajate erapooletus.

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

9. Kui vastutus ei kuulu siseriikliku 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 VI lisa või selle rakendamiseks kehtestatud siseriikliku 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 või tagab, et tema hindamise eest vastutavaid töötajaid on teavitatud asjakohastest standardiseerimistegevustest ja artikli 40 alusel loodud teavitatud asutuste koordineerimisrühma tegevusest ning kohaldab nimetatud rühma töö tulemusel koostatud haldusotsuseid ja -dokumente üldiste suunistena.

12. Vastavushindamisasutus tegutseb vastavalt sidusatele, õiglastele ja mõistlikele tingimustele, võttes tasude puhul arvesse eelkõige VKEde huve.

Artikkel 30

Vastavuse eeldamine teavitatud 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 29 nõuetele, kui kohaldatavad harmoneeritud standardid hõlmavad neid nõudeid.

Artikkel 31

Teavitatud asutuste tütarettevõtjad ja alltöövõtjad

1. Kui teavitatud asutus kasutab vastavushindamisega seotud ülesannete täitmiseks alltöövõtjat või tütarettevõtjat, siis tagab ta, et alltöövõtja või tütarettevõtja vastab artiklis 29 sätestatud nõuetele, ning teatab sellest teavitavale asutusele.

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

3. Alltöövõtjat või tütarettevõtjat võib kasutada ainult tootja nõusolekul.

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

Artikkel 32

Teatamise taotlus

1. Vastavushindamisasutus esitab teatamise taotluse oma asukohaks oleva liikmesriigi teavitavale asutusele.

2. Taotlusega koos esitatakse vastavushindamistoimingute, vastavushindamismenetluste ja toote või toodete tüübi kirjeldus, millega tegelemist asutus oma pädevusena taotleb, ning riikliku akrediteerimisasutuse väljastatud akrediteerimistunnistus (kui see on olemas), mis tõendab, et vastavushindamisasutus vastab artikli 29 nõuetele.

3. Kui vastavushindamisasutus ei saa akrediteerimistunnistust esitada, siis esitab ta teavitavale asutusele kõik dokumentaalsed tõendid, mida on vaja, et kontrollida, kinnitada ja regulaarselt jälgida tema vastavust artiklis 29 esitatud nõuetele.

Artikkel 33

Teatamise kord

1. Teavitav asutus teatab ainult nendest vastavushindamisasutustest, mis vastavad artiklis 29 esitatud nõuetele.

2. Teavitav asutus teavitab komisjoni ja liikmesriike teavitatud ja määratud organisatsioonide uue teabesüsteemi (NANDO) kaudu, mille on välja töötanud ja mida haldab komisjon.

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

4. Kui teade ei põhine artikli 32 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 29 nõuetele.

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

Ainult sellist asutust peetakse käesoleva määruse kohaldamisel teavitatud asutuseks.

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

Artikkel 34

Teavitatud asutuste identifitseerimisnumbrid ja loetelud

1. Komisjon määrab teavitatud asutusele identifitseerimisnumbri.

Ta määrab üheainsa identifitseerimisnumbri, isegi kui asutust teavitatakse liidu mitme õigusakti alusel.

2. Komisjon teeb üldsusele kättesaadavaks käesoleva määruse alusel teavitatud asutuste loetelu, mis sisaldab asutustele antud identifitseerimisnumbreid ja teavitatud vastavushindamistoiminguid.

Komisjon tagab loetelu ajakohastamise.

Artikkel 35

Teavituse muudatused

1. Kui teavitav asutus on kindlaks teinud või talle on teatatud, et teavitatud asutus ei vasta enam artikli 29 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 teavitatud asutus on lõpetanud tegevuse, siis on teavitava liikmesriigi ülesanne tagada, et selle asutuse dokumente menetleb mõni teine teavitatud asutus või et need oleksid taotluse korral kättesaadavad teavitamise ja turujärelevalve eest vastutavatele asutustele.

Artikkel 36

Teavitatud asutuse pädevuse vaidlustamine

1. Komisjon uurib iga juhtumit, mil tal tekib kahtlus või tema tähelepanu juhitakse kahtlusele, et teavitatud asutus ei ole pädev või ei täida enam talle esitatud nõudeid ega talle pandud kohustusi.

2. Komisjoni taotluse korral esitab teavitav liikmesriik talle kogu teabe selle kohta, mille alusel konkreetsele asutusele teavitus võimaldati 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 teavitatud asutus ei täida või enam ei täida teavitamise aluseks olevaid nõudeid, teavitab ta sellest teavitavat liikmesriiki ja nõuab temalt vajalike parandusmeetmete võtmist, sealhulgas vajaduse korral teavituse tühistamist.

Artikkel 37

Teavitatud asutuse tegevuskohustused

1. Teavitatud asutus teeb vastavushindamist kooskõlas artiklis 24 ja VI lisas esitatud vastavushindamismenetlustega.

2. Vastavushindamisi tehakse proportsionaalsel viisil, vältides ettevõtjate liigset koormamist. Vastavushindamisasutus võtab oma tegevuse käigus asjakohaselt arvesse ettevõtja suurust, tegevusvaldkonda, struktuuri, käsitletava tootetehnoloogia keerukusastet ning seda, kas tegemist on mass- või seeriatootmisega.

3. Seejuures arvestab teavitatud asutus, millist rangust ja kaitset on vaja, et toode vastaks käesoleva määruse nõuetele.

4. Kui teavitatud asutus leiab, et tootja ei ole kinni pidanud I lisas või vastavates harmoneeritud standardites või artikli 19 kohases ühtses kirjelduses sätestatud nõuetest, nõuab ta kõnealuselt tootjalt nõuetekohaste parandusmeetmete võtmist ja ei väljasta vastavussertifikaati.

5. Kui pärast sertifikaadi väljastamist avastab teavitatud asutus nõuetele vastavuse jälgimisel, et toode ei vasta enam käesoleva määruse nõuetele, nõuab ta tootjalt asjakohaste parandusmeetmete võtmist ja vajaduse korral peatab või tühistab sertifikaadi.

6. Kui parandusmeetmeid ei võeta või neil ei ole soovitud tulemust, siis teavitatud asutus vastavalt vajadusele kas kitsendab asjaomast sertifikaati või peatab või tühistab selle.

Artikkel 38

Teavitatud asutuse teatamiskohustus

1. Teavitatud asutus annab teavitavale asutusele teada järgmisest:

   (a) kõik juhtumid, kui sertifikaat jäetakse andmata, seda kitsendatakse, see peatatakse või tühistatakse;

   (b) teavitamise valdkonda ja tingimusi mõjutavad asjaolud;

   (c) kõik turujärelevalveasutustelt saadud teabetaotlused vastavushindamistoimingute kohta;

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

2. Teavitatud asutused esitavad teistele käesoleva määruse alusel teavitatud samalaadsete vastavushindamistoimingute ja samade toodetega tegelevatele asutustele asjakohase teabe negatiivsete ja taotluse korral ka positiivsete vastavushindamistulemuste kohta.

Artikkel 39

Kogemuste vahetamine

Komisjon korraldab kogemuste vahetamist liikmesriikides teavituspoliitika eest vastutavate ametiasutuste vahel.

Artikkel 40

Teavitatud asutuste tegevuse koordineerimine

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

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

V PEATÜKK

TURUJÄRELEVALVE JA TÄITMISE TAGAMINE

Artikkel 41

Digielemente sisaldavate toodete turujärelevalve ja kontroll liidu turul

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

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

3. Vajaduse korral teevad turujärelevalveasutused koostööd määruse (EL) 2019/881 artikli 58 kohaselt määratud riiklike küberturvalisuse sertifitseerimise asutustega ja vahetavad korrapäraselt teavet. Käesoleva määruse artikli 11 kohaste aruandekohustuste täitmise järelevalvel teevad määratud turujärelevalveasutused koostööd ENISAga.

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

5. 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 käesoleva artikli lõike 8 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.

6. Liikmesriigid tagavad, et määratud turujärelevalveasutustel on käesolevast määrusest tulenevate ülesannete täitmiseks piisavad rahalised ja inimressursid.

7. Komisjon hõlbustab määratud turujärelevalveasutuste vahelist kogemuste vahetamist.

8. Turujärelevalveasutused võivad komisjoni toetusel anda ettevõtjatele suuniseid ja nõu käesoleva määruse rakendamise kohta.

9. 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.

10. Käesoleva määruse kohaldamisalasse kuuluvate digielemente sisaldavate toodete puhul, mis on määruse [tehisintellektimäärus] artikli [artikkel 6] kohaselt liigitatud suure riskiga tehisintellektisüsteemideks, on määruse [tehisintellektimäärus] kohaselt määratud turujärelevalveasutused need asutused, kes vastutavad käesoleva määrusega nõutava turujärelevalve eest. Määruse [tehisintellektimäärus] kohaselt määratud turujärelevalveasutused teevad vajaduse korral koostööd käesoleva määruse kohaselt määratud turujärelevalveasutustega ning, mis puutub artikli 11 kohaste aruandluskohustuste täitmise järelevalvesse, ENISAga. Määruse [tehisintellektimäärus] kohaselt määratud turujärelevalveasutused teavitavad käesoleva määruse kohaselt määratud turujärelevalveasutusi eelkõige järeldustest, mis on asjakohased nende käesoleva määruse rakendamisega seotud ülesannete täitmiseks.

11. Käesoleva määruse ühetaoliseks kohaldamiseks luuakse spetsiaalne halduskoostöörühm (ADCO rühm) vastavalt määruse (EL) 2019/1020 artikli 30 lõikele 2. See halduskoostöörühm koosneb määratud turujärelevalveasutuste esindajatest ning vajaduse korral ühtsete kontaktasutuste esindajatest.

Artikkel 42

Juurdepääs andmetele ja dokumentatsioonile

Kui see on vajalik, et hinnata digielemente sisaldavate toodete ja tootjate rakendatud protsesside vastavust I lisas sätestatud olulistele nõuetele, antakse turujärelevalveasutustele

põhjendatud taotluse korral juurdepääs andmetele, mida on vaja selliste toodete projekteerimise, arendamise, tootmise ja nõrkuste käsitlemise hindamiseks, sealhulgas asjaomase ettevõtja sisedokumentidele.

Artikkel 43

Olulist küberriski põhjustava digielemente sisaldava toote riikliku tasandi menetlus

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

   Kui turujärelevalveasutus leiab hindamisel, et digielemente sisaldav toode ei vasta käesoleva määruse nõuetele, siis nõuab ta viivitamata, et asjaomane ettevõtja kas võtaks kõik vajalikud parandusmeetmed toote vastavusse viimiseks nende nõuetega või kõrvaldaks toote turult või nõuaks selle tagasi mõistliku aja jooksul, mis vastab riski laadile.

   Turujärelevalveasutus teatab sellest asjakohasele teavitatud asutusele. Asjakohaste parandusmeetmete suhtes kehtib määruse (EL) nr 2019/1020 artikkel 18.

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

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

4. Kui digielemente sisaldava toote tootja 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 nõuda.

   Turujärelevalveasutus teatab nendest meetmetest viivitamata komisjonile ja teistele liikmesriikidele.

5. Lõike 4 teises lõigus osutatud teave hõlmab kõiki kättesaadavaid andmeid: eelkõige nõuetele mittevastava digielemente sisaldava toote identifitseerimisandmed, 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) toode või tootja rakendatud protsessid ei vasta I lisas sätestatud olulistele nõuetele;

   (b) puudused artiklis 18 osutatud harmoneeritud standardites, küberturvalisuse sertifitseerimise kavades või ühtses kirjelduses.

6. 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 toote mittevastavusega seotud teabest ning kui nad ei ole teadaantud riigisisese meetmega nõus, siis ka oma vastuväidetest.

7. Kui teised liikmesriigid või komisjon ei ole kolme kuu jooksul alates lõikes 4 osutatud teabe kättesaamisest esitanud vastuväiteid liikmesriigi võetud ajutise meetme kohta, loetakse see meede põhjendatuks. See ei piira asjaomase ettevõtja määruse (EL) 2019/1020 artikli 18 kohaseid menetlusõigusi.

8. Kõigi liikmesriikide turujärelevalveasutused tagavad, et asjaomase toote suhtes võetakse viivitamata asjakohased piiravad meetmed, näiteks kõrvaldatakse toode liikmesriigi turult.

Artikkel 44

Liidu kaitsemeetmete menetlus

1. Kui kolme kuu jooksul alates artikli 43 lõikes 4 osutatud teate kättesaamisest esitab mõni liikmesriik teise liikmesriigi võetud meetmele vastuväiteid või kui komisjon arvab, et meede on liidu õigusaktidega 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 43 lõikes 4 osutatud teate saamisest, kas riiklik meede on põhjendatud või mitte, ning teatab oma 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 liikmesriigi meedet peetakse põhjendamatuks, siis liikmesriik tühistab selle meetme.

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 10 ettenähtud menetlust.

4. Kui riiklik meede loetakse põhjendatuks ja digielemente sisaldava toote mittevastavus loetakse tulenevat puudustest artiklis 18 osutatud Euroopa küberturvalisuse sertifitseerimise kavas, kaalub komisjon, kas muuta artikli 18 lõikes 4 osutatud rakendusakti, 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 19 osutatud ühtses kirjelduses, kaalub komisjon, kas muuta kõnealust ühtset kirjeldust käsitlevat artiklis 19 osutatud rakendusakti või tunnistada see kehtetuks.

Artikkel 45

Olulist küberriski põhjustava digielemente sisaldava toote ELi tasandi menetlus

1. Kui komisjonil on piisavalt alust arvata, muu hulgas ENISA-lt saadud teabe põhjal, et olulise küberriskiga digielemente sisaldav toode ei vasta käesolevas määruses sätestatud nõuetele, võib ta nõuda, et asjaomased turujärelevalveasutused hindaksid nõuetele vastavust ja järgiksid artiklis 43 osutatud menetlusi.

2. Erandlikel asjaoludel, mis õigustavad viivitamatut sekkumist siseturu hea toimimise jätkumiseks, ning kui komisjonil on piisavalt alust arvata, et lõikes 1 osutatud toode ei vasta endiselt käesoleva määruse nõuetele ja asjaomased turujärelevalveasutused ei ole võtnud tulemuslikke meetmeid, võib komisjon paluda ENISA-lt vastavushindamist. Komisjon teavitab sellest asjaomaseid turujärelevalveasutusi. Asjaomased ettevõtjad teevad ENISAga vajalikul viisil koostööd.

3. ENISA hinnangu põhjal võib komisjon otsustada, et liidu tasandil on vaja võtta parandusmeede või piirav meede. Komisjon konsulteerib viivitamata asjaomaste liikmesriikidega ja asjaomas(t)e ettevõtja(te)ga.

4. Lõikes 3 osutatud konsulteerimise põhjal võib komisjon võtta vastu rakendusakte, et teha otsus liidu tasandi parandusmeetmete või piiravate meetmete kohta, sealhulgas nõuda turult kõrvaldamist või tagasinõudmist mõistliku aja jooksul, mis vastab riski laadile. Kõnealuste rakendusaktide vastuvõtmisel järgitakse artikli 51 lõikes 2 osutatud kontrollimenetlust.

5. Komisjon teavitab lõikes 4 osutatud otsusest viivitamata asjaomast ettevõtjat või asjaomaseid ettevõtjaid. Liikmesriigid rakendavad lõikes 4 osutatud õigusakte viivitamata ja teatavad sellest komisjonile.

6. Lõikeid 2–5 kohaldatakse komisjoni sekkumist õigustanud erakorralise olukorra ajal ja seni, kuni asjaomast toodet ei ole viidud vastavusse käesoleva määrusega.

Artikkel 46

Nõuetele vastavad digielemente sisaldavad tooted, mis kujutavad endast olulist küberriski

1. Kui liikmesriigi turujärelevalveasutus leiab pärast artikli 43 kohast hindamist, et kuigi digielemente sisaldav toode ja tootja rakendatud protsessid on kooskõlas käesoleva määrusega, kujutavad need endast olulist küberriski ning ühtlasi riski inimeste tervisele või ohutusele, liidu või siseriiklikust põhiõiguste kaitseks mõeldud õigusest tulenevate kohustuste täitmisele, [direktiivi XXX/XXXX (NIS2) I lisas] osutatud liiki elutähtsate üksuste poolt elektroonilise infosüsteemi kaudu pakutavate teenuste käideldavusele, autentsusele, terviklusele või konfidentsiaalsusele või muudele avaliku huvi kaitse aspektidele, siis nõuab ta, et asjaomane ettevõtja võtaks kõik asjakohased meetmed, et digielemente sisaldav toode ja asjaomase tootja rakendatud protsessid ei kujutaks turule laskmisel endast enam riski, kõrvaldaks digielemente sisaldava toote turult või nõuaks selle tagasi mõistliku aja jooksul, mis vastab riski laadile.

2. Tootja või muud asjaomased ettevõtjad tagavad, et parandusmeetmed 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 lõike 1 kohaselt võetud meetmetest. Kõnealune teave hõlmab kõiki kasutadaolevaid andmeid: eelkõige kõnealuse digielemente sisaldava toote identifitseerimiseks vajalikud andmed, digielemente sisaldava toote päritolu ja tarneahel, kaasneva riski laad ning liikmesriigis võetud meetmete laad ja kestus.

4. Komisjon algatab viivitamata konsulteerimise liikmesriikidega ja asjaomas(t)e ettevõtja(te)ga 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 oma otsuse liikmesriikidele.

6. Kui komisjonil on piisavalt alust arvata, muu hulgas ENISA-lt saadud teabe põhjal, et digielemente sisaldava tootega, mis küll vastab käesoleva määruse nõuetele, kaasnevad lõikes 1 osutatud riskid, võib ta paluda asjaomas(t)el turujärelevalveasutus(t)elt vastavushindamist ja järgida artiklis 43 ning käesoleva artikli lõigetes 1, 2 ja 3 osutatud menetlusi.

7. Erandlikel asjaoludel, mis õigustavad viivitamatut sekkumist siseturu hea toimimise jätkumiseks ja kui komisjonil on piisavalt alust arvata, et lõikes 6 osutatud toode kujutab endast jätkuvalt lõikes 1 osutatud riski ja asjaomased riiklikud turujärelevalveasutused ei ole võtnud tulemuslikke meetmeid, võib komisjon paluda ENISA-l hinnata kõnealusest tootest tulenevaid riske ja teavitab sellest asjaomaseid turujärelevalveasutusi. Asjaomased ettevõtjad teevad ENISAga vajalikul viisil koostööd.

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

9. Lõikes 8 osutatud konsulteerimise põhjal võib komisjon võtta vastu rakendusakte, et teha otsus liidu tasandi parandusmeetmete või piiravate meetmete kohta, sealhulgas nõuda turult kõrvaldamist või tagasinõudmist mõistliku aja jooksul, mis vastab riski laadile. Kõnealuste rakendusaktide vastuvõtmisel järgitakse artikli 51 lõikes 2 osutatud kontrollimenetlust.

10. Komisjon teavitab lõikes 9 osutatud otsusest viivitamata asjaomast ettevõtjat või asjaomaseid ettevõtjaid. Liikmesriigid rakendavad neid akte viivitamata ja teatavad sellest komisjonile.

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

Artikkel 47

Vormiline mittevastavus

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

(a) vastavusmärgise kinnitamisel ei ole järgitud artiklite 21 ja 22 nõudeid;

(b) vastavusmärgist ei ole kinnitatud;

(c) ELi vastavusdeklaratsiooni ei ole koostatud;

(d) ELi vastavusdeklaratsioon ei ole koostatud nõuetekohaselt;

(e) vastavushindamises osaleva teavitatud asutuse identifitseerimisnumbrit ei ole kinnitatud, kui see on asjakohane.

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

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

Artikkel 48

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 toodetega, millega sageli kaasnevad küberriskid.

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

3. Turujärelevalveasutused ja vajaduse korral 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 meetmete võtmisel saadud teavet kasutada.

5. Turujärelevalveasutus ja vajaduse korral komisjon teevad ühismeetmete kokkuleppe, sealhulgas selle osaliste nimed, üldsusele kättesaadavaks.

Artikkel 49

Lauskontrollid

1. Turujärelevalveasutused võivad otsustada võtta teatavate digielemente sisaldavate toodete või nende kategooriate suhtes samaaegseid koordineeritud kontrollimeetmeid (teha lauskontrolle), et kontrollida nende vastavust käesolevale määrusele, või avastada määruse rikkumisi.

2. Kui asjaomased turujärelevalveasutused ei ole kokku leppinud teisiti, koordineerib lauskontrolle komisjon. Lauskontrolli koordinaator võib vajaduse korral teha koondtulemused üldsusele kättesaadavaks.

3. ENISA võib oma ülesannete täitmisel, sealhulgas artikli 11 lõigete 1 ja 2 kohaselt saadud teadete põhjal, kindlaks määrata tootekategooriad, mille puhul võib korraldada lauskontrolle. Lauskontrolli ettepanek esitatakse lõikes 2 osutatud koordinaatorile arutamiseks turujärelevalveasutustele.

4. Lauskontrolle tehes võivad turujärelevalveasutused kasutada artiklites 41–47 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 50

Delegeeritud volituste rakendamine

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

2. Komisjonile antakse artikli 2 lõikes 4, artikli 6 lõikes 2, artikli 6 lõikes 3, artikli 6 lõikes 5, artikli 20 lõikes 5 ja artikli 23 lõikes 5 osutatud volitused võtta vastu delegeeritud õigusakte.

3. Euroopa Parlament ja nõukogu võivad artikli 2 lõikes 4, artikli 6 lõikes 2, artikli 6 lõikes 3, artikli 6 lõikes 5, artikli 20 lõikes 5 ja artikli 23 lõikes 5 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse selles otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta nende delegeeritud õigusaktide kehtivust, mis on juba jõustunud.

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

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

6. Artikli 2 lõike 4, artikli 6 lõike 2, artikli 6 lõike 3, artikli 6 lõike 5, artikli 20 lõike 5 ja artikli 23 lõike 5 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kahe kuu jooksul pärast õigusakti Euroopa Parlamendile ja nõukogule teatavaks tegemist esitanud selle kohta 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 51

Komiteemenetlus

1. Komisjoni abistab komitee. See 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 52

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 2016/943[24] 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.

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 asutus, kust teave pärineb.

---

[24] 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).

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

4. Komisjon ja liikmesriigid võivad tundlikku teavet vahetada nende kolmandate riikide asutustega, kellega nad on konfidentsiaalsuse kohta sõlminud kahe- või mitmepoolse kokkuleppe, mis tagab piisava kaitsetaseme.

Artikkel 53

Karistused

1. Liikmesriigid kehtestavad õigusnormid käesoleva määruse sätete rikkumise eest ettevõtjate suhtes kohaldatavate karistuste kohta ning võtavad kõik vajalikud meetmed nende täitmise tagamiseks. Kehtestatavad karistused peavad olema tulemuslikud, proportsionaalsed ja hoiatavad.

2. Liikmesriigid teavitavad komisjoni viivitamata nimetatud normidest ja meetmetest ning kõikidest nende hilisematest muudatustest.

3. Kui toode ei vasta I lisa sätestatud olulistele küberturvalisuse nõuetele, ning artiklites 10 ja 11 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.

4. Käesolevas määruses sätestatud muude 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.

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

6. Kui otsustatakse igal konkreetsel juhul kohaldatava haldustrahvi suuruse üle, võetakse arvesse iga konkreetse olukorra kõiki asjaomaseid asjaolusid ning pööratakse asjakohast tähelepanu järgmisele:

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

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

   (c) rikkumise toime pannud ettevõtja suurus ja turuosa.

7. Haldustrahve kohaldavad turujärelevalveasutused jagavad seda teavet teiste liikmesriikide turujärelevalveasutustega määruse (EL) 2019/1020 artiklis 34 osutatud info- ja teavitussüsteemi kaudu.

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

9. 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.

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

VIII PEATÜKK

ÜLEMINEKU- JA LÕPPSÄTTED

Artikkel 54

Määruse (EL) 2019/1020 muutmine

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

„71. [Määrus XXX][küberkerksuse õigusakt]“.

Artikkel 55

Üleminekusätted

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

2. Digielemente sisaldavate toodete suhtes, mis on turule lastud enne [artiklis 57 osutatud käesoleva määruse kohaldamise alguskuupäev], kohaldatakse käesoleva määruse nõudeid üksnes juhul, kui alates nimetatud kuupäevast on nende toodete projekti või sihtotstarvet oluliselt muudetud.

3. Erandina lõikest 2 kohaldatakse artiklis 11 sätestatud kohustusi kõigi käesoleva määruse kohaldamisalasse kuuluvate digielemente sisaldavate toodete suhtes, mis on turule lastud enne [artiklis 57 osutatud käesoleva määruse kohaldamise alguskuupäev].

Artikkel 56

Hindamine ja läbivaatamine

Hiljemalt [36 kuud alates käesoleva määruse kohaldamise kuupäevast] ja seejärel iga nelja aasta tagant esitab komisjon Euroopa Parlamendile ja nõukogule aruande käesoleva määruse hindamise ja läbivaatamise kohta. Aruanded avalikustatakse.

Artikkel 57

Jõustumine ja kohaldamine

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

Käesolevat määrust kohaldatakse alates [24 kuud alates käesoleva määruse jõustumise kuupäevast]. Artiklit 11 kohaldatakse siiski alates [12 kuud alates käesoleva määruse jõustumise kuupäevast].

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

1.2. Asjaomased poliitikavaldkonnad

1.3. Ettepanek/algatus käsitleb

1.4. Eesmärgid

1.4.1. Üldeesmärgid

1.4.2. Erieesmärgid

1.4.3. Oodatavad tulemused ja mõju

1.4.4. Tulemusnäitajad

1.5. Ettepaneku/algatuse põhjendused

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused, sealhulgas algatuse rakendamise üksikasjalik ajakava

1.5.2. ELi meetme lisaväärtus (see võib tuleneda eri teguritest, nagu kooskõlastamisest saadav kasu, õiguskindlus, suurem tõhusus või vastastikune täiendavus). Käesoleva punkti kohaldamisel tähendab „ELi meetme lisaväärtus“ väärtust, mis tuleneb liidu sekkumisest ja lisandub väärtusele, mille liikmesriigid oleksid muidu üksi loonud.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

1.5.4. Kooskõla mitmeaastase finantsraamistikuga ja võimalik koostoime muude asjaomaste meetmetega

1.5.5. Erinevate kasutada olevate rahastamisvõimaluste, sealhulgas vahendite ümberpaigutamise võimaluste hinnang

1.6. Ettepaneku/algatuse kestus ja finantsmõju

1.7. Ettenähtud eelarve täitmise viisid

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

2.2. Haldus- ja kontrollisüsteem(id)

2.2.1. Eelarve täitmise viisi(de), rahastamise rakendamise mehhanismi(de), maksete tegemise korra ja kavandatava kontrollistrateegia selgitus

2.2.2. Teave kindlakstehtud riskide ja nende vähendamiseks kasutusele võetud sisekontrollisüsteemi(de) kohta

2.2.3. Kontrollide kulutõhususe (kontrollikulude suhe hallatavate vahendite väärtusse) hinnang ja põhjendus ning prognoositav veariski tase (maksete tegemise ja sulgemise ajal).

2.3. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

3.2. Ettepaneku hinnanguline finantsmõju assigneeringutele

3.2.1. Hinnanguline mõju tegevusassigneeringutele – ülevaade

3.2.2. Tegevusassigneeringutest rahastatav väljund (hinnang)

3.2.3. Hinnanguline mõju haldusassigneeringutele – ülevaade

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

3.2.5. Kolmandate isikute rahaline osalus

3.3. Hinnanguline mõju tuludele

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

Ettepanek: Määrus, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid (kübervastupidavusvõime määrus)

1.2. Asjaomased poliitikavaldkonnad

Sidevõrgud, sisu ja tehnoloogia

1.3. Ettepanek/algatus käsitleb

× **uut meedet**

☐ **uut meedet, mis tuleneb katseprojektist / ettevalmistavast meetmest**[37]

☐ **olemasoleva meetme pikendamist**

☐ **ühe või mitme meetme ümbersuunamist teise või uude meetmesse või ühendamist teise või uue meetmega**

1.4. Eesmärgid

1.4.1. Üldeesmärgid

Ettepanekul on kaks põhieesmärki, et tagada siseturu nõuetekohane toimimine: 1) **luua tingimused turvaliste digielemente sisaldavate toodete arendamiseks**, tagades, et turule lastakse vähemate nõrkustega riist- ja tarkvaratooted ning et tootjad suhtuvad turvalisusesse tõsiselt toote kogu elutsükli jooksul, ning 2) **luua tingimused, mis võimaldavad kasutajatel digielemente sisaldavate toodete valimisel ja kasutamisel küberturvalisust arvesse võtta**.

1.4.2. Erieesmärgid

Ettepanekule seati **neli erieesmärki**: i) tagada, et tootjad parandavad digielemente sisaldavate toodete turvalisust alates projekteerimis- ja arendamisetapist ning kogu elutsükli jooksul; ii) tagada sidus küberturvalisuse raamistik, mis hõlbustab riist- ja tarkvaratootjatel nõuete täitmist; iii) suurendada digielemente sisaldavate toodete turvaomaduste läbipaistvust ning iv) võimaldada ettevõtjatel ja tarbijatel digielemente sisaldavaid tooteid turvaliselt kasutada.

Oodatavad tulemused ja mõju

[37] Vastavalt finantsmääruse artikli 58 lõike 2 punktile a või b.

Märkige, milline peaks olema ettepaneku/algatuse oodatav mõju toetusesaajatele/sihtrühmale.

Ettepanek tooks eri sidusrühmadele märkimisväärset kasu. Ettevõtjate jaoks hoiaks see ära digielemente sisaldavate toodete suhtes kohaldatavate turvaeeskirjade lahknevuse ja vähendaks asjaomaste küberturvalisuse õigusaktide nõuete täitmisega seotud kulusid. See vähendaks küberintsidentide arvu, intsidentide käsitlemise kulusid ja mainekahju. Algatus võib kogu ELis vähendada ettevõtjaid mõjutavate intsidentidega seotud kulusid hinnanguliselt 180–290 miljardi euro võrra aastas[38]. See tooks kaasa käibe suurenemise, kuna nõudlus digielemente sisaldavate toodete järele suureneks. See parandaks ettevõtjate ülemaailmset mainet, mis tooks kaasa nõudluse suurenemise ka väljaspool ELi. Kasutajate jaoks suurendaks eelistatud variant turvaomaduste läbipaistvust ja hõlbustaks digielemente sisaldavate toodete kasutamist. Tarbijad ja kodanikud saaksid kasu ka oma põhiõiguste (nagu eraelu puutumatus ja andmekaitse) paremast kaitsest.

Samal ajal suurendaks ettepanek nõuete täitmise ja nende täitmise tagamisega seotud kulusid ettevõtjate, teavitatud asutuste ja avaliku sektori asutuste, sealhulgas akrediteerimis- ja turujärelevalveasutuste jaoks. Tarkvaraarendajate ja riistvaratootjate jaoks suurenevad otsesed nõuete täitmisega seotud kulud uute turvanõuete, vastavushindamise, dokumenteerimise ja aruandekohustuste tõttu, mille tulemusel nõuete täitmisega seotud kulud kokku on kuni ligikaudu 29 miljardit eurot, samal ajal kui hinnanguline turuväärtus käibe alusel on 1 485 miljardit eurot[39]. digielemente sisaldavate toodete hinnad võivad muutuda kasutajate, sealhulgas ärikasutajate, tarbijate ja kodanike jaoks kõrgemaks. Neid hindu vaadeldes tuleks siiski võtta arvesse eespool kirjeldatud märkimisväärset kasu.

1.4.3. Tulemusnäitajad

Märkige, milliste näitajate abil jälgitakse edusamme ja saavutusi.

Selleks et hinnata, kas tootjad parandavad oma digielemente sisaldavate toodete turvalisust alates nende toodete projekteerimis- ja arendamisetapist ning kogu nende elutsükli jooksul, võiks arvesse võtta mitut näitajat. Need võivad olla nõrkustest põhjustatud oluliste intsidentide arv liidus, selliste riist- ja tarkvaratootjate osakaal, kes järgivad süsteemset turvalise arenduse olelusringi, digielemente sisaldavate toodete turvalisuse kvalitatiivne analüüs, nõrkuste andmebaaside kvantitatiivne ja kvalitatiivne hindamine, tootjate poolt kättesaadavate turbepaikade pakkumise sagedus või nõrkuste avastamise ja turbepaikade pakkumise vahele jäävate päevade keskmine arv.

Sidusa küberturvalisuse raamistiku näitajaks võiks olla sihtotstarbeliste tootepõhiste riiklike küberturvalisuse õigusaktide puudumine.

---

[38] Vt [komisjoni talituste töödokument mõjuhinnangu kohta, mis on lisatud määrusele, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid].

[39] Vt [komisjoni talituste töödokument mõjuhinnangu kohta, mis on lisatud määrusele, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid].

Digielemente sisaldavate toodete turvaomaduste suurema läbipaistvuse näitajaks võiks olla selliste digielemente sisaldavate toodete osakaal, mis tarnitakse koos turvaomadusi käsitleva teabega. Lisaks võiks selliste digielemente sisaldavate toodete osakaalu, mis tarnitakse koos turvalist kasutamist käsitleva kasutusjuhendiga, kasutada näitajana selle kohta, kas organisatsioonidele ja tarbijatele tehakse võimalikuks digielemente sisaldavaid tooteid turvaliselt kasutada.

Seoses määruse mõju jälgimisega kaalutaks teatavaid näitajaid, mida komisjon peaks hindama, vajaduse korral ENISA toetusel. Sõltuvalt taotletavast tegevuseesmärgist on allpool esitatud mõned seirenäitajad, mille alusel hinnatakse horisontaalsete küberturvalisuse nõuete edukust.

Digielemente sisaldavate toodete küberturvalisuse taseme hindamiseks:

– statistika ja kvalitatiivne analüüs digielemente sisaldavaid tooteid mõjutavate intsidentide ja nende käsitlemise kohta. Neid andmeid võiks ENISA toetusel koguda ja hinnata komisjon;

– andmed teadaolevate nõrkuste kohta ja analüüsid nende käsitlemise kohta. Sellise analüüsi võiks teha ENISA, tuginedes [direktiivi XXX/XXXX (küberturvalisuse 2. direktiiv)] kohaselt loodud Euroopa nõrkuste andmebaasile;

– riist- ja tarkvaratootjate seas edusammude jälgimiseks tehtud uuringud.

Hindamiseks, mil määral esitatakse teavet turvaomaduste, turvalisusealase toe, olelusringi lõpu ja hoolsuskohustuse kohta: komisjoni poolt ENISA toetusel nii kasutajate kui ka ettevõtjate hulgas korraldatavate uuringute tulemused.

Rakendamise hindamiseks püüab komisjon tagada, et vastavushindamised viiakse ellu tulemuslikult. Selleks esitatakse standardimistaotlus ja jälgitakse selle rakendamist. Komisjon kontrollib ka teavitatud asutuste ja vajaduse korral sertifitseerimisasutuste suutlikkust.

Seoses kohaldamisega kontrollib komisjon liikmesriikide aruannete abil, ega riiklikud algatused ei käsitle määrusega hõlmatud aspekte.

1.5. Ettepaneku/algatuse põhjendused

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused, sealhulgas algatuse rakendamise üksikasjalik ajakava

Määrus peaks olema täielikult kohaldatav 24 kuud pärast selle jõustumist. Juhtimisstruktuuri elemendid peaksid aga enne seda paigas olema. Eelkõige peavad liikmesriikidel olema nimetatud olemasolevad asutused ja/või loodud uued asutused õigusaktides sätestatud ülesannete täitmiseks.

1.5.2. ELi meetme lisaväärtus (see võib tuleneda eri teguritest, nagu kooskõlastamisest saadav kasu, õiguskindlus, suurem tõhusus või vastastikune täiendavus). Käesoleva punkti kohaldamisel tähendab „ELi meetme lisaväärtus“ väärtust, mis tuleneb liidu sekkumisest ja lisandub väärtusele, mille liikmesriigid oleksid muidu üksi loonud.

Küberturvalisuse tugev piiriülene olemus ja selliste intsidentide kasvav arv, millel on piiriülene ning muudele sektoritele ja toodetele ülekanduv mõju, tähendavad, et liikmesriigid üksi ei suuda eesmärke tulemuslikult saavutada. Võttes arvesse digielemente sisaldavate toodete turgude ülemaailmset olemust, seistakse liikmesriikide territooriumil samade digielemente sisaldavate toodete puhul silmitsi samade riskidega. Kujunev ebaühtlane raamistik, mis koosneb potentsiaalselt lahknevatest siseriiklikest õigusnormidest, võib ka takistada digielemente sisaldavate toodete avatud ja konkurentsivõimelise ühtse turu toimimist. Seega on vaja ELi tasandi ühismeetmeid, et suurendada kasutajate usaldust ja digielemente sisaldavate ELi toodete populaarsust. Need tooksid kasu ka siseturule, tagades õiguskindluse ja luues võrdsed võimalused digielemente sisaldavate toodete müüjatele.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

Kübervastupidavusvõime määrus on esimene omataoline määrus, millega kehtestatakse küberturvalisuse nõuded digielemente sisaldavate toodete turule laskmiseks. See tugineb aga uue õigusraamistiku korrale ja kogemustele, mis on saadud mitmesuguste toodete suhtes kehtivate liidu ühtlustamisõigusaktide rakendamisel, eelkõige seoses rakendamise ettevalmistamisega, sealhulgas selliste aspektidega nagu harmoneeritud standardite ettevalmistamine.

1.5.4. Kooskõla mitmeaastase finantsraamistikuga ja võimalik koostoime muude asjaomaste meetmetega

Määruses, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid, määratakse kindlaks kõigi ELi turule lastavatele digielemente sisaldavate toodete suhtes kohaldatavad uued küberturvalisuse nõuded, mis lähevad kaugemale kehtivates õigusaktides sätestatud nõuetest. Samal ajal põhineb ettepanek uue õigusraamistiku õigusaktide kohasel kehtival korral. Seega tugineks see uue õigusraamistiku olemasolevatele struktuuridele ja menetlustele, nagu teavitatud asutuste koostöö ja turujärelevalve, vastavushindamismoodulid ja harmoneeritud standardite väljatöötamine. Uus ettepanek tugineks ka teatavatele struktuuridele, mis on välja töötatud kooskõlas muude küberturvalisust käsitlevate õigusaktidega, nagu direktiiv (EL) 2016/1148 (küberturvalisuse direktiiv), [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] või määrus (EL) 2019/881 (küberturvalisuse määrus).

1.5.5. Erinevate kasutada olevate rahastamisvõimaluste, sealhulgas vahendite ümberpaigutamise võimaluste hinnang

ENISA-le määratud tegevusvaldkondade haldamine on kooskõlas tema olemasolevate volituste ja üldiste ülesannetega. Need tegevusvaldkonnad võivad eeldada konkreetseid profiile või uusi ülesandeid, kuid need ei oleks märkimisväärsed ning need saaks katta ENISA olemasolevatest vahenditest ning erinevate ülesannete ümberjaotamise või ühendamise teel. Näiteks üks peamisi ENISA-le määratud tegevusvaldkondi on selliste teadete kogumine ja töötlemine,

mis on tootjatelt saadud toodete nõrkuste kohta, mida on ära kasutatud. [Direktiiviga XXX/XXXX (küberturvalisuse 2. direktiiv)] on juba antud ENISA-le ülesanne luua Euroopa nõrkuste andmebaas, kus saab avalikult teadaolevaid nõrkusi vabatahtlikult avalikustada ja registreerida, et võimaldada kasutajatel võtta asjakohaseid leevendusmeetmeid. Selleks eraldatud vahendeid võiks kasutada ka eespool nimetatud uute ülesannete jaoks, mis on seotud toodete nõrkustest teatamisega. See võiks tagada olemasolevate ressursside tulemusliku kasutamise ja looks ka vajaliku sünergia selliste ülesannete vahel, mis võivad aidata ENISA-l küberriske ja -ohte paremini analüüsida.

1.6. Ettepaneku/algatuse kestus ja finantsmõju

☐ **Piiratud kestusega**

– ☐ hõlmab ajavahemikku [PP/KK]AAAA–[PP/KK]AAAA

– ☐ finantsmõju kulukohustuste assigneeringutele avaldub ajavahemikul AAAA–AAAA ja maksete assigneeringutele ajavahemikul AAAA–AAAA.

× **Piiramatu kestusega**

– Rakendamise käivitumisperiood algab 2025. aastal,

– millele järgneb täieulatuslik rakendamine

1.7. Ettenähtud eelarve täitmise viisid[40]

☐ **Eelarve otsene täitmine** komisjoni poolt

– × oma talituste kaudu, sealhulgas kasutades liidu delegatsioonides töötavat komisjoni personali;

– ☐ rakendusametite kaudu

☐ **Eelarve jagatud täitmine** koostöös liikmesriikidega

☐ **Eelarve kaudne täitmine**, mille puhul eelarve täitmise ülesanded on delegeeritud:

– ☐ kolmandatele riikidele või nende määratud asutustele;

– ☐ rahvusvahelistele organisatsioonidele ja nende allasutustele (nimetage);

– ☐ Euroopa Investeerimispangale ja Euroopa Investeerimisfondile;

– ☐ finantsmääruse artiklites 70 ja 71 osutatud asutustele;

– ☐ avalik-õiguslikele asutustele;

– ☐ avalikke teenuseid osutavatele eraõiguslikele asutustele, kuivõrd neile antakse piisavad finantstagatised;

– ☐ liikmesriigi eraõigusega reguleeritud asutustele, kellele on delegeeritud avaliku ja erasektori partnerluse rakendamine ja kellele antakse piisavad finantstagatised;

– ☐ isikutele, kellele on delegeeritud Euroopa Liidu lepingu V jaotise kohaste ühise välis- ja julgeolekupoliitika erimeetmete rakendamine ja kes on kindlaks määratud asjaomases alusaktis.

---

[40] Eelarve täitmise viise koos viidetega finantsmäärusele on selgitatud veebisaidil https://myintracomm.ec.europa.eu/budgweb/ET/man/budgmanag/Pages/budgmanag.aspx.

– *Mitme eelarve täitmise viisi valimise korral esitage üksikasjad rubriigis „Märkused“.*

Märkused

Käesoleva määrusega määratakse ENISA-le teatavate meetmete võtmine kooskõlas tema olemasolevate volitustega, eelkõige määruse (EL) 2019/881 artikli 3 lõikega 2, milles on sätestatud, et ENISA peaks täitma ülesandeid, mis pannakse talle liidu õigusaktidega, milles sätestatakse meetmed liikmesriikide küberturvalisusega seotud õigus- ja haldusnormide lähendamiseks. Eelkõige antakse ENISA-le ülesanne võtta vastu tootjate teateid digielemente sisaldavate toodete nõrkuste kohta, mida aktiivselt ära kasutatakse, ning intsidentide kohta, mis mõjutavad nende toodete turvalisust. ENISA peaks edastama need teated ka asjaomastele CSIRTidele või asjaomasele liikmesriikide ühtsele kontaktpunktile, mis on määratud vastavalt direktiivi [direktiiv XXX/XXXX (küberturvalisuse 2. direktiiv)] artiklile [artikkel X], ning teavitama turujärelevalveasutusi. ENISA peaks kogutud teabe põhjal koostama iga kahe aasta tagant tehnilise aruande digielemente sisaldavate toodete küberriskidega seotud uute suundumuste kohta ning esitama selle võrgu- ja infoturbe koostöörühmale. Võttes arvesse ENISA eksperditeadmisi, kogutavat teavet ja ohuanalüüse, võib ENISA toetada käesoleva määruse rakendamise protsessi ettepanekute tegemisega riiklike turujärelevalveasutuste võetavate ühismeetmete kohta, tuginedes viidetele või teabele digielemente sisaldavate toodete kohta, mis ei pruugi mitmes liikmesriigis olla käesoleva määrusega vastavuses, või määrata kindlaks tootekategooriad, mille suhtes võiks võtta üheaegseid kooskõlastatud kontrollimeetmeid. Komisjon võib paluda ENISA-l viia erandlikel asjaoludel ellu konkreetsete toodete hindamisi, kui mõne digielemente sisaldava tootega kaasneb oluline küberrisk ja kui siseturu hea toimimise säilitamiseks on vaja viivitamata sekkuda.

Hinnangute kohaselt tuleb kõigi nende ülesannete täitmiseks ENISA olemasolevatest ressurssidest eraldada ligikaudu 4,5 täistööajale taandatud töötajat, võttes arvesse praegusi eksperditeadmisi ja ettevalmistustööd, mida ENISA praegu teeb muu hulgas selleks, et toetada [direktiivi XXX/XXXX (küberturvalisuse 2. direktiiv)] eelseisvat rakendamist, mille jaoks ENISA vahendeid täiendati.

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

Märkige sagedus ja tingimused.

Hiljemalt 36 kuud pärast käesoleva määruse kohaldamise algust ja seejärel iga nelja aasta tagant esitab komisjon Euroopa Parlamendile ja nõukogule aruande määruse hindamise ja läbivaatamise kohta. Aruanded avalikustatakse.

2.2. Haldus- ja kontrollisüsteem(id)

2.2.1. Eelarve täitmise viisi(de), rahastamise rakendamise mehhanismi(de), maksete tegemise korra ja kavandatava kontrollistrateegia selgitus

Käesoleva määrusega kehtestatakse uus poliitika seoses ühtlustatud küberturvalisuse nõuetega, mida kohaldatakse turule lastavate digielemente sisaldavate toodete suhtes kogu nende elutsükli jooksul. Õigusaktile järgnevad Euroopa standardiorganisatsioonidele esitatavad komisjoni taotlused standardite väljatöötamiseks. Nende uute ülesannete täitmiseks tuleb tagada komisjoni talitustele asjakohased ressursid. Uue määruse nõuete täitmise tagamiseks on hinnanguliselt vaja seitset täistööajale taandatud töötajat (kellest üks on riigi lähetatud ekspert), et täita järgmisi ülesandeid:

– koostada standardimistaotlus ja/või ühtsed kirjeldused rakendusaktide abil, kui standardimisprotsess ei ole edukas;

– koostada [12 kuu jooksul pärast määruse jõustumist] delegeeritud õigusakt, milles esitatakse digielemente sisaldavate kriitilise tähtsusega toodete määratlused;

– tõenäoliselt koostada delegeeritud õigusaktid I ja II klassi kuuluvate kriitilise tähtsusega toodete loetelu ajakohastamiseks; täpsustada, kas vajalik on piirang või väljajätmine selliste digielemente sisaldavate toodete puhul, mis on hõlmatud muude liidu õigusnormidega, milles kehtestatud nõuetega saavutatakse samasugune kaitsetase nagu käesoleva määrusega; kehtestada kohustus sertifitseerida teatavad digielemente sisaldavad ülikriitilise tähtsusega tooted käesolevas määruses sätestatud kriteeriumide alusel; määrata kindlaks ELi vastavusdeklaratsiooni minimaalne sisu ja täiendada tehnilises dokumentatsioonis esitatavaid elemente;

– tõenäoliselt koostada rakendusaktid seoses aruandekohustuste vormi või elementidega, tarkvaramaterjalide loeteluga, ühtsete kirjeldustega või CE-vastavusmärgise kinnitamisega;

– tõenäoliselt valmistada ette erandlikel asjaoludel toimuv viivitamatu sekkumine parandus- või piiravate meetmete kehtestamiseks, et säilitada siseturu hea toimimine, sealhulgas koostada rakendusakt;

– korraldada ja koordineerida teavitatud asutustest teavitamist liikmesriikide poolt ning koordineerida teavitatud asutuste tegevust;

– toetada liikmesriikide turujärelevalveasutuste tegevuse koordineerimist.

2.2.2. Teave kindlakstehtud riskide ja nende vähendamiseks kasutusele võetud sisekontrollisüsteemi(de) kohta

Selleks et tagada teavitatud asutuste ja turujärelevalveasutuste teabevahetus ja hea koostöö, vastutab komisjon nende tegevuse koordineerimise eest. Tehnilise ja turualase oskusteabe jagamiseks luuakse eksperdirühm.

2.2.3. Kontrollide kulutõhususe (kontrollikulude suhe hallatavate vahendite väärtusse) hinnang ja põhjendus ning prognoositav veariski tase (maksete tegemise ja sulgemise ajal).

2.3. Kuna ühe tehingu (nt koosolekul osaleva delegaadi reisikulude hüvitamine) väärtus on väike, näib koosolekukuludega seoses piisavat standardsest kontrollikorrast. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

Nimetage rakendatavad või kavandatud ennetus- ja kaitsemeetmed, nt pettustevastase võitluse strateegias esitatud meetmed.

Komisjoni suhtes kohaldatavad olemasolevad pettuste ennetamise meetmed hõlmavad käesoleva määruse täitmiseks vajalikke lisaassigneeringuid.

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

- Olemasolevad eelarveread

Skeem

- Uued eelarveread, mille loomist taotletakse

Ei kohaldata

3.2. Ettepaneku hinnanguline finantsmõju assigneeringutele

3.2.1. Hinnanguline mõju tegevusassigneeringutele – ülevaade

– ☑ Ettepanek/algatus ei hõlma tegevusassigneeringute kasutamist

– ☐ Ettepanek/algatus hõlmab tegevusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes (kolm kohta pärast koma)

Mitmeaastase finantsraamistiku rubriik	Nr	

DG: <…….>			Aasta **N**[41]	Aasta **N + 1**	Aasta **N + 2**	Aasta **N + 3**	Lisage vajalik arv aastaid, et kajastada kogu finantsmõju kestust (vt punkt 1.6)			**KOKKU**
• Tegevusassigneeringud										
Eelarverida[42]	Kulukohustused	(1a)								
	Maksed	(2a)								
Eelarverida	Kulukohustused	(1b)								
	Maksed	(2b)								
Eriprogrammide vahenditest rahastatavad haldusassigneeringud[43]										
Eelarverida		(3)								

41 N on aasta, mil alustatakse ettepaneku/algatuse rakendamist. „N“ asemel tuleb märkida esimene eeldatav rakendamise aasta (näiteks 2021). Sama tuleb teha ka järgnevate aastate puhul.

42 Eelarve ametliku liigenduse kohaselt.

43 Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamiseks antava toetusega seotud kulud (endised BA read), kaudne teadustegevus, otsene teadustegevus.

DG <…….> assigneeringud KOKKU	Kulukohustused	= 1a + 1b + 3								
	Maksed	= 2a + 2b +3								

• Tegevusassigneeringud KOKKU	Kulukohustused	(4)								
	Maksed	(5)								
• Eriprogrammide vahenditest rahastatavad haldusassigneeringud KOKKU		(6)								
Mitmeaastase finantsraamistiku **RUBRIIGI <….> assigneeringud KOKKU**	Kulukohustused	= 4 + 6								
	Maksed	= 5 + 6								

Juhul kui ettepanek/algatus mõjutab mitut rubriiki, tuleb eelmist jaotist korrata

• Tegevusassigneeringud KOKKU (kõik rubriigid)	Kulukohustused	(4)								
	Maksed	(5)								
Eriprogrammide vahenditest rahastatavad haldusassigneeringud KOKKU (kõik rubriigid)		(6)								
Mitmeaastase finantsraamistiku **RUBRIIKIDE 1–6 assigneeringud KOKKU** (võrdlussumma)	Kulukohustused	= 4 + 6								
	Maksed	= 5 + 6								

Mitmeaastase finantsraamistiku rubriik	**7**	„Halduskulud“

Selle punkti täitmisel tuleks kasutada haldusalaste eelarveandmete tabelit, mis on esitatud õigusaktile lisatava finantsselgituse lisas (sisekorraeeskirjade V lisa), ja laadida see üles DECIDE’i talitustevahelise konsulteerimise eesmärgil.

miljonites eurodes (kolm kohta pärast koma)

		Aasta **2024**	Aasta **2025**	Aasta **2026**	Aasta **2027**	**KOKKU**
DG: CNECT						
• Personalikulud		1,030	1,030	1,030	1,030	**4,120**
• Muud halduskulud		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
DG CNECT KOKKU	Assigneeringud	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

Mitmeaastase finantsraamistiku RUBRIIGI 7 assigneeringud KOKKU	(Kulukohustuste kogusumma = maksete kogusumma)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

miljonites eurodes (kolm kohta pärast koma)

		Aasta **2024**	Aasta **2025**	Aasta **2026**	Aasta **2027**	**KOKKU**
Mitmeaastase finantsraamistiku **RUBRIIKIDE 1–7 assigneeringud KOKKU**	Kulukohustused	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Maksed	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Tegevusassigneeringutest rahastatav väljund (hinnang)

kulukohustuste assigneeringud miljonites eurodes (kolm kohta pärast koma)

Märkige eesmärgid ja väljundid			Aasta **N**		Aasta **N + 1**		Aasta **N + 2**		Aasta **N + 3**		Lisage vajalik arv aastaid, et kajastada kogu finantsmõju kestust (vt punkt 1.6)						**KOKKU**	
	VÄLJUNDID																	
⇩	Väljundi liik[44]	Keskmine kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Väljundite arv kokku	Kulud kokku
ERIEESMÄRK nr 1[45] ...																		
- Väljund																		
- Väljund																		
- Väljund																		
Erieesmärk nr 1 kokku																		
ERIEESMÄRK nr 2 ...																		
- Väljund																		
Erieesmärk nr 2 kokku																		
KOKKU																		

44 Väljunditena käsitatakse tarnitud tooteid ja osutatud teenuseid (rahastatud üliõpilasvahetuste arv, ehitatud teede pikkus kilomeetrites jms).

45 Vastavalt punktile 1.4.2 „Erieesmärgid ...“

3.2.3. Hinnanguline mõju haldusassigneeringutele – ülevaade

– ☐ Ettepanek/algatus ei hõlma haldusassigneeringute kasutamist

– ☑ Ettepanek/algatus hõlmab haldusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes (kolm kohta pärast koma)

	Aasta **2024**	Aasta **2025**	Aasta **2026**	Aasta **2027**	
Mitmeaastase finantsraamistiku RUBRIIK 7					
Personalikulud	1,030	1,030	1,030	1,030	**4,120**
Muud halduskulud	0,222	0,222	0,222	0,222	**0,888**
Mitmeaastase finantsraamistiku RUBRIIGI 7 kulud kokku	1,252	1,252	1,252	1,252	**5,008**

Mitmeaastase finantsraamistiku RUBRIIGIST 7[46] välja jäävad kulud					
Personalikulud					
Muud halduskulud					
Mitmeaastase finantsraamistiku RUBRIIGIST 7 välja jäävad kulud kokku					

KOKKU	1,252	1,252	1,252	1,252	**5,008**

Personali ja muude halduskuludega seotud assigneeringute vajadused kaetakse asjaomase peadirektoraadi poolt kõnealuse meetme haldamiseks juba antud ja/või peadirektoraadi siseselt ümberpaigutatud assigneeringutest, mida vajaduse korral võidakse täiendada nendest lisaassigneeringutest, mis haldavale peadirektoraadile eraldatakse iga-aastase vahendite eraldamise menetluse käigus, arvestades eelarvepiirangutega.

46 Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamiseks antava toetusega seotud kulud (endised BA read), kaudne teadustegevus, otsene teadustegevus.

1.1.1.1. Hinnanguline personalivajadus

– ☐ Ettepanek/algatus ei hõlma personali kasutamist.

– ☑ Ettepanek/algatus hõlmab personali kasutamist, mis toimub järgmiselt:

Hinnanguline väärtus täistööaja ekvivalendina

		Aasta **2024**	Aasta **2025**	Aasta **2026**	Aasta **2027**
20 01 02 01 (komisjoni peakorteris ja esindustes)		6	6	6	6
20 01 02 03 (delegatsioonides)					
01 01 01 01 (kaudne teadustegevus)					
01 01 01 11 (otsene teadustegevus)					
Muud eelarveread (märkige)					
• Koosseisuväline personal (täistööajale taandatud töötajad)[47]					
20 02 01 (üldvahenditest rahastatavad lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud)		1	1	1	1
20 02 03 (lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud ja noored eksperdid delegatsioonides)					
XX 01 xx **yy zz**[48]	- peakorteris				
	- delegatsioonides				
01 01 01 02 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud kaudse teadustegevuse valdkonnas)					
01 01 01 12 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud otsese teadustegevuse valdkonnas)					
Muud eelarveread (märkige)					
KOKKU		**7**	**7**	**7**	**7**

XX tähistab asjaomast poliitikavaldkonda või eelarvejaotist.

Personalivajadused kaetakse juba meedet haldavate peadirektoraadi töötajatega ja/või töötajate peadirektoraadisisese ümberpaigutamise teel. Vajaduse korral võidakse personali täiendada iga-aastase vahendite eraldamise menetluse käigus, arvestades olemasolevate eelarvepiirangutega.

Ülesannete kirjeldus:

Ametnikud ja ajutised töötajad 6 täistööajale taandatud töötajat × 157 000 eurot aastas = 942 000 eurot	Vastavalt punktile 2.2.1: – koostada standardimistaotlus ja/või ühtsed kirjeldused rakendusaktide abil, kui standardimisprotsess ei ole edukas; – koostada [12 kuu jooksul pärast määruse jõustumist] delegeeritud õigusakt, milles esitatakse digielemente sisaldavate kriitilise tähtsusega toodete määratlused;

[47] Lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud; noored spetsialistid delegatsioonides.

[48] Tegevusassigneeringutest rahastatavate koosseisuväliste töötajate ülempiiri arvestades (endised BA read).

	– tõenäoliselt koostada delegeeritud õigusaktid I ja II klassi kuuluvate kriitilise tähtsusega toodete loetelu ajakohastamiseks; täpsustada, kas vajalik on piirang või väljajätmine selliste digielemente sisaldavate toodete puhul, mis on hõlmatud muude liidu õigusnormidega, milles kehtestatud nõuetega saavutatakse samasugune kaitsetase nagu käesoleva määrusega; kehtestada kohustus sertifitseerida teatavad digielemente sisaldavad ülikriitilise tähtsusega tooted käesolevas määruses sätestatud kriteeriumide alusel; määrata kindlaks ELi vastavusdeklaratsiooni minimaalne sisu ja täiendada tehnilises dokumentatsioonis esitatavaid elemente; – tõenäoliselt koostada rakendusaktid seoses aruandekohustuste vormi või elementidega, tarkvaramaterjalide loeteluga, ühtsete kirjeldustega või CE-vastavusmärgise kinnitamisega; – tõenäoliselt valmistada ette erandlikel asjaoludel toimuv viivitamatu sekkumine parandus- või piiravate meetmete kehtestamiseks, et säilitada siseturu hea toimimine, sealhulgas koostada rakendusakt; – korraldada ja koordineerida teavitatud asutustest teavitamist liikmesriikide poolt ning koordineerida teavitatud asutuste tegevust; – toetada liikmesriikide turujärelevalveasutuste tegevuse koordineerimist.
Koosseisuvälised töötajad 1 riigi lähetatud ekspert × 88 000 eurot aastas	Vastavalt punktile 2.2.1: – koostada standardimistaotlus ja/või ühtsed kirjeldused rakendusaktide abil, kui standardimisprotsess ei ole edukas; – koostada [12 kuu jooksul pärast määruse jõustumist] delegeeritud õigusakt, milles esitatakse digielemente sisaldavate kriitilise tähtsusega toodete määratlused; – tõenäoliselt koostada delegeeritud õigusaktid I ja II klassi kuuluvate kriitilise tähtsusega toodete loetelu ajakohastamiseks; täpsustada, kas vajalik on piirang või väljajätmine selliste digielemente sisaldavate toodete puhul, mis on hõlmatud muude liidu õigusnormidega, milles kehtestatud nõuetega saavutatakse samasugune kaitsetase nagu käesoleva määrusega; kehtestada kohustus sertifitseerida teatavad digielemente sisaldavad ülikriitilise tähtsusega tooted käesolevas määruses sätestatud kriteeriumide alusel; määrata kindlaks ELi vastavusdeklaratsiooni minimaalne sisu ja täiendada tehnilises dokumentatsioonis esitatavaid elemente; – tõenäoliselt koostada rakendusaktid seoses aruandekohustuste vormi või elementidega, tarkvaramaterjalide loeteluga, ühtsete kirjeldustega või CE-vastavusmärgise kinnitamisega; – tõenäoliselt valmistada ette erandlikel asjaoludel toimuv viivitamatu sekkumine parandus- või piiravate meetmete kehtestamiseks, et säilitada siseturu hea toimimine, sealhulgas koostada rakendusakt; – korraldada ja koordineerida teavitatud asutustest teavitamist liikmesriikide poolt ning koordineerida teavitatud asutuste tegevust; – toetada liikmesriikide turujärelevalveasutuste tegevuse koordineerimist.

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

Ettepanek/algatus:

– x on täielikult rahastatav mitmeaastase finantsraamistiku asjaomase rubriigi sisese vahendite ümberpaigutamise kaudu.

Ümberplaneerimist ei ole vaja.

– ☐ tingib mitmeaastase finantsraamistiku asjaomases rubriigi mittesihtotstarbelise varu ja/või mitmeaastase finantsraamistiku määruses sätestatud erivahendite kasutuselevõtu.

–

– ☐ nõuab mitmeaastase finantsraamistiku muutmist.

–

3.2.5. Kolmandate isikute rahaline osalus

Ettepanek/algatus:

– x ei hõlma kolmandate isikute poolset kaasrahastamist

– ☐ hõlmab kaasrahastamist, mille hinnanguline summa on järgmine:

assigneeringud miljonites eurodes (kolm kohta pärast koma)

	Aasta **N**[49]	Aasta **N + 1**	Aasta **N + 2**	Aasta **N + 3**	Lisage vajalik arv aastaid, et kajastada kogu finantsmõju kestust (vt punkt 1.6)			Kokku
Nimetage kaasrahastav asutus								
Kaasrahastatavad assigneeringud KOKKU								

[49] N on aasta, mil alustatakse ettepaneku/algatuse rakendamist. „N“ asemel tuleb märkida esimene eeldatav rakendamise aasta (näiteks 2021). Sama tuleb teha ka järgnevate aastate puhul.

3.3. Hinnanguline mõju tuludele

– ☐ Ettepanekul/algatusel puudub finantsmõju tuludele

– ☐ Ettepanekul/algatusel on järgmine finantsmõju:

  – ☐ omavahenditele

  – ☐ muudele tuludele

  – palun märkige, kas see on kulude eelarveridasid mõjutav sihtotstarbeline tulu ☐

miljonites eurodes (kolm kohta pärast koma)

Tulude eelarverida	Jooksva aasta eelarves kättesaadavad assigneeringud	Ettepaneku/algatuse mõju[50]						
		Aasta **N**	Aasta **N + 1**	Aasta **N + 2**	Aasta **N + 3**	Lisage vajalik arv aastaid, et kajastada kogu finantsmõju kestust (vt punkt 1.6)		
Artikkel ….								

Sihtotstarbeliste tulude puhul märkige, milliseid kulude eelarveridasid ettepanek mõjutab.

Muud märkused (nt tuludele avaldatava mõju arvutamise meetod/valem või muu teave)

[50] Traditsiooniliste omavahendite (tollimaksud ja suhkrumaksud) korral tuleb märkida netosummad, st brutosumma pärast 20 % sissenõudmiskulude mahaarvamist.