EIROPAS SAVIENĪBA

EIROPAS PARLAMENTS **PADOME**

Briselē, 2024. gada 25. septembrī
(OR. en)

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

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

LEĢISLATĪVIE AKTI UN CITI DOKUMENTI

Temats:	EIROPAS PARLAMENTA UN PADOMES REGULA par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulu (ES) Nr. 168/2013, Regulu (ES) 2019/1020 un Direktīvu (ES) 2020/1828 (Kibernoturības akts)

EIROPAS PARLAMENTA UN PADOMES

REGULA (ES) 2024/...

(... gada ...)

par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulu (ES) Nr. 168/2013, Regulu (ES) 2019/1020 un Direktīvu (ES) 2020/1828 (Kibernoturības akts)

(Dokuments attiecas uz EEZ)

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 114. pantu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu[1],

pēc apspriešanās ar Reģionu komiteju,

saskaņā ar parasto likumdošanas procedūru[2],

---

1 OV C 100, 16.3.2023., 101. lpp.

2 Eiropas Parlamenta 2024. gada 12. marta nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes ... lēmums.

tā kā:

(1) Kiberdrošība ir viens no svarīgākajiem Savienībai risināmajiem uzdevumiem. Savienoto ierīču skaits un dažādība turpmākajos gados ļoti strauji pieaugs. Kiberuzbrukumi ir sabiedrības interešu jautājums, jo tie ārkārtīgi lielā mērā ietekmē ne tikai Savienības ekonomiku, bet arī demokrātiju un patērētāju drošību un veselību. Tādēļ ir jāstiprina Savienības pieeja attiecībā uz kiberdrošību, jāpievēršas kibernoturībai Savienības līmenī un jāuzlabo iekšējā tirgus darbība, nosakot vienotu tiesisko regulējumu kiberdrošības pamatprasībām attiecībā uz produktu ar digitāliem elementiem laišanu Savienības tirgū. Būtu jārisina divas galvenās problēmas, kas rada papildu izmaksas lietotājiem un sabiedrībai, proti, zems kiberdrošības līmenis produktiem ar digitāliem elementiem, ko atspoguļo plaši izplatītas ievainojamības un nepietiekama un nekonsekventa drošības atjauninājumu nodrošināšana to novēršanai, un nepietiekama lietotāju izpratne un piekļuve informācijai, kas neļauj lietotājiem izvēlēties produktus ar atbilstošām kiberdrošības īpašībām vai tos izmantot drošā veidā.

(2) Šīs regulas mērķis ir noteikt robežnosacījumus drošu produktu ar digitāliem elementiem izstrādei, nodrošinot, ka aparatūras un programmatūras produkti tiek laisti tirgū ar mazāk ievainojamībām un ka ražotājiem ir nopietna attieksme pret drošību visā produkta aprites ciklā. Tās mērķis ir arī radīt apstākļus, kas lietotājiem, izvēloties un lietojot produktus ar digitāliem elementiem, dod iespēju ņemt vērā kiberdrošību, piemēram, uzlabojot pārredzamību par tirgū pieejamo produktu ar digitāliem elementiem atbalsta periodu.

(3) Attiecīgie patlaban spēkā esošie Savienības tiesību akti ietver vairākus horizontālo noteikumu kopumus, kas no dažādiem skatupunktiem pievēršas noteiktiem ar kiberdrošību saistītiem aspektiem, ieskaitot pasākumus digitālās piegādes ķēdes drošības uzlabošanai. Tomēr spēkā esošie Savienības tiesību akti attiecībā uz kiberdrošību, to vidū Eiropas Parlamenta un Padomes Regula (ES) 2019/881[3]un Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555[4], tieši neaptver produktu ar digitāliem elementiem drošības obligātās prasības.

---

[3] Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp.).

[4] Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris) par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (OV L 333, 27.12.2022., 80. lpp.).

(4) Lai gan spēkā esošie Savienības tiesību akti attiecas uz noteiktiem produktiem ar digitāliem elementiem, nav horizontāla Savienības tiesiskā regulējuma, kas noteiktu visaptverošas kiberdrošības prasības attiecībā uz visiem produktiem ar digitāliem elementiem. Dažādie ES un valstu līmenī līdz šim īstenotie tiesību akti un iniciatīvas tikai daļēji risina konstatētās ar kiberdrošību saistītās problēmas un riskus, izraisot likumdošanas sadrumstalotību iekšējā tirgū, palielinot juridisko nenoteiktību gan šo produktu ražotājiem, gan lietotājiem un radot nevajadzīgu slogu uzņēmumiem un organizācijām, lai tie izpildītu vairākas prasības un pienākumus attiecībā uz līdzīgiem produktu veidiem. Minēto produktu kiberdrošībai ir īpaši izteikta pārrobežu dimensija, jo vienā dalībvalstī vai trešā valstī ražotus produktus ar digitāliem elementiem bieži izmanto organizācijas un patērētāji visā iekšējā tirgū. Tāpēc šī joma ir jāreglamentē Savienības līmenī, lai nodrošinātu saskaņotu tiesisko regulējumu un juridisko noteiktību lietotājiem, organizācijām un uzņēmumiem, tostarp mikrouzņēmumiem un maziem un vidējiem uzņēmumiem, kā definēts Komisijas Ieteikuma 2003/361/EK pielikumā[5]. Savienības regulatīvā vide būtu jāsaskaņo, ieviešot horizontālas kiberdrošības prasības attiecībā uz produktiem ar digitāliem elementiem. Turklāt būtu jānodrošina juridiskā noteiktība attiecībā uz uzņēmējiem un lietotājiem visā Savienībā, kā arī iekšējā tirgus labāka saskaņošana un samērīgums mikrouzņēmumiem un vidējiem un maziem uzņēmumiem, radot labvēlīgākus apstākļus uzņēmējiem, kuru mērķis ir ienākt Savienības tirgū.

---

[5] Komisijas Ieteikums 2003/361/EK (2003. gada 6. maijs) par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju (OV L 124, 20.5.2003., 36. lpp.).

(5) Attiecībā uz mikrouzņēmumiem un maziem un vidējiem uzņēmumiem Komisijas Ieteikuma 2003/361/EK pielikuma noteikumi būtu jāpiemēro pilnībā, kad tiek noteikta kategorija, kurā ietilpst attiecīgais uzņēmums. Tāpēc, aprēķinot darbinieku skaitu un finanšu maksimālo apjomu, pēc kā nosaka uzņēmumu kategorijas, būtu jāpiemēro arī Komisijas Ieteikuma 2003/361/EK pielikuma 6. panta noteikumi par uzņēmuma datu noteikšanu, un jāņem vērā konkrēti uzņēmumu veidi, piemēram, partneruzņēmumi vai saistīti uzņēmumi.

(6) Komisijai būtu jāsniedz norādījumi, lai palīdzētu uzņēmējiem, jo īpaši mikrouzņēmumiem un maziem un vidējiem uzņēmumiem, piemērot šo regulu. Šādiem norādījumiem cita starpā būtu jāaptver šīs regulas darbības joma, jo īpaši attālināta datu apstrāde un tās ietekme uz brīvi pieejamas atvērtā pirmkoda programmatūras izstrādātājiem, to kritēriju piemērošana, kurus izmanto atbalsta periodu noteikšanai produktiem ar digitāliem elementiem, šīs regulas un citu Savienības tiesību aktu mijiedarbība un būtisku modifikāciju jēdziens.

(7) Savienības līmenī dažādos programmatiskos un politiskos dokumentos, piemēram, Komisijas un Savienības Augstā pārstāvja ārlietās un drošības politikas jautājumos 2020. gada 16. decembra kopīgajā paziņojumā "ES kiberdrošības stratēģija digitālajai desmitgadei", Padomes 2020. gada 2. decembra secinājumos par savienoto ierīču kiberdrošību un 2022. gada 23. maija secinājumos par Eiropas Savienības pozīcijas izstrādi kiberjautājumos, kā arī Eiropas Parlamenta 2021. gada 10. jūnija rezolūcijā par ES kiberdrošības stratēģiju digitālajai desmitgadei[6] ir pausts aicinājums noteikt īpašas Savienības kiberdrošības prasības digitāliem vai savienotiem produktiem, un visā pasaulē vairākas valstis ievieš pasākumus, lai risinātu šo jautājumu pēc savas iniciatīvas. Konferences par Eiropas nākotni galīgajā ziņojumā pilsoņi aicināja stiprināt ES lomu cīņā pret kiberdraudiem. Lai Savienība starptautiskā mērogā kiberdrošības jomā varētu ieņemt vadošo lomu, ir svarīgi izveidot vērienīgu tiesisko regulējumu.

(8) Lai palielinātu vispārējo kiberdrošības līmeni visiem iekšējā tirgū laistiem produktiem ar digitāliem elementiem, attiecībā uz šiem produktiem ir jāievieš uz mērķi vērstas un tehnoloģiski neitrālas kiberdrošības pamatprasības, kuras piemēro horizontāli.

---

[6] OV C 67, 8.2.2022., 81. lpp.

(9) Noteiktos apstākļos visi produkti ar digitāliem elementiem, kas integrēti lielākā elektroniskā informācijas sistēmā vai savienoti ar to, var kalpot par ļaundaru uzbrukuma vektoru. Tā rezultātā pat tāda aparatūra un programmatūra, kas tiek uzskatīta par mazāk kritiski svarīgu, var sekmēt ierīces vai tīkla sākotnējo apdraudējumu, ļaujot ļaundariem iegūt privileģētu piekļuvi sistēmai vai horizontāli pārvietoties starp sistēmām. Tāpēc ražotājiem būtu jānodrošina, ka visi produkti ar digitāliem elementiem tiek projektēti un izstrādāti saskaņā ar šajā regulā noteiktajām kiberdrošības pamatprasībām. Šī prasība attiecas gan uz produktiem, kurus var fiziski savienot ar aparatūras saskarņu palīdzību, gan produktiem, kuri ir loģiski savienoti, piemēram, izmantojot tīkla ligzdas, programmkanālus, datnes, lietojumprogrammu saskarnes vai cita veida programmatūras saskarnes. Tā kā kiberdraudi pirms noteikta mērķa sasniegšanas var izplatīties ar dažādiem produktiem ar digitāliem elementiem, piemēram, saķēdējot kopā vairākus ievainojamības izmantotājus, ražotājiem būtu arī jānodrošina to produktu ar digitāliem elementiem kiberdrošība, kuri ir tikai netieši savienoti ar citām ierīcēm vai tīkliem.

(10) Nosakot kiberdrošības prasības produktu ar digitāliem elementiem laišanai tirgū, ir paredzēts uzlabot šo produktu kiberdrošību gan patērētājiem, gan uzņēmumiem. Šīs prasības arī nodrošinās, ka visās piegādes ķēdēs tiks pievērsta uzmanība kiberdrošībai, padarot galaproduktus ar digitāliem elementiem un to komponentus drošākus. Tas ietver arī prasības tādu patēriņa produktu ar digitāliem elementiem laišanai tirgū, kas paredzēti neaizsargātiem patērētājiem, piemēram, rotaļlietu un bērnu uzraudzības sistēmu laišanai tirgū. Patēriņa produkti ar digitāliem elementiem, kas šajā regulā klasificēti kā nozīmīgi produkti ar digitāliem elementiem, rada augstāku kiberdrošības risku, jo tie veic funkciju, kas rada būtisku negatīvas ietekmes risku, ņemot vērā tās intensitāti un spēju kaitēt šādu preču lietotāju veselībai, drošībai vai drošumam, un tiem būtu jāpiemēro stingrāka atbilstības novērtēšanas procedūra. Tas attiecas uz tādiem produktiem kā viedās mājas produkti ar drošības funkcijām, tostarp viedajām durvju slēdzenēm, bērnu uzraudzības sistēmām un signalizācijas sistēmām, savienotajām rotaļlietām un personīgajām valkājamām veselības tehnoloģijām. Turklāt stingrākas atbilstības novērtēšanas procedūras, kas jāveic attiecībā uz citiem produktiem ar digitāliem elementiem, kuri šajā regulā klasificēti kā nozīmīgi vai kritiski svarīgi produkti ar digitāliem elementiem, palīdzēs novērst iespējamo negatīvo ietekmi uz patērētājiem, ko varētu radīt ievainojamību izmantošana.

(11) Šīs regulas mērķis ir nodrošināt augstu kiberdrošības līmeni produktiem ar digitāliem elementiem un to integrētas attālinātas datu apstrādes risinājumiem. Šādi attālinātas datu apstrādes risinājumi būtu jādefinē kā attālināta datu apstrāde, kurai programmatūru ir projektējis un izstrādājis attiecīgā produkta ar digitāliem elementiem ražotājs vai tas darīts tā vārdā un kuras neesamība liegtu produktam ar digitāliem elementiem pildīt kādu no savām funkcijām. Šī pieeja nodrošina, ka ražotāji šādus produktus pilnībā pienācīgi aizsargā neatkarīgi no tā, vai datus apstrādā vai glabā lokāli lietotāja ierīcē, vai arī ražotājs tos apstrādā vai glabā attālināti. Tajā pašā laikā apstrāde vai glabāšana attālināti ietilpst šīs regulas darbības jomā tikai tiktāl, ciktāl tas ir nepieciešams, lai produkts ar digitāliem elementiem varētu pildīt savas funkcijas. Šāda apstrāde vai attālināta glabāšana ietver situāciju, kad mobilajai lietojumprogrammai nepieciešama piekļuve lietojumprogrammas saskarnei vai datubāzei, ko nodrošina ar ražotāja izstrādāta pakalpojuma palīdzību. Šādā gadījumā pakalpojums ietilpst šīs regulas darbības jomā kā attālinātas datu apstrādes risinājums. Tāpēc prasības attiecībā uz attālinātas datu apstrādes risinājumiem, kas ietilpst šīs regulas darbības jomā, neietver tehniskus, operatīvus vai organizatoriskus pasākumus, kuru mērķis ir pārvaldīt ražotāja tīkla un informācijas sistēmu drošības riskus kopumā.

(12) Mākoņdatošanas risinājumi ir attālinātas datu apstrādes risinājumi šīs regulas nozīmē tikai tad, ja tie atbilst šajā regulā noteiktajai definīcijai. Piemēram, mākoņdatošanas iespējotas funkcijas, ko nodrošina viedo mājas ierīču ražotājs un kas ļauj lietotājiem kontrolēt ierīci no attāluma, ietilpst šīs regulas darbības jomā. No otras puses, šīs regulas darbības jomā neietilpst tīmekļa vietnes, kas neatbalsta produkta ar digitāliem elementiem funkcionalitāti, vai mākoņpakalpojumi, kas projektēti un izstrādāti ārpus produkta ar digitāliem elementiem ražotāja atbildības. Direktīva (ES) 2022/2555 attiecas uz mākoņdatošanas pakalpojumiem un mākoņdatošanas pakalpojumu modeļiem, piemēram, programmatūru kā pakalpojumu (SaaS), platformu kā pakalpojumu (PaaS) vai infrastruktūru kā pakalpojumu (IaaS). Vienības, kas sniedz mākoņdatošanas pakalpojumus Savienībā un kas saskaņā ar Komisijas Ieteikuma 2003/361/EK pielikuma 2. pantu uzskatāmas par vidējiem uzņēmumiem vai pārsniedz minētā panta 1. punktā noteiktās maksimālās robežas vidējiem uzņēmumiem, ietilpst minētās direktīvas darbības jomā.

(13) Rīkojoties saskaņā ar šīs regulas mērķi novērst šķēršļus produktu ar digitāliem elementiem brīvai apritei, aspektos, kurus aptver šī regula, dalībvalstīm nevajadzētu kavēt tādu produktu ar digitāliem elementiem pieejamību tirgū, kuri atbilst šai regulai. Tāpēc aspektos, kas tiek saskaņoti ar šo regulu, dalībvalstis nevar noteikt papildu kiberdrošības prasības attiecībā uz to, ka produktus ar digitāliem elementiem dara pieejamus tirgū. Tomēr jebkura publiska vai privāta vienība var noteikt papildu prasības līdzās šajā regulā noteiktajām prasībām attiecībā uz produktu ar digitāliem elementiem iepirkumu vai izmantošanu saviem konkrētajiem mērķiem un tādējādi var izvēlēties izmantot produktus ar digitāliem elementiem, kas atbilst stingrākām vai specifiskākām kiberdrošības prasībām nekā tās, kas piemērojamas nolūkā darīt tos pieejamus tirgū saskaņā ar šo regulu. Neskarot Eiropas Parlamenta un Padomes Direktīvas 2014/24/ES[7] un 2014/25/ES[8], dalībvalstīm, iepērkot produktus ar digitāliem elementiem, kuriem jāatbilst šajā regulā noteiktajām kiberdrošības pamatprasībām, tostarp tām, kas attiecas uz ievainojamību novēršanu, būtu jānodrošina, ka šādas prasības tiek ņemtas vērā iepirkuma procesā un ka tiek ņemta vērā arī ražotāju spēja efektīvi piemērot kiberdrošības pasākumus un pārvaldīt kiberdraudus.

---

7 Eiropas Parlamenta un Padomes Direktīva 2014/24/ES (2014. gada 26. februāris) par publisko iepirkumu un ar ko atceļ Direktīvu 2004/18/EK (OV L 94, 28.3.2014., 65. lpp.).

8 Eiropas Parlamenta un Padomes Direktīva 2014/25/ES (2014. gada 26. februāris) par iepirkumu, ko īsteno subjekti, kuri darbojas ūdensapgādes, enerģētikas, transporta un pasta pakalpojumu nozarēs, un ar ko atceļ Direktīvu 2004/17/EK (OV L 94, 28.3.2014., 243. lpp.).

Turklāt Direktīvā (ES) 2022/2555 ir noteikti kiberdrošības riska pārvaldības pasākumi minētās direktīvas 3. pantā minētām būtiskām un svarīgām vienībām, kas var ietvert piegādes ķēdes drošības pasākumus, kuri paredz, ka šādas vienības izmanto produktus ar digitāliem elementiem, kuri atbilst stingrākām kiberdrošības prasībām nekā šajā regulā noteiktās. Tāpēc saskaņā ar Direktīvu (ES) 2022/2555 un tajā paredzēto minimālās saskaņošanas principu dalībvalstis var noteikt papildu kiberdrošības prasības IKT produktu izmantošanai būtiskās vai svarīgās vienībās saskaņā ar minēto direktīvu, lai nodrošinātu augstāku kiberdrošības līmeni, ar nosacījumu, ka šādas prasības atbilst Savienības tiesību aktos noteiktajiem dalībvalstu pienākumiem. Jautājumi, uz kuriem šī regula neattiecas, var ietvert netehniskus faktorus, kas saistīti ar produktiem ar digitāliem elementiem un to ražotājiem. Tāpēc dalībvalstis, ņemot vērā netehniskus faktorus, var noteikt valsts pasākumus, tostarp ierobežojumus attiecībā uz produktiem ar digitāliem elementiem vai šādu produktu piegādātājiem. Valsts pasākumiem, kas saistīti ar šādiem faktoriem, ir jāatbilst Savienības tiesību aktiem.

(14) Šai regulai nevajadzētu skart dalībvalstu atbildību par valsts drošības aizsardzību saskaņā ar Savienības tiesību aktiem. Dalībvalstīm vajadzētu būt iespējai uz produktiem ar digitāliem elementiem, kurus iepērk vai izmanto valsts drošības vai aizsardzības vajadzībām, attiecināt papildu pasākumus ar noteikumu, ka šādi pasākumi ir saskaņā ar dalībvalstu pienākumiem, kas noteikti Savienības tiesību aktos.

(15) Šo regulu piemēro uzņēmējiem tikai attiecībā uz produktiem ar digitāliem elementiem, kas darīti pieejami tirgū, tātad, veicot komercdarbību, piegādāti izplatīšanai vai izmantošanai Savienības tirgū. Piegādei, veicot komercdarbību, var būt raksturīga ne tikai cenas noteikšana par produktu ar digitāliem elementiem, bet arī cenas noteikšana par tehniskā atbalsta pakalpojumiem, ja to ar nolūku izteikt naudas izteiksmē dara ne tikai faktisko izmaksu atgūšanai, piemēram, nodrošinot programmatūras platformu, ar kuras palīdzību ražotājs monetizē citus pakalpojumus, kā lietošanas nosacījumu izvirzot personas datu apstrādi tādu iemeslu dēļ, kas nav tikai programmatūras drošības, savietojamības vai sadarbspējas uzlabošana, vai pieņemot ziedojumus, kas pārsniedz uz produkta ar digitāliem elementiem projektēšanu, izstrādi un piegādi attiecināmās izmaksas. Ziedojumu pieņemšana bez nodoma gūt peļņu nebūtu jāuzskata par komercdarbību.

(16) Produkti ar digitāliem elementiem, kas tiek nodrošināti kā daļa no sniegta pakalpojuma, par kuru maksa tiek iekasēta tikai tādēļ, lai atgūtu faktiskās izmaksas, kas tieši saistītas ar minētā pakalpojuma sniegšanu, kā tas var būt dažu valsts pārvaldes struktūru nodrošinātu produktu ar digitāliem elementiem gadījumā, šā iemesla dēļ vien nebūtu jāuzskata par komercdarbību šīs regulas izpratnē. Turklāt produkti ar digitāliem elementiem, kurus valsts pārvaldes struktūra izstrādājusi vai modificējusi vienīgi savai lietošanai, nebūtu jāuzskata par tādiem, kas darīti pieejami tirgū šīs regulas izpratnē.

(17) Programmatūra un dati, kas ir atvērti koplietojami un kam lietotāji var brīvi piekļūt, izmantot, modificēt un tālāk izplatīt tos vai pārveidotas to versijas, var sekmēt pētniecību un inovācijas tirgū. Lai veicinātu brīvi pieejamas atvērtā pirmkoda programmatūras izstrādi un ieviešanu, jo īpaši attiecībā uz mikrouzņēmumiem un maziem un vidējiem uzņēmumiem, tostarp jaunuzņēmumiem, privātpersonām, bezpeļņas organizācijām un akadēmiskās pētniecības organizācijām, šīs regulas piemērošanā produktiem ar digitāliem elementiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra, ko piegādā izplatīšanai vai izmantošanai komercdarbības gaitā, būtu jāņem vērā saskaņā ar brīvi pieejamas atvērtā pirmkoda programmatūras licencēm izplatītās un izstrādātās programmatūras dažādu izstrādes modeļu raksturs.

(18) Brīvi pieejama atvērtā pirmkoda programmatūra ir programmatūra, kuras pirmkods ir atvērti koplietojams un kuras licencēšana paredz visas tiesības padarīt to brīvi pieejamu, lietojamu, modificējamu un tālāk izplatāmu. Brīvi pieejamu atvērtā pirmkoda programmatūru izstrādā, uztur un izplata atvērti, tostarp tiešsaistes platformās. Attiecībā uz uzņēmējiem, kas ietilpst šīs regulas darbības jomā, šīs regulas darbības jomā būtu jāiekļauj tikai tāda brīvi pieejama atvērtā pirmkoda programmatūra, kas darīta pieejama tirgū un tādējādi piegādāta izplatīšanai vai izmantošanai komercdarbības procesā. Tāpēc, nosakot šīs darbības komerciālo vai nekomerciālo raksturu, nevajadzētu ņemt vērā tikai apstākļus, kādos produkts ar digitāliem elementiem ir izstrādāts, vai to, kā šī izstrāde ir finansēta. Konkrētāk, lai panāktu skaidru nošķiršanu starp izstrādes un piegādes posmu, šajā regulā un attiecībā uz uzņēmējiem, kas ietilpst tās darbības jomā, par komercdarbību nebūtu jāuzskata tādu produktu ar digitāliem elementiem nodrošināšana, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra un kurus to ražotāji nemonetizē. Turklāt tādu produktu ar digitāliem elementiem piegāde, kas kvalificējami kā brīvi pieejamas atvērtā pirmkoda programmatūras komponenti, kuri paredzēti citiem ražotājiem integrēšanai to produktos ar digitāliem elementiem, būtu jāuzskata par darīšanu pieejamu tirgū tikai tad, ja šo komponentu sākotnējais ražotājs tos monetizējis. Piemēram, tas vien, ka atvērtā pirmkoda programmatūras produkts ar digitāliem elementiem saņem finansiālu atbalstu no ražotājiem vai ka ražotāji piedalās šāda produkta izstrādē, pats par sevi nenozīmē, ka darbība ir komerciāla rakstura.

Turklāt produkta regulārai izlaišanai pašai par sevi nevajadzētu būt pamatam secināt, ka produkts ar digitāliem elementiem tiek piegādāts komercdarbības procesā. Visbeidzot, šajā regulā bezpeļņas organizāciju veikta produktu ar digitāliem elementiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra, izstrāde nebūtu jāuzskata par komercdarbību, ja organizācija ir izveidota tā, lai nodrošinātu, ka visi ieņēmumi pēc izmaksu segšanas tiek izmantoti bezpeļņas mērķu sasniegšanai. Šī regula neattiecas uz fiziskām vai juridiskām personām, kas ar pirmkodu sniedz ieguldījumu produktos ar digitāliem elementiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra un par kuriem tās nav atbildīgas.

(19) Ņemot vērā to, cik svarīgi kiberdrošībai ir daudzi produkti ar digitāliem elementiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra, kura ir publicēta, bet nav darīta pieejama tirgū šīs regulas nozīmē, būtu jāpiemēro atvieglots un pielāgots regulatīvais režīms tām juridiskajām personām, kuras pastāvīgi atbalsta komercdarbībai paredzētu produktu izstrādi un kurām ir galvenā loma minēto produktu dzīvotspējas nodrošināšanā (atvērtā pirmkoda programmatūras pārziņi). Pie atvērtā pirmkoda programmatūras pārziņiem pieder noteikti fondi, kā arī vienības, kas izstrādā un publicē brīvi pieejamu atvērtā pirmkoda programmatūru uzņēmējdarbības kontekstā, tostarp bezpeļņas organizācijas. Regulatīvajā režīmā būtu jāņem vērā to īpašais raksturs un saderība ar uzlikto pienākumu veidu. Tam būtu jāattiecas tikai uz produktiem ar digitāliem elementiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra un kas galu galā ir paredzēti komerciālai darbībai, piemēram, integrēšanai komercpakalpojumos vai naudas izteiksmē izteiktos produktos ar digitāliem elementiem. Minētā regulatīvā režīma nolūkos nodoms integrēt naudas izteiksmē izteiktos produktos ar digitāliem elementiem ietver gadījumus, kad ražotāji, kas kādu komponentu integrē savos produktos ar digitāliem elementiem, vai nu regulāri piedalās minētā komponenta izstrādē, vai sniedz regulāru finansiālu palīdzību ar mērķi nodrošināt programmatūras produkta nepārtrauktību. Pastāvīga atbalsta sniegšana produkta ar digitāliem elementiem izstrādei ietver, bet neaprobežojas ar programmatūras izstrādes sadarbības platformu mitināšanu un pārvaldību, pirmkoda vai programmatūras mitināšanu, produktu ar digitāliem elementiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra, pārvaldību vai vadību, kā arī šādu produktu izstrādes vadību. Ņemot vērā to, ka atvieglotajā un pielāgotajā regulatīvajā režīmā vienībām, kas darbojas kā atvērtā pirmkoda programmatūras pārziņi, nav noteikti tādi paši pienākumi kā ražotājiem saskaņā ar šo regulu, tiem nebūtu jāļauj uzlikt CE zīmi produktiem ar digitāliem elementiem, kuru izstrādi tie atbalsta.

(20) Produktu ar digitāliem elementiem mitināšana atvērtos repozitorijos, tostarp izmantojot pakotņu pārvaldītājus vai sadarbības platformas, pati par sevi nav uzskatāma par produkta ar digitāliem elementiem darīšanu pieejamu tirgū. Šādu pakalpojumu sniedzēji būtu jāuzskata par izplatītājiem tikai tad, ja tie šādu programmatūru dara pieejamu tirgū un tādējādi piegādā to izplatīšanai vai izmantošanai Savienības tirgū, veicot komercdarbību.

(21) Lai atbalstītu un atvieglotu to ražotāju pienācīgas rūpības pienākuma veikšanu, kuri savos produktos ar digitāliem elementiem integrē brīvi pieejamas atvērtā pirmkoda programmatūras komponentus, uz kuriem neattiecas šajā regulā noteiktās kiberdrošības pamatprasības, Komisijai vajadzētu būt iespējai izveidot brīvprātīgas drošības atestācijas programmas vai nu ar deleģēto aktu, ar ko papildina šo regulu, vai pieprasot Eiropas kiberdrošības sertifikācijas shēmu saskaņā ar Regulas (ES) 2019/881 48. pantu, kurā ņemtas vērā brīvi pieejamas atvērtā pirmkoda programmatūras izstrādes modeļu īpatnības. Drošības atestācijas programmas būtu jāveido tā, lai ne tikai fiziskas vai juridiskas personas, kas izstrādā vai palīdz izstrādāt produktu ar digitāliem elementiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra, bet arī trešās personas, piemēram, ražotāji, kas integrē šādus produktus savos produktos ar digitāliem elementiem, lietotāji vai Savienības un valstu publiskās pārvaldes iestādes, varētu ierosināt vai finansēt drošības atestāciju.

(22) Ņemot vērā šīs regulas publiskos kiberdrošības mērķus un ar mērķi uzlabot dalībvalstu informētību par situāciju attiecībā uz Savienības atkarību no programmatūras komponentiem un jo īpaši par potenciāli brīvi pieejamiem atvērtā pirmkoda programmatūras komponentiem, ar šo regulu izveidotajai īpašajai administratīvās sadarbības grupai (*ADCO*) vajadzētu būt iespējai pieņemt lēmumu kopīgi veikt Savienības atkarības novērtējumu. Tirgus uzraudzības iestādēm vajadzētu būt iespējai pieprasīt, lai to kategoriju produktu ražotāji, kuriem ir *ADCO* noteiktie digitālie elementi, iesniegtu programmatūras materiālu komplektus (*SBOM*), ko tie ir sagatavojuši saskaņā ar šo regulu. Lai aizsargātu *SBOM* konfidencialitāti, tirgus uzraudzības iestādēm attiecīgā informācija par atkarību būtu jāiesniedz *ADCO* anonimizētā un apkopotā veidā.

(23) Šīs regulas īstenošanas efektivitāte būs atkarīga arī no atbilstošu kiberdrošības prasmju pieejamības. Savienības līmenī dažādos programmatiskos un politiskos dokumentos, tostarp Komisijas 2023. gada 18. aprīļa paziņojumā "Kiberdrošības talantu deficīta pārvarēšana ES konkurētspējas, izaugsmes un noturības vairošanai" un Padomes 2023. gada 22. maija secinājumos par ES kiberaizsardzības politiku ir atzīts kiberdrošības prasmju trūkums Savienībā un nepieciešamība prioritārā kārtā risināt šādas problēmas gan publiskajā, gan privātajā sektorā. Lai panāktu šīs regulas efektīvu īstenošanu, dalībvalstīm būtu jānodrošina, ka tirgus uzraudzības iestādēm un atbilstības novērtēšanas struktūrām ir pieejami pietiekami resursi pienācīgam nodrošinājumam ar darbiniekiem savu uzdevumu veikšanai, kā noteikts šajā regulā. Minētajiem pasākumiem būtu jāveicina darbaspēka mobilitāte kiberdrošības jomā un ar to saistītās karjeras iespējas. Tiem būtu arī jāpalīdz padarīt kiberdrošības darbaspēku noturīgāku un iekļaujošāku, arī dzimumu līdztiesības ziņā. Tāpēc dalībvalstīm būtu jāveic pasākumi ar mērķi panākt, ka minētos uzdevumus veic atbilstoši apmācīti speciālisti, kuriem ir nepieciešamās kiberdrošības prasmes. Tāpat ražotājiem būtu jānodrošina, ka viņu darbiniekiem ir nepieciešamās prasmes savu pienākumu izpildei, kā noteikts šajā regulā. Dalībvalstīm un Komisijai saskaņā ar savām prerogatīvām, kompetencēm un konkrētajiem uzdevumiem, kas tām uzticēti ar šo regulu, būtu jāveic pasākumi ražotāju un jo īpaši mikrouzņēmumu un mazo un vidējo uzņēmumu, tostarp jaunuzņēmumu, atbalstam, arī tādās jomās kā prasmju attīstība, lai tie varētu izpildīt savus pienākumus, ka noteikts šajā regulā. Turklāt, tā kā Direktīvā (ES) 2022/2555 ir noteikts, ka dalībvalstīm kā daļa no valsts kiberdrošības stratēģijām ir jāpieņem politika, kas veicina un attīsta apmācību kiberdrošības un kiberdrošības prasmju jomā, dalībvalstis, pieņemot šādas stratēģijas, var arī apsvērt iespēju pievērsties arī no šīs regulas izrietošajām kiberdrošības prasmju vajadzībām, tostarp saistībā ar pārkvalificēšanos un prasmju pilnveidi.

(24) Drošs internets ir neaizstājams kritiski svarīgās infrastruktūras darbībai un sabiedrībai kopumā. Direktīvas (ES) 2022/2555 mērķis ir nodrošināt augstu kiberdrošības līmeni pakalpojumiem, ko sniedz būtiskas un svarīgas vienības, kā norādīts minētās direktīvas 3. pantā, to vidū digitālās infrastruktūras nodrošinātāji, kuri atbalsta atvērtā interneta pamatfunkcijas, nodrošina piekļuvi internetam un sniedz interneta pakalpojumus. Tāpēc ir svarīgi, lai produkti ar digitāliem elementiem, kas digitālās infrastruktūras nodrošinātājiem ir nepieciešami, lai nodrošinātu interneta darbību, tiktu izstrādāti drošā veidā un lai tie atbilstu vispāratzītiem interneta drošības standartiem. Šīs regulas, kas attiecas uz visiem savienojamiem aparatūras un programmatūras produktiem, mērķis ir arī sekmēt digitālās infrastruktūras nodrošinātāju atbilstību piegādes ķēdes prasībām saskaņā ar Direktīvu (ES) 2022/2555, nodrošinot, ka produkti ar digitāliem elementiem, ko tie izmanto savu pakalpojumu sniegšanai, tiek izstrādāti drošā veidā un ka tiem ir piekļuve šādu produktu savlaicīgiem drošības atjauninājumiem.

(25) Eiropas Parlamenta un Padomes Regulā (ES) 2017/745[9] ir paredzēti noteikumi par medicīniskajām ierīcēm, un Eiropas Parlamenta un Padomes Regulā (ES) 2017/746[10] – par *in vitro* diagnostikas medicīniskajām ierīcēm. Šīs regulas pievēršas kiberdrošības riskiem un izmanto konkrētas pieejas, kas ir izskatītas arī šajā regulā. Konkrētāk, Regulā (ES) 2017/745 un Regulā (ES) 2017/746 ir noteiktas pamatprasības attiecībā uz medicīniskajām ierīcēm, kuras darbojas ar elektroniskas sistēmas starpniecību vai kuras pašas ir programmatūra. Minētās regulas attiecas arī uz noteiktu neiegulto programmatūru un visa aprites cikla pieeju. Šīs prasības nosaka, ka ražotājiem jāizstrādā un jāveido savi produkti, piemērojot riska pārvaldības principus un nosakot prasības attiecībā uz IT drošības pasākumiem, kā arī attiecīgas atbilstības novērtēšanas procedūras. Turklāt kopš 2019. gada decembra ir spēkā īpaši norādījumi par medicīnisko ierīču kiberdrošību, kuros medicīnisko ierīču, ieskaitot *in vitro* diagnostikas ierīces, ražotājiem ir sniegti norādījumi par to, kā izpildīt visas attiecīgās minēto regulu I pielikumā noteiktās pamatprasības attiecībā uz kiberdrošību. Tāpēc šai regulai nebūtu jāattiecas uz produktiem ar digitāliem elementiem, kam piemēro kādu no minētajām regulām.

---

[9] Eiropas Parlamenta un Padomes Regula (ES) 2017/745 (2017. gada 5. aprīlis), kas attiecas uz medicīniskām ierīcēm, ar ko groza Direktīvu 2001/83/EK, Regulu (EK) Nr. 178/2002 un Regulu (EK) Nr. 1223/2009 un atceļ Padomes Direktīvas 90/385/EEK un 93/42/EEK (OV L 117, 5.5.2017., 1. lpp.).

[10] Eiropas Parlamenta un Padomes Regula (ES) 2017/746 (2017. gada 5. aprīlis) par *in vitro* diagnostikas medicīniskām ierīcēm un ar ko atceļ Direktīvu 98/79/EK un Komisijas Lēmumu 2010/227/ES (OV L 117, 5.5.2017., 176. lpp.).

(26) Šī regula neattiecas uz produktiem ar digitāliem elementiem, kas izstrādāti vai modificēti tikai valsts drošības vai aizsardzības vajadzībām, vai produktiem, kas īpaši projektēti klasificētas informācijas apstrādei. Dalībvalstis tiek aicinātas nodrošināt šiem produktiem tādu pašu vai augstāku aizsardzības līmeni kā produktiem, uz kuriem attiecas šī regula.

(27) Eiropas Parlamenta un Padomes Regulā (ES) 2019/2144[11] ir noteiktas prasības transportlīdzekļu un to sistēmu un komponentu tipa apstiprināšanai, ieviešot konkrētas kiberdrošības prasības, arī attiecībā uz sertificētas kiberdrošības pārvaldības sistēmas darbību, programmatūras atjauninājumiem, ietverot organizāciju politiku un procesus attiecībā uz kiberdrošības riskiem, kas saistīti ar transportlīdzekļu, iekārtu un pakalpojumu visu aprites ciklu, saskaņā ar piemērojamajiem Apvienoto Nāciju Organizācijas noteikumiem par tehniskajām specifikācijām un kiberdrošību, jo īpaši ANO Noteikumiem Nr. 155 jeb Vienotajiem noteikumiem par transportlīdzekļu apstiprināšanu attiecībā uz kiberdrošību un kiberdrošības pārvaldības sistēmu, un paredzot īpašas atbilstības novērtēšanas procedūras.

---

11 Eiropas Parlamenta un Padomes Regula (ES) 2019/2144 (2019. gada 27. novembris) par prasībām mehānisko transportlīdzekļu un to piekabju un šiem transportlīdzekļiem paredzētu sistēmu, sastāvdaļu un atsevišķu tehnisko vienību tipa apstiprināšanai attiecībā uz to vispārīgo drošību un transportlīdzekļa braucēju un neaizsargāto ceļu satiksmes dalībnieku aizsardzību, ar ko groza Eiropas Parlamenta un Padomes Regulu (ES) 2018/858 un atceļ Eiropas Parlamenta un Padomes Regulas (EK) Nr. 78/2009, (EK) Nr. 79/2009 un (EK) Nr. 661/2009 un Komisijas Regulas (EK) Nr. 631/2009, (ES) Nr. 406/2010, (ES) Nr. 672/2010, (ES) Nr. 1003/2010, (ES) Nr. 1005/2010, (ES) Nr. 1008/2010, (ES) Nr. 1009/2010, (ES) Nr. 19/2011, (ES) Nr. 109/2011, (ES) Nr. 458/2011, (ES) Nr. 65/2012, (ES) Nr. 130/2012, (ES) Nr. 347/2012, (ES) Nr. 351/2012, (ES) Nr. 1230/2012 un (ES) 2015/166 (OV L 325, 16.12.2019., 1. lpp.).

Aviācijas jomā Eiropas Parlamenta un Padomes Regulas (ES) 2018/1139[12] galvenais mērķis ir izveidot un uzturēt vienādi augstu civilās aviācijas drošības līmeni Savienībā. Ar to izveido pamatprasību sistēmu attiecībā uz lidojumderīgumu aeronavigācijas produktiem, daļām un ierīcēm, ieskaitot programmatūru, kurā iekļauti pienākumi aizsargāt pret informācijas drošības apdraudējumiem. Saskaņā ar Regulu (EU) 2018/1139 noteiktais sertifikācijas process nodrošina tādu uzticamības līmeni, kas atbilst šīs regulas mērķim. Tāpēc uz produktiem ar digitāliem elementiem, kam piemēro Regulu (ES) 2019/2144, un uz produktiem, kas sertificēti saskaņā ar Regulu (ES) 2018/1139, nebūtu jāattiecas šajā regulā noteiktajām kiberdrošības pamatprasībām un atbilstības novērtēšanas procedūrām.

[12] Eiropas Parlamenta un Padomes Regula (ES) 2018/1139 (2018. gada 4. jūlijs) par kopīgiem noteikumiem civilās aviācijas jomā un ar ko izveido Eiropas Savienības Aviācijas drošības aģentūru, un ar ko groza Eiropas Parlamenta un Padomes regulas (EK) Nr. 2111/2005, (EK) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 un direktīvas 2014/30/ES un 2014/53/ES un atceļ Eiropas Parlamenta un Padomes regulas (EK) Nr. 552/2004 un (EK) Nr. 216/2008 un Padomes Regulu (EEK) Nr. 3922/91 (OV L 212, 22.8.2018., 1. lpp.).

(28) Šajā regulā ir noteikti horizontālie kiberdrošības noteikumi, kas nav paredzēti konkrētām nozarēm vai konkrētiem produktiem ar digitāliem elementiem. Tomēr noteiktām nozarēm vai konkrētiem produktiem paredzētus Savienības noteikumus būtu iespējams ieviest, nosakot prasības, kuras piemēro visiem vai dažiem riskiem, uz kuriem attiecas šajā regulā noteiktās kiberdrošības pamatprasības. Šādos gadījumos šīs regulas piemērošanu produktiem ar digitāliem elementiem, kas ietverti citos Savienības noteikumos, kuros ir noteiktas visiem vai dažiem tiem riskiem piemērojamas prasības, uz kuriem attiecas šajā regulā noteiktās kiberdrošības pamatprasības, var ierobežot vai izslēgt, ja šāds ierobežojums vai izslēgšana atbilst vispārējam tiesiskajam regulējumam, ko piemēro minētajiem produktiem, un ja nozares noteikumi nodrošina vismaz tādu pašu aizsardzības līmeni, kāds paredzēts šajā regulā. Komisija būtu jāpilnvaro pieņemt deleģētos aktus, lai papildinātu šo regulu, identificējot šādus produktus un noteikumus. Attiecībā uz spēkā esošajiem Savienības tiesību aktiem, kuros būtu jāpiemēro šādi ierobežojumi vai izslēgšana, šajā regulā ir ietverti īpaši noteikumi, lai precizētu tās saistību ar minētajiem Savienības tiesību aktiem.

(29) Lai nodrošinātu, ka produktus ar digitāliem elementiem, kas darīti pieejami tirgū, var efektīvi remontēt un pagarināt to ilgizturību, būtu jāparedz izņēmums attiecībā uz rezerves daļām. Minētajam izņēmumam būtu jāattiecas gan uz tādām rezerves daļām, kas paredzētas senāku produktu remontam, kuri darīti pieejami pirms šīs regulas piemērošanas dienas, gan uz tādām rezerves daļām, kurām jau ir veikta atbilstības novērtēšanas procedūra saskaņā ar šo regulu.

(30) Komisijas Deleģētajā regulā (ES) 2022/30[13] ir norādīts, ka virkne Eiropas Parlamenta un Padomes Direktīvas 2014/53/ES[14] 3. panta 3. punkta d), e) un f) apakšpunktā noteikto pamatprasību, kas attiecas uz kaitējumu tīklam un tīkla resursu pārmērīgu izmantošanu, personas datiem un privātumu un krāpšanu, piemēro noteiktām radioiekārtām. Komisijas Īstenošanas lēmumā C(2022)5637 (2022. gada 5. augusts) par standartizācijas pieprasījumu Eiropas Standartizācijas komitejai un Eiropas Elektrotehnikas standartizācijas komitejai ir noteiktas prasības īpašu standartu izstrādei, papildus precizējot, kā šīs trīs pamatprasības būtu jārisina. Šajā regulā noteiktās kiberdrošības pamatprasības ietver visus Direktīvas 2014/53/ES 3. panta 3. punkta d), e) un f) apakšpunktā minēto pamatprasību elementus. Turklāt šajā regulā noteiktās kiberdrošības pamatprasības ir saskaņotas ar minētajā standartizācijas pieprasījumā iekļauto īpašo standartu prasību mērķiem. Tāpēc gadījumā, kad Komisija atceļ vai groza Deleģēto regulu (ES) 2022/30, kā rezultātā tā vairs nav piemērojama noteiktiem produktiem, uz kuriem attiecas šī regula, Komisijai un Eiropas standartizācijas organizācijām būtu jāņem vērā standartizācijas darbs, kas veikts saistībā ar Īstenošanas lēmumu C(2022)5637, saskaņoto standartu sagatavošanā un izstrādē ar mērķi sekmēt šīs regulas īstenošanu. Šīs regulas piemērošanai noteiktā pārejas periodā Komisijai būtu jāsniedz norādījumi ražotājiem, uz kuriem attiecas šī regula un arī Deleģētā regula (ES) 2022/30, lai sekmētu pierādīšanu par atbilstību abām regulām.

---

[13] Komisijas Deleģētā regula (ES) 2022/30 (2021. gada 29. oktobris), kas papildina Eiropas Parlamenta un Padomes Direktīvu 2014/53/ES attiecībā uz minētās direktīvas 3. panta 3. punkta pirmās daļas d), e) un f) punktā norādīto pamatprasību piemērošanu (OV L 7, 12.1.2022., 6. lpp.).

[14] Eiropas Parlamenta un Padomes Direktīva 2014/53/ES (2014. gada 16. aprīlis) par dalībvalstu tiesību aktu saskaņošanu attiecībā uz radioiekārtu pieejamību tirgū un ar ko atceļ Direktīvu 1999/5/EK (OV L 153, 22.5.2014., 62. lpp.).

(31) Eiropas Parlamenta un Padomes Direktīva (ES) 2024/...[15+] papildina šo regulu. Minētajā direktīvā ir paredzēti noteikumi par atbildību attiecībā uz produktiem ar trūkumiem, lai aizskartās personas varētu pieprasīt kompensāciju, ja kaitējumu ir izraisījuši produkti ar trūkumiem. Tajā ir noteikts princips, saskaņā ar kuru produkta ražotājs neatkarīgi no vainas ir atbildīgs par kaitējumu, ko izraisījis viņa produkta drošuma trūkums ("stingrā atbildība"). Ja šāds drošības trūkums izpaužas kā drošības atjauninājumu trūkums pēc produkta laišanas tirgū un tas rada kaitējumu, varētu iestāties ražotāja atbildība. Šajā regulā būtu jānosaka ražotāju pienākumi, kas attiecas uz šādu drošības atjauninājumu nodrošināšanu.

---

15 Eiropas Parlamenta un Padomes Direktīva (ES) .../... (... gada ...) ... par... (OV ..., ELI: ...).

+ OV: lūgums ievietot tekstā dokumentā (2022/0302(COD)) ietvertās direktīvas numuru un zemsvītras piezīmē ievietot minētās direktīvas numuru, datumu, nosaukumu un OV publikācijas atsauci.

(32) Šai regulai nebūtu jāskar Eiropas Parlamenta un Padomes Regula (ES) 2016/679[16], ieskaitot noteikumus, kas attiecas uz datu aizsardzības sertifikācijas mehānismu ieviešanu un datu aizsardzības zīmogiem un marķējumu, kam uzskatāmi jāparāda datu pārziņu un apstrādātāju veikto apstrādes darbību atbilstība minētajai regulai. Šādas darbības varētu iestrādāt produktā ar digitāliem elementiem. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, kā arī kiberdrošība kopumā ir Regulas (ES) 2016/679 galvenie elementi. Aizsargājot patērētājus un organizācijas no kiberdrošības riskiem, šajā regulā noteiktajām kiberdrošības pamatprasībām ir arī jāpalīdz uzlabot personas datu un personu privātuma aizsardzību. Būtu jāapsver sinerģija gan standartizācijas, gan sertifikācijas jomā attiecībā uz kiberdrošības aspektiem, kurā izmantotu sadarbību starp Komisiju, Eiropas standartizācijas organizācijām, Eiropas Savienības Kiberdrošības aģentūru (*ENISA*), ar Regulu (ES) 2016/679 izveidoto Eiropas Datu aizsardzības kolēģiju un valstu datu aizsardzības uzraudzības iestādēm. Sinerģija starp šo regulu un Savienības datu aizsardzības tiesību aktiem būtu jāizveido arī tirgus uzraudzības un izpildes panākšanas jomā. Šajā nolūkā atbilstīgi šai regulai izraudzītajām valstu tirgus uzraudzības iestādēm būtu jāsadarbojas ar iestādēm, kuras uzrauga Savienības datu aizsardzības tiesību aktu piemērošanu. Tām vajadzētu būt arī piekļuvei informācijai, kas ir būtiska tām paredzēto uzdevumu veikšanai.

---

16 Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

(33) Eiropas digitālās identitātes maku nodrošinātājiem, kas minēti Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014[17] 5.a panta 2. punktā, ciktāl to produkti ietilpst šīs regulas darbības jomā, būtu jāievēro gan šajā regulā noteiktās horizontālās kiberdrošības pamatprasības, gan īpašās drošības prasības, kas noteiktās Regulas (ES) Nr. 910/2014 5.a pantā. Lai sekmētu atbilstību, maku nodrošinātājiem būtu jāspēj pierādīt Eiropas digitālās identitātes maku atbilstību attiecīgi šajā regulā un Regulā (ES) Nr. 910/2014 noteiktajām prasībām, sertificējot savus produktus saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu, kas izveidota atbilstīgi Regulai (ES) 2019/881 un attiecībā uz kuru Komisija, izmantojot deleģētos aktus, ir precizējusi pieņēmumu par atbilstību šai regulai, ciktāl sertifikāts vai tā daļas attiecas uz minētajām prasībām.

[17] Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK (OV L 257, 28.8.2014., 73. lpp.).

(34) Projektēšanas un izstrādes posmā integrējot no trešām personām iegūtus komponentus produktos ar digitāliem elementiem, ražotājiem, lai nodrošinātu, ka produkti tiek projektēti, izstrādāti un ražoti saskaņā ar šajā regulā noteiktajām kiberdrošības pamatprasībām, būtu jāievēro pienācīgas rūpības pienākums attiecībā uz minētajiem komponentiem, tostarp brīvi pieejamas atvērtā pirmkoda programmatūras komponentiem, kas nav darīti pieejami tirgū. Atbilstošais pienācīgas rūpības pienākuma līmenis ir atkarīgs no kiberriska veida un līmeņa, kas saistīts ar komponentu, un šajā nolūkā būtu jāņem vērā viena vai vairākas no turpmāk minētajām darbībām: attiecīgā gadījumā verificējot, vai komponenta ražotājs ir pierādījis atbilstību šai regulai, tostarp pārbaudot, vai sastāvdaļai jau ir CE zīme; verificējot, vai komponents regulāri saņem drošības atjauninājumus, piemēram, kontrolējot tā drošības atjauninājumu vēsturi; verificējot, vai komponentam nav kāda no ievainojamībām, kas reģistrētas saskaņā ar Direktīvas (ES) 2022/2555 12. panta 2. punktu izveidotajā Eiropas ievainojamību datubāzē vai citās publiski pieejamās ievainojamību datubāzēs, vai veicot papildu drošības testus. Šajā regulā noteiktie ievainojamības novēršanas pienākumi, kas ražotājiem jāievēro, laižot tirgū produktu ar digitāliem elementiem, un arī atbalsta periodā, attiecas uz produktiem ar digitāliem elementiem kopumā, tostarp uz visiem integrētajiem komponentiem. Ja, īstenojot pienācīgas rūpības pienākumu, produkta ar digitāliem elementiem ražotājs konstatē ievainojamību komponentā, tostarp brīvi pieejama atvērtā pirmkoda komponentā, tam būtu jāinformē persona vai vienība, kas ražo vai uztur komponentu, jāpievēršas ievainojamībai un tā jānovērš un attiecīgā gadījumā jāsniedz personai vai vienībai drošības risinājums, kas ticis piemērots.

(35) Tūlīt pēc šīs regulas piemērošana noteiktā pārejas perioda beigām ražotājs, kas izgatavo produktu ar digitāliem elementiem, kurā ir integrēts viens vai vairāki komponenti, kas iegūti no trešām personām, uz kurām arī attiecas šī regula, var nespēt pienācīgas rūpības pienākuma īstenošanā, piemēram, pārbaudot, vai komponentiem jau ir CE zīme, verificēt, vai minēto komponentu ražotāji ir pierādījuši atbilstību šai regulai. Tas var notikt, ja komponenti ir integrēti vēl pirms šo regulu sāk piemērot šo komponentu ražotājiem. Šādā gadījumā ražotājam, kas integrē šādus komponentus, pienācīgas rūpības pienākums jāīsteno ar citiem līdzekļiem.

(36) Produkti ar digitāliem elementiem būtu jāmarķē ar CE zīmi, kas redzami, salasāmi un neizdzēšami norādītu uz to atbilstību šai regulai, lai tos varētu laist brīvā apritē iekšējā tirgū. Dalībvalstīm nebūtu jārada nepamatoti šķēršļi tādu produktu ar digitāliem elementiem laišanai tirgū, kas atbilst šajā regulā noteiktajām prasībām un ir marķēti ar CE zīmi. Turklāt tirdzniecības gadatirgos, izstādēs un demonstrācijās vai līdzīgos pasākumos dalībvalstīm nebūtu jāaizliedz tāda produkta ar digitāliem elementiem, kas neatbilst šai regulai, tostarp to prototipu, prezentācija vai izmantošana, ar noteikumu, ka uz produkta ir redzama zīme, kas skaidri norāda, ka produkts neatbilst šai regulai un ka to nedrīkst darīt pieejamu tirgū, kamēr tas neatbilst šai regulai.

(37) Lai nodrošinātu, ka ražotāji pirms savu produktu ar digitāliem elementiem atbilstības novērtēšanas var izlaist programmatūru testēšanas vajadzībām, dalībvalstīm nevajadzētu liegt darīt pieejamu nepabeigtu programmatūru, piemēram, alfa versijas, beta versijas vai izlaišanas kandidātus, ar nosacījumu, ka nepabeigta programmatūra ir pieejama tikai uz laiku, kas nepieciešams tās testēšanai un atsauksmju saņemšanai. Ražotājiem būtu jānodrošina, ka programmatūra, kas darīta pieejama saskaņā ar šiem nosacījumiem, tiek izlaista tikai pēc riska novērtējuma un ka tā, ciktāl iespējams, atbilst šajā regulā noteiktajām drošības prasībām attiecībā uz produktu ar digitāliem elementiem īpašībām. Ražotājiem pēc iespējas būtu jāīsteno arī ievainojamību novēršanas prasības. Ražotājiem nevajadzētu piespiest lietotājus veikt jaunin--šanu uz versijām, kas ir izlaistas tikai testēšanas vajadzībām.

(38) Lai nodrošinātu, ka, laižot tirgū produktus ar digitāliem elementiem, tie nerada kiberdrošības riskus personām un organizācijām, šādiem produktiem būtu jānosaka kiberdrošības pamatprasības. Šīs kiberdrošības pamatprasības, tostarp ievainojamības pārvaldības prasības, piemēro katram atsevišķam produktam ar digitāliem elementiem, kad to laiž tirgū, neatkarīgi no tā, vai produkts ar digitāliem elementiem tiek ražots kā atsevišķa vienība vai sērijveidā. Piemēram, attiecībā uz produkta tipu katram atsevišķam produktam ar digitāliem elementiem, kad tas tiek laists tirgū, būtu jāsaņem visi pieejamie drošības labojumi vai atjauninājumi ar mērķi risināt attiecīgās drošības problēmas. Ja šādi produkti ar digitāliem elementiem pēc tam ar fiziskiem vai digitāliem līdzekļiem tiek modificēti tā, kā ražotājs nav paredzējis sākotnējā riska novērtējumā, un tas varētu nozīmēt, ka tie vairs neatbilst attiecīgajām kiberdrošības pamatprasībām, modifikācija būtu jāuzskata par būtisku. Piemēram, remontu varētu pielīdzināt uzturēšanas darbībām ar noteikumu, ka tie nemodificē jau tirgū laistu produktu ar digitāliem elementiem tā, ka var tikt ietekmēta atbilstība piemērojamajām prasībām, vai ka var tikt mainīts paredzētais nolūks, attiecībā uz kuru produkts ir izvērtēts.

(39) Tāpat kā fizisku remontu vai modifikāciju gadījumā, arī produkts ar digitāliem elementiem būtu jāuzskata par būtiski modificētu ar programmatūras izmaiņām, ja programmatūras atjauninājums modificē produkta paredzēto nolūku un ražotājs šīs izmaiņas nav paredzējis sākotnējā riska novērtējumā vai ja programmatūras atjauninājuma dēļ ir mainījies apdraudējuma raksturs vai palielinājies kiberdrošības riska līmenis, un atjauninātā produkta versija ir darīta pieejama tirgū. Ja drošības atjauninājums, kura mērķis ir samazināt produkta ar digitāliem elementiem kiberdrošības riska līmeni, nemodificē produkta ar digitāliem elementiem paredzēto nolūku, tas netiek uzskatīts par būtisku modifikāciju. Tas parasti attiecas uz situācijām, kad drošības atjauninājumi ietver tikai nelielas pirmkoda korekcijas. Piemēram, tas varētu būt gadījums, kad ar drošības atjauninājumu tiek novērsta zināma ievainojamība, tostarp tiek modificētas produkta ar digitāliem elementiem funkcijas vai veiktspēja tikai ar mērķi samazināt kiberdrošības riska līmeni. Tāpat arī nelielu funkcionalitātes atjauninājumu, piemēram, vizuālu uzlabojumu vai jaunu piktogrammu vai valodu pievienošanu lietotāja saskarnei lietotāja saskarnei, parasti nebūtu jāuzskata par būtisku modifikāciju. Turpretī, ja elementu atjauninājums modificē sākotnēji paredzētās funkcijas vai produkta ar digitāliem elementiem veidu vai veiktspēju un atbilst iepriekš minētajiem kritērijiem, tas būtu jāuzskata par būtisku modifikāciju, jo jaunu elementu pievienošana parasti rada plašāku uzbrukuma virsmu, tādējādi palielinot kiberdrošības risku. Piemēram, tas varētu būt gadījums, kad lietojumprogrammai tiek pievienots jauns ievades elements, tāpēc ražotājam ir jānodrošina atbilstoša ievades validācija. Novērtējot, vai elementa atjauninājums ir uzskatāms par būtisku modifikāciju, nav svarīgi, vai tas tiek sniegts kā atsevišķs atjauninājums vai kopā ar drošības atjauninājumu. Komisijai būtu jāizdod norādījumi par to, kā noteikt, kas ir būtiska modifikācija.

(40) Ņemot vērā programmatūras izstrādes iteratīvo raksturu, ražotājiem, kuri ir laiduši tirgū programmatūras produkta turpmākās versijas vēlāku šā produkta būtiskas modifikācijas rezultātā, atbalsta periodā būtu jāspēj nodrošināt drošības atjauninājumus tikai tai programmatūras produkta versijai, kuru tie laiduši tirgū pēdējo. Tiem vajadzētu būt iespējai to darīt tikai tad, ja attiecīgo iepriekšējo produkta versiju lietotājiem bez maksas ir pieejama pēdējā tirgū laistā produkta versija un viņiem nerodas papildu izmaksas, lai pielāgotu aparatūras vai programmatūras vidi, kurā viņi izmanto produktu. Tas varētu būt, piemēram, gadījums, kad datora operētājsistēmas atjaunināšanai nav vajadzīga jauna aparatūra, piemēram, ātrāks centrālais procesors vai lielāka atmiņa. Tomēr atbalsta periodā ražotājam būtu jāturpina ievērot citas ievainojamības novēršanas prasības, piemēram, jāievieš politika koordinētai ievainojamības atklāšanai vai pasākumi, kas sekmē informācijas apmaiņu par iespējamām ievainojamībām attiecībā uz visām turpmākajām būtiski modificētajām programmatūras produkta versijām, kas laistas tirgū. Ražotājiem vajadzētu būt iespējai sniegt nelielus drošības vai funkcionalitātes atjauninājumus, kas nav būtiskas modifikācijas, tikai attiecībā uz programmatūras produkta jaunāko versiju vai apakšversiju, kas nav būtiski modificēta. Tajā pašā laikā, ja aparatūras produkts, piemēram, viedtālrunis, nav savietojams ar tās operētājsistēmas jaunāko versiju, ar kuru tas sākotnēji piegādāts, ražotājam atbalsta periodā būtu jāturpina nodrošināt drošības atjauninājumus vismaz jaunākajai saderīgajai operētājsistēmas versijai.

(41) Saskaņā ar vispāratzīto jēdzienu par produktu būtisku modifikāciju, ko reglamentē Savienības saskaņošanas tiesību akti, ikreiz, kad notiek būtiska modifikācija, kas var ietekmēt produkta ar digitāliem elementiem atbilstību šai regulai, vai ja mainās minētā produkta paredzētais nolūks, ir lietderīgi pārbaudīt produkta ar digitāliem elementiem atbilstību un attiecīgā gadījumā veikt jaunu atbilstības novērtēšanu. Attiecīgā gadījumā, ja ražotājs veic atbilstības novērtēšanu, kurā tiek iesaistīta trešā persona, par izmaiņām, kas varētu izraisīt būtisku modifikāciju, būtu jāinformē trešā persona.

(42) Ja uz produktu ar digitāliem elementiem attiecas "atjaunošana", "uzturēšana" un "remontēšana", kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2024/1781[18] 2. panta 18., 19. un 20. punktā, tad tas ne vienmēr izraisa produkta būtisku modifikāciju, piemēram, ja paredzētais lietojums un funkcijas netiek mainītas un netiek ietekmēts riska līmenis. Tomēr ražotāja veikta produkta jaunināšana varētu izraisīt izmaiņas produkta projektēšanā un izstrādē un tādējādi varētu ietekmēt produkta paredzēto nolūku un atbilstību šajā regulā noteiktajām prasībām. Tomēr ražotāja veikta produkta ar digitāliem elementiem jaunināšana varētu izraisīt izmaiņas produkta projektēšanā un izstrādē un tāpēc varētu ietekmēt tā paredzēto nolūku un atbilstību šajā regulā noteiktajām prasībām.

---

[18] Eiropas Parlamenta un Padomes Regula (ES) 2024/1781 (2024. gada 13. jūnijs), ar ko izveido satvaru ekodizaina prasību noteikšanai ilgtspējīgiem produktiem, groza Direktīvu (ES) 2020/1828 un Regulu (ES) 2023/1542 un atceļ Direktīvu 2009/125/EK (OV L, 2024/1781, 28.6.2024., ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

(43) Produkti ar digitāliem elementiem būtu jāuzskata par svarīgiem, ja produkta iespējamo kiberdrošības ievainojamību izmantošanas negatīvā ietekme var būt nopietna, cita starpā ar kiberdrošību saistītas funkcionalitātes vai funkcijas dēļ, kam piemīt būtisks nelabvēlīgas ietekmes risks saistībā ar intensitāti un spēju traucēt, kontrolēt vai nodarīt kaitējumu lielam skaitam citu produktu ar digitāliem elementiem vai tā lietotāju veselībai, drošībai vai drošumam, izmantojot tiešas manipulācijas, piemēram, saistībā ar centrālām sistēmas funkcijām, tostarp tīkla pārvaldību, konfigurācijas kontroli, virtualizāciju vai personas datu apstrādi. Jo īpaši tādu produktu ar digitāliem elementiem ievainojamība, kam ir ar kiberdrošību saistīta funkcionalitāte, piemēram, sāknēšanas pārvaldnieki, var izraisīt drošības problēmu izplatīšanos visā piegādes ķēdē. Kiberdrošības incidenta ietekmes nopietnības pakāpe var pieaugt arī tad, ja produkts galvenokārt veic centrālas sistēmas funkcijas, tostarp tīkla pārvaldības, konfigurācijas kontroles, virtualizācijas vai personas datu apstrādes funkcijas.

(44) Dažām produktu ar digitāliem elementiem kategorijām būtu jāpiemēro stingrākas atbilstības novērtēšanas procedūras, vienlaikus saglabājot samērīgu pieeju. Šajā nolūkā nozīmīgi produkti ar digitāliem elementiem būtu jāiedala divās klasēs, kas atspoguļo ar šīm produktu kategorijām saistītā kiberdrošības riska līmeni. Incidentam, kurā iesaistīti nozīmīgi II klasē ietilpstoši produkti ar digitāliem elementiem, varētu būt lielāka negatīvā ietekme nekā incidentam, kurā iesaistīti nozīmīgi I klasē ietilpstoši produkti ar digitāliem elementiem, piemēram, attiecīgo produktu ar kiberdrošību saistītās funkcijas rakstura vai citas funkcijas veiktspējas dēļ, kas saistīta ar ievērojamu negatīvas ietekmes risku. Par šādu lielāku negatīvu ietekmi liecina tas, ka produkti ar digitāliem elementiem, kas ietilpst II klasē, varētu vai nu pildīt ar kiberdrošību saistītu funkciju, vai citu funkciju, kas saistīta ar būtisku negatīvas ietekmes risku, kurš ir lielāks nekā I klasē uzskaitītajiem produktiem, vai arī atbilst abiem iepriekš minētajiem kritērijiem. Tāpēc nozīmīgiem produktiem ar digitāliem elementiem, kas ietilpst II klasē, būtu jāpiemēro stingrāka atbilstības novērtēšanas procedūra.

(45) Šajā regulā minētie nozīmīgie produkti ar digitāliem elementiem būtu jāsaprot kā produkti, kuriem ir šajā regulā noteiktās svarīgo produktu ar digitāliem elementiem kategorijas pamatfunkcijas. Piemēram, šajā regulā ir noteiktas tādu svarīgu produktu ar digitāliem elementiem kategorijas, kas pēc to pamatfunkcijas ir noteikti kā II klases ugunsmūri vai ielaušanās atklāšanas vai novēršanas sistēmas. Tādējādi uz ugunsmūriem un ielaušanās atklāšanas vai novēršanas sistēmām attiecas obligāta trešās personas veikta atbilstības novērtēšana. Tas neattiecas uz citiem produktiem ar digitāliem elementiem, kas nav klasificēti kā nozīmīgi produkti ar digitāliem elementiem, kuros var būt integrēti ugunsmūri vai ielaušanās atklāšanas vai novēršanas sistēmas. Komisijai būtu jāpieņem īstenošanas akts, lai precizētu I un II klases svarīgo produktu ar digitāliem elementiem kategoriju tehnisko aprakstu, kā noteikts šajā regulā.

(46) Šajā regulā noteiktajām kritiski svarīgu produktu ar digitāliem elementiem kategorijām ir ar kiberdrošību saistīta funkcionalitāte, un tās veic funkciju, kas rada būtisku negatīvas ietekmes risku, ņemot vērā intensitāti un spēju tiešas manipulācijas rezultātā traucēt, kontrolēt vai nodarīt kaitējumu lielam skaitam citu produktu ar digitāliem elementiem. Turklāt minētās produktu ar digitāliem elementiem kategorijas tiek uzskatītas par kritisku atkarību Direktīvas (ES) 2022/2555 3. panta 1. punktā minētām būtiskām vienībām. Šīs regulas pielikumā minētām kritiski svarīgu produktu ar digitāliem elementiem kategorijām to kritiskuma dēļ jau plaši piemēro dažādus sertifikācijas veidus un uz tām attiecas arī uz kopīgiem kritērijiem balstīta Eiropas kiberdrošības sertifikācijas shēma (*EUCC*), kas noteikta Komisijas Īstenošanas regulā (ES) 2024/482[19]. Tāpēc, lai Savienībā nodrošinātu kopēju pienācīgu kiberdrošības aizsardzību kritiski svarīgiem produktiem ar digitāliem elementiem, varētu būt atbilstoši un samērīgi ar deleģēto aktu šādām produktu kategorijām noteikt obligātu Eiropas kiberdrošības sertifikāciju, ja jau ir ieviesta attiecīga Eiropas kiberdrošības sertifikācijas shēma, kas attiecas uz šiem produktiem, un Komisija ir veikusi paredzētās obligātās sertifikācijas iespējamās ietekmes uz tirgu novērtējumu. Minētajā novērtējumā būtu jāņem vērā gan piedāvājuma, gan pieprasījuma aspekts, tostarp tas, vai ir pietiekams pieprasījums pēc attiecīgajiem produktiem ar digitāliem elementiem gan no dalībvalstīm, gan lietotājiem, lai būtu nepieciešama Eiropas kiberdrošības sertifikācija, kā arī mērķi, kādiem produktus ar digitāliem elementiem paredzēts izmantot, tostarp būtisko vienību kritiskā atkarība no tiem, kā minēts Direktīvas (ES) 2022/2555 3. panta 1. punktā. Novērtējumā būtu jāanalizē arī obligātās sertifikācijas iespējamā ietekme uz minēto produktu pieejamību iekšējā tirgū un dalībvalstu spējas un gatavība īstenot attiecīgās Eiropas kiberdrošības sertifikācijas shēmas.

---

19 Komisijas Īstenošanas regula (ES) 2024/482 (2024. gada 31. janvāris) par to, kā vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) pieņemšanas sakarā piemērojama Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (OV L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(47) Deleģētajos aktos, kas paredz obligātu Eiropas kiberdrošības sertifikāciju, būtu jānosaka produkti ar digitāliem elementiem, kuriem ir šajā regulā noteiktas kritiski svarīgu produktu ar digitāliem elementiem kategorijas pamatfunkcijas, uz kuriem attiecas obligāta sertifikācija, kā arī nepieciešamais apliecinājuma līmenis, kam vajadzētu būt vismaz būtiskam. Nepieciešamajam apliecinājuma līmenim vajadzētu būt samērīgam ar kiberdrošības riska līmeni, kas saistīts ar produktu ar digitāliem elementiem. Piemēram, ja produktam ar digitāliem elementiem ir šajā regulā noteiktas kritiski svarīgu produktu ar digitāliem elementiem kategorijas pamatfunkcija un tas ir paredzēts lietošanai jutīgā vai kritiskā vidē, piemēram, produktiem, kas paredzēti Direktīvas (ES) 2022/2555 3. panta 1. punktā minēto būtisko vienību lietošanai, tam var būt nepieciešams augstākais apliecinājuma līmenis.

(48) Lai Savienībā nodrošinātu to produktu ar digitāliem elementiem kopīgu pienācīgu kiberdrošības aizsardzību, kuriem ir šajā regulā noteiktas kritiski svarīgu produktu ar digitāliem elementiem kategorijas pamatfunkcijas, Komisija būtu arī jāpilnvaro pieņemt deleģētos aktus šīs regulas grozīšanai, pievienojot vai svītrojot kritiski svarīgu produktu ar digitāliem elementiem kategorijas, kuru ražotājiem nolūkā pierādīt atbilstību šai regulai varētu pieprasīt iegūt Eiropas kiberdrošības sertifikātu saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu atbilstīgi Regulai (ES) 2019/881. Šīm kategorijām var pievienot jaunu kritiski svarīgu produktu ar digitāliem elementiem kategoriju, ja no tām ir kritiski atkarīgas būtiskās vienības, kā minēts Direktīvas (ES) 2022/2555 3. panta 1. punktā, vai ja tās skar incidenti vai arī ja tās satur izmantotas ievainojamības, kas varētu izraisīt traucējumus kritiski svarīgās piegādes ķēdēs. Novērtējot nepieciešamību ar deleģēto aktu pievienot vai svītrot kritiski svarīgu produktu ar digitāliem elementiem kategorijas, Komisijai vajadzētu būt iespējai ņemt vērā to, vai dalībvalstis valsts līmenī ir identificējušas produktus ar digitāliem elementiem, kuriem ir kritiski svarīga nozīme būtisko vienību noturībā, kā minēts Direktīvas (ES) 2022/2555 3. panta 1. punktā, un kuri arvien biežāk piegādes ķēdē saskaras ar kiberuzbrukumiem ar iespējamu nopietnu traucējošu ietekmi. Turklāt Komisijai vajadzētu būt iespējai ņemt vērā rezultātus, kas gūti saskaņā ar Direktīvas (ES) 2022/2555 22. pantu veiktajā Savienības līmeņa koordinētā kritiski svarīgo piegādes ķēžu drošības riska novērtējumā.

(49) Komisijai būtu jānodrošina, ka, sagatavojot pasākumus šīs regulas īstenošanai, strukturēti un regulāri notiek apspriešanās ar plašu attiecīgo ieinteresēto personu loku. Tam jo īpaši būtu jāattiecas uz gadījumiem, kad Komisija novērtē vajadzību pēc potenciāliem atjauninājumiem svarīgu vai kritiski svarīgu produktu ar digitāliem elementiem kategoriju sarakstos, kad būtu jāapspriežas ar attiecīgajiem ražotājiem un jāņem vērā viņu viedoklis, lai analizētu kiberdrošības riskus, kā arī izmaksu un ieguvumu līdzsvaru, nosakot šādas produktu kategorijas kā svarīgas vai kritiski svarīgas.

(50) Šī regula mērķtiecīgi pievēršas kiberdrošības riskiem. Tomēr produkti ar digitāliem elementiem vienmēr var radīt arī citus drošības riskus, kas ne vienmēr ir saistīti ar kiberdrošību, bet var izrietēt no drošības pārkāpuma. Minētie riski arī turpmāk būtu jāreglamentē ar attiecīgajiem Savienības saskaņošanas tiesību aktiem, kas nav šī regula. Ja nav piemērojami citi Savienības saskaņošanas tiesību akti, izņemot šo regulu, uz tiem būtu jāattiecina Eiropas Parlamenta un Padomes Regula (ES) 2023/988[20]. Tāpēc, ņemot vērā šīs regulas mērķtiecīgo raksturu, atkāpjoties no Regulas (ES) 2023/988 2. panta 1. punkta trešās daļas b) apakšpunkta, ja uz produktiem ar digitāliem elementiem Regulas (ES) 2023/988 3. panta 27. punkta nozīmē neattiecas īpašas prasības, kas noteiktas citos Savienības saskaņošanas tiesību aktos, kuri nav šī regula, tad minētajiem produktiem attiecībā uz šajā regulā neietvertiem drošības riskiem būtu jāpiemēro Regulas (ES) 2023/988 III nodaļas 1. iedaļa, V un VII nodaļa un IX–XI nodaļa.

---

[20] Eiropas Parlamenta un Padomes Regula (ES) 2023/988 (2023. gada 10. maijs) par ražojumu vispārēju drošumu, ar ko groza Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1025/2012 un Eiropas Parlamenta un Padomes Direktīvu (ES) 2020/1828 un atceļ Eiropas Parlamenta un Padomes Direktīvu 2001/95/EK un Padomes Direktīvu 87/357/EEK (OV L 135, 23.5.2023., 1. lpp.).

(51) Produktiem ar digitāliem elementiem, kas klasificēti kā augsta riska MI sistēmas saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2024/1689[21] 6. pantu un kas ietilpst šīs regulas darbības jomā, būtu jāatbilst šajā regulā noteiktajām kiberdrošības pamatprasībām. Ja šīs augsta riska MI sistēmas atbilst šīs regulas kiberdrošības pamatprasībām, būtu jāuzskata, ka tās atbilst Regulas (ES) 2024/1689 15. pantā noteiktajām kiberdrošības prasībām, ciktāl uz šīm prasībām attiecas ES atbilstības deklarācija vai tās daļas, kas izdotas atbilstīgi šai regulai. Šim nolūkam to kiberdrošības risku novērtēšanā, kas saistīti ar produktu ar digitāliem elementiem, kurš, ievērojot Regulu (ES) 2024/1689, klasificēts kā augsta riska MI sistēma, un kas jāņem vērā šāda produkta plānošanas, projektēšanas, izstrādes, ražošanas, piegādes un uzturēšanas posmos, kā prasa šī regula, būtu jāņem vērā riski MI sistēmas kibernoturībai attiecībā uz nepilnvarotu trešo personu mēģinājumiem mainīt tās lietošanu, uzvedību vai veiktspēju, tostarp MI specifiskas ievainojamības, piemēram, datu saindēšana vai ļaunprātīgi uzbrukumi, kā arī attiecīgā gadījumā riski pamattiesībām saskaņā ar Regulu (ES) 2024/1689. Attiecībā uz atbilstības novērtēšanas procedūrām, kas saistītas ar kiberdrošības pamatprasībām produktam ar digitāliem elementiem, kurš ietilpst šīs regulas darbības jomā un kurš ir klasificēts kā augsta riska MI sistēma, šīs regulas attiecīgo noteikumu vietā parasti būtu jāpiemēro Regulas (ES) 2024/1689 43. pants.

---

21 Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (OV L, 2024/1689, 12.7.2024., ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Tomēr minētā noteikuma piemērošanai nevajadzētu samazināt nepieciešamo uzticamības līmeni attiecībā uz šajā regulā minētajiem svarīgajiem vai kritiski svarīgajiem produktiem ar digitāliem elementiem. Tāpēc, atkāpjoties no minētā noteikuma, augsta riska MI sistēmām, kuras ietilpst Regulas (ES) 2024/1689 darbības jomā un kuras, kā minēts šajā regulā, arī tiek kvalificētas kā nozīmīgi vai kritiski svarīgi produkti ar digitāliem elementiem, un uz kurām attiecas Regulas (ES) 2024/1689 VI pielikumā minētā uz iekšējo kontroli pamatotā atbilstības novērtēšanas procedūra, būtu jāpiemēro šajā regulā paredzētie atbilstības novērtēšanas noteikumi, ciktāl tas attiecas uz šajā regulā noteiktajām kiberdrošības pamatprasībām. Šādā gadījumā attiecībā uz visiem pārējiem Regulā (ES) 2024/1689 ietvertajiem aspektiem būtu jāpiemēro attiecīgie uz iekšējo kontroli pamatotas atbilstības novērtēšanas noteikumi, kas izklāstīti minētās regulas VI pielikumā.

(52) Lai uzlabotu drošību attiecībā uz produktiem ar digitāliem elementiem, kurus laiž iekšējā tirgū, ir jānosaka šādiem produktiem piemērojamas kiberdrošības pamatprasības. Šīm kiberdrošības pamatprasībām nebūtu jāskar Savienības līmenī koordinētie kritisko piegādes ķēžu drošības riska novērtējumi, kas noteikti Direktīvas (ES) 2022/2555 22. pantā, un kuros tiek ņemti vērā gan tehniski, gan attiecīgā gadījumā netehniski riska faktori, piemēram, trešās valsts neatļauta ietekme uz piegādātājiem. Turklāt tām nebūtu jāskar dalībvalstu prerogatīvas noteikt papildu prasības, kurās augsta noturības līmeņa nodrošināšanai tiek ņemti vērā netehniski faktori, arī tie, kas noteikti Komisijas Ieteikumā (ES) 2019/534[22], ES koordinētajā 5G tīklu kiberdrošības riska novērtējumā un ES rīkkopā par 5G kiberdrošību, kuru saskaņojusi sadarbības grupa, kas izveidota, ievērojot Direktīvas (ES) 2022/2555 14. pantu.

[22] Komisijas Ieteikums (ES) 2019/534 (2019. gada 26. marts) par 5G tīklu kiberdrošību (OV L 88, 29.3.2019., 42. lpp.).

(53) Tādu produktu ražotājiem, kuri ietilpst Eiropas Parlamenta un Padomes Regulas (ES) 2023/1230[23] darbības jomā un kuri ir arī produkti ar digitāliem elementiem šīs regulas nozīmē, būtu jāievēro gan šajā regulā noteiktās kiberdrošības pamatprasības, gan Regulā (ES) 2023/1230 noteiktās veselības un drošības pamatprasības. Šajā regulā noteiktās kiberdrošības pamatprasības un dažas Regulā (ES) 2023/1230 noteiktās pamatprasības varētu attiekties uz līdzīgiem kiberdrošības riskiem. Tāpēc atbilstība šajā regulā noteiktajām kiberdrošības pamatprasībām varētu sekmēt atbilstību pamatprasībām, kas aptver arī konkrētus kiberdrošības riskus, kā noteikts Regulā (ES) 2023/1230, un jo īpaši prasībām attiecībā uz aizsardzību pret korupciju un kontroles sistēmu drošumu un uzticamību, kas noteiktas minētās Regulas III pielikuma 1.1.9. un 1.2.1. iedaļā. Šāda sinerģija ražotājam ir jāpierāda, piemēram, pēc minēto kiberdrošības risku aptveroša riska novērtējuma veikšanas piemērojot saskaņotos standartus, ja tādi ir pieejami, vai citas tehniskās specifikācijas, kas attiecas uz attiecīgajām kiberdrošības pamatprasībām. Ražotājam būtu arī jāievēro piemērojamās atbilstības novērtēšanas procedūras, kas noteiktas šajā regulā un Regulā (ES) 2023/1230. Komisijai un Eiropas standartizācijas organizācijām, veicot sagatavošanas darbus ar mērķi atbalstīt šīs regulas un Regulas (ES) 2023/1230 īstenošanu un ar to saistītos standartizācijas procesus, būtu jāveicina konsekvence attiecībā uz to, kā jānovērtē kiberdrošības riski un kā šie riski jāiekļauj saskaņotajos standartos, ņemot vērā attiecīgās pamatprasības.

---

[23] Eiropas Parlamenta un Padomes Direktīva (ES) 2023/1230 (2023. gada 14. jūnijs) par mašīnām un ar ko atceļ Eiropas Parlamenta un Padomes Direktīvu 2006/42/EK un Padomes Direktīvu 73/361/EEK (OV L 165, 29.6.2023., 1. lpp.).

Jo īpaši Komisijai un Eiropas standartizācijas organizācijām šī regula būtu jāņem vērā, sagatavojot un izstrādājot saskaņotos standartus ar mērķi sekmēt Regulas (ES) 2023/1230 īstenošanu, jo īpaši attiecībā uz kiberdrošības aspektiem, kas saistīti ar aizsardzību pret korupciju un kontroles sistēmu drošumu un uzticamību, kā noteikts minētās regulas III pielikuma 1.1.9. un 1.2.1. iedaļā. Komisijai būtu jāsniedz norādījumi nolūkā atbalstīt ražotājus, uz kuriem attiecas šī regula un arī Regula (ES) 2023/1230, jo īpaši, lai sekmētu atbilstības pierādīšanu attiecīgajām šajā regulā un Regulā (ES) 2023/1230 noteiktajām pamatprasībām.

(54) Lai nodrošinātu, ka produkti ar digitāliem elementiem ir droši gan brīdī, kad tos laiž tirgū, gan arī laikā, kad produktu ar digitāliem elementiem paredzēts lietot, ir jānosaka kiberdrošības pamatprasības ievainojamību novēršanai un kiberdrošības pamatprasības attiecībā uz produktu ar digitāliem elementiem īpašībām. Lai gan ražotājiem visā atbalsta periodā būtu jāievēro visas ar ievainojamību novēršanu saistītās kiberdrošības pamatprasības, tiem būtu jānosaka, kuras citas ar produktu īpašībām saistītas kiberdrošības pamatprasības ir būtiskas attiecīgajam produktu ar digitāliem elementiem veidam. Šajā nolūkā ražotājiem būtu jāveic ar produktu ar digitāliem elementiem saistīto kiberdrošības risku novērtējums, lai konstatētu attiecīgos riskus un attiecīgās kiberdrošības pamatprasības, kā arī lai darītu pieejamus savus produktus ar digitāliem elementiem bez zināmām izmantojamām ievainojamībām, kas varētu ietekmēt šo produktu drošību, un pienācīgi piemērotu atbilstošus saskaņotos standartus, kopīgas specifikācijas vai Eiropas vai starptautiskos standartus.

(55) Ja noteiktas kiberdrošības pamatprasības produktam ar digitāliem elementiem nav piemērojamas, ražotājam tehniskajā dokumentācijā iekļautajā kiberdrošības riska novērtējumā būtu jāiekļauj skaidrs pamatojums. Tas varētu būt gadījumos, kad kiberdrošības pamatprasība nav saderīga ar produkta ar digitāliem elementiem būtību. Piemēram, produkta ar digitāliem elementiem paredzētā nolūka dēļ ražotājam var būt jāievēro vispāratzīti sadarbspējas standarti pat tad, ja tā drošības elementi vairs netiek uzskatīti par jaunākajiem iespējamiem. Tāpat arī citos Savienības tiesību aktos ražotājiem tiek prasīts piemērot īpašas sadarbspējas prasības. Ja kiberdrošības pamatprasība nav piemērojama produktam ar digitāliem elementiem, bet ražotājs ir identificējis kiberdrošības riskus saistībā ar šo kiberdrošības pamatprasību, tam būtu jāveic pasākumi, lai novērstu šos riskus ar citiem līdzekļiem, piemēram, ierobežojot produkta paredzēto nolūku līdz uzticamai videi vai informējot lietotājus par šiem riskiem.

(56) Viens no vissvarīgākajiem pasākumiem, kas lietotājiem jāveic nolūkā aizsargāt savus produktus ar digitāliem elementiem pret kiberuzbrukumiem, ir pēc iespējas drīzāk instalēt jaunākos pieejamos drošības atjauninājumus. Tāpēc ražotājiem būtu jāprojektē savi produkti un jāievieš procesi tā, lai nodrošinātu, ka produkti ar digitāliem elementiem ietver funkcijas, kas ļauj automātiski paziņot, izplatīt, lejupielādēt un instalēt drošības atjauninājumus, jo īpaši patēriņa produktu gadījumā. Tiem būtu jānodrošina arī iespēja kā pēdējo soli apstiprināt drošības atjauninājumu lejupielādi un instalēšanu. Būtu jāsaglabā iespēja lietotājiem deaktivizēt automātiskos atjauninājumus ar skaidru un viegli lietojamu mehānismu, ko papildina skaidri norādījumi par to, kā lietotāji var atteikties. Šīs regulas pielikumā noteiktās prasības attiecībā uz automātiskajiem atjauninājumiem nav piemērojamas produktiem ar digitāliem elementiem, kurus galvenokārt paredzēts integrēt kā komponentus citos produktos. Tie neattiecas arī uz produktiem ar digitāliem elementiem, attiecībā uz kuriem lietotāji pamatoti negaida automātiskus atjauninājumus, tostarp produktiem ar digitāliem elementiem, kas paredzēti izmantošanai profesionālos IKT tīklos, un jo īpaši kritiskās un rūpnieciskās vidēs, kur automātisks atjauninājums varētu radīt darbības traucējumus. Neatkarīgi no tā, vai produkts ar digitāliem elementiem ir paredzēts automātisku atjauninājumu saņemšanai vai nav, tā ražotājam būtu jāinformē lietotāji par ievainojamībām un nekavējoties jānodrošina drošības atjauninājumu pieejamība. Ja produktam ar digitāliem elementiem ir lietotāja saskarne vai līdzīgi tehniski līdzekļi, kas nodrošina tiešu mijiedarbību ar tā lietotājiem, ražotājam būtu jāizmanto šādas iespējas, lai informētu lietotājus, ka produkta ar digitāliem elementiem atbalsta periods ir beidzies. Paziņojumiem būtu jāaprobežojas tikai ar to, kas nepieciešams šīs informācijas efektīvas saņemšanas nodrošināšanai, un tiem nevajadzētu negatīvi ietekmēt produkta ar digitāliem elementiem lietošanas pieredzi.

(57) Lai uzlabotu ievainojamības novēršanas procesu pārredzamību un nodrošinātu, ka lietotājiem nav jāinstalē jauni funkcionalitātes atjauninājumi tikai tādēļ, lai saņemtu jaunākos drošības atjauninājumus, ražotājiem būtu jānodrošina, ja tas ir tehniski iespējams, ka jaunie drošības atjauninājumi tiek nodrošināti atsevišķi no funkcionalitātes atjauninājumiem.

(58) Komisijas un Savienības Augstā pārstāvja ārlietās un drošības politikas jautājumos 2023. gada 20. jūnija kopīgajā paziņojumā "Par Eiropas ekonomiskās drošības stratēģiju" ir norādīts, ka Savienībai, izmantojot vienotu Savienības ekonomiskās drošības stratēģisko satvaru, ir maksimāli jāpalielina ieguvumi no savas ekonomiskās atvērtības, vienlaikus līdz minimumam samazinot riskus, ko rada ekonomiskā atkarība no augsta riska piegādātājiem. Atkarība no produktu ar digitāliem elementiem augsta riska piegādātājiem var radīt stratēģisku risku, kas jānovērš Savienības līmenī, jo īpaši tad, ja produkti ar digitāliem elementiem ir paredzēti izmantošanai būtiskajās vienībās, kā minēts Direktīvā (ES) 2022/2555. Šādi riski var būt saistīti, bet neaprobežojas ar ražotājam piemērojamo jurisdikciju, tā korporatīvo īpašumtiesību iezīmēm un kontroles saiknēm ar kādas trešās valsts valdību, kurā tas ir iedibināts, jo īpaši to, vai trešās valsts iesaistās ekonomiskajā spiegošanā vai bezatbildīgā valsts rīcībā kibertelpā un tās tiesību akti ļauj patvaļīgi piekļūt jebkāda veida uzņēmuma darbībai vai datiem, tostarp komerciāli sensitīviem datiem, un var uzlikt pienākumus izlūkošanas mērķiem, nepastāvot demokrātiskai kontrolei un līdzsvaram, pārraudzības mehānismam, pienācīgam procesam vai tiesībām vērsties neatkarīgā tiesā. Nosakot kiberdrošības riska nozīmīgumu šīs regulas nozīmē, Komisijai un tirgus uzraudzības iestādēm saskaņā ar šajā regulā noteiktajiem pienākumiem būtu jāņem vērā arī ar tehniku nesaistīti riska faktori, jo īpaši tie, kas konstatēti Savienības līmenī koordinētos kritisko piegādes ķēžu drošības riska novērtējumos saskaņā ar Direktīvas (ES) 2022/2555 22. pantu.

(59) Lai nodrošinātu produktu ar digitāliem elementiem drošību pēc to laišanas tirgū, ražotājiem būtu jānosaka atbalsta periods, kurā būtu jāatspoguļo produkta ar digitāliem elementiem paredzamais lietošanas laiks. Nosakot atbalsta periodu, ražotājam jo īpaši būtu jāņem vērā lietotāju pamatotās cerības, produkta raksturs, kā arī attiecīgie Savienības tiesību akti, kas nosaka produktu ar digitāliem elementiem darbmūžu. Ražotājiem vajadzētu būt iespējai ņemt vērā arī citus būtiskus faktorus. Kritēriji būtu jāpiemēro tā, lai nodrošinātu proporcionalitāti atbalsta perioda noteikšanā. Ražotājam pēc pieprasījuma būtu jāsniedz tirgus uzraudzības iestādēm informācija, kas tika ņemta vērā atbalsta periodu produktam ar digitāliem elementiem noteikšanā.

(60) Atbalsta periodam, kurā ražotājs nodrošina efektīvu rīcību attiecībā uz ievainojamībām, nevajadzētu būt īsākam par pieciem gadiem, ja vien produkta ar digitāliem elementiem darbmūžs nav īsāks par pieciem gadiem, un tādā gadījumā ražotājam jānodrošina ievainojamību novēršana šā darbmūža laikā. Ja pamatoti paredzams, ka produkts ar digitāliem elementiem tiks izmantots ilgāk nekā piecus gadus, kā tas bieži ir aparatūras komponentu gadījumā, piemēram, mātesplatēm vai mikroprocesoriem, tīkla ierīcēm, piemēram, maršrutētājiem, modemiem vai slēdžiem, kā arī programmatūrai, piemēram, operētājsistēmām vai video rediģēšanas rīkiem, ražotājiem attiecīgi būtu jānodrošina garāki atbalsta periodi. Jo īpaši izstrādājumi ar digitāliem elementiem, kas paredzēti izmantošanai rūpnieciskos apstākļos, piemēram, rūpnieciskās vadības sistēmas, bieži tiek izmantoti ievērojami ilgāku laiku. Ražotājam vajadzētu būt iespējai noteikt par pieciem gadiem īsāku atbalsta periodu tikai tad, ja to pamato attiecīgā produkta ar digitāliem elementiem raksturs un ja paredzams, ka produkts tiks lietots mazāk nekā piecus gadus, un šādā gadījumā atbalsta periodam būtu jāatbilst paredzamajam lietošanas laikam. Piemēram, kontaktu izsekošanas lietotnes, kas paredzēta lietošanai pandēmijas laikā, darbmūžs varētu būt ierobežots līdz pandēmijas ilgumam. Turklāt dažas lietojumprogrammas pēc būtības var būt pieejamas tikai uz abonēšanas modeļa pamata, jo īpaši tad, ja pēc abonēšanas termiņa beigām lietojumprogramma kļūst nepieejama lietotājam un attiecīgi vairs nav izmantojama.

(61) Kad pienāk produktu ar digitāliem elementiem atbalsta perioda beigas, tad ražotājiem būtu jāapsver šādu produktu ar digitāliem elementiem pirmkoda nodošana citiem uzņēmumiem, kas apņemas paplašināt ievainojamību novēršanas pakalpojumu sniegšanu, vai arī sabiedrībai, lai tādā veidā tiktu nodrošināts, ka ievainojamības var novērst pēc atbalsta perioda beigām. Ja ražotāji nodod pirmkodu citiem uzņēmumiem, tiem jāspēj aizsargāt produkta ar digitāliem elementiem īpašumtiesības un jānovērš pirmkoda izplatīšana sabiedrībai, piemēram, izmantojot līgumiskas vienošanās.

(62) Lai nodrošinātu, ka ražotāji visā Savienībā nosaka līdzīgus atbalsta periodus salīdzināmiem produktiem ar digitāliem elementiem, *ADCO* būtu jāpublicē statistikas dati par ražotāju noteiktajiem vidējiem atbalsta periodiem produktu ar digitāliem elementiem kategorijām un jāizdod vadlīnijas, kurās norādīti attiecīgie atbalsta periodi šādām kategorijām. Turklāt, lai nodrošinātu saskaņotu pieeju visā iekšējā tirgū, Komisijai vajadzētu būt iespējai pieņemt deleģētos aktus, lai noteiktu minimālos atbalsta periodus konkrētām produktu kategorijām, ja tirgus uzraudzības iestāžu sniegtie dati liecina, ka ražotāju noteiktie atbalsta periodi vai nu sistemātiski neatbilst šajā regulā noteiktajiem atbalsta periodu noteikšanas kritērijiem, vai arī ražotāji dažādās dalībvalstīs nepamatoti nosaka atšķirīgus atbalsta periodus.

(63) Ražotājiem būtu jāizveido vienots kontaktpunkts, kas ļauj lietotājiem viegli sazināties ar tiem, tostarp nolūkā ziņot un saņemt informāciju par produkta ar digitāliem elementiem ievainojamībām. Tām būtu jānodrošina, ka vienotais kontaktpunkts ir viegli piekļūstams lietotājiem un skaidri jānorāda tā pieejamība, pastāvīgi atjauninot šo informāciju. Ja ražotāji izvēlas piedāvāt automatizētus rīkus, piemēram, sarunu botus, tiem būtu jāpiedāvā arī tālruņa numurs vai citi digitāli saziņas līdzekļi, piemēram, e-pasta adrese vai saziņas veidlapa. Vienotajam kontaktpunktam nevajadzētu paļauties tikai uz automatizētiem rīkiem.

(64) Ražotājiem būtu jānodrošina, ka viņu produkti ar digitāliem elementiem ir pieejami tirgū ar drošu noklusējuma konfigurāciju, un bez maksas būtu jānodrošina lietotājiem drošības atjauninājumi. Ražotājiem vajadzētu būt iespējai atkāpties no kiberdrošības pamatprasībām tikai attiecībā uz īpaši pielāgotiem produktiem, kas konkrētam komerciālajam lietotājam ir uzstādīti konkrētam nolūkam, un ja gan ražotājs, gan lietotājs ir skaidri vienojušies par atšķirīgiem līguma noteikumiem.

(65) Ražotājiem, izmantojot vienoto ziņošanas platformu, vienlaicīgi jāziņo gan par koordinatoru izraudzītajai Datordrošības incidentu reaģēšanas grupai (*CSIRT*), gan *ENISA* par aktīvi izmantotām ievainojamībām, kas ir produktos ar digitāliem elementiem, kā arī par nopietniem incidentiem, kas ietekmē minēto produktu drošību. Paziņojumi būtu jāiesniedz, izmantojot par koordinatoru izraudzītas *CSIRT* elektroniskās paziņošanas galapunktu, un tiem vajadzētu būt vienlaikus pieejamiem *ENISA*.

(66) Ražotājiem būtu jāziņo par aktīvi izmantotām ievainojamībām, lai nodrošinātu, ka par koordinatoru izraudzītām *CSIRT* un *ENISA* ir pietiekams pārskats par šādām ievainojamībām un tās saņem informāciju, kas nepieciešama to uzdevumu izpildei, kā noteikts Direktīvā (ES) 2022/2555 un būtisko un svarīgo vienību vispārējā kiberdrošības līmeņa paaugstināšanai, kā norādīts minētās direktīvas 3. pantā, kā arī lai nodrošinātu tirgus uzraudzības iestāžu efektīvu darbību. Tā kā lielākā daļa produktu ar digitāliem elementiem tiek tirgoti visā iekšējā tirgū, jebkura izmantota ievainojamība attiecībā uz produktu ar digitāliem elementiem būtu jāuzskata par apdraudējumu iekšējā tirgus darbībai. *ENISA*, vienojoties ar ražotāju, būtu jāpublisko izlabotās ievainojamības Eiropas ievainojamību datubāzē, kas izveidota, ievērojot Direktīvas (ES) 2022/2555 12. panta 2. punktu. Eiropas ievainojamību datubāzei vajadzētu palīdzēt ražotājiem atklāt zināmas izmantojamas ievainojamības viņu produktos, lai tā tiktu nodrošināts, ka tirgū tiek darīti pieejami droši produkti.

(67) Ražotājiem būtu arī jāpaziņo par koordinatoru izraudzītai *CSIRT* un *ENISA* par jebkuru nopietnu incidentu, kas ietekmē produkta ar digitāliem elementiem drošību. Lai nodrošinātu, ka lietotāji var ātri reaģēt uz nopietniem incidentiem, kas ietekmē viņu produktu ar digitāliem elementiem drošību, ražotājiem būtu jāinformē arī savi lietotāji par jebkuru šādu incidentu un attiecīgā gadījumā par jebkādiem korektīviem pasākumiem, ko lietotāji var veikt, lai mazinātu incidenta ietekmi, piemēram, publicējot attiecīgu informāciju savās tīmekļvietnēs vai, ja ražotājs spēj sazināties ar lietotājiem un ja kiberdrošības riski to pamato, tiešā veidā vēršoties pie lietotājiem.

(68) Aktīvi izmantotas ievainojamības attiecas uz gadījumiem, kad ražotājs konstatē, ka drošības pārkāpums, kas ietekmē tā lietotājus vai jebkuru citu fizisku vai juridisku personu, ir radies ļaundaru darbības rezultātā, izmantojot nepilnības kādā no produktiem ar digitāliem elementiem, ko ražotājs darījis pieejamu tirgū. Šādu ievainojamību piemēri varētu būt trūkumi produkta identifikācijas un autentifikācijas funkcijās. Nebūtu obligāti jāziņo par ievainojamībām, kas tiek atklātas bez ļaunprātīga nolūka godprātīgas testēšanas, izmeklēšanas, labošanas vai izpaušanas nolūkā ar mērķi veicināt sistēmas īpašnieka un tās lietotāju drošību vai drošumu. Savukārt nopietni incidenti, kas ietekmē produkta ar digitāliem elementiem drošību, attiecas uz situācijām, kad kiberdrošības incidents ietekmē ražotāja izstrādes, ražošanas vai uzturēšanas procesus tādā veidā, ka tas varētu palielināt kiberdrošības risku lietotājiem vai citām personām. Šāds nopietns incidents varētu būt situācija, kad uzbrucējs ir veiksmīgi ieviesis ļaunprātīgu kodu izplatīšanas kanālā, ar kura starpniecību ražotājs izlaiž drošības atjauninājumus lietotājiem.

(69) Lai nodrošinātu, ka paziņojumus var ātri izplatīt visām attiecīgajām par koordinatoriem izraudzītajām *CSIRT*, un lai ražotāji varētu iesniegt vienu paziņojumu katrā paziņošanas procesa posmā, *ENISA* būtu jāizveido vienotā ziņošanas platforma ar valstu elektroniskās paziņošanas galapunktiem. Vienotās ziņošanas platformas ikdienas darbības būtu jāpārvalda un jāuztur *ENISA*. Par koordinatoriem izraudzītajām *CSIRT* būtu jāinformē to attiecīgās tirgus uzraudzības iestādes par paziņotajām ievainojamībām vai incidentiem. Vienotā ziņošanas platforma būtu jāveido tā, lai tā nodrošinātu paziņojumu konfidencialitāti, jo īpaši attiecībā uz ievainojamībām, par kurām vēl nav pieejams drošības atjauninājums. Turklāt *ENISA* būtu jāievieš procedūras drošai un konfidenciālai informācijas apstrādei. Pamatojoties uz savākto informāciju, *ENISA* reizi divos gados būtu jāsagatavo tehniskais ziņojums par jaunākajām tendencēm attiecībā uz kiberdrošības riskiem produktos ar digitāliem elementiem, un tas jāiesniedz sadarbības grupai, kas izveidota saskaņā ar Direktīvas (ES) 2022/2555 14. pantu.

(70) Ārkārtas apstākļos un jo īpaši pēc ražotāja pieprasījuma tai par koordinatoru izraudzītajai *CSIRT*, kas sākotnēji saņem paziņojumu, vajadzētu būt iespējai nolemt atlikt tā izplatīšanu citām attiecīgajām par koordinatoriem izraudzītajām *CSIRT*, izmantojot vienoto ziņošanas platformu, ja to var pamatot ar kiberdrošību saistītu iemeslu dēļ un tik ilgi, cik absolūti nepieciešams. Par koordinatoru izraudzītajai *CSIRT* būtu nekavējoties jāinformē *ENISA* par lēmumu atlikt izplatīšanu un par to, kādu iemeslu dēļ tas notiek, kā arī par to, kad tā plāno izplatīšanu veikt. Komisijai, izmantojot deleģēto aktu, būtu jāizstrādā specifikācijas par to, kādos gadījumos varētu piemērot ar kiberdrošību saistītus pamatojumus, un deleģētā akta projekta sagatavošanā būtu jāsadarbojas ar *CSIRT* tīklu, kas izveidots saskaņā ar Direktīvas (ES) 2022/2555 15. pantu, un *ENISA*. Ar kiberdrošību saistītu iemeslu piemēri ir notiekoša koordinēta ievainojamību atklāšanas procedūra vai situācijas, kurās ir paredzams, ka ražotājs drīzumā nodrošinās risku mazinošu pasākumu, un kiberdrošības riski, kas saistīti ar tūlītēju izplatīšanu, izmantojot vienoto ziņošanas platformu, ir lielāki par ieguvumiem. Ja to pieprasa par koordinatoru izraudzītā *CSIRT*, *ENISA* būtu jāspēj atbalstīt šo *CSIRT* ar kiberdrošību saistītu iemeslu piemērošanā saistībā ar paziņojuma izplatīšanas atlikšanu, pamatojoties uz informāciju, ko *ENISA* ir saņēmusi no šīs *CSIRT* par lēmumu aizturēt paziņojumu minēto kiberdrošības iemeslu dēļ. Turklāt īpašos izņēmuma apstākļos *ENISA* nebūtu vienlaicīgi jāsaņem sīkāka informācija par paziņojumu par aktīvi izmantotu ievainojamību.

Tā tas būtu gadījumā, ja ražotājs savā paziņojumā norāda, ka paziņoto ievainojamību ir aktīvi izmantojis ļaundaris un ka saskaņā ar pieejamo informāciju tā ir izmantota tikai tajā dalībvalstī, kurā ir par koordinatoru izraudzītā *CSIRT*, kam ražotājs ir paziņojis par šo ievainojamību, ja paziņotās ievainojamības tūlītēja tālāka izplatīšana, visticamāk, novestu pie informācijas sniegšanas, kuras izpaušana būtu pretrunā minētās dalībvalsts būtiskām interesēm, vai ja paziņotā ievainojamība rada nenovēršamu augstu kiberdrošības risku, kas izriet no tālākas izplatīšanas. Šādos gadījumos *ENISA* vienlaicīgi saņems piekļuvi tikai informācijai par to, ka ražotājs ir iesniedzis paziņojumu, vispārīgai informācijai par attiecīgo produktu ar digitāliem elementiem, informācijai par izmantošanas vispārīgo raksturu un informācijai par to, ka šos drošības apsvērumus ir norādījis ražotājs un ka tāpēc netiek izpausts pilns paziņojuma saturs. Pilns paziņojums pēc tam būtu jādara pieejams *ENISA* un citām attiecīgajām par koordinatoriem izraudzītajām *CSIRT*, kad par koordinatoru izraudzītā *CSIRT*, kura sākotnēji saņēma paziņojumu, konstatē, ka šie drošības apsvērumi, kas atspoguļo šajā regulā noteiktos īpašos izņēmuma apstākļus, vairs nepastāv. Ja, pamatojoties uz pieejamo informāciju, *ENISA* uzskata, ka pastāv sistēmisks risks, kas ietekmē drošību iekšējā tirgū, *ENISA* būtu jāiesaka saņēmējai *CSIRT* izplatīt pilnīgu paziņojumu pārējām par koordinatoriem izraudzītajām *CSIRT*, un pašai *ENISA*.

(71) Ja ražotāji paziņo par aktīvi izmantotu ievainojamību vai nopietnu incidentu, kas ietekmē produkta ar digitāliem elementiem drošību, tiem būtu jānorāda, cik sensitīva, viņuprāt, ir paziņotā informācija. Par koordinatoru izraudzītajai *CSIRT*, kas sākotnēji saņem paziņojumu, šī informācija būtu jāņem vērā, novērtējot, vai paziņojuma dēļ rodas izņēmuma apstākļi, kas attaisno paziņojuma izplatīšanas aizkavēšanu citām attiecīgajām par koordinatoriem izraudzītajām *CSIRT*, balstoties uz pamatotiem ar kiberdrošību saistītiem iemesliem. Tai būtu arī jāņem vērā šī informācija, novērtējot, vai paziņojums par aktīvi izmantotu ievainojamību rada īpašus izņēmuma apstākļus, kas attaisno to, ka pilns paziņojums nav vienlaicīgi pieejams *ENISA*. Visbeidzot, par koordinatoriem izraudzītajām *CSIRT* vajadzētu būt iespējai ņemt vērā šo informāciju, nosakot piemērotus pasākumus no šādām ievainojamībām un incidentiem izrietošo risku mazināšanai.

(72) Lai vienkāršotu šajā regulā prasītās informācijas paziņošanu, ņemot vērā citas papildu ziņošanas prasības, kas noteiktas Savienības tiesību aktos, piemēram, Regulā (ES) 2016/679, Eiropas Parlamenta un Padomes Regulā (ES) 2022/2554[24], Eiropas Parlamenta un Padomes Direktīvā 2002/58/EK[25] un Direktīvā (ES) 2022/2555, kā arī lai samazinātu administratīvo slogu vienībām, dalībvalstis tiek mudinātas apsvērt iespēju valsts līmenī nodrošināt vienotus kontaktpunktus šādām ziņošanas prasībām. Šāda vienota kontaktpunkta izmantošanai ziņošanai par drošības incidentiem saskaņā ar Regulu (ES) 2016/679 un Direktīvu 2002/58/EK nevajadzētu ietekmēt Regulas (ES) 2016/679 un Direktīvas 2002/58/EK noteikumu piemērošanu, jo īpaši to noteikumu, kas attiecas uz tajās minēto iestāžu neatkarību. Izveidojot šajā regulā minēto vienoto ziņošanas platformu, *ENISA* būtu jāņem vērā iespēja šajā regulā minētos valstu elektroniskās paziņošanas galapunktus integrēt valsts vienotajos kontaktpunktos, kuros var integrēt arī cita veida paziņošanu, kas prasīta saskaņā ar Savienības tiesību aktiem.

---

24 Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 (OV L 333, 27.12.2022., 1. lpp.).

25 Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp.).

(73) Izveidojot šajā regulā minēto vienoto ziņošanas platformu un lai izmantotu iepriekšējo pieredzi, *ENISA* būtu jāapspriežas ar citām Savienības iestādēm vai aģentūrām, kas pārvalda platformas vai datubāzes, uz kurām attiecas stingras drošības prasības, piemēram, ar Eiropas Savienības Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*). *ENISA* būtu arī jāanalizē iespējamā savstarpējā papildināmība ar Eiropas ievainojamību datubāzi, kas izveidota saskaņā ar Direktīvas (ES) 2022/2555 12. panta 2. punktu.

(74) Ražotājiem un citām fiziskām un juridiskām personām vajadzētu būt iespējai brīvprātīgi paziņot par koordinatoru izraudzītajai *CSIRT* vai *ENISA* par jebkuru ievainojamību, kas ir produktā ar digitāliem elementiem, par kiberdraudiem, kas varētu ietekmēt produkta ar digitāliem elementiem riska profilu, par jebkuru incidentu, kas ietekmē produkta ar digitāliem elementiem drošību, kā arī par situācijām, kad šādi incidenti varētu būt gandrīz notikuši.

(75) Dalībvalstīm būtu jācenšas, cik vien iespējams, risināt problēmas, kas skar ievainojamības pētniekus, tostarp to, ka saskaņā ar valsts tiesību aktiem tiem var tikt noteikta krimināltatbildība. Ņemot vērā to, ka dažās dalībvalstīs fiziskām un juridiskām personām, kas pēta ievainojamības, var draudēt krimināltatbildība un civiltiesiskā atbildība, dalībvalstis tiek mudinātas pieņemt vadlīnijas par informācijas drošības pētnieku nesodīšanu un atbrīvojumu no civiltiesiskās atbildības par viņu darbībām.

(76) Produktu ar digitāliem elementiem ražotājiem būtu jāievieš koordinēta ievainojamības atklāšanas politika, lai sekmētu personu vai vienību ziņošanu par ievainojamībām vai nu tieši ražotājam, vai netieši, un, ja tas tiek pieprasīts, anonīmi, ar *CSIRT* starpniecību, kas izraudzītas par koordinatoriem koordinētai ievainojamību atklāšanai saskaņā ar Direktīvas (ES) 2022/2555 12. panta 1. punktu. Ražotāju koordinētai ievainojamības atklāšanas politikai vajadzētu būt strukturētam procesam, kurā par ievainojamību tiek ziņots ražotājam tādā veidā, lai ražotājs varētu diagnosticēt un novērst šādas ievainojamības, pirms sīkāka informācija par to tiek darīta zināma trešām personām vai sabiedrībai. Turklāt ražotājiem būtu arī jāapsver iespēja publicēt savu drošības politiku mašīnlasāmā formātā. Ņemot vērā to, ka informāciju par izmantojamām ievainojamībām plaši lietotos produktos ar digitāliem elementiem var pārdot par augstām cenām melnajā tirgū, šādu produktu ražotājiem vajadzētu būt iespējai izmantot programmas, lai savas koordinētās ievainojamības atklāšanas politikas satvarā stimulētu ziņošanu par ievainojamībām, nodrošinot, ka personas vai vienības saņem atzinību un kompensāciju par saviem centieniem. Tas attiecas uz tā sauktajām ievainojamību atklāšanas atlīdzinājuma programmām.

(77) Lai sekmētu ievainojamības analīzi, ražotājiem būtu jāidentificē un jādokumentē produktu ar digitāliem elementiem komponenti, arī sagatavojot *SBOM*. Tiem, kas ražo, pērk un ekspluatē programmatūru, *SBOM* var sniegt informāciju, kas uzlabo viņu izpratni par piegādes ķēdi, sniedzot vairākus ieguvumus, un tas jo īpaši palīdz ražotājiem un lietotājiem veikt zināmu nesen konstatētu ievainojamību un kiberdrošības risku izsekošanu. Ražotājiem ir īpaši svarīgi nodrošināt, ka viņu produkti ar digitāliem elementiem nesatur trešo personu izstrādātus komponentus ar ievainojamību. Ražotājiem nevajadzētu būt pienākumam publiskot *SBOM*.

(78) Atbilstoši jaunajiem sarežģītajiem uzņēmējdarbības modeļiem, kas saistīti ar pārdošanu tiešsaistē, uzņēmums, kas darbojas tiešsaistē, var sniegt dažādus pakalpojumus. Atkarībā no tā, kādi pakalpojumi tiek sniegti saistībā ar konkrētu produktu ar digitāliem elementiem, viena un tā pati vienība var tikt iedalīta dažādās uzņēmējdarbības modeļu vai uzņēmēju kategorijās. Ja vienība sniedz tikai tiešsaistes starpniecības pakalpojumus konkrētam produktam ar digitāliem elementiem un ir tikai tiešsaistes tirdzniecības vietas nodrošinātājs, kā definēts Regulas (ES) 2023/988 3. panta 14. punktā, tā nav uzskatāma par vienu no šajā regulā definētajiem uzņēmēju veidiem. Ja viena un tā pati vienība ir tiešsaistes tirdzniecības vietas nodrošinātājs un darbojas arī kā šajā regulā definētais uzņēmējs, kad tā pārdod konkrētus produktus ar digitāliem elementiem, uz to būtu jāattiecina šajā regulā noteiktie pienākumi, kas attiecas uz šāda veida uzņēmējiem. Piemēram, ja tiešsaistes tirdzniecības vietas nodrošinātājs arī izplata produktu ar digitāliem elementiem, tad attiecībā uz minētā produkta pārdošanu tas būtu uzskatāms par izplatītāju. Līdzīgi, ja attiecīgā vienība pārdod sava zīmola produktus ar digitāliem elementiem, tā tiktu uzskatīta par ražotāju, un tādējādi tai būtu jāievēro ražotājiem piemērojamās prasības. Turklāt dažas vienības var kvalificēt kā izpildes pakalpojumu sniedzējus, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2019/1020[26] 3. panta 11. punktā, ja tās piedāvā šādus pakalpojumus. Tāpēc šādi gadījumi būtu jāizvērtē katrs atsevišķi. Ņemot vērā tiešsaistes tirdzniecības vietu nozīmīgo lomu elektroniskās komercijas veicināšanā, tām būtu jācenšas sadarboties ar dalībvalstu tirgus uzraudzības iestādēm, lai palīdzētu nodrošināt, ka produkti ar digitāliem elementiem, kas iegādāti tiešsaistes tirdzniecības vietās, atbilst šajā regulā noteiktajām kiberdrošības prasībām.

---

[26] Eiropas Parlamenta un Padomes Regula (ES) 2019/1020 (2019. gada 20. jūnijs) par tirgus uzraudzību un produktu atbilstību un ar ko groza Direktīvu 2004/42/EK un Regulas (EK) Nr. 765/2008 un (ES) Nr. 305/2011 (OV L 169, 25.6.2019., 1. lpp.).

(79) Lai sekmētu atbilstības izvērtēšanu attiecībā uz šajā regulā noteiktajām prasībām, būtu jānosaka pieņēmums par atbilstību attiecībā uz produktiem ar digitāliem elementiem, kas atbilst saskaņotajiem standartiem, kuros šajā regulā noteiktās kiberdrošības pamatprasības pārveidotas sīki izstrādātās tehniskajās specifikācijās un kuri tiek pieņemti saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1025/2012[27]. Šajā regulā paredzēta kārtība iebildumu iesniegšanai par saskaņotajiem standartiem, ja minētie standarti pilnībā neatbilst šajā regulā noteiktajām prasībām. Standartizācijas procesam būtu jānodrošina līdzsvarota interešu pārstāvība un efektīva pilsoniskās sabiedrības pārstāvju, tostarp patērētāju organizāciju, līdzdalība. Būtu jāņem vērā arī starptautiskie standarti, kas atbilst kiberdrošības aizsardzības līmenim, kas paredzēts šajā regulā noteiktajās kiberdrošības pamatprasībās, lai sekmētu saskaņoto standartu izstrādi un šīs regulas īstenošanu, kā arī uzņēmumiem, jo īpaši mikrouzņēmumiem, mazajiem un vidējiem uzņēmumiem un uzņēmumiem, kas darbojas visā pasaulē, atvieglotu atbilstības panākšanu.

---

[27] Eiropas Parlamenta un Padomes Regula (ES) Nr. 1025/2012 (2012. gada 25. oktobris) par Eiropas standartizāciju, ar ko groza Padomes Direktīvas 89/686/EEK un 93/15/EEK un Eiropas Parlamenta un Padomes Direktīvas 94/9/EK, 94/25/EK, 95/16/EK, 97/23/EK, 98/34/EK, 2004/22/EK, 2007/23/EK, 2009/23/EK un 2009/105/EK un ar ko atceļ Padomes Lēmumu 87/95/EEK un Eiropas Parlamenta un Padomes Lēmumu Nr. 1673/2006/EK (OV L 316, 14.11.2012., 12. lpp.).

(80) Šīs regulas efektīvai īstenošanai īpaši svarīga būs savlaicīga saskaņoto standartu izstrāde šīs regulas piemērošanai noteiktajā pārejas periodā un to pieejamība pirms regulas piemērošanas dienas. Tas jo īpaši attiecas uz nozīmīgiem produktiem ar digitāliem elementiem, kas ietilpst I klasē. Saskaņoto standartu pieejamība ļaus šādu produktu ražotājiem veikt atbilstības novērtēšanu, izmantojot iekšējās kontroles procedūru, un tādējādi varēs izvairīties no sastrēgumposmiem un kavējumiem atbilstības novērtēšanas struktūru darbībā.

(81) Ar Regulu (ES) 2019/881 ir izveidots brīvprātīgs Eiropas kiberdrošības sertifikācijas satvars IKT produktiem, IKT procesiem un IKT pakalpojumiem. Eiropas kiberdrošības sertifikācijas shēmas nodrošina vienotu uzticības satvaru, lai lietotāji varētu izmantot produktus ar digitāliem elementiem, kuri ietilpst šīs regulas darbības jomā. Tādējādi šai regulai būtu jārada sinerģija ar Regulu (ES) 2019/881. Lai sekmētu atbilstības novērtēšanu šajā regulā noteiktajām prasībām, tiek uzskatīts, ka produkti ar digitāliem elementiem, kas ir sertificēti vai par kuriem izdots atbilstības apliecinājums saskaņā ar Eiropas kiberdrošības shēmu atbilstīgi Regulai (ES) 2019/881 un kurus Komisija identificējusi īstenošanas aktā, atbilst šajā regulā noteiktajām kiberdrošības pamatprasībām, ciktāl Eiropas kiberdrošības sertifikāts vai atbilstības apliecinājums vai tā daļas attiecas uz minētajām prasībām. Nepieciešamība pēc jaunām Eiropas kiberdrošības sertifikācijas shēmām attiecībā uz produktiem ar digitāliem elementiem būtu jāizvērtē, ņemot vērā šo regulu, tostarp sagatavojot Savienības mainīgo darba programmu saskaņā ar Regulu (ES) 2019/881. Ja ir vajadzīga jauna shēma, kas aptvertu produktus ar digitāliem elementiem, tostarp nolūkā sekmēt atbilstību šai regulai, Komisija var lūgt *ENISA* sagatavot kandidātshēmas saskaņā ar Regulas (ES) 2019/881 48. pantu. Šādās turpmākās Eiropas kiberdrošības sertifikācijas shēmās, kas attiecas uz produktiem ar digitāliem elementiem, būtu jāņem vērā šajā regulā noteiktās kiberdrošības pamatprasības un atbilstības novērtēšanas procedūras, un tām būtu jāsekmē atbilstība šai regulai. Eiropas kiberdrošības sertifikācijas shēmām, kas stājas spēkā pirms šīs regulas stāšanās spēkā, var būt nepieciešamas papildu specifikācijas par detalizētiem aspektiem attiecībā uz to, kā būtu piemērojams pieņēmums par atbilstību.

Komisija būtu jāpilnvaro ar deleģētajiem aktiem precizēt, ar kādiem nosacījumiem Eiropas kiberdrošības sertifikācijas shēmas var izmantot, lai pierādītu atbilstību šajā regulā noteiktajām kiberdrošības pamatprasībām. Turklāt, lai novērstu nevajadzīgu administratīvo slogu, ražotājiem nevajadzētu būt pienākumam nodrošināt trešās personas veiktu atbilstības novērtējumu, kā tas šajā regulā noteikts saistībā ar attiecīgajām prasībām, ja saskaņā ar šādām Eiropas kiberdrošības sertifikācijas shēmām ir izdots kiberdrošības sertifikāts vismaz būtiskā līmenī.

(82) Stājoties spēkā Īstenošanas Regulai (ES) 2024/482, kas attiecas uz produktiem, kuri ietilpst šīs regulas darbības jomā, piemēram, aparatūras drošības moduļiem un mikroprocesoriem, Komisija vajadzētu būt iespējai ar deleģēto aktu precizēt, kā *EUCC* izdara pieņēmumu par atbilstību šajā regulā vai tās daļās noteiktajām kiberdrošības pamatprasībām. Turklāt šādā deleģētajā aktā var precizēt veidu, kā atbilstīgi *EUCC* izdots sertifikāts atceļ ražotāju pienākumu nodrošināt trešās personas veiktu novērtējumu, kas attiecībā uz atbilstošajām prasībām noteikts saskaņā ar šo regulu.

(83) Pašreizējais Eiropas standartizācijas regulējums, kura pamatā ir gan jaunās pieejas principi, kas noteikti Padomes 1985. gada 7. maija Rezolūcijā par jaunu pieeju tehniskajai saskaņošanai un standartiem, gan Regula (ES) Nr. 1025/2012, pēc noklusējuma veido satvaru tādu standartu izstrādei, kuri nodrošina pieņēmumu par atbilstību attiecīgajām šajā regulā noteiktajām kiberdrošības pamatprasībām. Eiropas standartiem vajadzētu būt tādiem, ko virzījis tirgus, un tajos būtu jāņem vērā sabiedrības intereses, kā arī politikas mērķi, kas skaidri norādīti Komisijas pieprasījumā vienai vai vairākām Eiropas standartizācijas organizācijām izstrādāt saskaņotos standartus noteiktā termiņā, un tiem vajadzētu būt balstītiem uz konsensu. Tomēr, ja nav attiecīgu atsauču uz saskaņotajiem standartiem, Komisijai vajadzētu būt iespējai pieņemt īstenošanas aktus, ar kuriem nosaka kopīgās specifikācijas šajā regulā noteiktajām kiberdrošības pamatprasībām, ar noteikumu, ka, to darot, tā pienācīgi ņem vērā standartizācijas organizāciju lomu un funkcijas, un tas būtu ārkārtas alternatīvs risinājums, ar kuru atvieglo ražotāja pienākumu ievērot šīs kiberdrošības pamatprasības, ja standartizācijas process ir bloķēts vai ja kavējas atbilstīgu saskaņoto standartu izstrāde. Ja šāda kavēšanās ir saistīta ar attiecīgā standarta tehnisko sarežģītību, Komisijai tas būtu jāņem vērā, pirms tiek apsvērta kopīgo specifikāciju izstrāde.

(84) Lai visefektīvākajā veidā izstrādātu kopīgās specifikācijas, kas aptver šajā regulā noteiktās kibredrošības pamatprasības, Komisijai šajā procesā būtu jāiesaista attiecīgās ieinteresētās personas.

(85) "Saprātīgs laikposms" attiecībā uz atsauču uz saskaņotajiem standartiem publicēšanu "*Eiropas Savienības Oficiālajā Vēstnesī*" saskaņā ar Regulu (ES) Nr. 1025/2012 ir laikposms, kurā "*Eiropas Savienības Oficiālajā Vēstnesī*" paredzēts publicēt atsauci uz standartu, tā labojumu vai grozījumu un kurš nedrīkstētu pārsniegt vienu gadu pēc Eiropas standarta izstrādes termiņa, kas noteikts saskaņā ar Regulu (ES) Nr. 1025/2012.

(86) Lai sekmētu novērtējumu par atbilstību šajā regulā noteiktajām kiberdrošības pamatprasībām, būtu jānosaka pieņēmums par atbilstību attiecībā uz produktiem ar digitāliem elementiem, kas atbilst kopīgajām specifikācijām, kuras Komisija saskaņā ar šo regulu pieņēmusi nolūkā formulēt minēto prasību detalizētas tehniskās specifikācijas.

(87) To saskaņoto standartu, kopīgo specifikāciju vai Eiropas kiberdrošības sertifikācijas shēmu piemērošana, kas pieņemti saskaņā ar Regulu (ES) 2019/881 un kas paredz pieņēmumu par atbilstību attiecībā uz kiberdrošības pamatprasībām, kuras piemērojamas produktiem ar digitāliem elementiem, atvieglos ražotāju veikto atbilstības novērtēšanu. Ja ražotājs izvēlas nepiemērot šādus līdzekļus noteiktām prasībām, tam savā tehniskajā dokumentācijā ir jānorāda, kā atbilstība tiek panākta citādi. Turklāt, ja tiktu piemēroti saskaņotie standarti, kopīgas specifikācijas vai Eiropas kiberdrošības sertifikācijas shēmas, kas pieņemtas saskaņā ar Regulu (ES) 2019/881 un paredz ražotāju pieņēmumu par atbilstību, tad tirgus uzraudzības iestādēm būtu iespēja vieglāk pārbaudīt produktu ar digitāliem elementiem atbilstību. Tāpēc produktu ar digitāliem elementiem ražotāji tiek mudināti piemērot šādus saskaņotos standartus, kopīgas specifikācijas vai Eiropas kiberdrošības sertifikācijas shēmas.

(88) Ražotājiem būtu jāsagatavo ES atbilstības deklarācija, tajā sniedzot šajā regulā prasīto informāciju par produktu ar digitāliem elementiem atbilstību kiberdrošības pamatprasībām, kas noteiktas šajā regulā, un vajadzības gadījumā prasībām, kas noteiktas citos attiecīgos Savienības saskaņošanas tiesību aktos, kuros ietverts konkrētais produkts ar digitāliem elementiem. Ražotājiem var pieprasīt arī sagatavot ES atbilstības deklarāciju attiecībā uz citiem Savienības tiesību aktiem. Lai nodrošinātu efektīvu piekļuvi informācijai tirgus uzraudzības nolūkā, būtu jāsagatavo vienota ES atbilstības deklarācija par atbilstību visiem attiecīgajiem Savienības tiesību aktiem. Lai uzņēmējiem samazinātu administratīvo slogu, vajadzētu būt iespējamam, ka minēto vienoto ES atbilstības deklarāciju veido dokumentācija, kas sastāv no atsevišķām atbilstības deklarācijām.

(89) CE zīme, kas norāda uz produkta atbilstību, ir redzamais rezultāts veselam procesam, kas plašākā nozīmē ietver arī atbilstības novērtēšanu Vispārējie principi, kas reglamentē CE zīmi, ir noteikti Eiropas Parlamenta un Padomes Regulā (EK) Nr. 765/2008[28]. Noteikumi attiecībā uz CE zīmes uzlikšanu produktiem ar digitāliem elementiem būtu jānosaka šajā regulā. CE zīmei vajadzētu būt vienīgajai, kas garantē, ka produkti ar digitāliem elementiem atbilst prasībām, kas noteiktas šajā regulā.

---

[28] Eiropas Parlamenta un Padomes Regula (EK) Nr. 765/2008 (2008. gada 9. jūlijs), ar ko nosaka akreditācijas prasības un atceļ Regulu (EEK) Nr. 339/93 (OV L 218, 13.8.2008., 30. lpp.).

(90) Lai uzņēmēji varētu pierādīt atbilstību kiberdrošības pamatprasībām, kas noteiktas šajā regulā, un lai tirgus uzraudzības iestādes varētu nodrošināt, ka produkti ar digitāliem elementiem, kas darīti pieejami tirgū, atbilst šīm prasībām, ir jāparedz atbilstības novērtēšanas procedūras. Eiropas Parlamenta un Padomes Lēmumā Nr. 768/2008/EK[29] ir noteikti atbilstības novērtēšanas procedūru moduļi proporcionāli konkrētā riska līmenim un nepieciešamajam drošības līmenim. Lai nodrošinātu saskaņotību starp nozarēm un izvairītos no *ad hoc* variantiem, atbilstības novērtēšanas procedūrām, kas piemērotas tam, lai verificētu produktu atbilstību šajā regulā noteiktajām kiberdrošības pamatprasībām, būtu jābalstās uz minētajiem moduļiem. Atbilstības novērtēšanas procedūrās būtu jāpārbauda un jāverificē gan ar produktu, gan procesu saistītās prasības, ietverot visu aprites ciklu, kas attiecas uz produktiem ar digitāliem elementiem, ieskaitot produkta ar digitāliem elementiem plānošanu, projektēšanu, izstrādi vai ražošanu, testēšanu un uzturēšanu.

[29] Eiropas Parlamenta un Padomes Lēmums Nr. 768/2008/EK (2008. gada 9. jūlijs) par produktu tirdzniecības vienotu sistēmu un ar ko atceļ Padomes Lēmumu 93/465/EEK (OV L 218, 13.8.2008., 82. lpp.).

(91) Atbilstības novērtēšana attiecībā uz produktiem ar digitāliem elementiem, kas šajā regulā nav uzskaitīti kā nozīmīgi vai kritiski svarīgi produkti ar digitāliem elementiem, var veikt ražotājs uz savu atbildību, ievērojot iekšējās kontroles procedūru, kas pamatota uz Lēmuma 768/2008/EK A moduli, rīkojoties saskaņā ar šo regulu. Tas attiecas arī uz gadījumiem, kad ražotājs izvēlas pilnībā vai daļēji neizmantot piemērojamo saskaņoto standartu, kopīgo specifikāciju vai Eiropas kiberdrošības sertifikācijas shēmu. Ražotājam saglabā rīcības brīvību izvēlēties stingrāku atbilstības novērtēšanas procedūru, kurā tiktu iesaistīta trešā persona. Saskaņā ar iekšējās kontroles atbilstības novērtēšanas procedūru ražotājs uz savu atbildību nodrošina un deklarē, ka produkts ar digitāliem elementiem un ražotāja procesi atbilst kiberdrošības pamatprasībām, kas noteiktas šajā regulā. Ja svarīgs produkts ar digitāliem elementiem ietilpst I klasē, ir vajadzīga papildu garantija, lai pierādītu atbilstību šajā regulā noteiktajām kiberdrošības pamatprasībām. Ražotājam, ja tas vēlas veikt atbilstības novērtēšanu uz savu atbildību (A modulis), būtu jāpiemēro saskaņotie standarti, kopīgās specifikācijas vai Eiropas kiberdrošības sertifikācijas shēmas, kas pieņemtas, ievērojot Regulu (ES) 2019/881, un kuras Komisija identificējusi īstenošanas aktā. Ja ražotājs nepiemēro šādus saskaņotos standartus, kopīgās specifikācijas vai Eiropas kiberdrošības sertifikācijas shēmas, ražotājam būtu jāveic atbilstības novērtēšana, kurā tiek iesaistīta trešā persona (pamatojoties uz B un C modeli vai H moduli). Ņemot vērā administratīvo slogu ražotājiem un to, ka kiberdrošībai ir svarīga nozīme materiālo un nemateriālo produktu ar digitāliem elementiem projektēšanas un izstrādes posmā, nolūkā samērīgi un efektīvi novērtēt svarīgu produktu ar digitāliem elementiem atbilstību kā vispiemērotākās ir izvēlētas atbilstības novērtēšanas procedūras, kas attiecīgi pamatojas uz Lēmuma 768/2008/EK B un C moduli vai H moduli.

Ražotājs, kas īsteno trešās personas veiktu atbilstības novērtēšanu, var izvēlēties procedūru, kas ir vislabāk piemērota tā projektēšanas un ražošanas procesam. Ņemot vērā vēl lielāku kiberdrošības risku, kas saistīts ar tādu svarīgu produktu ar digitāliem elementiem lietošanu, kuri klasificēti kā II klases produkti, atbilstības izvērtēšanā vienmēr būtu jāiesaista trešā persona, turklāt pat tad, ja produkts pilnībā vai daļēji atbilst saskaņotajiem standartiem, kopīgajām specifikācijām vai Eiropas kiberdrošības sertifikācijas shēmām. Ražotājiem, kas ražo svarīgus produktus ar digitāliem elementiem, kuri kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra, vajadzētu būt iespējai ievērot iekšējās kontroles procedūru, kuras pamatā ir A modulis, ar nosacījumu, ka tie dara publiski pieejamu tehnisko dokumentāciju.

(92) Lai gan materiālo produktu ar digitāliem elementiem izveide parasti prasa no ražotājiem ievērojamas pūles visos projektēšanas, izstrādes un ražošanas posmos, produktu ar digitāliem elementiem izveide programmatūras veidā gandrīz pilnībā ir koncentrēta uz projektēšanu un izstrādi, savukārt ražošanas posmam ir maznozīmīgāka loma. Tomēr daudzos gadījumos programmatūras produkti pirms to laišanas tirgū vēl ir jākompilē, jāizgatavo, jākomplektē, jādara pieejami lejupielādēšanai vai jāpārkopē fiziskajos datu nesējos. Piemērojot attiecīgos atbilstības novērtēšanas moduļus nolūkā pārbaudīt produkta atbilstību šajā regulā noteiktajām kiberdrošības pamatprasībām visos projektēšanas, izstrādes un ražošanas posmos, šīs darbības būtu jāuzskata par ražošanu veidojošām darbībām.

(93) Attiecībā uz mikrouzņēmumiem un maziem uzņēmumiem ir lietderīgi mazināt administratīvās izmaksas, lai tā nodrošinātu proporcionalitāti, taču neietekmējot šīs regulas darbības jomā ietilpstošo produktu ar digitāliem elementiem kiberdrošības aizsardzības līmeni vai vienlīdzīgus konkurences apstākļus ražotājiem. Tāpēc Komisijai ir lietderīgi izveidot vienkāršotu tehniskās dokumentācijas veidlapu, kas paredzēta mikrouzņēmumu un mazo uzņēmumu vajadzībām. Komisijas pieņemtajai vienkāršotajai tehniskās dokumentācijas veidlapai būtu jāaptver visi šajā regulā noteiktie piemērojamie elementi, kas saistīti ar tehnisko dokumentāciju, un jānorāda, kā mikrouzņēmums vai mazais uzņēmums var kodolīgi sniegt pieprasītos elementus, piemēram, produkta ar digitāliem elementiem projektēšanas, izstrādes un ražošanas aprakstu. Tādējādi veidlapa palīdzētu atvieglot administratīvās atbilstības slogu, nodrošinot attiecīgajiem uzņēmumiem juridisko noteiktību par sniedzamās informācijas apjomu un detalizētību. Mikrouzņēmumiem un mazajiem uzņēmumiem vajadzētu būt iespējai izvēlēties sniegt ar tehnisko dokumentāciju saistītos piemērojamos elementus arī plašā formā un neizmantot tiem pieejamo vienkāršoto tehnisko formu.

(94) Lai veicinātu un aizsargātu inovācijas, ir svarīgi īpaši ņemt vērā ražotāju, kuri ir mikrouzņēmumi vai mazie vai vidējie uzņēmumi, jo īpaši mikrouzņēmumi un mazie uzņēmumi, tostarp jaunuzņēmumi, intereses. Šajā nolūkā dalībvalstis varētu izstrādāt iniciatīvas, kas vērstas uz ražotājiem, kuri ir mikrouzņēmumi vai mazie uzņēmumi, tostarp attiecībā uz apmācību, izpratnes veicināšanu, informācijas izplatīšanu, testēšanu un trešo personu atbilstības novērtēšanas darbībām, kā arī izmēģināšanas vides (smilškastu) izveidi. Ievērojamus izdevumus ražotājiem, jo īpaši tiem, kas ir mazāki, var radīt tulkošanas izmaksas, kas saistītas gan ar šajā regulā prasīto obligāto dokumentāciju, piemēram, tehnisko dokumentāciju un informāciju un norādījumiem lietotājam, gan saziņu ar iestādēm. Tāpēc dalībvalstīm vajadzētu būt iespējai uzskatīt, ka viena no valodām, ko tās noteikušas un akceptējušas attiecīgajai ražotāju dokumentācijas sagatavošanai un saziņai ar ražotājiem, ir valoda, kas ir plaši saprotama iespējami lielākam skaitam lietotāju.

(95) Lai nodrošinātu šīs regulas raitu piemērošanu, dalībvalstīm pirms šīs regulas piemērošanas dienas būtu jācenšas nodrošināt, ka ir pieejams pietiekams skaits paziņoto struktūru, kas īsteno trešās personas veiktu atbilstības novērtēšanu. Komisijai būtu jācenšas palīdzēt dalībvalstīm un citām attiecīgajām pusēm šajos centienos, lai izvairītos no tā, ka ražotāji saskaras ar šķēršļiem un traucējumiem ienākšanai tirgū. Dalībvalstu vadīti mērķtiecīgi apmācības pasākumi, tostarp attiecīgā gadījumā ar Komisijas atbalstu, var veicināt kvalificētu speciālistu pieejamību, tostarp atbalstīt paziņoto struktūru darbības, kas veiktas saskaņā ar šo regulu. Turklāt, ņemot vērā izmaksas, ko var radīt trešās personas veikta atbilstības novērtēšana, būtu jāapsver iespēja finansēt Savienības un valstu līmeņa iniciatīvas, kuru mērķis ir mazināt šādas izmaksas mikrouzņēmumiem un mazajiem uzņēmumiem.

(96) Lai nodrošinātu proporcionalitāti, atbilstības novērtēšanas struktūrām, nosakot maksu par atbilstības novērtēšanas procedūrām, būtu jāņem vērā mikrouzņēmumu un mazo un vidējo uzņēmumu, tostarp jaunuzņēmumu, specifiskās intereses un vajadzības. Jo īpaši atbilstības novērtēšanas struktūrām attiecīgā šajā regulā paredzētā pārbaudes procedūra un testi būtu jāpiemēro tikai vajadzības gadījumā un izmantojot uz risku balstītu pieeju.

(97) Par “regulatīvo smilškastu” mērķiem būtu jānosaka uzņēmumu inovācijas un konkurētspējas veicināšana, kas tiktu panākta, izveidojot kontrolētu testēšanas vidi pirms produktu ar digitāliem elementiem laišanas tirgū. “Regulatīvajām smilškastēm” būtu jāpalīdz uzlabot juridisko noteiktību visiem dalībniekiem, kas ietilpst šīs regulas darbības jomā, un atvieglot un paātrināt produktu ar digitāliem elementiem piekļuvi Savienības tirgum, jo īpaši, ja tos nodrošina mikrouzņēmumi un mazie uzņēmumi, tostarp jaunuzņēmumi.

(98) Lai īstenotu trešo personu veiktu atbilstības novērtēšanu produktiem ar digitāliem elementiem, valstu paziņojošajām iestādēm būtu jāpaziņo Komisijai un pārējām dalībvalstīm atbilstības novērtēšanas struktūras ar noteikumu, ka tās atbilst prasību kopumam, jo īpaši attiecībā uz neatkarību, kompetenci un interešu konflikta neesamību.

(99) Lai attiecībā uz produktiem ar digitāliem elementiem nodrošinātu saskaņotu atbilstības novērtēšanas kvalitātes līmeni, ir arī jānosaka prasības paziņojošajām iestādēm un citām struktūrām, kuras piedalās paziņoto struktūru novērtēšanā, paziņošanā un pārraudzīšanā. Šajā regulā noteiktā sistēma būtu jāpapildina ar akreditācijas sistēmu, kas paredzēta Regulā (EK) Nr. 765/2008. Akreditācija ir svarīgs līdzeklis, kā verificēt atbilstības novērtēšanas struktūru kompetenci, tāpēc tā arī būtu jāizmanto paziņošanā.

(100) Atbilstības novērtēšanas struktūras, kas ir akreditētas un paziņotas saskaņā ar Savienības tiesību aktiem, kuros noteiktas prasībām, kas ir līdzīgas šajā regulā noteiktajām prasībām, piemēram, atbilstības novērtēšanas struktūra, kas paziņota Eiropas kiberdrošības sertifikācijas shēmai, kura pieņemta, ievērojot Regulu (ES) 2019/881, vai paziņota saskaņā ar Deleģēto regulu (ES) 2022/30, būtu no jauna jānovērtē un jāpaziņo saskaņā ar šo regulu. Tomēr attiecīgās iestādes var noteikt sinerģiju attiecībā uz prasībām, kas pārklājas, lai novērstu nevajadzīgu finansiālo un administratīvo slogu un nodrošinātu raitu un savlaicīgu paziņošanas procesu.

(101) Regulā (EK) Nr. 765/2008 paredzētā pārredzamā akreditācija, kas nodrošina atbilstības sertifikātu vajadzīgo uzticamību, valstu publiskā sektora iestādēm visā Savienībā būtu jāuzskata par vēlamāko līdzekli, kā pierādīt atbilstības novērtēšanas struktūru tehnisko kompetenci. Tomēr valstu iestādes var uzskatīt, ka tām ir piemēroti līdzekļi, ar ko pašām veikt minēto izvērtēšanu. Šādos gadījumos, lai nodrošinātu citu valsts iestāžu veiktās izvērtēšanas pienācīgu uzticamības līmeni, valsts iestādēm būtu jāiesniedz Komisijai un pārējām dalībvalstīm vajadzīgie dokumentārie pierādījumi, ka izvērtētās atbilstības novērtēšanas struktūras atbilst attiecīgajām regulatīvajām prasībām.

(102) Atbilstības novērtēšanas struktūras bieži slēdz apakšlīgumus par kādām to darbības daļām saistībā ar atbilstības novērtēšanu vai izmanto meitasuzņēmumu. Lai nodrošinātu tāda līmeņa aizsardzību, kāda nepieciešama tirgū laižamajam produktam ar digitāliem elementiem, ir ļoti svarīgi, lai atbilstības novērtēšanā iesaistītie apakšuzņēmēji un meitasuzņēmumi attiecībā uz atbilstības novērtēšanas uzdevumu veikšanu atbilstu tādām pašām prasībām, kādām atbilst paziņotās struktūras.

(103) Paziņojošajai iestādei atbilstības novērtēšanas struktūras paziņojums būtu jānosūta Komisijai un pārējām dalībvalstīm, izmantojot atbilstīgi jaunajai pieejai paziņoto un izraudzīto organizāciju (*NANDO*) informācijas sistēmu. *NANDO* ir Komisijas izstrādāts un pārvaldīts elektroniskās paziņošanas rīks, kurā ir atrodams visu paziņoto struktūru saraksts.

(104) Paziņotās struktūras var piedāvāt savus pakalpojumus visā Savienībā, tāpēc ir lietderīgi dot pārējām dalībvalstīm un Komisijai iespēju iebilst pret paziņoto struktūru. Tādēļ ir svarīgi noteikt laikposmu, kurā var novērst visas šaubas vai bažas par atbilstības novērtēšanas struktūru kompetenci, pirms tās sāk darboties kā paziņotās struktūras.

(105) Konkurētspējas nolūkos ir svarīgi, lai paziņotās struktūras piemērotu atbilstības novērtēšanas procedūras, neradot lieku slogu uzņēmējiem. Tā paša iemesla dēļ, kā arī lai nodrošinātu vienlīdzīgu attieksmi pret uzņēmējiem, jānodrošina saskaņotība atbilstības novērtēšanas procedūru tehniskajā piemērošanā. Vislabāk to var panākt ar atbilstīgu koordinēšanu un sadarbību starp paziņotajām struktūrām.

(106) Tirgus uzraudzība ir būtisks instruments Savienības tiesību aktu pareizas un vienotas piemērošanas nodrošināšanā. Tādēļ ir lietderīgi ieviest tiesisko regulējumu, saskaņā ar kuru tirgus uzraudzību var veikt pienācīgā veidā. Eiropas Parlamenta un Padomes Regulā (ES) 2019/1020 paredzētos noteikumus par Savienības tirgus uzraudzību un kontroli attiecībā uz produktiem, ko ieved Savienības tirgū, piemēro produktiem ar digitāliem elementiem, kas ietilpst šīs regulas darbības jomā.

(107) Saskaņā ar Regulu (ES) 2019/1020 tirgus uzraudzības iestāde veic tirgus uzraudzību tās dalībvalsts teritorijā, kura to ir izraudzījusi. Šai regulai nebūtu jāliedz dalībvalstīm izraudzīties kompetentās iestādes tirgus uzraudzības uzdevumu veikšanai. Katrai dalībvalstij savā teritorijā būtu jāizraugās viena vai vairākas tirgus uzraudzības iestādes. Dalībvalstīm būtu jāspēj izraudzīties jebkuru esošu vai jaunu iestādi, kas darbosies kā tirgus uzraudzības iestāde, tostarp kompetentās iestādes, kas izraudzītas vai izveidotas saskaņā ar Direktīvas (ES) 2022/2555 8. pantu, valsts kiberdrošības sertifikācijas iestādes, kas izraudzītas saskaņā ar Regulas (ES) 2019/881 58. pantu, vai tirgus uzraudzības iestādes, kas izraudzītas Direktīvas 2014/53/ES vajadzībām. Uzņēmējiem būtu pilnībā jāsadarbojas ar tirgus uzraudzības iestādēm un citām kompetentajām iestādēm. Katrai dalībvalstij būtu jāinformē Komisija un pārējās dalībvalstis par savām tirgus uzraudzības iestādēm un par katras minētās iestādes kompetences jomām un jānodrošina ar šo regulu saistīto tirgus uzraudzības uzdevumu veikšanai vajadzīgie resursi un prasmes. Saskaņā ar Regulas (ES) 2019/1020 10. panta 2. un 3. punktu katrai dalībvalstij būtu jāizraugās vienotais sadarbības birojs, kam cita starpā vajadzētu atbildēt par tirgus uzraudzības iestāžu saskaņotas nostājas pārstāvēšanu un palīdzības sniegšanu dažādu dalībvalstu tirgus uzraudzības iestāžu sadarbībā.

(108) Šīs regulas vienotai piemērošanai būtu jāizveido īpaša administratīvās sadarbības grupa (*ADCO*) produktu ar digitāliem elementiem kibernoturībai, ievērojot Regulas (ES) 2019/1020 30. panta 2. punktu. *ADCO* sastāvā vajadzētu būt izraudzīto tirgus uzraudzības iestāžu pārstāvjiem un attiecīgā gadījumā arī vienoto sadarbības biroju pārstāvjiem. Komisijai būtu jāatbalsta un jāsekmē sadarbība starp tirgus uzraudzības iestādēm, izmantojot Savienības produktu atbilstības tīklu, kas izveidots saskaņā ar Regulas (ES) 2019/1020 29. pantu, un kurā piedalās pārstāvji no katras dalībvalsts, to vidū pārstāvis no katra vienotā sadarbības biroja, kā norādīts minētās regulas 10. pantā, kā arī fakultatīvs valsts eksperts, *ADCO* priekšsēdētāji un Komisijas pārstāvji. Komisijai būtu jāpiedalās Savienības produktu atbilstības tīkla, tā apakšgrupu un *ADCO* sanāksmēs. Tai arī būtu jāpalīdz *ADCO*, nodrošinot izpildsekretariātu, kas sniedz tehnisko un loģistikas atbalstu. *ADCO* var arī uzaicināt piedalīties neatkarīgus ekspertus, un tās sadarboties ar citām *ADCO*, piemēram, tām, kas izveidotas saskaņā ar Direktīvu 2014/53/ES.

(109) Tirgus uzraudzības iestādēm, izmantojot *ADCO*, kas izveidotas saskaņā ar šo regulu, būtu cieši jāsadarbojas un būtu jāspēj izstrādāt norādījumus, lai atvieglotu tirgus uzraudzības darbības valsts līmenī, piemēram, izstrādājot paraugpraksi un rādītājus, lai efektīvi pārbaudītu produktu ar digitāliem elementiem atbilstību šai regulai.

(110) Lai nodrošinātu savlaicīgus, samērīgus un efektīvus pasākumus attiecībā uz produktiem ar digitāliem elementiem, kas rada būtisku kiberdrošības risku, būtu jānodrošina Savienības drošības procedūra, saskaņā ar kuru ieinteresētās personas tiek informētas par pasākumiem, kurus paredzēts veikt attiecībā uz šādiem produktiem. Tai arī būtu jādod iespēja tirgus uzraudzības iestādēm sadarbībā ar attiecīgajiem uzņēmējiem vajadzības gadījumā rīkoties savlaicīgāk. Ja dalībvalstis un Komisija vienojas par kādas dalībvalsts veiktā pasākuma pamatotību, Komisijai vairs nebūtu jāiesaistās, izņemot gadījumus, kad neatbilstība var būt izskaidrojama ar saskaņotā standarta nepilnībām.

(111) Noteiktos gadījumos produkts ar digitāliem elementiem, kas atbilst šai regulai, tomēr var radīt būtisku kiberdrošības risku vai izraisīt risku cilvēka veselībai vai drošībai, atbilstībai Savienības vai valstu tiesību aktos noteiktajiem pienākumiem, kuru mērķis ir aizsargāt pamattiesības, to pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus, izmantojot elektronisko informācijas sistēmu, piedāvā būtiskās vienības, kā minēts Direktīvas (ES) 2022/2555 3. panta 1. punktā, vai citiem sabiedrības interešu aizsardzības aspektiem. Tādēļ ir jāizveido noteikumi, kas nodrošina minēto risku mazināšanu. Tāpēc tirgus uzraudzības iestādēm būtu jāveic pasākumi, lai pieprasītu uzņēmējam nodrošināt, ka produkts vairs nerada šādu risku, vai atkarībā no riska to atsauktu vai izņemtu. Tiklīdz tirgus uzraudzības iestāde šādā veidā ierobežo vai aizliedz produkta ar digitāliem elementiem brīvu apriti, dalībvalstij būtu nekavējoties jāpaziņo Komisijai un pārējām dalībvalstīm par pagaidu pasākumiem, norādot šāda lēmuma iemeslus un pamatojumu. Ja tirgus uzraudzības iestāde pieņem šādus pasākumus attiecībā uz produktiem ar digitāliem elementiem, kuri rada risku, Komisijai nekavējoties būtu jāsāk apspriešanās ar dalībvalstīm un attiecīgo uzņēmēju vai uzņēmējiem un būtu jāizvērtē valsts pasākums. Pamatojoties uz šā izvērtējuma rezultātiem, Komisijai būtu jālemj, vai valsts pasākums ir vai nav pamatots. Komisijai savs lēmums būtu jāadresē visām dalībvalstīm un tas nekavējoties jāpaziņo tām un attiecīgajam uzņēmējam vai uzņēmējiem. Ja pasākums tiek uzskatīts par pamatotu, Komisijai būtu arī jāapsver iespēja pieņemt priekšlikumus attiecīgo Savienības tiesību aktu pārskatīšanai.

(112) Attiecībā uz produktiem ar digitāliem elementiem, kas rada būtisku kiberdrošības risku, un ja ir pamats uzskatīt, ka tie neatbilst šai regulai, vai attiecībā uz produktiem, kas atbilst šai regulai, bet rada citus nozīmīgus riskus, piemēram, riskus cilvēka veselībai vai drošībai, atbilstībai Savienības vai valstu tiesību aktos noteiktajiem pienākumiem, ar kuriem paredzēts aizsargāt pamattiesības, vai tādu pakalpojumu pieejamībai, autentiskumam, integritātei vai konfidencialitātei, ko, izmantojot elektronisku informācijas sistēmu, piedāvā būtiskās vienības, kā minēts Direktīvas (ES) 2022/2555 3. panta 1. punktā, Komisijai vajadzētu būt iespējai pieprasīt *ENISA* veikt izvērtēšanu. Pamatojoties uz minēto izvērtējumu, Komisijai ar īstenošanas aktiem būtu jāspēj pieņemt korektīvus vai ierobežojošus pasākumus Savienības līmenī, tostarp pieprasot attiecīgos produktus ar digitāliem elementiem izņemt no tirgus vai atsaukt pienācīgā termiņā, kas samērīgs ar risku. Komisijai vajadzētu būt iespējai izmantot šādu intervenci tikai izņēmuma apstākļos, kas attaisno tūlītēju intervenci, lai saglabātu pareizu iekšējā tirgus darbību, un tikai tādā gadījumā, ja tirgus uzraudzības iestādes nav veikušas efektīvus pasākumus situācijas risināšanai. Šādi izņēmuma apstākļi var būt ārkārtas situācijas, kad, piemēram, ražotājs neatbilstīgu produktu ar digitāliem elementiem ir darījis plaši pieejamu vairākās dalībvalstīs, to arī galvenajās nozarēs lieto vienības, kas ietilpst Direktīvas (ES) 2022/2555 darbības jomā, lai gan tam ir zināmas ievainojamības, kuras izmanto ļaundari un attiecībā uz kurām ražotājs nenodrošina pieejamus programmatūras ielāpus. Komisijai šādās ārkārtas situācijās vajadzētu būt iespējai iejaukties tikai uz laiku, kamēr pastāv izņēmuma apstākļi, un tad, ja neatbilstība šai regulai vai radītie nozīmīgie riski saglabājas.

(113) Gadījumos, kad vairākās dalībvalstīs ir pazīmes, kas liecina par neatbilstību šai regulai, tirgus uzraudzības iestādēm būtu jāspēj veikt kopīgas darbības ar citām iestādēm, lai pārbaudītu atbilstību un identificētu kiberdrošības riskus produktiem ar digitāliem elementiem.

(114) Vienlaicīgas koordinētas kontroles darbības (“kontrolreidi”) ir tirgus uzraudzības iestāžu veiktas īpašas izpildes panākšanas darbības, kas var papildus uzlabot produktu drošību. Kontrolreidi jo īpaši būtu jāveic gadījumos, kad tirgus tendences, patērētāju sūdzības vai citas pazīmes liecina par bieži konstatētiem kiberdrošības riskiem, ko rada noteiktas produktu ar digitāliem elementiem kategorijas. Turklāt, nosakot produktu kategorijas, attiecībā uz kurām jāveic kontrolreidi, tirgus uzraudzības iestādēm būtu jāņem vērā arī apstākļi, kas saistīti ar netehniskiem riska faktoriem. Šajā nolūkā tirgus uzraudzības iestādēm būtu jāspēj ņemt vērā saskaņā ar Direktīvas (ES) 2022/2555 22. pantu veikto kritisko piegādes ķēžu koordinēto drošības riska novērtējumu rezultāti, tostarp apstākļi, kas saistīti ar netehniskiem riska faktoriem. *ENISA* būtu jāiesniedz tirgus uzraudzības iestādēm priekšlikumi par tām produktu ar digitāliem elementiem kategorijām, attiecībā uz kurām varētu rīkot kontrolreidus, cita starpā pamatojoties uz tās saņemtajiem paziņojumiem par ievainojamībām un incidentiem.

(115) Ņemot vērā *ENISA* speciālās zināšanas un pilnvaras, tai būtu jāspēj atbalstīt šīs regulas īstenošanas procesu. Jo īpaši *ENISA* būtu jāspēj ierosināt kopīgas darbības, kas tirgus uzraudzības iestādēm jāveic, pamatojoties uz norādēm vai informāciju par produktu ar digitāliem elementiem iespējamu neatbilstību šai regulai vairākās dalībvalstīs, vai noteikt produktu kategorijas, attiecībā uz kurām būtu jāorganizē kontrolreidi. Izņēmuma apstākļos *ENISA* būtu jāspēj pēc Komisijas pieprasījuma veikt izvērtēšanu attiecībā uz konkrētiem produktiem ar digitāliem elementiem, kas rada būtisku kiberdrošības risku, ja ir nepieciešama tūlītēja intervence ar mērķi saglabāt pareizu iekšējā tirgus darbību.

(116) Ar šo regulu *ENISA* tiek uzticēti konkrēti uzdevumi, kam nepieciešami atbilstoši resursi gan attiecībā uz speciālajām zināšanām, gan cilvēkresursiem, lai *ENISA* varētu efektīvi veikt minētos uzdevumus. Sagatavojot Savienības vispārējā budžeta projektu, Komisija ierosinās *ENISA* štatu sarakstam nepieciešamos budžeta resursus saskaņā ar Regulas (ES) 2019/881 29. pantā noteikto procedūru. Minētā procesa laikā Komisija apsvērs *ENISA* vispārējos resursus, lai tā varētu pildīt savus uzdevumus, tostarp tos, kas *ENISA* uzticēti saskaņā ar šo regulu.

(117) Lai nodrošinātu, ka vajadzības gadījumā tiesisko regulējumu var pielāgot, būtu jādeleģē Komisijai pilnvaras pieņemt aktus saskaņā ar Līguma par Eiropas Savienības darbību (LESD) 290. pantu attiecībā uz svarīgo produktu ar digitāliem elementiem saraksta atjaunināšanu un pievienošanu pielikumā. Saskaņā ar minēto pantu pilnvaras pieņemt aktus būtu jādeleģē Komisijai, lai identificētu produktus ar digitāliem elementiem, uz kuriem attiecas citi Savienības noteikumi, kas nodrošina tādu pašu aizsardzības līmeni kā šī regula, precizējot, vai būtu nepieciešams ierobežojums vai izslēgšana no šīs regulas darbības jomas, kā arī attiecīgā gadījumā minētā ierobežojuma darbības jomu. Saskaņā ar minēto pantu pilnvaras pieņemt aktus būtu jādeleģē Komisijai arī attiecībā uz šīs regulas pielikumā izklāstīto kritiski svarīgo produktu ar digitāliem elementiem iespējamo sertificēšanas pilnvarojumu Eiropas kiberdrošības sertifikācijas shēmas satvarā, kā arī lai atjauninātu kritiski svarīgo produktu ar digitāliem elementiem sarakstu, pamatojoties uz kritiskuma kritērijiem, kas izklāstīti šajā regulā, un lai precizētu konkrētas Eiropas kiberdrošības sertifikācijas shēmas, kas pieņemtas saskaņā ar Regulu (ES) 2019/881 un ko var izmantot, lai pierādītu atbilstību kiberdrošības pamatprasībām vai to daļām, kā izklāstīts šīs regulas pielikumā. Komisijai būtu jādeleģē arī pilnvaras pieņemt aktus, lai noteiktu minimālo atbalsta periodu konkrētām produktu kategorijām, kurās tirgus uzraudzības dati liecina par neatbilstošiem atbalsta periodiem, kā arī lai precizētu noteikumus ar kiberdrošību saistītu iemeslu piemērošanai attiecībā uz paziņojumu par aktīvi izmantotām ievainojamībām izplatīšanas aizkavēšanu.

Turklāt Komisijai būtu jādeleģē pilnvaras pieņemt aktus, lai izveidotu brīvprātīgas drošības apliecinājuma programmas, ar kurām novērtē to, cik lielā mērā produkti ar digitāliem elementiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra, atbilst visām vai dažām šajā regulā noteiktajām kiberdrošības pamatprasībām vai citiem pienākumiem, kā arī lai precizētu ES atbilstības deklarācijas minimālo saturu un papildinātu tehniskajā dokumentācijā iekļaujamos elementus. Ir īpaši būtiski, lai Komisija, veicot sagatavošanas darbus, rīkotu atbilstīgas apspriešanās, tostarp ekspertu līmenī, un lai minētās apspriešanās tiktu rīkotas saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu[30]. Jo īpaši, lai deleģēto aktu sagatavošanā nodrošinātu vienādu dalību, Eiropas Parlaments un Padome visus dokumentus saņem vienlaicīgi ar dalībvalstu ekspertiem, un minēto iestāžu ekspertiem ir sistemātiska piekļuve Komisijas ekspertu grupu sanāksmēm, kurās notiek deleģēto aktu sagatavošana. Pilnvaras pieņemt deleģētos aktus saskaņā ar šo regulu Komisijai būtu jāpiešķir uz piecu gadu laikposmu no ... [šīs regulas spēkā stāšanās diena]. Komisijai būtu jāsagatavo ziņojums par pilnvaru deleģēšanu vēlākais deviņus mēnešus pirms piecu gadu laikposma beigām. Pilnvaru deleģēšana būtu automātiski jāpagarina uz tāda paša ilguma laikposmiem, ja vien Eiropas Parlaments vai Padome neiebilst pret šādu pagarinājumu vēlākais trīs mēnešus pirms katra laikposma beigām.

[30] OV L 123, 12.5.2016., 1. lpp.

(118) Lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, būtu jāpiešķir īstenošanas pilnvaras Komisijai precizēt šīs regulas pielikumā izklāstīto svarīgo produktu ar digitāliem elementiem kategoriju tehnisko aprakstu, precizēt *SBOM* formātu un elementus, sīkāk precizēt formātu un procedūru paziņojumiem par aktīvi izmantotām ievainojamībām un nopietniem incidentiem, kas ietekmē ražotāju iesniegto produktu ar digitāliem elementiem drošību, noteikt kopīgas specifikācijas, kas aptver tehniskās prasības, kuras nodrošina līdzekļus šīs regulas pielikumā noteikto kiberdrošības pamatprasību izpildei, noteikt tehniskās specifikācijas marķējumiem, piktogrammām vai jebkādām citām zīmēm, kas saistītas ar produktu ar digitāliem elementiem drošību, to atbalsta periodu un mehānismus to izmantošanas veicināšanai un sabiedrības labākai informēšanai par produktu ar digitāliem elementiem drošību, precizēt vienkāršoto dokumentācijas veidlapu, kas paredzēta mikrouzņēmumu un mazo uzņēmumu vajadzībām, un ārkārtas apstākļos kas pamato tūlītēju iejaukšanos, lai saglabātu iekšējā tirgus pienācīgu darbību, lemt par korektīviem vai ierobežojošiem pasākumiem Savienības līmenī. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011[31].

(119) Lai nodrošinātu tirgus uzraudzības iestāžu uzticamu un konstruktīvu sadarbību Savienības un valstu līmenī, visām šīs regulas piemērošanā iesaistītajām pusēm būtu jāievēro to uzdevumu izpildē iegūtās informācijas un datu konfidencialitāte.

---

[31] Eiropas Parlamenta un Padomes Regula (ES) Nr. 182/2011 (2011. gada 16. februāris), ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13. lpp., ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(120) Lai nodrošinātu šajā regulā noteikto pienākumu efektīvu izpildi, katrai tirgus uzraudzības iestādei vajadzētu būt pilnvarām uzlikt administratīvus naudas sodus vai pieprasīt to uzlikšanu. Tāpēc būtu jānosaka maksimālie administratīvo naudas sodu līmeņi, kas valstu tiesību aktos ir jāparedz attiecībā uz šajā regulā noteikto pienākumu neizpildi. Lemjot par administratīvā naudas soda apmēru katrā atsevišķā gadījumā, būtu jāņem vērā visi konkrētās situācijas attiecīgie apstākļi un vismaz tie, kas skaidri noteikti šajā regulā, tostarp tas, vai ražotājs ir mikrouzņēmums, mazais vai vidējais uzņēmums, arī jaunuzņēmums, un vai tā pati vai citas tirgus uzraudzības iestādes tam pašam uzņēmējam jau ir piemērojušas administratīvos naudas sodus par līdzīgiem pārkāpumiem. Šādi apstākļi varētu būt vai nu atbildību pastiprinoši – gadījumos, kad tā paša uzņēmēja pārkāpums turpinās citu dalībvalstu teritorijā, nevis tās dalībvalsts teritorijā, kurā jau ir ticis piemērots administratīvais naudas sods, – vai arī atbildību mīkstinoši, nodrošinot, ka attiecībā uz jebkuru citu administratīvo naudas sodu, ko cita tirgus uzraudzības iestāde apsver attiecībā uz to pašu uzņēmēju vai tāda paša veida pārkāpumu, kopā ar citiem attiecīgiem īpašiem apstākļiem jau būtu jāņem vērā citās dalībvalstīs uzliktais sods un tā apmērs. Visos šādos gadījumos attiecībā uz kumulatīvo administratīvo naudas sodu, ko vairāku dalībvalstu tirgus uzraudzības iestādes varētu piemērot vienam un tam pašam uzņēmējam par viena un tā paša veida pārkāpumu, būtu jānodrošina proporcionalitātes principa ievērošana. Ņemot vērā to, ka administratīvie naudas sodi neattiecas uz mikrouzņēmumiem vai mazajiem uzņēmumiem par to, ka nav ievērots 24 stundu termiņš agrīnās brīdināšanas paziņojumam par aktīvi izmantotām ievainojamībām vai nopietniem incidentiem, kas ietekmē produkta ar digitāliem elementiem drošību, nedz arī uz atvērtā pirmkoda programmatūras pārzini par jebkādiem šīs regulas pārkāpumiem, un ievērojot principu, ka sankcijām vajadzētu būt efektīvām, samērīgām un atturošām, dalībvalstīm nebūtu jāpiemēro minētajām vienībām cita veida finansiālas sankcijas.

(121) Ja administratīvie naudas sodi tiek uzlikti personām, kas nav uzņēmums, kompetentajai iestādei, apsverot atbilstošo naudas soda apjomu, būtu jāņem vērā vispārējais ienākumu līmenis dalībvalstī, kā arī attiecīgās personas ekonomiskā situācija. Dalībvalstīm būtu jānosaka, vai un kādā apmērā administratīvie naudas sodi būtu piemērojami publiskām iestādēm.

(122) Dalībvalstīm, ņemot vērā apstākļus valstī, būtu jāizskata iespēja izmantot ieņēmumus no šajā regulā paredzētajiem sodiem vai to finansiālo ekvivalentu, lai atbalstītu kiberdrošības politiku un paaugstinātu kiberdrošības līmeni Savienībā, cita starpā palielinot kvalificētu kiberdrošības speciālistu skaitu, stiprinot mikrouzņēmumu un mazo un vidējo uzņēmumu spēju veidošanu un uzlabojot sabiedrības informētību par kiberdraudiem.

(123) Savienība attiecībās ar trešām valstīm *inter alia* cenšas veicināt reglamentēto produktu starptautisku tirdzniecību. Lai sekmētu tirdzniecību, var piemērot plašu pasākumu klāstu, ieskaitot vairākus juridiskus instrumentus, piemēram, divpusējus (starpvaldību) savstarpējas atzīšanas nolīgumus (SAN) par reglamentēto produktu atbilstības novērtēšanu un marķēšanu. SAN tiek izveidoti starp Savienību un trešām valstīm, kurām ir salīdzināms tehniskās attīstības līmenis un kurām ir saderīga pieeja attiecībā uz atbilstības novērtēšanu. Saskaņā ar minētajiem nolīgumiem tiek savstarpēji atzīti sertifikāti, atbilstības zīmes un testēšanas ziņojumi, ko vienas nolīguma puses atbilstības novērtēšanas struktūras ir izdevušas atbilstīgi otras nolīguma puses tiesību aktiem. Pašlaik ir spēkā SAN ar vairākām trešām valstīm. Minētie SAN attiecas uz vairākām konkrētām nozarēm, kas dažādās trešās valstīs var būt atšķirīgas. Lai papildus sekmētu tirdzniecību un atzīstot, ka produktu ar digitāliem elementiem piegādes ķēdes ir globālas, SAN par atbilstības novērtēšanu var noslēgt attiecībā uz produktiem, kurus atbilstīgi šai regulai reglamentē Savienība saskaņā ar LESD 218. pantu. Svarīga ir arī sadarbība ar trešām partnervalstīm, lai stiprinātu kibernoturību visā pasaulē, jo ilgtermiņā tā sekmēs kiberdrošības satvara stiprināšanu gan Savienībā, gan ārpus tās.

(124) Patērētājiem vajadzētu būt tiesīgiem īstenot savas tiesības saistībā ar pienākumiem, kas ar šo regulu noteikti uzņēmējiem, un to darīt, izmantojot pārstāvības prasības, ievērojot Eiropas Parlamenta un Padomes Direktīvu (ES) 2020/1828[32]. Minētajā nolūkā šajā regulā būtu jāparedz, ka Direktīva (ES) 2020/1828 ir piemērojama pārstāvības prasībām par šīs regulas pārkāpumiem, kas kaitē vai var kaitēt patērētāju kolektīvajām interesēm. Tādēļ būtu attiecīgi jāgroza minētās direktīvas I pielikums. Dalībvalstu ziņā ir nodrošināt, ka minētie grozījumi tiek atspoguļoti to transponēšanas pasākumos, ko pieņem saskaņā ar minēto direktīvu, lai gan valsts transponēšanas pasākumu pieņemšana šajā sakarā nav nosacījums tam, lai minēto direktīvu piemērotu šīm pārstāvības prasībām. Minēto direktīvu būtu jāsāk piemērot pārstāvības prasībām par ražotāju un attiecīgā gadījumā importētāju, pilnvaroto pārstāvju un izpildes pakalpojumu sniedzēju izdarītiem šīs regulas noteikumu pārkāpumiem, kuri kaitē vai var kaitēt patērētāju kolektīvajām interesēm, no ... [36 mēneši no šīs regulas spēkā stāšanās dienas].

(125) Komisijai, apspriežoties ar attiecīgajām ieinteresētajām personām, būtu periodiski jāizvērtē un jāpārskata šī regula, jo īpaši lai noteiktu izmaiņu veikšanas nepieciešamību, ņemot vērā izmaiņas sociālajos, politiskajos, tehnoloģiskajos vai tirgus apstākļos. Šī regula atvieglos to vienību atbilstību piegādes ķēdes drošības pienākumiem, kas ietilpst Regulas (ES) 2022/2554 un Direktīvas (ES) 2022/2555 darbības jomā un kas izmanto produktus ar digitāliem elementiem. Komisijai, veicot minēto periodisko pārskatīšanu, būtu jāizvērtē Savienības kiberdrošības satvara kopējā ietekme.

---

[32] Eiropas Parlamenta un Padomes Direktīva (ES) 2020/1828 (2020. gada 25. novembris) par pārstāvības prasībām patērētāju kolektīvo interešu aizsardzībai un ar ko atceļ Direktīvu 2009/22/EK (OV L 409, 4.12.2020., 1. lpp.).

(126) Uzņēmējiem būtu jādod pietiekami daudz laika, lai tie varētu pielāgoties prasībām, kas noteiktas šajā regulā. Šī regula būtu jāsāk piemērot no ... [36 mēneši no šīs regulas spēkā stāšanās dienas], izņemot ziņošanas pienākumus, kuri attiecas uz aktīvi izmantotām ievainojamībām un nopietniem incidentiem, kas ietekmē produktu ar digitāliem elementiem drošību, un kuri būtu jāsāk piemērot no ... [21 mēnesis no šīs regulas spēkā stāšanās dienas], un izņemot noteikumus par atbilstības novērtēšanas struktūru paziņošanu, kuri būtu jāsāk piemērot no ... [18 mēneši no šīs regulas spēkā stāšanās dienas].

(127) Ir svarīgi sniegt atbalstu mikrouzņēmumiem un mazajiem un vidējiem uzņēmumiem, tostarp jaunuzņēmumiem, šīs regulas īstenošanā un līdz minimumam samazināt īstenošanas riskus, ko rada zināšanu un lietpratības trūkums tirgū, kā arī lai atvieglotu ražotāju atbilstības panākšanu šajā regulā noteiktajiem pienākumiem. Programma "Digitālā Eiropa" un citas attiecīgās Savienības programmas sniedz finansiālu un tehnisku atbalstu, kas ļauj minētajiem uzņēmumiem veicināt Savienības ekonomikas izaugsmi un kopējā kiberdrošības līmeņa stiprināšanu Savienībā. Arī Eiropas Kiberdrošības kompetenču centrs un nacionālie koordinācijas centri, kā arī Eiropas digitālās inovācijas centri, ko Komisija un dalībvalstis izveidojušas Savienības vai valstu līmenī, varētu atbalstīt uzņēmumus un publiskā sektora organizācijas un veicināt šīs regulas īstenošanu. Tās varētu savu attiecīgo uzdevumu un kompetences jomu satvarā sniegt tehnisku un zinātnisku atbalstu mikrouzņēmumiem un maziem un vidējiem uzņēmumiem, piemēram, testēšanas darbībām un trešo personu veiktiem atbilstības novērtējumiem. Tās varētu arī veicināt rīku ieviešanu, lai atvieglotu šīs regulas īstenošanu.

(128) Turklāt dalībvalstīm būtu jāapsver iespēja veikt papildu darbības, kuru mērķis ir sniegt norādījumus un atbalstu mikrouzņēmumiem un maziem un vidējiem uzņēmumiem, tostarp izveidojot "regulatīvās smilškastes" un īpašus saziņas kanālus. Lai stiprinātu kiberdrošības līmeni Savienībā, dalībvalstis var arī apsvērt iespēju sniegt atbalstu, lai attīstītu spējas un prasmes, kas saistītas ar produktu ar digitāliem elementiem kiberdrošību, uzlabojot uzņēmēju, jo īpaši mikrouzņēmumu un mazo un vidējo uzņēmumu, kibernoturību un veicinot sabiedrības informētību par produktu ar digitāliem elementiem kiberdrošību.

(129) Ņemot vērā to, ka šīs regulas mērķi nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet rīcības ietekmes dēļ to var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minētā mērķa sasniegšanai.

(130) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725[33] 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2022. gada 9. novembrī sniedza atzinumu[34],

IR PIEŅĒMUSI ŠO REGULU.

---

[33] Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).

[34] OV C 452, 29.11.2022., 23. lpp.

I nodaļa
Vispārīgie noteikumi

1. pants

Priekšmets

Šī regula nosaka:

a) noteikumus par to, kā darīt pieejamus tirgū produktus ar digitāliem elementiem, lai nodrošinātu šādu produktu kiberdrošību;

b) kiberdrošības pamatprasības attiecībā uz produktu ar digitāliem elementiem projektēšanu, izstrādi un ražošanu, kā arī ar šiem produktiem saistītos uzņēmēju pienākumus attiecībā uz kiberdrošību;

c) kiberdrošības pamatprasības par ievainojamību novēršanas procesiem, ko ražotāji ieviesuši, lai attiecībā uz produktiem ar digitāliem elementiem nodrošinātu kiberdrošību produktu sagaidāmās izmantošanas laikposmā, kā arī ar šiem procesiem saistītos uzņēmēju pienākumus;

d) noteikumus par tirgus uzraudzību, tostarp kontroli, un šajā pantā minēto noteikumu un prasību izpildi.

2. pants

Darbības joma

1. Šo regulu piemēro produktiem ar digitāliem elementiem, kuri darīti pieejami tirgū un kuru paredzētais nolūks vai pamatoti paredzamais lietojums ietver tiešu vai netiešu loģisku vai fizisku datu savienojumu ar ierīci vai tīklu.

2. Šo regulu nepiemēro produktiem ar digitāliem elementiem, uz kuriem attiecas šādi Savienības tiesību akti:

   a) Regula (ES) 2017/745;

   b) Regula (ES) 2017/746;

   c) Regula (ES) 2019/2144.

3. Šo regulu nepiemēro produktiem ar digitāliem elementiem, kuri sertificēti saskaņā ar Regulu (ES) 2018/1139.

4. Šo regulu nepiemēro iekārtām, kas ietilpst Eiropas Parlamenta un Padomes Direktīvas 2014/90/ES[35] darbības jomā.

[35] Eiropas Parlamenta un Padomes Direktīva 2014/90/ES (2014. gada 23. jūlijs) par kuģu aprīkojumu un ar ko atceļ Padomes Direktīvu 96/98/EK (OV L 257, 28.8.2014., 146. lpp.).

5. Šīs regulas piemērošanu produktiem ar digitāliem elementiem, uz kuriem attiecas citi Savienības noteikumi, kas nosaka prasības saistībā ar visiem vai dažiem riskiem, uz kuriem attiecas I pielikumā izklāstītās kiberdrošības pamatprasības, var ierobežot vai izslēgt, ja:

a) šāda ierobežošana vai izslēgšana atbilst vispārējam tiesiskajam regulējumam, ko piemēro šiem produktiem; kā arī

b) nozaru noteikumi nodrošina tādu pašu aizsardzības līmeni, kāds paredzēts šajā regulā, vai augstāku līmeni.

Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 61. pantu, lai papildinātu šo regulu, precizējot, vai šāda ierobežošana vai izslēgšana ir nepieciešama, attiecīgos produktus un noteikumus, kā arī attiecīgā gadījumā ierobežojuma darbības jomu.

6. Šo regulu nepiemēro rezerves daļām, kas darītas pieejamas tirgū, lai aizstātu identiskus komponentus produktos ar digitāliem elementiem, un kas ražotas saskaņā ar tādām pašām specifikācijām kā komponenti, kurus ar tām paredzēts aizstāt.

7. Šo regulu nepiemēro produktiem ar digitāliem elementiem, kas izstrādāti vai modificēti vienīgi valsts drošības vai aizsardzības mērķiem, vai produktiem, kuri īpaši projektēti klasificētas informācijas apstrādei.

8. Šajā regulā noteiktajos pienākumos neietilpst tādas informācijas sniegšana, kuras izpaušana būtu pretrunā dalībvalstu nacionālās drošības, sabiedriskās drošības vai aizsardzības pamatinteresēm.

3. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "produkts ar digitāliem elementiem" ir programmatūras vai aparatūras produkts un tā attālinātās datu apstrādes risinājumi, ieskaitot programmatūras vai aparatūras komponentus, kas tiek laisti tirgū atsevišķi;

2) "attālināta datu apstrāde" ir tāda datu apstrāde no attāluma, kurai programmatūras projektēšanu un izstrādi ir veicis vai par to ir bijis atbildīgs ražotājs un kuras neesamība liegtu izpildīt kādu no produkta ar digitāliem elementiem funkcijām;

3) "kiberdrošība" ir kiberdrošība, kā definēts Regulas (ES) 2019/881 2. panta 1) punktā;

4) "programmatūra" ir elektroniskās informācijas sistēmas daļa, kura sastāv no datora koda;

5) "aparatūra" ir fiziska elektroniskā informācijas sistēma vai tās daļas, kas spēj apstrādāt, uzglabāt vai pārraidīt digitālos datus;

6) “komponents” ir programmatūra vai aparatūra, kas paredzēta integrēšanai elektroniskajā informācijas sistēmā;

7) “elektroniskā informācijas sistēma” ir sistēma, ieskaitot elektriskas vai elektroniskas iekārtas, kas spēj apstrādāt, uzglabāt vai pārraidīt digitālos datus;

8) “loģiskais savienojums” ir virtuāls datu savienojuma attēlojums, ko īsteno ar programmatūras saskarnes palīdzību;

9) “fiziskais savienojums” ir savienojums starp elektroniskām informācijas sistēmām vai komponentiem, ko panāk, izmantojot fiziskos līdzekļus, tostarp elektriskās, optiskās vai mehāniskās saskarnes, vadus vai radioviļņus;

10) “netiešais savienojums” ir tāds savienojums ar ierīci vai tīklu, kas nenotiek tieši, bet gan kā daļa no lielākas sistēmas, kas ir tieši savienojama ar šādu ierīci vai tīklu;

11) “galapunkts” ir jebkura ierīce, kas savienota ar tīklu un kalpo kā minētā tīkla ieejas punkts;

12) “uzņēmējs” ir ražotājs, pilnvarotais pārstāvis, importētājs, izplatītājs vai cita fiziska vai juridiska persona, kurai saskaņā ar šo regulu ir pienākumi attiecībā uz produktu ar digitāliem elementiem ražošanu vai to, lai produktus ar digitāliem elementiem darītu pieejamus tirgū;

13) “ražotājs” ir fiziska vai juridiska persona, kas izstrādā vai ražo produktus ar digitāliem elementiem vai kas ir projektējusi, izstrādājusi vai ražojusi produktus ar digitāliem elementiem un tirgo tos ar savu vārdu vai preču zīmi par atlīdzību, par naudas izteiksmē izteiktiem līdzekļiem vai bez maksas;

14) “atvērtā pirmkoda programmatūras pārzinis” ir juridiska persona, kura nav ražotājs un kuras nolūks vai mērķis ir sistemātiski un ilgstoši sniegt atbalstu tādu konkrētu produktu ar digitāliem elementiem izstrādei, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra un paredzēti komerciālai darbībai, un kura nodrošina minēto produktu dzīvotspēju;

15) “pilnvarotais pārstāvis” ir fiziska vai juridiska persona, kas iedibināta Savienībā un ir saņēmusi ražotāja rakstisku pilnvaru rīkoties tā vārdā, veicot konkrētus uzdevumus;

16) “importētājs” ir fiziska vai juridiska persona, kas iedibināta Savienībā un laiž tirgū produktu ar digitāliem elementiem, uz kura ir tādas fiziskas vai juridiskas personas nosaukums vai preču zīme, kas iedibināta ārpus Savienības;

17) “izplatītājs” ir tāda fiziska vai juridiska persona piegādes ķēdē, kas nav ražotājs vai importētājs un kas produktu ar digitāliem elementiem, neietekmējot tā īpašības, dara pieejamu Savienības tirgū;

18) “patērētājs” ir fiziska persona, kas darbojas nolūkos, kas nav saistīti ar šīs personas veiktu tirdzniecību, uzņēmējdarbību, amatniecību vai profesiju;

19) “mikrouzņēmumi”, “mazie uzņēmumi” un “vidējie uzņēmumi” ir attiecīgi mikrouzņēmumi, mazie uzņēmumi un vidējie uzņēmumi, kā definēts Komisijas Ieteikuma 2003/361/EK pielikumā;

20) “atbalsta periods” ir periods, kurā ražotājam ir jānodrošina, ka produkta ar digitāliem elementiem ievainojamības tiek novērstas efektīvi un saskaņā ar I pielikuma II daļā noteiktajām kiberdrošības pamatprasībām;

21) “laist tirgū” nozīmē darīt pieejamu Savienības tirgū produktu ar digitāliem elementiem pirmo reizi;

22) “darīt pieejamu tirgū” nozīmē, veicot komercdarbību, par maksu vai bez maksas piegādāt izplatīšanai vai izmantošanai Savienības tirgū produktu ar digitāliem elementiem;

23) “paredzētais nolūks” ir lietojums, kuram ražotājs ir paredzējis produktu ar digitāliem elementiem, ietverot konkrēto kontekstu un lietošanas nosacījumus, kas norādīti informācijā, ko ražotājs sniedzis norādījumos lietotājam, reklāmas vai tirdzniecības materiālos un paziņojumos, kā arī tehniskajā dokumentācijā;

24) “pamatoti paredzams lietojums” ir lietojums, kas ne vienmēr ir paredzētais nolūks, par ko ražotājs informāciju sniedzis norādījumos lietotājam, reklāmas vai tirdzniecības materiālos un paziņojumos, kā arī tehniskajā dokumentācijā, bet kas, visticamāk, var rasties pamatoti paredzamas cilvēka uzvedības vai tehnisku darbību, vai mijiedarbības rezultātā;

25) “pamatoti paredzams nepareizs lietojums” ir produkta ar digitāliem elementiem izmantošana veidā, kas neatbilst paredzētajam nolūkam, bet kas var izrietēt no pamatoti paredzamas cilvēka uzvedības vai mijiedarbības ar citām sistēmām;

26) “paziņojošā iestāde” ir valsts iestāde, kas atbild par to procedūru noteikšanu un veikšanu, kuras nepieciešamas atbilstības novērtēšanas struktūru novērtēšanai, izraudzīšanai un paziņošanai, kā arī to pārraudzībai;

27) “atbilstības novērtēšana” ir process, kurā verificē, vai ir ievērotas I pielikumā izklāstītās kiberdrošības pamatprasības;

28) “atbilstības novērtēšanas struktūra” ir atbilstības novērtēšanas struktūra, kā definēts Regulas (EK) Nr. 765/2008 2. panta 13) punktā;

29) “paziņotā struktūra” ir atbilstības novērtēšanas struktūra, kas izraudzīta saskaņā ar 43. pantu un citiem attiecīgajiem Savienības saskaņošanas tiesību aktiem;

30) “būtiska modifikācija” ir tādas produkta ar digitāliem elementiem izmaiņas pēc laišanas tirgū, kas ietekmē produkta atbilstību I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām vai izraisa izmaiņas paredzētajā nolūkā, par kuru ir saņemts produkta ar digitāliem elementiem novērtējums;

31) “CE zīme” ir marķējums, ar ko ražotājs norāda, ka produkts ar digitāliem elementiem un ražotāja ieviestie procesi atbilst I pielikumā izklāstītajām kiberdrošības pamatprasībām un citiem piemērojamiem Savienības saskaņošanas tiesību aktiem, kuros noteikta šādas zīmes uzlikšana;

32) “Savienības saskaņošanas tiesību akti” ir Savienības tiesību akti, kas uzskaitīti Regulas (ES) 2019/1020 I pielikumā, un jebkuri citi Savienības tiesību akti, ar ko saskaņo to produktu tirdzniecības nosacījumus, uz kuriem attiecas minētā regula;

33) “tirgus uzraudzības iestāde” ir tirgus uzraudzības iestāde, kā definēts Regulas (ES) 2019/1020 3. panta 4) punktā;

34) “starptautisks standarts” ir starptautisks standarts, kā definēts Regulas (ES) Nr. 1025/2012 2. panta 1. punkta a) apakšpunktā;

35) “Eiropas standarts” ir Eiropas standarts, kā definēts Regulas (ES) Nr. 1025/2012 2. panta 1. punkta b) apakšpunktā;

36) “saskaņotais standarts” ir saskaņots standarts, kā definēts Regulas (ES) Nr. 1025/2012 2. panta 1. punkta c) apakšpunktā;

37) “kiberdrošības risks” ir incidenta izraisītu zaudējumu vai traucējumu iespējamība, un to izsaka kā šādu zaudējumu vai traucējumu apmēra un incidenta varbūtības apvienojumu;

38) “būtisks kiberdrošības risks” ir kiberdrošības risks, attiecībā uz kuru, pamatojoties uz tā tehniskajām īpašībām, var pieņemt, ka pastāv liela tāda incidenta varbūtība, kas varētu izraisīt nopietnu negatīvu ietekmi, tajā skaitā radīt ievērojamus materiālus vai nemateriālus zaudējumus vai traucējumus;

39) “programmatūras materiālu komplekts” ir oficiāls reģistrs, kas ietver datus par tiem komponentiem un piegādes ķēdes attiecībām, kuri iekļauti produkta ar digitāliem elementiem programmatūras sastāvdaļās;

40) “ievainojamība” ir produkta ar digitāliem elementiem vājums, uzņēmība pret tehniskām problēmām vai nepilnība, ko var izmantot kā kiberdraudus;

41) “izmantojama ievainojamība” ir ievainojamība, ko pretinieki var efektīvi izmantot praktiskos ekspluatācijas apstākļos;

42) “aktīvi izmantota ievainojamība” ir ievainojamība sistēmā, par kuru ir ticami pierādījumi, ka ļaunprātīgs dalībnieks bez sistēmas īpašnieka atļaujas ir to izmantojis;

43) “incidents” ir incidents, kā definēts Direktīvas (ES) 2022/2555 6. panta 6) punktā;

44) “incidents, kas ietekmē produkta ar digitāliem elementiem drošību” ir incidents, kas negatīvi ietekmē vai spēj negatīvi ietekmēt produkta ar digitāliem elementiem spēju aizsargāt datu vai funkciju pieejamību, autentiskumu, integritāti vai konfidencialitāti;

45) “gandrīz noticis notikums” ir gandrīz noticis notikums, kā definēts Direktīvas (ES) 2022/2555 6. panta 5) punktā;

46) “kiberdraudi” ir kiberdraudi, kā definēts Regulas (ES) 2019/881 2. panta 8) punktā;

47) “personas dati” ir personas dati, kā definēts Regulas (ES) 2016/679 4. panta 1) punktā;

48) “brīvi pieejama atvērtā pirmkoda programmatūra” ir programmatūra, kuras pirmkods tiek atklāti kopīgots un kura ir pieejama saskaņā ar brīvi pieejama atvērtā pirmkoda licenci, kas nodrošina visas tiesības padarīt to brīvi pieejamu, lietojamu, modificējamu un tālāk izplatāmu;

49) “atsaukšana” ir atsaukšana, kā definēts Regulas (ES) 2019/1020 3. panta 22) punktā;

50) “izņemšana” ir izņemšana, kā definēts Regulas (ES) 2019/1020 3. panta 23) punktā;

51) “par koordinatoru izraudzītā *CSIRT*” ir *CSIRT*, kas izraudzīta par koordinatoru, ievērojot Direktīvas (ES) 2022/2555 12. panta 1. punktu.

4. pants

Brīva aprite

1. Dalībvalstis aspektos, kurus aptver šī regula, nekavē darīt pieejamus tirgū produktus ar digitāliem elementiem, kas atbilst šai regulai.

2. Tirdzniecības gadatirgos, izstādēs, demonstrācijās vai līdzīgos pasākumos dalībvalstis neliedz prezentēt vai izmantot tādus produktus ar digitāliem elementiem, kas neatbilst šai regulai, tostarp to prototipus, ar noteikumu, ka uz produkta ir redzama zīme, kas skaidri norāda, ka tas neatbilst šai regulai un ka to nedrīkst darīt pieejamu tirgū, kamēr tas neatbilst šai regulai.

3. Dalībvalstis neliedz darīt pieejamu tirgū nepabeigtu programmatūru, kas neatbilst šai regulai, ar noteikumu, ka programmatūra ir pieejama tikai ierobežotu laiku, kas nepieciešams testēšanas vajadzībām, ka uz tās ir labi redzama zīme, kas skaidri norāda uz to, ka programmatūra neatbilst šai regulai un nebūs pieejama tirgū citiem nolūkiem kā vien testēšanai.

4. Šā panta 3. punktu nepiemēro drošības sastāvdaļām, kas minētas citos Savienības saskaņošanas tiesību aktos, kas nav šī regula.

5. pants

Produktu ar digitāliem elementiem publiskais iepirkums un izmantošana

1. Šī regula neliedz dalībvalstīm piemērot produktiem ar digitāliem elementiem papildu kiberdrošības prasības attiecībā uz minēto produktu iepirkumu vai izmantošanu konkrētiem nolūkiem, tostarp tad, ja minētie produkti tiek iepirkti vai izmantoti valsts drošības vai aizsardzības nolūkos, ar noteikumu, ka šādas prasības atbilst dalībvalstu pienākumiem, kas noteikti Savienības tiesību aktos, un ka tās ir nepieciešamas un samērīgas minēto mērķu sasniegšanai.

2. Neskarot Direktīvas 2014/24/ES un 2014/25/ES, ja tiek iepirkti produkti ar digitāliem elementiem, kas ietilpst šīs regulas darbības jomā, dalībvalstis nodrošina, ka iepirkuma procesā tiek ņemta vērā atbilstība šīs regulas I pielikumā izklāstītajām kiberdrošības pamatprasībām, tostarp ražotāju spēja efektīvi novērst ievainojamības.

6. pants

Prasības produktiem ar digitāliem elementiem

Produktus ar digitāliem elementiem dara pieejamus tirgū tikai tad, ja:

a) tie atbilst I pielikuma I daļā izklāstītajām kiberdrošības pamatprasībām ar noteikumu, ka tie ir pareizi instalēti, uzturēti, lietoti tiem paredzētajā nolūkā vai apstākļos, kurus var pamatoti paredzēt, un attiecīgā gadījumā ir instalēti vajadzīgie drošības atjauninājumi; un

b) ražotāja ieviestie procesi atbilst I pielikuma II daļā izklāstītajām kiberdrošības pamatprasībām.

7. pants

Nozīmīgi produkti ar digitāliem elementiem

1. Produktus ar digitāliem elementiem, kuriem ir III pielikumā noteiktās produktu kategorijas pamatfunkcionalitāte, uzskata par nozīmīgiem produktiem ar digitāliem elementiem, un tiem piemēro 32. panta 2. un 3. punktā minētās atbilstības novērtēšanas procedūras. Tas, ka kādā produktā tiek integrēts produkts ar digitāliem elementiem, kam ir III pielikumā noteiktās produktu kategorijas pamatfunkcionalitāte, pats par sevi nenozīmē, ka uz produktu, kurā tas ir integrēts, attiecas 32. panta 2. un 3. punktā minētās atbilstības novērtēšanas procedūras.

2. Šā panta 1. punktā minētās produktu ar digitāliem elementiem kategorijas, kas iedalītas I un II klasē, kā izklāstīts III pielikumā, atbilst vismaz vienam no šādiem kritērijiem:

a) produkts ar digitāliem elementiem galvenokārt pilda funkcijas, kas ir kritiski svarīgas citu produktu, tīklu vai pakalpojumu kiberdrošībai, tostarp nodrošina autentifikāciju un piekļuvi, ielaušanās novēršanu un atklāšanu, galapunktu drošību vai tīkla aizsardzību;

b) produkts ar digitāliem elementiem pilda funkciju, kam piemīt būtisks nelabvēlīgas ietekmes risks saistībā ar intensitāti un spēju traucēt, kontrolēt vai nodarīt kaitējumu lielam skaitam citu produktu vai tā lietotāju veselībai, drošībai vai drošumam, izmantojot tiešas manipulācijas, piemēram, saistībā ar centrālās sistēmas funkcijām, tostarp tīkla pārvaldību, konfigurācijas kontroli, virtualizāciju vai personas datu apstrādi.

3. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 61. pantu, lai grozītu III pielikumu, katrā produktu ar digitāliem elementiem kategoriju klasē iekļaujot jaunu kategoriju un precizējot tās definīciju, pārvietojot produktu kategoriju no vienas klases uz citu vai svītrojot no minētā saraksta tajā esošu kategoriju. Izvērtējot vajadzību grozīt III pielikumā iekļauto sarakstu, Komisija ņem vērā ar kiberdrošību saistītās funkcionalitātes vai funkciju un kiberdrošības riska līmeni, ko rada produkti ar digitāliem elementiem, kā noteikts šā panta 2. punktā minētajos kritērijos.

Šā punkta pirmajā daļā minētajos deleģētajos aktos attiecīgā gadījumā paredz 12 mēnešu minimālo pārejas periodu, jo īpaši, ja I vai II klasei pievieno jaunu nozīmīgu produktu ar digitāliem elementiem kategoriju vai to pārvieto no I klases uz II klasi, kā norādīts III pielikumā, pirms sāk piemērot attiecīgās atbilstības novērtēšanas procedūras, kā minēts 32. panta 2. un 3. punktā, ja vien nenovēršamu steidzamu iemeslu dēļ nav attaisnojams īsāks pārejas periods.

4. Līdz ... [12 mēneši no šīs regulas spēkā stāšanās dienas] Komisija pieņem īstenošanas aktu, kurā precizē III pielikumā noteikto I un II klases produktu ar digitāliem elementiem kategoriju tehnisko aprakstu un IV pielikumā noteikto produktu ar digitāliem elementiem kategoriju tehnisko aprakstu. Minēto īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 62. panta 2. punktā.

8. pants

Kritiski svarīgi produkti ar digitāliem elementiem

1. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 61. pantu, lai papildinātu šo regulu nolūkā noteikt, kuriem produktiem ar digitāliem elementiem, kam ir šīs regulas IV pielikumā noteikta produktu kategorijas pamatfunkcionalitāte, ir jāsaņem Eiropas kiberdrošības sertifikāts vismaz apliecinājuma līmenī "būtisks" saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu, kas pieņemta, ievērojot Regulu (ES) 2019/881, lai pierādītu atbilstību šīs regulas I pielikumā noteiktajām kiberdrošības pamatprasībām vai to daļām, ar noteikumu, ka, ievērojot Regulu (ES) 2019/881, ir pieņemta Eiropas kiberdrošības sertifikācijas shēma, kas attiecas uz minēto kategoriju produktiem ar digitāliem elementiem, un šī shēma ir pieejama ražotājiem. Minētajos deleģētajos aktos precizē nepieciešamo apliecinājuma līmeni, kas ir samērīgs ar kiberdrošības riska līmeni, kurš saistīts ar produktiem ar digitāliem elementiem, un ņem vērā to paredzēto nolūku, tostarp būtisko vienību kritisko atkarību no tiem, kā minēts Direktīvas (ES) 2022/2555 3. panta 1. punktā.

Pirms šādu deleģēto aktu pieņemšanas Komisija novērtē paredzēto pasākumu iespējamo ietekmi uz tirgu un apspriežas ar attiecīgajām ieinteresētajām personām, tostarp ar Eiropas Kiberdrošības sertifikācijas grupu, kas izveidota ar Regulu (ES) 2019/881. Novērtējumā ņem vērā dalībvalstu gatavību un spēju līmeni attiecīgās Eiropas kiberdrošības sertifikācijas shēmas īstenošanai. Ja šā punkta pirmajā daļā minētie deleģētie akti nav pieņemti, produktiem ar digitāliem elementiem, kuriem ir IV pielikumā noteiktās produktu kategorijas pamatfunkcionalitāte, piemēro 32. panta 3. punktā minētās atbilstības novērtēšanas procedūras.

Šā punkta pirmajā daļā minētajos deleģētajos aktos paredz sešu mēnešu minimālo pārejas periodu to piemērošanai, ja vien nenovēršamu steidzamu iemeslu dēļ nav attaisnojams īsāks pārejas periods.

2. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 61. pantu, lai, pievienojot vai svītrojot produktu ar digitāliem elementiem kategorijas, grozītu IV pielikumu. Nosakot šādas kritiski svarīgu produktu ar digitāliem elementiem kategorijas un nepieciešamo apliecinājuma līmeni saskaņā ar šā panta 1. punktu, Komisija ņem vērā 7. panta 2. punktā minētos kritērijus un nodrošināt, ka produktu ar digitāliem elementiem kategorijas atbilst vismaz vienam no šiem kritērijiem:

a) būtiskās vienības, kā minēts Direktīvas (ES) 2022/2555 3. pantā, ir kritiski atkarīgas no produktu ar digitāliem elementiem kategorijas;

b) incidenti un izmantotās ievainojamības attiecībā uz produktu ar digitāliem elementiem kategoriju varētu radīt nopietnus traucējumus kritiski svarīgās piegādes ķēdēs visā iekšējā tirgū.

Pirms šādu deleģēto aktu pieņemšanas Komisija veic 1. punktā minētā veida novērtējumu.

Pirmajā daļā minētajos deleģētajos aktos paredz sešu mēnešu minimālo pārejas periodu, ja vien nenovēršamu steidzamu iemeslu dēļ nav attaisnojams īsāks pārejas periods.

9. pants

Apspriešanās ar ieinteresētajām personām

1. Sagatavojot pasākumus šīs regulas īstenošanai, Komisija apspriežas ar attiecīgajām ieinteresētajām personām, piemēram, attiecīgajām dalībvalstu iestādēm, privātā sektora uzņēmumiem, tostarp mikrouzņēmumiem un maziem un vidējiem uzņēmumiem, atvērtā pirmkoda programmatūras kopienu, patērētāju apvienībām, akadēmiskajām aprindām un attiecīgajām Savienības aģentūrām un struktūrām, kā arī ekspertu grupām, kas izveidotas Savienības līmenī, un ņem vērā to viedokļus. Komisija attiecīgā gadījumā strukturētā veidā apspriežas ar minētajām ieinteresētajām personām un lūdz to viedokļus jo īpaši gadījumos, kad tā:

   a) izstrādā 26. pantā minētos norādījumus;

   b) izstrādā III pielikumā noteikto produktu kategoriju tehniskos aprakstus saskaņā ar 7. panta 4. punktu, novērtējot vajadzību atjaunināt produktu kategoriju sarakstu saskaņā ar 7. panta 3. punktu un 8. panta 2. punktu vai veicot 8. panta 1. punktā minēto iespējamās ietekmes uz tirgu novērtējumu, neskarot šīs regulas 61. pantu;

   c) veic sagatavošanas darbus šīs regulas izvērtēšanai un pārskatīšanai.

2. Komisija vismaz reizi gadā organizē regulāras apspriešanās un informatīvas sanāksmes, lai apkopotu 1. punktā minēto ieinteresēto personu viedokļus par šīs regulas īstenošanu.

10. pants

Prasmju pilnveide kibernoturīgā digitālajā vidē

Šīs regulas nolūkos un lai reaģētu uz speciālistu vajadzībām, atbalstot šīs regulas īstenošanu, dalībvalstis attiecīgā gadījumā ar Komisijas, Eiropas Kiberdrošības kompetenču centra un *ENISA* atbalstu, vienlaikus pilnībā respektējot dalībvalstu atbildību izglītības jomā, veicina pasākumus un stratēģijas, kuru mērķis ir:

a) attīstīt kiberdrošības prasmes un izveidot organizatoriskus un tehnoloģiskus rīkus, lai nodrošinātu kvalificētu speciālistu pietiekamu pieejamību nolūkā atbalstīt tirgus uzraudzības iestāžu un atbilstības novērtēšanas struktūru darbības;

b) palielināt sadarbību starp privāto sektoru, uzņēmējiem, tostarp pārkvalificējot ražotāju darbiniekus, patērētājus, apmācības sniedzējus, kā arī valsts pārvaldes darbiniekus vai pilnveidojot viņu prasmes un tādējādi paplašinot jauniešu iespējas piekļūt darbvietām kiberdrošības nozarē.

11. pants

Produktu vispārējais drošums

Atkāpjoties no Regulas (ES) 2023/988 2. panta 1. punkta trešās daļas b) apakšpunkta, saistībā ar aspektiem un riskiem vai risku kategorijām, kas nav ietvertas šajā regulā, produktiem ar digitāliem elementiem piemēro minētās regulas III nodaļas 1. iedaļu, V un VII nodaļu un IX–XI nodaļu, ja minētajiem produktiem netiek piemērotas specifiskas drošības prasības, kas noteiktas citos Savienības saskaņošanas tiesību aktos, kā definēts Regulas (ES) 2023/988 3. panta 27. punktā.

12. pants

Augsta riska MI sistēmas

1. Neskarot prasības attiecībā uz precizitāti un robustumu, kas noteiktas Regulas (ES) 2024/1689 15. pantā, produktus ar digitāliem elementiem, kas ietilpst šīs regulas darbības jomā un kas, ievērojot minētās regulas 6. pantu, ir klasificēti kā augsta riska MI sistēmas, uzskata par atbilstīgiem minētās regulas 15. pantā noteiktajām kiberdrošības prasībām, ja:

   a) minētie produkti atbilst I pielikuma I daļā izklāstītajām kiberdrošības pamatprasībām;

b) ražotāja ieviestie procesi atbilst I pielikuma II daļā izklāstītajām kiberdrošības pamatprasībām; un

c) Regulas (ES) 2024/1689 15. pantā prasītā kiberdrošības aizsardzības līmeņa sasniegšana ir apliecināta saskaņā ar šo regulu izsniegtajā ES atbilstības deklarācijā.

2. Attiecībā uz šā panta 1. punktā minētajiem produktiem ar digitāliem elementiem un kiberdrošības prasībām piemēro attiecīgo atbilstības novērtēšanas procedūru, kas noteikta Regulas (ES) 2024/1689 43. pantā. Minētās novērtēšanas nolūkā paziņotās struktūras, kuras saskaņā ar Regulu (ES) 2024/1689 ir kompetentas kontrolēt augsta riska MI sistēmu atbilstību, ir arī kompetentas kontrolēt šīs regulas darbības jomā ietilpstošo augsta riska MI sistēmu atbilstību šīs regulas I pielikumā izklāstītajām prasībām ar noteikumu, ka minēto paziņoto struktūru atbilstība šīs regulas 39. pantā noteiktajām prasībām ir izvērtēta saistībā ar Regulā (ES) 2024/1689 noteikto paziņošanas procedūru.

3. Atkāpjoties no šā panta 2. punkta, šīs regulas III pielikumā uzskaitītajiem nozīmīgiem produktiem ar digitāliem elementiem, kuriem piemēro atbilstības novērtēšanas procedūras, kas minētas šīs regulas 32. panta 2. punkta a) un b) apakšpunktā un 32. panta 3. punktā, un kritiski svarīgiem produktiem ar digitāliem elementiem, kuri ir uzskaitīti šīs regulas IV pielikumā un kuriem, ievērojot šīs regulas 8. panta 1. punktu, ir jāsaņem Eiropas kiberdrošības sertifikāts vai, ja tā nav, kuriem piemēro šīs regulas 32. panta 3. punktā minētās atbilstības novērtēšanas procedūras, kuri ir arī klasificēti kā augsta riska MI sistēmas saskaņā ar Regulas (ES) 2024/1689 6. pantu un uz kuriem attiecas Regulas (ES) 2024/1689 VI pielikumā minētā uz iekšējo kontroli pamatotā atbilstības novērtēšanas procedūra, piemēro šajā regulā paredzētās atbilstības novērtēšanas procedūras, ciktāl tās attiecas uz šīs regulas noteiktajām kiberdrošības pamatprasībām.

4. Regulas (ES) 2024/1689 57. pantā minētajās "MI regulatīvajās smilškastēs" var piedalīties šā panta 1. punktā minēto produktu ar digitāliem elementiem ražotāji.

II nodaļa

Uzņēmēju pienākumi un noteikumi attiecībā uz brīvi pieejamu atvērtā pirmkoda programmatūru

13. pants

Ražotāju pienākumi

1. Laižot tirgū produktu ar digitāliem elementiem, ražotāji nodrošina, ka tas ir projektēts, izstrādāts un ražots saskaņā ar I pielikuma I daļā izklāstītajām kiberdrošības pamatprasībām.

2. Nolūkā izpildīt 1. punktā noteikto pienākumu, ražotāji izvērtē ar produktu ar digitāliem elementiem saistītos kiberdrošības riskus un šā novērtējuma rezultātus ņem vērā produkta ar digitāliem elementiem plānošanas, projektēšanas, izstrādes, ražošanas, piegādes un uzturēšanas posmos, lai samazinātu kiberdrošības riskus, novērstu incidentus un samazinātu to ietekmi, arī attiecībā uz lietotāju veselību un drošību.

3. Kiberdrošības riska novērtējumu dokumentē un attiecīgā gadījumā atjaunina atbalsta periodā, kas jānosaka saskaņā ar šā panta 8. punktu. Minētajā kiberdrošības riska novērtējumā ietver vismaz kiberdrošības risku analīzi, kuras pamatā ir produkta ar digitāliem elementiem paredzētais nolūks un pamatoti paredzamais lietojums, kā arī lietošanas nosacījumi, piemēram, darbības vide vai aizsargājamie aktīvi, ņemot vērā paredzamo produkta lietošanas ilgumu. Kiberdrošības riska novērtējumā norāda, vai I pielikuma I daļas 2. punktā izklāstītās drošības prasības ir piemērojamas attiecīgajam produktam ar digitāliem elementiem un, ja ir, tad kādā veidā, un kā minētās prasības tiek īstenotas, pamatojoties uz kiberdrošības riska novērtējumu. Tajā arī norāda, kā ražotājam jāpiemēro I pielikuma I daļas 1. punkts un I pielikuma II daļā noteiktās ievainojamības novēršanas prasības.

4. Laižot tirgū produktu ar digitāliem elementiem, ražotājs iekļauj šā panta 3. punktā minēto kiberdrošības riska novērtējumu tehniskajā dokumentācijā, kas vajadzīga, ievērojot 31. pantu un V pielikumu. Attiecībā uz 12. pantā minētajiem produktiem ar digitāliem elementiem, uz kuriem attiecas arī citi Savienības tiesību akti, kiberdrošības riska novērtējums var būt daļa no minētajos Savienības tiesību aktos prasītā riska novērtējuma. Ja konkrētas kiberdrošības pamatprasības nav piemērojamas tirgotajam produktam ar digitāliem elementiem, ražotājs minētajā tehniskajā dokumentācijā iekļauj skaidru pamatojumu.

5. Lai izpildītu 1. punktā noteikto pienākumu, ražotāji veic uzticamības pārbaudi, ja produktos ar digitāliem elementiem tiek integrēti no trešām personām iegūti komponenti, lai minētie komponenti neapdraudētu produkta ar digitāliem elementiem drošību, tostarp tad, kad tiek integrēti brīvi pieejamas atvērtā pirmkoda programmatūras komponenti, kas nav darīti pieejami tirgū, veicot komercdarbību.

6. Ražotāji pēc tam, kad identificējuši ievainojamību kādā komponentā, tostarp atvērtā pirmkoda komponentā, kas integrēts produktā ar digitāliem elementiem, ziņo par šo ievainojamību personai vai vienībai, kas ražo vai uztur šo komponentu, un pievēršas ievainojamībai un to novērš saskaņā ar I pielikuma II daļā noteiktajām ievainojamības novēršanas prasībām. Ja ražotāji ir izstrādājuši programmatūras vai aparatūras modifikāciju, lai novērstu minētā komponenta ievainojamību, tie attiecīgo kodu vai dokumentāciju dara zināmu personai vai vienībai, kas ražo vai uztur komponentu, attiecīgā gadījumā mašīnlasāmā formātā.

7. Ražotāji tādā veidā, kas ir proporcionāls kiberdrošības risku raksturam, attiecībā uz produktiem ar digitāliem elementiem sistemātiski dokumentē būtiskos kiberdrošības aspektus, ieskaitot ievainojamību, kas tiem kļūst zināma, un jebkādu trešās personas sniegtu būtisku informāciju, kā arī attiecīgā gadījumā atjaunina produktu kiberdrošības riska novērtējumu.

8. Laižot tirgū produktu ar digitāliem elementiem, un atbalsta periodā ražotāji nodrošina to, ka minētā produkta ievainojamības tiek risinātas efektīvi un saskaņā ar I pielikuma II daļā noteiktajām kiberdrošības pamatprasībām.

Ražotāji nosaka atbalsta periodu tā, lai tas atspoguļotu laikposmu, kurā sagaidāms, ka produkts tiks izmantots, jo īpaši ņemot vērā pamatotas lietotāju cerības, produkta raksturu, tostarp tā paredzēto nolūku, kā arī attiecīgos Savienības tiesību aktus, kas nosaka produktu ar digitāliem elementiem darbmūžu. Nosakot atbalsta periodu, ražotāji var ņemt vērā arī atbalsta periodus, ko saviem tirgū laistajiem produktiem ar digitāliem elementiem, kuriem ir līdzīga funkcionalitāte, noteikuši citi ražotāji, darbības vides pieejamību, to integrēto komponentu atbalsta periodus, kuri nodrošina pamatfunkcijas un ir iegūti no trešām personām, kā arī attiecīgos norādījumus, ko sniegusi saskaņā ar 52. panta 15. punktu izveidotā īpašā administratīvās sadarbības grupa (*ADCO*) un Komisija. Jautājumus atbalsta perioda noteikšanai ņem vērā tā, lai nodrošinātu proporcionalitāti.

Neskarot otro daļu, atbalsta periods ir vismaz pieci gadi. Ja sagaidāms, ka produkts ar digitāliem elementiem tiks lietots mazāk nekā piecus gadus, atbalsta periods atbilst paredzamajam lietošanas laikam.

Ņemot vērā 52. panta 16. punktā minētos *ADCO* ieteikumus, Komisija var pieņemt deleģētos aktus saskaņā ar 61. pantu, lai papildinātu šo regulu, nosakot minimālo atbalsta periodu konkrētām produktu kategorijām, ja tirgus uzraudzības dati liecina par nepiemērotiem atbalsta periodiem.

Informāciju, kas ņemta vērā, lai noteiktu produkta ar digitāliem elementiem atbalsta periodu, ražotāji iekļauj VII pielikumā izklāstītajā tehniskajā dokumentācijā.

Ražotājiem ir atbilstīga politika un procedūras, tostarp I pielikuma II daļas 5. punktā minētā koordinētā ievainojamības atklāšanas politika, lai apstrādātu un izlabotu produkta ar digitāliem elementiem iespējamo ievainojamību, par kuru saņemts ziņojums no iekšējiem vai ārējiem avotiem.

9. Ražotāji nodrošina, ka katrs I pielikuma II daļas 8. punktā minētais drošības atjauninājums, kas lietotājiem darīts pieejams atbalsta periodā, pēc tā izdošanas ir pieejams vismaz 10 gadus vai atlikušajā atbalsta periodā atkarībā no tā, kurš termiņš ir ilgāks.

10. Ja ražotājs ir laidis tirgū vēlāk būtiski modificētas programmatūras versijas, minētais ražotājs var nodrošināt atbilstību I pielikuma II daļas 2. punktā noteiktajai kiberdrošības pamatprasībai tikai attiecībā uz to versiju, kuru ražotājs pēdējo reizi laidis tirgū, ar noteikumu, ka iepriekš tirgū laisto versiju lietotājiem bez maksas ir piekļuve pēdējai tirgū laistai versijai un viņiem nerodas papildu izmaksas, lai pielāgotu aparatūras un programmatūras vidi, kurā viņi izmanto minētā produkta oriģinālo versiju.

11. Ražotāji var uzturēt publiskus programmatūras arhīvus, kas uzlabo lietotāju piekļuvi vēsturiskajām versijām. Šādos gadījumos lietotājus viegli pieejamā veidā skaidri informē par riskiem, kas saistīti ar neatbalstītas programmatūras izmantošanu.

12. Pirms produkta ar digitāliem elementiem laišanas tirgū ražotāji sagatavo 31. pantā norādīto tehnisko dokumentāciju.

    Tie veic izvēlētās atbilstības novērtēšanas procedūras, kā minēts 32. pantā, vai nodrošina to veikšanu.

    Ja minētajā atbilstības novērtēšanas procedūrā ir pierādīts, ka produkts ar digitāliem elementiem atbilst I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām un ražotāja ieviestie procesi atbilst I pielikuma II daļā noteiktajām kiberdrošības pamatprasībām, ražotāji sagatavo ES atbilstības deklarāciju saskaņā ar 28. pantu un uzliek CE zīmi saskaņā ar 30. pantu.

13. Ražotāji tehnisko dokumentāciju un ES atbilstības deklarāciju glabā pieejamu tirgus uzraudzības iestādēm vismaz 10 gadus pēc produkta ar digitāliem elementiem laišanas tirgū vai atbalsta periodā atkarībā no tā, kurš termiņš ir ilgāks.

14. Ražotāji nodrošina, ka ir ieviestas procedūras, ar kurām attiecībā uz produktiem ar digitāliem elementiem, kas ietverti ražojumu sērijās, tiek panākta pastāvīga atbilstība šai regulai. Ražotāji pienācīgi ņem vērā izmaiņas izstrādes un ražošanas procesā vai produkta ar digitāliem elementiem projektējumā vai īpašībās, kā arī izmaiņas saskaņotajos standartos, Eiropas kiberdrošības sertifikācijas shēmās vai kopīgajās specifikācijās, kā minēts 27. pantā, uz kurām atsaucoties deklarēta produkta ar digitāliem elementiem atbilstība vai kuras piemērojot verificēta tā atbilstība.

15. Ražotāji nodrošina, ka uz viņu produktiem ar digitāliem elementiem ir tipa, partijas vai sērijas numurs vai cits identifikācijas elements vai, ja tas nav iespējams, ka minētā informācija ir sniegta uz iepakojuma vai produktam ar digitāliem elementiem pievienotajā dokumentā.

16. Ražotāji uz produkta ar digitāliem elementiem, tā iepakojuma vai produktam ar digitāliem elementiem pievienotajā dokumentā norāda ražotāja nosaukumu, reģistrēto komercnosaukumu vai reģistrēto preču zīmi un pasta adresi, e-pasta adresi vai citu digitālu kontaktinformāciju, kā arī attiecīgā gadījumā tīmekļa vietni, kurā var sazināties ar ražotāju. Minēto informāciju iekļauj arī II pielikumā izklāstītajā informācijā un norādījumos lietotājiem. Kontaktinformācija ir lietotājiem un tirgus uzraudzības iestādēm viegli saprotamā valodā.

17. Šīs regulas nolūkiem ražotāji izraugās vienotu kontaktpunktu, lai lietotāji varētu tieši un ātri sazināties ar tiem, tostarp, lai atvieglotu ziņošanu par produkta ar digitāliem elementiem ievainojamībām.

Ražotāji nodrošina, ka lietotāji var viegli identificēt vienoto kontaktpunktu. Tie arī iekļauj informāciju par vienoto kontaktpunktu II pielikumā noteiktajā informācijā un norādījumos lietotājiem.

Vienotais kontaktpunkts ļauj lietotājiem izvēlēties vēlamos saziņas līdzekļus, un šādi līdzekļi neaprobežojas ar automatizētiem rīkiem.

18. Ražotāji nodrošina, ka produktiem ar digitāliem elementiem tiek pievienota II pielikumā noteiktā informācija un norādījumi lietotājiem papīra vai elektroniskā formātā. Šādu informāciju un norādījumus sniedz lietotājiem un tirgus uzraudzības iestādēm viegli saprotamā valodā. Tie ir skaidri, saprotami, nepārprotami un salasāmi. Tie ļauj droši instalēt, ekspluatēt un lietot produktus ar digitāliem elementiem. Ražotāji II pielikumā noteikto informāciju un norādījumus lietotājam glabā pieejamus lietotājiem un tirgus uzraudzības iestādēm vismaz 10 gadus pēc produkta ar digitāliem elementiem laišanas tirgū vai atbalsta periodā atkarībā no tā, kurš laikposms ir ilgāks. Ja šādu informāciju un instrukcijas sniedz tiešsaistē, ražotāji nodrošina, ka ir piekļūstami, lietotājdraudzīgi un pieejami tiešsaistē vismaz 10 gadus pēc produkta ar digitāliem elementiem laišanas tirgū vai atbalsta periodā atkarībā no tā, kurš laikposms ir ilgāks.

19. Ražotāji nodrošina, ka 8. punktā minētā atbalsta perioda beigu datums, tostarp vismaz gads un mēnesis, pirkuma brīdī ir skaidri un saprotami norādīts viegli piekļūstamā veidā un attiecīgā gadījumā uz produkta ar digitāliem elementiem, tā iepakojuma vai ar digitāliem līdzekļiem.

Ja tas ir tehniski iespējams, ņemot vērā produkta ar digitāliem elementiem raksturu, ražotāji izvieto paziņojumu lietotājiem, lai informētu, ka viņu produkts ar digitāliem elementiem ir sasniedzis atbalsta perioda beigas.

20. Ražotāji vai nu pievieno produktam ar digitāliem elementiem ES atbilstības deklarācijas kopiju, vai vienkāršotu ES atbilstības deklarāciju. Ja tiek pievienota vienkāršota ES atbilstības deklarācija, tajā norāda precīzu interneta adresi, kurā var piekļūt pilnīgai ES atbilstības deklarācijai.

21. Sākot no laišanas tirgū un atbalsta periodā ražotāji, kas zina vai kam ir iemesls uzskatīt, ka produkts ar digitāliem elementiem vai ražotāja ieviestie procesi neatbilst I pielikumā izklāstītajām kiberdrošības pamatprasībām, nekavējoties veic korektīvus pasākumus, kas nepieciešami, lai panāktu produkta ar digitāliem elementiem vai ražotāja procesu atbilstību, attiecīgā gadījumā šo produktu izņemtu vai atsauktu.

22. Pēc tirgus uzraudzības iestādes pamatota pieprasījuma ražotāji minētajai iestādei viegli saprotamā valodā papīra vai elektroniskā formātā sniedz visu informāciju un dokumentāciju, kas nepieciešama, lai pierādītu produkta ar digitāliem elementiem un ražotāja ieviesto procesu atbilstību I pielikumā izklāstītajām kiberdrošības pamatprasībām. Pēc minētās iestādes pieprasījuma ražotāji ar to sadarbojas visos pasākumos, kas tiek veikti, lai novērstu kiberdrošības riskus, ko rada produkts ar digitāliem elementiem, ko tie laiduši tirgū.

23. Ražotājs, kas pārtrauc darbību un līdz ar to nespēj nodrošināt atbilstību šai regulai, pirms faktiskās darbības pārtraukšanas informē attiecīgās tirgus uzraudzības iestādes, kā arī – izmantojot jebkādus pieejamos līdzekļus un ciktāl iespējams – attiecīgo tirgū laisto produktu ar digitāliem elementiem lietotājus par gaidāmo darbības pārtraukšanu.

24. Komisija, ņemot vērā Eiropas un starptautiskos standartus un labāko praksi, ar īstenošanas aktiem var precizēt I pielikuma II daļas 1. punktā noteikto programmatūras materiālu komplekta formātu un elementus. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 62. panta 2. punktā.

25. Lai novērtētu dalībvalstu un visas Savienības atkarību no programmatūras komponentiem un jo īpaši no komponentiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra, *ADCO* var nolemt veikt Savienības mēroga atkarības novērtējumu konkrētām produktu ar digitāliem elementiem kategorijām. Šajā nolūkā tirgus uzraudzības iestādes var pieprasīt šādu produktu ar digitāliem elementiem kategoriju ražotājiem iesniegt attiecīgos programmatūras materiālu komplektus, kā minēts I pielikuma II daļas 1. punktā. Pamatojoties uz šādu informāciju, tirgus uzraudzības iestādes var sniegt *ADCO* anonimizētu un apkopotu informāciju par atkarību programmatūras jomā. *ADCO* iesniedz ziņojumu par atkarības novērtējuma rezultātiem sadarbības grupai, kas izveidota, ievērojot Direktīvas (ES) 2022/2555 14. pantu.

14. pants

Ražotāju ziņošanas pienākumi

1. Ražotājs par jebkuru aktīvi izmantotu ievainojamību, ko satur produkts ar digitāliem elementiem un par ko tam kļūst zināms, saskaņā ar šā panta 7. punktu paziņo vienlaikus par koordinatoru izraudzītajai *CSIRT* un *ENISA*. Ražotājs paziņo par šo aktīvi izmantoto ievainojamību, izmantojot vienoto ziņošanas platformu, kas izveidota, ievērojot 16. pantu.

2. Šā panta 1. punktā minētā paziņojuma nolūkos ražotājs iesniedz:

   a) agrīno brīdinājumu par aktīvi izmantotu ievainojamību bez liekas kavēšanās un jebkurā gadījumā 24 stundu laikā pēc tam, kad ražotājs par to uzzinājis, attiecīgā gadījumā norādot dalībvalstis, kuru teritorijā saskaņā ar ražotāja rīcībā esošo informāciju tā produkts ar digitāliem elementiem ir darīts pieejams;

b) ja vien attiecīgā informācija jau nav sniegta, bez liekas kavēšanās un jebkurā gadījumā 72 stundu laikā pēc tam, kad ražotājs ir uzzinājis par aktīvi izmantotu ievainojamību, paziņojumu par ievainojamību, kurā sniedz vispārēju informāciju, cik lielā mērā tāda ir pieejama, par attiecīgo produktu ar digitāliem elementiem, par izmantošanas un attiecīgās ievainojamības vispārējo raksturu, kā arī par veiktajiem korektīvajiem vai riska mazināšanas pasākumiem, kā arī korektīvajiem vai riska mazināšanas pasākumiem, ko var veikt lietotāji, attiecīgā gadījumā norādot arī to, cik lielā mērā ražotājs uzskata paziņoto informāciju par sensitīvu;

c) ja vien attiecīgā informācija jau nav sniegta, ne vēlāk kā 14 dienas pēc tam, kad ir pieejams korektīvs vai riska mazināšanas pasākums, galīgo ziņojumu, kurā iekļauj vismaz šādu informāciju:

   i) ievainojamības apraksts, tostarp tās nopietnības pakāpe un ietekme;

   ii) ja pieejama, informācija par visiem ļaundariem, kas ir izmantojuši vai izmanto ievainojamību;

   iii) sīkāka informācija par drošības atjauninājumu vai citiem korektīviem pasākumiem, kas darīti pieejami, lai novērstu ievainojamību.

3. Ražotājs par jebkuru nopietnu incidentu, kas ietekmē produkta ar digitāliem elementiem drošību un par ko tam kļūst zināms, saskaņā ar šā panta 7. punktu paziņo vienlaikus par koordinatoru izraudzītajai *CSIRT* un *ENISA*. Ražotājs par šo incidentu paziņo, izmantojot vienoto ziņošanas platformu, kas izveidota, ievērojot 16. pantu.

4. Šā panta 3. punktā minētās paziņošanas nolūkos ražotājs iesniedz:

a) agrīno brīdinājumu par nopietnu incidentu, kas ietekmē produkta ar digitāliem elementiem drošību bez nepamatotas kavēšanās un jebkurā gadījumā 24 stundu laikā pēc tam, kad ražotājs par to uzzinājis, tostarp vismaz to, vai pastāv aizdomas, ka incidentu ir izraisījušas nelikumīgas vai ļaunprātīgas darbības, attiecīgā gadījumā norādot arī dalībvalstis, kuru teritorijā saskaņā ar ražotāja rīcībā esošo informāciju tā produkts ar digitāliem elementiem ir darīts pieejams;

b) ja vien attiecīgā informācija jau nav sniegta, bez liekas kavēšanās un jebkurā gadījumā 72 stundu laikā pēc tam, kad ražotājs uzzinājis par incidentu, paziņojumu par incidentu, kurā sniedz vispārīgu informāciju, ja tāda ir pieejama, par incidenta būtību, incidenta sākotnējo novērtējumu, kā arī par veiktajiem korektīvajiem vai riska mazināšanas pasākumiem un korektīvajiem vai riska mazināšanas pasākumiem, ko var veikt lietotāji, attiecīgā gadījumā norādot arī to, cik lielā mērā ražotājs uzskata paziņoto informāciju par sensitīvu;

c) ja vien attiecīgā informācija jau nav sniegta, galīgo ziņojumu viena mēneša laikā pēc b) apakšpunktā minētā paziņojuma par incidentu iesniegšanas, tajā iekļaujot vismaz:

i) incidenta, tostarp tā nopietnības un ietekmes, sīku aprakstu;

ii) apdraudējuma veidu vai pamatcēloni, kas, visticamāk, izraisījis incidentu;

iii) piemērotos un piemērošanas stadijā esošos riska mazināšanas pasākumus.

5. Šā panta 3. punkta nolūkos incidentu, kas ietekmē produkta ar digitāliem elementiem drošību, uzskata par nopietnu, ja:

a) tas negatīvi ietekmē vai var negatīvi ietekmēt produkta ar digitāliem elementiem spēju aizsargāt sensitīvu vai svarīgu datu vai funkciju pieejamību, autentiskumu, integritāti vai konfidencialitāti; vai

b) tā rezultātā produktā ar digitāliem elementiem vai produkta ar digitāliem elementiem lietotāja tīklā un informācijas sistēmās ir ielaists vai izpildīts ļaunprātīgs kods vai var tikt ielaists vai izpildīts ļaunprātīgs kods.

6. Vajadzības gadījumā par koordinatoru izraudzītā *CSIRT*, kas saņēmusi sākotnējo paziņojumu, var pieprasīt ražotājiem iesniegt starpposma ziņojumu par attiecīgajiem statusa atjauninājumiem saistībā ar aktīvi izmantotu ievainojamību vai nopietnu incidentu, kas ietekmē produkta ar digitāliem elementiem drošību.

7. Šā panta 1. un 3. punktā minētos paziņojumus iesniedz 16. pantā minētajā vienotajā ziņošanas platformā, izmantojot vienu no 16. panta 1. punktā minētajiem elektroniskā paziņojuma galapunktiem. Paziņojumu iesniedz, izmantojot tās *CSIRT* elektroniskā paziņojuma galapunktu, kas izraudzīta par tās dalībvalsts koordinatoru, kurā ir ražotāju galvenā iedibinājuma vieta Savienībā, un tas vienlaikus ir pieejams *ENISA*.

Šīs regulas nolūkos tiks uzskatīts, ka ražotāja galvenā iedibinājuma vieta Savienībā ir tajā dalībvalstī, kurā lielākoties tiek pieņemti lēmumi saistībā ar tā produktu ar digitāliem elementiem kiberdrošības riska pārvaldības pasākumiem. Ja šādu dalībvalsti nevar noteikt, uzskata, ka galvenais iedibinājums ir dalībvalstī, kurā attiecīgajam ražotājam ir iedibinājums ar vislielāko darbinieku skaitu Savienībā.

Ja ražotājam Savienībā nav galvenās iedibinājuma vietas, tas 1. un 3. punktā minētos paziņojumus iesniedz, izmantojot tās *CSIRT* elektroniskā paziņojuma galapunktu, kas izraudzīta par koordinatoru dalībvalstī, kura noteikta saskaņā ar šādu secību un pamatojoties uz ražotājam pieejamo informāciju:

a) dalībvalsts, kurā ir iedibināts pilnvarotais pārstāvis, kas darbojas ražotāja vārdā attiecībā uz lielāko skaitu minētā ražotāja produktu ar digitāliem elementiem;

b) dalībvalsts, kurā ir iedibināts importētājs, kas laiž tirgū lielāko skaitu minētā ražotāja produktu ar digitāliem elementiem;

c) dalībvalsts, kurā ir iedibināts izplatītājs, kas dara pieejamu tirgū lielāko skaitu minētā ražotāja produktu ar digitāliem elementiem;

d) dalībvalsts, kurā atrodas lielākais minētā ražotāja produktu ar digitāliem elementiem lietotāju skaits.

Saistībā ar trešās daļas d) apakšpunktu ražotājs var iesniegt paziņojumus par jebkuru turpmāku aktīvi izmantotu ievainojamību vai nopietnu incidentu, kas ietekmē produkta ar digitāliem elementiem drošību, tai pašai *CSIRT*, kura izraudzīta par koordinatoru un kurai tas ziņojis pirmoreiz.

8. Pēc tam, kad ražotājs uzzinājis par aktīvi izmantotu ievainojamību vai nopietnu incidentu, kas ietekmē produkta ar digitāliem elementiem drošību, ražotājs informē skartos produkta ar digitāliem elementiem lietotājus un attiecīgā gadījumā visus lietotājus par minēto ievainojamību vai incidentu, un vajadzības gadījumā par jebkādu riska mazināšanu un korektīviem pasākumiem, ko lietotāji var veikt, lai mazinātu minētās ievainojamības vai incidenta ietekmi, attiecīgā gadījumā strukturētā, mašīnlasāmā formātā, kas ir viegli automātiski apstrādājams. Ja ražotājs laikus neinformē produkta ar digitāliem elementiem lietotājus, paziņotās *CSIRT*, kas izraudzītas par koordinatoriem, var sniegt šādu informāciju lietotājiem, ja tā tiek uzskatīta par samērīgu un nepieciešamu, lai novērstu vai mazinātu minētās ievainojamības vai incidenta ietekmi.

9. Līdz ... [12 mēneši no šis regulas stāšanās spēkā dienas] Komisija pieņem deleģētos aktus saskaņā ar 61. pantu, lai papildinātu šo regulu, precizējot noteikumus ar kiberdrošību saistītu iemeslu izmantošanai par attaisnojumu 16. panta 2. punktā minēto paziņojumu par aktīvi izmantotām ievainojamībām izplatīšanas atlikšanai. Sagatavojot deleģēto aktu projektus, Komisija sadarbojas ar *CSIRT* tīklu, kas izveidots, ievērojot Direktīvas (ES) 2022/2555 15. pantu, un *ENISA*.

10. Komisija ar īstenošanas aktiem var papildus precizēt šajā pantā, kā arī 15. un 16. pantā minēto paziņojumu formātu un paziņošanas procedūras. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 62. panta 2. punktā. Komisija minēto īstenošanas aktu projektu sagatavošanā sadarbojas ar *CSIRT* tīklu un *ENISA*.

15. pants

Brīvprātīga ziņošana

1. Ražotāji, kā arī citas fiziskas vai juridiskas personas var brīvprātīgi paziņot par koordinatoru izraudzītajai *CSIRT* vai *ENISA* par jebkuru ievainojamību, ko satur produkts ar digitāliem elementiem, kā arī par kiberdraudiem, kas varētu ietekmēt produkta ar digitāliem elementiem riska profilu.

2. Ražotāji, kā arī citas fiziskas vai juridiskas personas par jebkuru incidentu, kas ietekmē produkta ar digitāliem elementiem drošību, kā arī par gandrīz notikušajiem notikumiem, kuru rezultātā varētu būt noticis šāds incidents, brīvprātīgi var paziņot par koordinatoru izraudzītajai *CSIRT* vai *ENISA*.

3. Par koordinatoru izraudzītā *CSIRT* vai *ENISA* šā panta 1. un 2. punktā minētos paziņojumus apstrādā saskaņā ar 16. pantā noteikto procedūru.

   Par koordinatoru izraudzītā *CSIRT* var prioritārā kārtībā apstrādāt vispirms obligātos paziņojumus un pēc tam brīvprātīgos paziņojumus.

4. Ja fiziska vai juridiska persona, kas nav ražotājs, paziņo par aktīvi izmantotu ievainojamību vai nopietnu incidentu, kas ietekmē produkta ar digitāliem elementiem drošību, saskaņā ar 1. vai 2. punktu, par koordinatoru izraudzītā *CSIRT* bez liekas kavēšanās informē ražotāju.

5. Par koordinatoru izraudzītā *CSIRT* kā arī *ENISA* nodrošina konfidencialitāti un pienācīgu tās informācijas aizsardzību, ko sniegusi fiziskā vai juridiskā persona, kura iesniegusi paziņojumu. Neskarot noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem, brīvprātīgās paziņošanas rezultātā paziņotājai fiziskai vai juridiskai personai netiek uzlikti nekādi papildu pienākumi, kādi tai nebūtu jāievēro, ja tā nebūtu iesniegusi minēto paziņojumu.

16. pants

Vienotās ziņošanas platformas izveide

1. Lai sniegtu 14. panta 1. un 3. punktā un 15. panta 1. un 2. punktā minētos paziņojumus un lai vienkāršotu ražotāju ziņošanas pienākumus, *ENISA* izveido vienotu ziņošanas platformu. Minētās vienotās ziņošanas platformas ikdienas darbības pārvalda un uztur *ENISA*. Vienotās ziņošanas platformas uzbūve ļauj dalībvalstīm un *ENISA* ieviest savus elektroniskās paziņošanas galapunktus.

2. Pēc paziņojuma saņemšanas par koordinatoru izraudzītā *CSIRT*, kas ir sākotnējā paziņojuma saņēmēja, vienotajā ziņošanas platformā paziņojumu nekavējoties nosūta tām *CSIRT*, kuras izraudzītas par koordinatoriem un kuru teritorijā saskaņā ar ražotāja sniegto informāciju produkts ar digitāliem elementiem ir darīts pieejams.

Ārkārtas apstākļos un jo īpaši pēc ražotāja pieprasījuma un ņemot vērā paziņotās informācijas sensitivitātes līmeni, ko ražotājs norādījis saskaņā ar šīs regulas 14. panta 2. punkta a) apakšpunktu, pamatotu, ar kiberdrošību saistītu iemeslu dēļ, tostarp tad, ja uz ievainojamību attiecas koordinēta ievainojamības atklāšanas procedūra, kā minēts Direktīvas (ES) 2022/2555 12. panta 1. punktā, paziņojuma izplatīšanu var atlikt uz laiku, kas ir absolūti nepieciešams. Ja *CSIRT* nolemj aizturēt paziņojumu, tā nekavējoties informē *ENISA* par šo lēmumu un sniedz gan pamatojumu paziņojuma aizturēšanai, gan norādi par to, kad tā izplatīs paziņojumu saskaņā ar šajā punktā noteikto izplatīšanas procedūru. *ENISA* var atbalstīt *CSIRT* ar kiberdrošību saistītu iemeslu piemērošanā saistībā ar paziņojuma izplatīšanas aizkavēšanu.

Īpaši izņēmuma apstākļi ir tad, ja ražotājs 14. panta 2. punkta b) apakšpunktā minētajā paziņojumā norāda, ka:

a) paziņoto ievainojamību ir aktīvi izmantojis ļaundaris un saskaņā ar pieejamo informāciju tā ir izmantota tikai tajā dalībvalstī, kurā *CSIRT*, kam ražotājs ir paziņojis par ievainojamību, ir izraudzīta par koordinatoru;

b) paziņotās ievainojamības tūlītēja tālāka izplatīšana, visticamāk, novestu pie tādas informācijas sniegšanas, kuras izpaušana būtu pretrunā minētās dalībvalsts būtiskām interesēm; vai

c) paziņotā ievainojamība rada nenovēršamu augstu kiberdrošības risku, kas izriet no tālākas izplatīšanas;

tikai informāciju par to, ka ražotājs ir iesniedzis paziņojumu, vispārīgu informāciju par produktu, informāciju par izmantošanas vispārīgo raksturu un informāciju, attiecībā uz kuru tika sniegts ar drošību saistīts pamatojums jādara vienlaikus pieejamu *ENISA*, līdz pilnīgs paziņojums tiek izplatīts attiecīgajām *CSIRT* un *ENISA*. Ja, pamatojoties uz minēto informāciju, *ENISA* uzskata, ka pastāv sistēmisks risks, kas ietekmē drošību iekšējā tirgū, tā iesaka saņēmējai *CSIRT* izplatīt pilnīgu paziņojumu pārējām par koordinatoriem izraudzītajām *CSIRT* un pašai *ENISA*.

3. Pēc tam, kad ir saņemts paziņojums par produkta ar digitāliem elementiem aktīvi izmantotu ievainojamību vai nopietnu incidentu, kas ietekmē produkta ar digitāliem elementiem drošību, par koordinatoriem izraudzītās *CSIRT* sniedz savu attiecīgo dalībvalstu tirgus uzraudzības iestādēm paziņoto informāciju, kas vajadzīga, lai tirgus uzraudzības iestādes varētu pildīt savus pienākumus saskaņā ar šo regulu.

4. *ENISA* veic atbilstīgus un samērīgus tehniskus, operatīvus un organizatoriskus pasākumus, lai pārvaldītu riskus, kas radīti vienotās ziņošanas platformai un vienotajā ziņošanas platformā iesniegtās vai izplatītās informācijas drošībai. Tā bez liekas kavēšanās paziņo *CSIRT* tīklam, kā arī Komisijai par visiem drošības incidentiem, kas ietekmē vienoto ziņošanas platformu.

5. *ENISA* sadarbībā ar *CSIRT* tīklu nodrošina un īsteno specifikācijas par tehniskajiem, operatīvajiem un organizatoriskajiem pasākumiem attiecībā uz 1. punktā minētās vienotās ziņošanas platformas izveidi, uzturēšanu un drošu darbību, tostarp vismaz drošības pasākumus, kas saistīti ar vienotās ziņošanas platformas izveidi, darbību un uzturēšanu, kā arī par elektroniskās paziņošanas galapunktiem, ko izveidojušas *CSIRT*, kuras izraudzītas par koordinatoriem valsts līmenī, un *ENISA* Savienības līmenī, tostarp procedūras aspektus, lai nodrošinātu, ka gadījumā, ja attiecībā uz paziņoto ievainojamību nav pieejami korektīvi vai riska mazināšanas pasākumi, informācija par minēto ievainojamību tiek kopīgota saskaņā ar stingriem drošības protokoliem un pamatojoties uz vajadzību pēc informācijas.

6. Ja par koordinatoru izraudzītā *CSIRT* ir informēta par aktīvi izmantotu ievainojamību kā daļu no koordinētās ievainojamības atklāšanas procedūras, kā minēts Direktīvas (ES) 2022/2555 12. panta 1. punktā, tā par koordinatoru izraudzītā *CSIRT*, kas saņem sākotnējo paziņojumu, var atlikt attiecīgā paziņojuma izplatīšanu vienotajā ziņošanas platformā, balstoties uz pamatotiem ar kiberdrošību saistītiem iemesliem, uz laikposmu, kas nav ilgāks par absolūti nepieciešamo, un līdz brīdim, kad koordinētās ievainojamības izpaušanā iesaistītās puses ir devušas piekrišanu informācijas izpaušanai. Minētā prasība neliedz ražotājiem brīvprātīgi paziņot par šādu ievainojamību saskaņā ar šajā pantā noteikto procedūru.

17. pants

Citi noteikumi, kas saistīti ar ziņošanu

1. *ENISA* var iesniegt saskaņā ar Direktīvas (ES) 2022/2555 16. pantu izveidotajam Eiropas Kiberkrīžu sadarbības organizāciju tīklam (*EU-CyCLONe*) informāciju, kas paziņota, ievērojot šīs regulas 14. panta 1. un 3. punktu un 15. panta 1. un 2. punktu, ja šāda informācija ir noderīga plaša mēroga kiberdrošības incidentu un krīžu koordinētai pārvaldībai operatīvā līmenī. Lai noteiktu šādu noderīgumu, *ENISA* var apsvērt *CSIRT* tīkla veiktās tehniskās analīzes, ja tādas ir pieejamas.

2. Ja sabiedrības informētība ir nepieciešama, lai novērstu vai mazinātu nopietnu incidentu, kas ietekmē produkta ar digitāliem elementiem drošību, vai lai risinātu notiekošu incidentu, vai ja informācijas par incidentu izpaušana kā citādi ir sabiedrības interesēs, attiecīgajā dalībvalstī par koordinatoru izraudzītā *CSIRT* pēc apspriešanās ar attiecīgo ražotāju un attiecīgā gadījumā sadarbībā ar *ENISA* var informēt sabiedrību par incidentu vai prasīt to darīt ražotājam.

3. *ENISA*, pamatojoties uz paziņojumiem, kas saņemti, ievērojot šīs regulas 14. panta 1. un 3. punktu vai 15. panta 1. un 2. punktu, reizi 24 mēnešos sagatavo tehnisko ziņojumu par jaunākajām tendencēm attiecībā uz kiberdrošības riskiem produktos ar digitāliem elementiem un to iesniedz sadarbības grupai, kas izveidota, ievērojot Direktīvas (ES) 2022/2555 14. pantu. Pirmo šādu ziņojumu iesniedz 24 mēnešu laikā no dienas, kad sāk piemērot 14. panta 1. un 3. punktā noteiktos pienākumus. *ENISA* ziņojumā par kiberdrošības stāvokli Savienībā, ievērojot Direktīvas (ES) 2022/2555 18. pantu, iekļauj attiecīgo informāciju no tās tehniskajiem ziņojumiem.

4. Tikai paziņošanas darbība vien saskaņā ar 14. panta 1. un 3. punktu vai 15. panta 1. un 2. punktu nerada lielāku atbildību paziņojošajai fiziskajai vai juridiskajai personai.

5. Pēc tam, kad ir pieejams drošības atjauninājums vai cita veida korektīvs vai riska mazināšanas pasākums, *ENISA*, vienojoties ar attiecīgā produkta ar digitāliem elementiem ražotāju, iekļauj Eiropas ievainojamību datubāzē, kas izveidota, ievērojot Direktīvas (ES) 2022/2555 12. panta 2. punktu, publiski zināmo ievainojamību, par ko paziņots, ievērojot šīs regulas 14. panta 1. punktu vai 15. panta 1. punktu.

6. Par koordinatoriem izraudzītās *CSIRT* sniedz ražotājiem un jo īpaši ražotājiem, kas kvalificējami kā mikrouzņēmumi vai mazie vai vidējie uzņēmumi, atbalstu kā palīdzības dienests saistībā ar 14. pantā paredzētajiem ziņošanas pienākumiem.

18. pants

Pilnvarotie pārstāvji

1. Ražotājs var ar rakstisku pilnvaru iecelt pilnvaroto pārstāvi.

2. Pilnvarotā pārstāvja pilnvarās neietilpst pienākumi, kas noteikti 13. panta 1. līdz 11. punktā un 12. punkta pirmajā daļā, un 14. punktā.

3. Pilnvarotais pārstāvis veic uzdevumus, kas noteikti no ražotāja saņemtajā pilnvarojumā. Pilnvarotais pārstāvis pēc pieprasījuma iesniedz tirgus uzraudzības iestādēm pilnvarojuma kopiju. Pilnvarojums pilnvarotajam pārstāvim ļauj veikt vismaz šādas darbības:

a) vismaz 10 gadus vai atbalsta periodā atkarībā no tā, kurš termiņš ir ilgāks, pēc produkta ar digitāliem elementiem laišanas tirgū glabāt 28. pantā minēto ES atbilstības deklarāciju un 31. pantā minēto tehnisko dokumentāciju, lai tā būtu pieejama tirgus uzraudzības iestādēm;

b) pēc pamatota tirgus uzraudzības iestādes pieprasījuma sniegt šai iestādei visu informāciju un dokumentāciju, kas nepieciešama, lai pierādītu produkta ar digitāliem elementiem atbilstību;

c) pēc tirgus uzraudzības iestāžu pieprasījuma sadarboties ar tām visos pasākumos, kas tiek veikti nolūkā likvidēt tāda produkta ar digitāliem elementiem radītos riskus, uz kuru attiecas pilnvarotā pārstāvja pilnvarojums.

19. pants

Importētāju pienākumi

1. Importētāji laiž tirgū tikai tādus produktus ar digitāliem elementiem, kuri atbilst I pielikuma I daļā izklāstītajām kiberdrošības pamatprasībām, un tikai tad, ja ražotāja ieviestie procesi atbilst I pielikuma II daļā izklāstītajām kiberdrošības pamatprasībām.

2. Pirms produkta ar digitāliem elementiem laišanas tirgū importētāji nodrošina, ka:

   a) ražotājs ir veicis pienācīgas atbilstības novērtēšanas procedūras, kā minēts 32. pantā;

   b) ražotājs ir sagatavojis tehnisko dokumentāciju;

   c) produktam ar digitāliem elementiem ir 30. pantā minētā CE zīme, un tam ir pievienota 13. panta 20. punktā minētā ES atbilstības deklarācija un II pielikumā noteiktā informācija un norādījumi lietotājam valodā, kas ir viegli saprotama lietotājiem un tirgus uzraudzības iestādēm;

   d) ražotājs ir izpildījis 13. panta 15., 16. un 19. punktā noteiktās prasības.

   Šā punkta nolūkos importētāji var iesniegt vajadzīgos dokumentus, kas apliecina šajā pantā noteikto prasību izpildi.

3. Ja importētājs uzskata vai tam ir iemesls uzskatīt, ka produkts ar digitāliem elementiem vai ražotāja ieviestie procesi neatbilst šai regulai, importētājs produktu nelaiž tirgū, kamēr nav panākta minētā produkta vai ražotāja ieviesto procesu atbilstība šai regulai. Turklāt, ja produkts ar digitāliem elementiem rada būtisku kiberdrošības risku, importētājs par to informē ražotāju un tirgus uzraudzības iestādes.

Ja importētājam ir iemesls uzskatīt, ka produkts ar digitāliem elementiem var radīt ievērojamu kiberdrošības risku netehnisku riska faktoru dēļ, importētājs par to informē tirgus uzraudzības iestādes. Saņemot šādu informāciju, tirgus uzraudzības iestādes rīkojas saskaņā ar 54. panta 2. punktā minētajām procedūrām.

4. Importētāji uz produkta ar digitāliem elementiem vai uz tā iepakojuma, vai produktam ar digitāliem elementiem pievienotajā dokumentā norāda sava uzņēmuma nosaukumu, reģistrēto komercnosaukumu vai reģistrēto preču zīmi un pasta adresi, e-pasta adresi vai citu digitālu kontaktinformāciju, kā arī attiecīgā gadījumā tīmekļa vietni, kurā ar tiem var sazināties. Kontaktinformācija ir lietotājiem un tirgus uzraudzības iestādēm viegli saprotamā valodā.

5. Importētāji, kas zina vai kam ir iemesls uzskatīt, ka produkts ar digitāliem elementiem, kuru tie ir laiduši tirgū, neatbilst šai regulai, nekavējoties veic nepieciešamos korektīvos pasākumus, lai nodrošinātu to, ka produkts ar digitāliem elementiem atbilst šai regulai, vai arī, ja vajadzīgs, lai to izņemtu vai atsauktu.

   Uzzinot par ievainojamību produktā ar digitāliem elementiem, importētāji bez nepamatotas kavēšanās informē ražotāju par šo ievainojamību. Turklāt, ja produkts ar digitāliem elementiem rada būtisku kiberdrošības risku, importētāji nekavējoties par to informē to dalībvalstu tirgus uzraudzības iestādes, kurās viņi produktu ar digitāliem elementiem darījuši pieejamu tirgū, norādot sīku informāciju, jo īpaši par neatbilstību un veiktajiem korektīvajiem pasākumiem.

6. Importētāji vismaz 10 gadus pēc produkta ar digitāliem elementiem laišanas tirgū vai atbalsta periodā atkarībā no tā, kurš termiņš ir ilgāks, glabā ES atbilstības deklarācijas kopiju, lai tā būtu pieejama tirgus uzraudzības iestādēm, un nodrošina, ka minētajām iestādēm pēc pieprasījuma ir pieejama tehniskā dokumentācija.

7. Pēc tirgus uzraudzības iestādes pamatota pieprasījuma importētāji šai iestādei tai viegli saprotamā valodā papīra vai elektroniskā formātā sniedz visu informāciju un dokumentāciju, kas vajadzīga, lai pierādītu, ka produkts ar digitāliem elementiem atbilst I pielikumā I daļā izklāstītajām kiberdrošības pamatprasībām un ka ražotāja ieviestie procesi atbilst I pielikuma II daļā izklāstītajām kiberdrošības pamatprasībām. Importētāji pēc minētās iestādes pieprasījuma sadarbojas ar to visos pasākumos, kas tiek veikti, lai novērstu kiberdrošības riskus, ko rada produkts ar digitāliem elementiem, kuru tie laiduši tirgū.

8. Ja produkta ar digitāliem elementiem importētājam ir kļuvis zināms, ka minētā produkta ražotājs ir pārtraucis darbību un līdz ar to nespēj izpildīt šajā regulā noteiktos pienākumus, importētājs par šo situāciju informē attiecīgās tirgus uzraudzības iestādes, kā arī – izmantojot jebkādus pieejamos līdzekļus un ciktāl iespējams – attiecīgo tirgū laisto produktu ar digitāliem elementiem lietotājus.

20. pants

Izplatītāju pienākumi

1. Darot produktu ar digitāliem elementiem pieejamu tirgū, izplatītāji rūpīgi ievēro šajā regulā noteiktās prasības.

2. Pirms produktu ar digitāliem elementiem dara pieejamu tirgū, izplatītāji pārliecinās, ka:

a) produktam ar digitāliem elementiem ir CE zīme;

b) ražotājs un importētājs ir izpildījuši 13. panta 15., 16., 18., 19. un 20. punktā un 19. panta 4. punktā noteiktos pienākumus un ir iesnieguši izplatītājam visus nepieciešamos dokumentus.

3. Ja izplatītājs, pamatojoties uz tā rīcībā esošo informāciju, uzskata vai ja tam ir iemesls uzskatīt, ka produkts ar digitāliem elementiem vai ražotāja ieviestie procesi neatbilst I pielikumā izklāstītajām kiberdrošības pamatprasībām, izplatītājs produktu ar digitāliem elementiem nedara pieejamu tirgū, kamēr nav panākta šā produkta vai ražotāja ieviesto procesu atbilstība šai regulai. Turklāt, ja produkts ar digitāliem elementiem rada būtisku kiberdrošības risku, izplatītājs par to bez nepamatotas kavēšanās informē ražotāju un tirgus uzraudzības iestādes.

4. Izplatītāji, kuri, pamatojoties uz to rīcībā esošo informāciju, zina vai kuriem ir iemesls uzskatīt, ka produkts ar digitāliem elementiem, ko tie darījuši pieejamu tirgū, vai tā ražotāja ieviestie procesi neatbilst šai regulai, pārliecinās, ka tiek veikti korektīvi pasākumi, kas nepieciešami, lai panāktu minētā produkta ar digitāliem elementiem vai tā ražotāja ieviesto procesu atbilstību vai attiecīgā gadījumā šo produktu izņemtu vai atsauktu.

Uzzinot par ievainojamību produktā ar digitāliem elementiem, izplatītāji bez nepamatotas kavēšanās par šo ievainojamību informē ražotāju. Turklāt, ja produkts ar digitāliem elementiem rada būtisku kiberdrošības risku, izplatītāji nekavējoties par to informē to dalībvalstu tirgus uzraudzības iestādes, kurās viņi produktu ar digitāliem elementiem darījuši pieejamu tirgū, norādot sīku informāciju, jo īpaši par neatbilstību un veiktajiem korektīvajiem pasākumiem.

5. Pēc tirgus uzraudzības iestādes pamatota pieprasījuma izplatītāji šai iestādei viegli saprotamā valodā papīra vai elektroniskā formātā sniedz visu informāciju un dokumentāciju, kas vajadzīga, lai pierādītu, ka produkts ar digitāliem elementiem un tā ražotāja ieviestie procesi atbilst šai regulai. Izplatītāji pēc minētās iestādes pieprasījuma sadarbojas ar to visos pasākumos, kas tiek veikti, lai novērstu kiberdrošības riskus, ko rada produkts ar digitāliem elementiem, kuru tie darījuši pieejamu tirgū.

6. Ja produkta ar digitāliem elementiem izplatītājam, pamatojoties uz tā rīcībā esošo informāciju, ir kļuvis zināms, ka minētā produkta ražotājs ir pārtraucis darbību un līdz ar to nespēj izpildīt šajā regulā noteiktos pienākumus, izplatītājs par šo situāciju bez nepamatotas kavēšanās informē attiecīgās tirgus uzraudzības iestādes, kā arī – izmantojot jebkādus pieejamos līdzekļus un ciktāl iespējams – attiecīgo tirgū laisto produktu ar digitāliem elementiem lietotājus.

21. pants

Gadījumi, kad ražotāju pienākumus piemēro importētājiem un izplatītājiem

Ja importētājs vai izplatītājs laiž tirgū produktu ar digitāliem elementiem ar savu vārdu vai preču zīmi vai veic jau tirgū laista produkta ar digitāliem elementiem būtisku modifikāciju, minēto importētāju vai izplatītāju šīs regulas vajadzībām uzskata par ražotāju un uz viņu attiecas 13. un 14. pants.

22. pants

Citi gadījumi, kad piemēro ražotāja pienākumus

1. Fizisku vai juridisku personu, kas nav ražotājs, importētājs vai izplatītājs un kas veic produkta ar digitāliem elementiem būtisku modifikāciju un minēto produktu dara pieejamu tirgū, šīs regulas vajadzībām uzskata par ražotāju.

2. Šā panta 1. punktā minētajai personai 13. un 14. pantā noteiktos pienākumus piemēro attiecībā uz to produkta ar digitāliem elementiem daļu, kuru ir skārusi būtiskā modifikācija, vai attiecībā uz visu produktu, ja būtiskā modifikācija ietekmē produkta ar digitāliem elementiem kiberdrošību kopumā.

23. pants

Uzņēmēju identifikācija

1. Uzņēmēji pēc pieprasījuma sniedz tirgus uzraudzības iestādēm šādu informāciju:

   a) jebkura uzņēmēja, kurš viņiem piegādājis produktu ar digitāliem elementiem, nosaukums un adrese;

   b) ja pieejams, jebkura uzņēmēja, kuram viņi piegādājuši produktu ar digitāliem elementiem, nosaukums un adrese;

2. Uzņēmēji spēj sniegt 1. punktā minēto informāciju 10 gadus pēc tam, kad produkts ar digitāliem elementiem viņiem piegādāts, un 10 gadus pēc tam, kad viņi ir piegādājuši produktu ar digitāliem elementiem.

24. pants

Atvērtā pirmkoda programmatūras pārziņa pienākumi

1. Atvērtā pirmkoda programmatūras pārziņi ievieš un pārbaudāmā veidā dokumentē kiberdrošības politiku, lai veicinātu droša produkta ar digitāliem elementiem izstrādi, kā arī šā produkta izstrādātāju efektīvu rīcību attiecībā uz ievainojamībām. Minētā politika arī veicina to, ka minētā produkta izstrādātāji brīvprātīgi ziņo par ievainojamībām, kā noteikts 15. pantā, un ņem vērā atvērtā pirmkoda programmatūras pārziņa īpašo raksturu un juridiskos un organizatoriskos pasākumus, kas uz to attiecas. Minētā politika jo īpaši ietver aspektus, kas saistīti ar ievainojamību dokumentēšanu, risināšanu un novēršanu, un veicina informācijas apmaiņu par konstatētajām ievainojamībām atvērtā pirmkoda kopienā.

2. Atvērtā pirmkoda programmatūras pārziņi pēc tirgus uzraudzības iestāžu pieprasījuma sadarbojas ar tām, lai mazinātu kiberdrošības riskus, ko rada produkts ar digitāliem elementiem, kurš kvalificējams kā brīvi pieejama atvērtā pirmkoda programmatūra.

   Pēc tirgus uzraudzības iestādes pamatota pieprasījuma atvērtā pirmkoda programmatūras pārziņi minētajai iestādei viegli saprotamā valodā papīra vai elektroniskā formātā iesniedz 1. punktā minēto dokumentāciju.

3. Uz atvērtā pirmkoda programmatūras pārziņiem attiecas 14. panta 1. punktā noteiktie pienākumi, ciktāl tie ir iesaistīti produktu ar digitāliem elementiem izstrādē. Pienākumi, kas noteikti 14. panta 3. un 8. punktā, uz atvērtā pirmkoda programmatūras pārziņiem attiecas, ciktāl nopietni incidenti, kas ietekmē produktu ar digitāliem elementiem drošību, ietekmē tīklu un informācijas sistēmas, ko atvērtā pirmkoda programmatūras pārziņi nodrošina šādu produktu izstrādei.

25. pants

Brīvi pieejamas atvērtā pirmkoda programmatūras drošības apliecinājums

Lai atvieglotu 13. panta 5. punktā noteiktā pienācīgas pārbaudes pienākuma izpildi, jo īpaši attiecībā uz ražotājiem, kuri savos produktos ar digitāliem elementiem integrē brīvi pieejamas atklātā pirmkoda programmatūras komponentus, Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 61. pantu, lai papildinātu šo regulu, izveidojot brīvprātīgas drošības apliecinājuma programmas, kas ļauj tādu produktu ar digitāliem elementiem izstrādātājiem vai lietotājiem, kuri kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra, kā arī citām trešām personām novērtēt šādu produktu atbilstību visām vai konkrētām kiberdrošības pamatprasībām vai citiem šajā regulā noteiktajiem pienākumiem.

26. pants

Norādījumi

1. Lai veicinātu īstenošanu un nodrošinātu šādas īstenošanas konsekvenci, Komisija publisko norādījumus, kas uzņēmējiem palīdz piemērot šo regulu, un pievērš īpašu uzmanību tam, lai sekmētu to, ka mikrouzņēmumi un mazie un vidējie uzņēmumi panāk atbilstību.

2. Ja Komisija plāno sniegt 1. punktā minētos norādījumus, tā pievēršas vismaz šādiem aspektiem:

   a) šīs regulas darbības joma, īpašu uzmanību pievēršot attālinātas datu apstrādes risinājumiem un brīvi pieejamai atvērtā pirmkoda programmatūrai;

   b) atbalsta periodu piemērošana konkrētām produktu ar digitāliem elementiem kategorijām;

   c) norādījumi ražotājiem, uz kuriem attiecas šī regula un arī citi Savienības saskaņošanas tiesību akti, kas nav šī regula, vai citi saistīti Savienības tiesību akti;

   d) būtisku modifikāciju jēdziens.

   Komisija arī uztur viegli pieejamu sarakstu ar deleģētajiem un īstenošanas aktiem, kas pieņemti, ievērojot šo regulu.

3. Izstrādājot norādījumus saskaņā ar šo pantu, Komisija apspriežas ar attiecīgajām ieinteresētajām personām.

III nodaļa

Produkta ar digitāliem elementiem atbilstība

27. pants

Pieņēmums par atbilstību

1. Produktus ar digitāliem elementiem un ražotāja ieviestos procesus, kas atbilst tiem saskaņotajiem standartiem vai to daļām, uz kuriem atsauces ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, uzskata par atbilstīgiem I pielikumā izklāstītajām kiberdrošības pamatprasībām, uz kurām attiecas minētie standarti vai to daļas.

Komisija saskaņā ar Regulas (ES) Nr. 1025/2012 10. panta 1. punktu prasa vienai vai vairākām Eiropas standartizācijas organizācijām izstrādāt saskaņotu standartu projektu šīs regulas I pielikumā izklāstītajām kiberdrošības pamatprasībām. Sagatavojot standartizācijas pieprasījumus šīs regulas vajadzībām, Komisija cenšas ņemt vērā pastāvošos Eiropas un starptautiskos kiberdrošības standartus, kas jau ir ieviesti vai tiek izstrādāti, lai vienkāršotu saskaņoto standartu izstrādi, saskaņā ar Regulu (ES) Nr. 1025/2012.

2. Komisija var pieņemt īstenošanas aktus, ar kuriem nosaka kopīgās specifikācijas, kas aptver vajadzīgās tehniskās prasības, lai varētu ievērot I pielikumā noteiktās kiberdrošības pamatprasības attiecībā uz produktiem ar digitāliem elementiem, kas ietilpst šīs regulas darbības jomā.

Minētos īstenošanas aktus pieņem tikai tad, ja ir izpildīti šādi nosacījumi:

a) Komisija, ievērojot Regulas (ES) Nr. 1025/2012 10. panta 1. punktu, ir pieprasījusi vienai vai vairākām Eiropas standartizācijas organizācijām izstrādāt saskaņotu standartu projektu attiecībā uz I pielikumā izklāstītajām kiberdrošības pamatprasībām, un:

i) šis pieprasījums nav pieņemts;

ii) saskaņotie standarti, kas attiecas uz minēto pieprasījumu, nav iesniegti termiņā, kas noteikts saskaņā ar Regulas (ES) Nr. 1025/2012 10. panta 1. punktu; vai

iii) saskaņotie standarti neatbilst pieprasījumam; un

b) *Eiropas Savienības Oficiālajā Vēstnesī* saskaņā ar Regulu (ES) Nr. 1025/2012 nav publicēta atsauce uz saskaņotiem standartiem, kuri attiecas uz I pielikumā izklāstītajām attiecīgajām kiberdrošības pamatprasībām, un nav sagaidāms, ka šāda atsauce tiks publicēta pieņemamā laikposmā.

Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 62. panta 2. punktā.

3. Pirms šā panta 2. punktā minētā īstenošanas akta projekta sagatavošanas Komisija informē Regulas (ES) Nr. 1025/2012 22. pantā minēto komiteju, ka tā uzskata, ka šā panta 2. punkta nosacījumi ir izpildīti.

4. Sagatavojot 2. punktā minēto īstenošanas akta projektu, Komisija ņem vērā attiecīgo struktūru viedokli un pienācīgi apspriežas ar visām attiecīgajām ieinteresētajām personām.

5. Produktus ar digitāliem elementiem un ražotāja ieviestos procesus, kas atbilst kopīgajām specifikācijām, kuras ieviestas ar šā panta 2. punktā minētajiem īstenošanas aktiem, vai to daļām, uzskata par atbilstīgiem I pielikumā izklāstītajām kiberdrošības pamatprasībām, kas ietvertas minētajās kopīgajās specifikācijas vai to daļās.

6. Ja saskaņotais standarts ir pieņemts Eiropas standartizācijas organizācijā un Komisijai ir ierosināts atsauci uz attiecīgo standartu publicēt *Eiropas Savienības Oficiālajā Vēstnesī*, Komisija saskaņoto standartu izvērtē saskaņā ar Regulu (ES) Nr. 1025/2012. Pēc tam, kad atsauce uz saskaņoto standartu ir publicēta *Eiropas Savienības Oficiālajā Vēstnesī*, Komisija atceļ 2. punktā minētos īstenošanas aktus vai to daļas, kas attiecas uz tām pašām kiberdrošības pamatprasībām, kuras ietvertas attiecīgajā saskaņotajā standartā.

7. Ja kāda dalībvalsts uzskata, ka kopīgā specifikācija pilnībā neizpilda I pielikumā izklāstītās kiberdrošības pamatprasības, tā par to informē Komisiju un iesniedz detalizētu skaidrojumu. Komisija izvērtē detalizēto skaidrojumu un vajadzības gadījumā var grozīt īstenošanas aktu, ar ko nosaka attiecīgo kopīgo specifikāciju.

8. Produktus ar digitāliem elementiem un ražotāja ieviestos procesus, par kuriem ir izdots ES atbilstības apliecinājums vai sertifikāts atbilstīgi Eiropas kiberdrošības sertifikācijas shēmai, kas pieņemta, ievērojot Regulu (ES) 2019/881, uzskata par atbilstīgiem I pielikumā izklāstītajām kiberdrošības pamatprasībām, ciktāl ES atbilstības apliecinājums vai Eiropas kiberdrošības sertifikāts vai tā daļas attiecas uz minētajām prasībām.

9. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar šīs regulas 61. pantu, lai papildinātu šo regulu, precizējot Eiropas kiberdrošības sertifikācijas shēmas, kuras pieņemtas, ievērojot Regulu (ES) 2019/881, un kuras var izmantot, lai pierādītu produktu ar digitāliem elementiem atbilstību šīs regulas I pielikumā izklāstītajām kiberdrošības pamatprasībām vai to daļām. Turklāt Eiropas kiberdrošības sertifikāts, ja tas izdots saskaņā ar šādām shēmām, kuru apliecinājuma līmenis ir vismaz "būtisks", atceļ ražotāja pienākumu īstenot trešās personas veiktu atbilstības novērtēšanu attiecīgajām prasībām, kā noteikts šīs regulas 32. panta 2. punkta a) un b) apakšpunktā un 32. panta 3. punkta a) un b) apakšpunktā.

28. pants

ES atbilstības deklarācija

1. ES atbilstības deklarāciju sagatavo ražotāji saskaņā ar 13. panta 12. punktu, un tā norāda, ka ir pierādīta atbilstība piemērojamām I pielikumā izklāstītajām kiberdrošības pamatprasībām.

2. ES atbilstības deklarāciju veido pēc V pielikumā norādītās parauga struktūras, un tajā ir elementi, kas precizēti attiecīgajās atbilstības novērtēšanas procedūrās, kas izklāstītas VIII pielikumā. Šādu deklarāciju pēc vajadzības atjaunina. To dara pieejamu valodās, ko noteikusi dalībvalsts, kurā produkts ar digitāliem elementiem tiek laists tirgū vai ir darīts pieejams tirgū.

Šīs regulas 13. panta 20. punktā minētās vienkāršotās ES atbilstības deklarācijas struktūra atbilst VI pielikumā norādītajam paraugam. To dara pieejamu valodās, ko noteikusi dalībvalsts, kurā produkts ar digitāliem elementiem tiek laists tirgū vai ir darīts pieejams tirgū.

3. Ja uz produktu ar digitāliem elementiem attiecas vairāk nekā viens Savienības tiesību akts, kurš prasa ES atbilstības deklarāciju, tiek sagatavota vienota ES atbilstības deklarācija attiecībā uz visiem šādiem Savienības tiesību aktiem. Minētajā deklarācijā norāda attiecīgos Savienības tiesību aktus, kā arī atsauces uz to publicēšanu.

4. Sagatavojot ES atbilstības deklarāciju, ražotājs uzņemas atbildību par produkta ar digitāliem elementiem atbilstību.

5. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 61. pantu nolūkā papildināt šo regulu, pievienojot elementus V pielikumā sniegtās ES atbilstības deklarācijas minimālajam saturam, lai ņemtu vērā tehnoloģiju attīstību.

29. pants

CE zīmes vispārējie principi

Uz CE zīmi attiecas Regulas (EK) Nr. 765/2008 30. pantā izklāstītie vispārējie principi.

30. pants

CE zīmes uzlikšanas noteikumi un nosacījumi

1. CE zīmi produktam ar digitāliem elementiem uzliek tā, lai tā būtu redzama, salasāma un neizdzēšama. Ja produkta ar digitāliem elementiem īpatnību dēļ tas nav iespējams vai nodrošināms, zīmi uzliek uz iepakojuma un 28. pantā minētajā ES atbilstības deklarācijā, kas pievienota produktam ar digitāliem elementiem. Tādiem produktiem ar digitāliem elementiem, kas ir programmatūra, CE zīmi norāda vai nu 28. pantā minētajā ES atbilstības deklarācijā, vai attiecīgo programmatūras produktu papildinošajā tīmekļvietnē. Ja CE zīme tiek norādīta tīmekļvietnē, tās attiecīgā sadaļa ir viegli un tieši pieejama patērētājiem.

2. Ievērojot produkta ar digitāliem elementiem īpatnības, tādas CE zīmes augstums, ko uzliek produktam ar digitāliem elementiem, var būt mazāks par 5 mm, ja tas joprojām ir redzams un salasāms.

3. CE zīmi uzliek pirms produkta ar digitāliem elementiem laišanas tirgū. Aiz tās var ievietot piktogrammu vai jebkādu citu zīmi, kas norāda uz īpašu kiberdrošības risku vai lietojumu, kas noteikts 6. punktā minētajos īstenošanas aktos.

4. Aiz CE zīmes norāda paziņotās struktūras identifikācijas numuru, ja minētā struktūra ir iesaistīta 32. pantā minētajā atbilstības novērtēšanas procedūrā, kuras pamatā ir visaptveroša kvalitātes nodrošināšana (pamatojoties uz H moduli).

Paziņotās struktūras identifikācijas numuru uzliek pati struktūra vai pēc tās norādījumiem to uzliek ražotājs vai ražotāja pilnvarotais pārstāvis.

5. Dalībvalstis izmanto esošos mehānismus, lai nodrošinātu CE zīmes izmantošanas kārtības pareizu piemērošanu, un minētās zīmes neatbilstīgas izmantošanas gadījumā attiecīgi rīkojas. Ja produkts ar digitāliem elementiem ir reglamentēts ar Savienības saskaņošanas tiesību aktiem, kas nav šī regula un kas arī paredz CE zīmes uzlikšanu, CE zīme norāda uz to, ka šis produkts arī atbilst prasībām, kas noteiktas šādos citos Savienības saskaņošanas tiesību aktos.

6. Komisija ar īstenošanas aktiem var noteikt tehniskās specifikācijas marķējumam, piktogrammām vai citām zīmēm, kas saistītas ar produktu ar digitāliem elementiem drošību, kā arī var noteikt šādu produktu atbalsta periodus un mehānismus to lietošanas veicināšanai un sabiedrības labākai informēšanai par produktu ar digitāliem elementiem drošību. Sagatavojot īstenošanas aktu projektus, Komisija apspriežas ar attiecīgajām ieinteresētajām personām un gadījumā, ja īstenošanas akti jau ir pieņemti, ievērojot 52. panta 15. punktu, Komisija apspriežas ar *ADCO*. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 62. panta 2. punktā.

31. pants

Tehniskā dokumentācija

1. Tehniskajā dokumentācijā ietver visus attiecīgos datus vai informāciju par līdzekļiem, ko ražotājs izmantojis, lai nodrošinātu, ka produkts ar digitāliem elementiem un ražotāja ieviestie procesi atbilst I pielikumā izklāstītajām kiberdrošības pamatprasībām. Tajā ir ietverti vismaz tie elementi, kas izklāstīti VII pielikumā.

2. Tehnisko dokumentāciju sagatavo pirms produkta ar digitāliem elementiem laišanas tirgū un vajadzības gadījumā pastāvīgi atjaunina vismaz atbalsta periodā.

3. Attiecībā uz 12. pantā minētajiem produktiem ar digitāliem elementiem, kam piemēro arī citus Savienības tiesību aktus, kuros izklāstīta tehniskā dokumentācija, sagatavo vienu vienotu tehnisko dokumentāciju, kurā tiek ietverta VII pielikumā minētā informācija un attiecīgajos Savienības tiesību aktos prasītā informācija.

4. Tehnisko dokumentāciju un korespondenci, kas attiecas uz jebkuru atbilstības novērtēšanas procedūru, sagatavo tās dalībvalsts oficiālajā valodā, kurā paziņotā struktūra ir iedibināta, vai citā šai struktūrai pieņemamā valodā.

5. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 61. pantu nolūkā papildināt šo regulu, pievienojot elementus, kas iekļaujami VII pielikumā izklāstītajā tehniskajā dokumentācijā, lai ņemtu vērā tehnoloģiju attīstību, kā arī šīs regulas īstenošanas procesā konstatētās attīstības norises. Šajā nolūkā Komisija cenšas nodrošināt, lai mikrouzņēmumiem un maziem un vidējiem uzņēmumiem radītais administratīvais slogs būtu samērīgs.

32. pants

Atbilstības novērtēšanas procedūras attiecībā uz produktiem ar digitāliem elementiem

1. Ražotājs veic produkta ar digitāliem elementiem un ražotāja ieviesto procesu atbilstības novērtēšanu, lai noteiktu, vai ir izpildītas I pielikumā noteiktās kiberdrošības pamatprasības. Ražotājs pierāda atbilstību kiberdrošības pamatprasībām, izmantojot jebkuru no šādām procedūrām:

   a) iekšējās kontroles procedūra (pamatojoties uz A moduli), kas norādīta VIII pielikumā;

   b) ES tipa pārbaudes procedūra (pamatojoties uz B moduli), kura paredzēta VIII pielikumā un kurai seko VIII pielikumā norādītā procedūra, kurā pārbauda atbilstību ES tipam, pamatojoties uz iekšējo ražošanas kontroli (pamatojoties uz C moduli);

c) uz visaptverošu kvalitātes nodrošināšanu pamatota atbilstības novērtēšanas procedūra (pamatojoties uz H moduli), kas norādīta VIII pielikumā; vai

d) Eiropas kiberdrošības sertifikācijas shēma, ja tāda ir pieejama un piemērojama, ievērojot 27. panta 9. punktu.

2. Ja, izvērtējot nozīmīga produkta ar digitāliem elementiem, kas ietilpst I klasē, kā noteikts III pielikumā, un tā ražotāja ieviesto procesu atbilstību I pielikumā izklāstītajām kiberdrošības pamatprasībām, ražotājs nav piemērojis vai ir tikai daļēji piemērojis 27. pantā minētos saskaņotos standartus, kopīgās specifikācijas vai Eiropas kiberdrošības sertifikācijas shēmas, kuru apliecinājuma līmenis ir vismaz "būtisks", vai ja šādu saskaņotu standartu, kopīgu specifikāciju vai Eiropas kiberdrošības sertifikācijas shēmu nav, attiecīgajam produktam ar digitāliem elementiem un ražotāja ieviestajiem procesiem attiecībā uz minētajām kiberdrošības pamatprasībām paredz jebkuru no šādām procedūrām:

a) ES tipa pārbaudes procedūra (pamatojoties uz B moduli), kura izklāstīta VIII pielikumā un kurai seko VIII pielikumā norādītā procedūra, kurā pārbauda atbilstību ES tipam, pamatojoties uz iekšējo ražošanas kontroli (pamatojoties uz C moduli); vai

b) uz visaptverošu kvalitātes nodrošināšanu pamatota atbilstības novērtēšanas procedūra (pamatojoties uz H moduli), kas norādīta VIII pielikumā;

3. Ja produkts ir nozīmīgs produkts ar digitāliem elementiem, kas ietilpst II klasē, kā noteikts III pielikumā, ražotājs pierāda atbilstību I pielikumā izklāstītajām kiberdrošības pamatprasībām, izmantojot jebkuru no šādām procedūrām:

a) ES tipa pārbaudes procedūra (pamatojoties uz B moduli), kura paredzēta VIII pielikumā un kurai seko VIII pielikumā norādītā procedūra, kurā pārbauda atbilstību ES tipam, pamatojoties uz iekšējo ražošanas kontroli (pamatojoties uz C moduli);

b) uz visaptverošu kvalitātes nodrošināšanu pamatota atbilstības novērtēšanas procedūra (pamatojoties uz H moduli), kas norādīta VIII pielikumā; vai

c) Eiropas kiberdrošības sertifikācijas shēma, ievērojot šīs regulas 27. panta 9. punktu, ja tāda ir pieejama un piemērojama, kuras apliecinājuma līmenis, ievērojot Regulu (ES) 2019/881, ir vismaz "būtisks".

4. IV pielikumā uzskaitīto kritiski svarīgo produktu ar digitāliem elementiem atbilstību I pielikumā izklāstītajām kiberdrošības pamatprasībām pierāda, izmantojot vienu no šādām procedūrām:

a) Eiropas kiberdrošības sertifikācijas shēma saskaņā ar 8. panta 1. punktu; vai

b) ja nav izpildīti 8. panta 1. punkta nosacījumi – jebkura no šā panta 3. punktā minētajām procedūrām.

5. Tādu produktu ar digitāliem elementiem ražotāji, kas uzskatāmi par brīvi pieejamu un atvērtā pirmkoda programmatūru, kura ietilpst III pielikumā minētajās kategorijās, atbilstību I pielikumā izklāstītajām kiberdrošības pamatprasībām pierāda, izmantojot vienu no šā panta 1. punktā minētajām procedūrām, ar noteikumu, ka brīdī, kad šie produkti tiek laisti tirgū, 31. pantā minētā tehniskā dokumentācija ir publiski pieejama.

6. Nosakot maksas par atbilstības novērtēšanas procedūrām, ņem vērā mikrouzņēmumu un mazo un vidējo uzņēmumu, tostarp jaunuzņēmumu, specifiskās intereses un vajadzības un šīs maksas samazina proporcionāli minēto uzņēmumu specifiskajām interesēm un vajadzībām.

33. pants

Atbalsta pasākumi mikrouzņēmumiem un maziem un vidējiem uzņēmumiem, tostarp jaunuzņēmumiem

1. Dalībvalstis vajadzības gadījumā veic šādas darbības, kas ir pielāgotas mikrouzņēmumu un mazo uzņēmumu vajadzībām:

   a) organizē īpašus izpratnes veicināšanas un mācību pasākumus par šīs regulas piemērošanu;

b) izveido īpašu kanālu saziņai ar mikrouzņēmumiem un maziem uzņēmumiem un vajadzības gadījumā ar vietējām publiskām iestādēm, lai sniegtu konsultācijas un atbildētu uz jautājumiem par šīs regulas īstenošanu;

c) atbalsta testēšanas un atbilstības novērtēšanas darbības, tostarp attiecīgā gadījumā ar Eiropas Kiberdrošības kompetenču centra atbalstu.

2. Dalībvalstis vajadzības gadījumā var izveidot kibernoturības "regulatīvās smilškastes". Šādas "regulatīvās smilškastes" nodrošina kontrolētu testēšanas vidi inovatīviem produktiem ar digitāliem elementiem, lai atvieglotu šādu produktu izstrādi, projektēšanu, validēšanu un testēšanu un ierobežotā termiņā pirms to laišanas tirgū nodrošinātu atbilstību šai regulai. Komisija un attiecīgā gadījumā *ENISA* var sniegt tehnisko atbalstu, konsultācijas un rīkus "regulatīvo smilškastu" izveidei un darbībai. "Regulatīvās smilškastes" izveido tirgus uzraudzības iestāžu tiešā uzraudzībā, tiešā vadībā un ar šo iestāžu atbalstu. Dalībvalstis ar *ADCO* starpniecību informē Komisiju un pārējās tirgus uzraudzības iestādes par "regulatīvās smilškastes" izveidi. "Regulatīvās smilškastes" neietekmē kompetento iestāžu uzraudzības un korektīvās pilnvaras. Dalībvalstis nodrošina atvērtu, taisnīgu un pārredzamu piekļuvi "regulatīvajām smilškastēm" un jo īpaši veicina mikrouzņēmumu un mazo uzņēmumu, tostarp jaunuzņēmumu, piekļuvi tām.

3. Komisija saskaņā ar 26. pantu sniedz norādījumus mikrouzņēmumiem un maziem un vidējiem uzņēmumiem par šīs regulas īstenošanu.

4. Komisija esošo Savienības programmu tiesiskajā regulējumā cenšas nodrošināt finansiālā atbalsta pieejamību, jo īpaši nolūkā atvieglot mikrouzņēmumiem un maziem un vidējiem uzņēmumiem radīto finansiālo slogu.

5. Mikrouzņēmumi un mazie uzņēmumi visus VII pielikumā norādītās tehniskās dokumentācijas elementus var iesniegt vienkāršotā formātā. Šajā nolūkā Komisija ar īstenošanas aktiem precizē vienkāršoto tehniskās dokumentācijas formātu, kas pielāgots mikrouzņēmumu un mazo uzņēmumu vajadzībām, tostarp izklāsta, kā iesniedzami VII pielikumā norādītie elementi. Ja mikrouzņēmums vai mazais uzņēmums VII pielikumā noteikto informāciju izvēlas sniegt vienkāršotā veidā, tas izmanto šajā punktā minēto formātu. Paziņotās struktūras pieņem, ka minētais formāts ir derīgs atbilstības novērtēšanas vajadzībām.

Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 62. panta 2. punktā.

34. pants

Savstarpējās atzīšanas nolīgumi

Ņemot vērā trešās valsts tehniskās attīstības līmeni un pieeju atbilstības novērtēšanai, Savienība saskaņā ar LESD 218. pantu var noslēgt savstarpējās atzīšanas nolīgumus ar trešām valstīm, lai veicinātu un atvieglotu starptautisko tirdzniecību.

IV nodaļa

Atbilstības novērtēšanas struktūru paziņošana

35. pants

Paziņošana

1. Dalībvalstis Komisijai un pārējām dalībvalstīm paziņo struktūras, kas ir pilnvarotas veikt atbilstības novērtēšanu saskaņā ar šo regulu.

2. Dalībvalstis līdz ... [24 mēneši no šīs regulas spēkā stāšanās dienas] cenšas nodrošināt, ka Savienībā ir pietiekams skaits paziņoto struktūru atbilstības novērtējumu veikšanai, lai izvairītos no šķēršļiem un traucējumiem ienākšanai tirgū.

36. pants

Paziņojošās iestādes

1. Katra dalībvalsts nozīmē paziņojošo iestādi, kuras pienākums ir noteikt un veikt procedūras, kas nepieciešamas, lai novērtētu, izraudzītu un paziņotu atbilstības novērtēšanas struktūras un pārraudzītu tās, tostarp izpildīt 41. panta prasības.

2. Dalībvalstis var nolemt, ka 1. punktā minēto novērtēšanu un pārraudzību veic kāda valsts akreditācijas struktūra Regulas (EK) Nr. 765/2008 nozīmē un saskaņā ar to.

3. Ja šā panta 1. punktā minēto novērtēšanu, paziņošanu vai pārraudzību paziņojošā iestāde deleģē vai kā citādi uztic struktūrai, kas nav valdības vienība, attiecīgā struktūra ir tiesību subjekts un *mutatis mutandis* ievēro 37. pantu. Turklāt tā ir ieviesusi nepieciešamos pasākumus, lai pildītu saistības, kas izriet no tās darbībām.

4. Paziņojošā iestāde uzņemas pilnu atbildību par 3. punktā minētās struktūras veiktajiem uzdevumiem.

37. pants

Prasības paziņojošajām iestādēm

1. Paziņojošo iestādi izveido tā, lai nebūtu interešu konfliktu ar atbilstības novērtēšanas struktūrām.

2. Paziņojošā iestāde ir organizēta un darbojas tā, lai nodrošinātu tās darbības objektivitāti un taisnīgumu.

3. Paziņojošā iestāde ir organizēta tā, lai visus lēmumus par atbilstības novērtēšanas struktūras paziņošanu pieņemtu kompetentas personas, kas nav tās pašas personas, kuras veikušas novērtēšanu.

4. Paziņojošā iestāde nepiedāvā vai neveic darbības, ko veic atbilstības novērtēšanas struktūras, un nesniedz konsultāciju pakalpojumus komerciālā vai konkurences nolūkā.

5. Paziņojošā iestāde nodrošina iegūtās informācijas konfidencialitāti.

6. Paziņojošās iestādes rīcībā ir pietiekams skaits kompetentu darbinieku tās uzdevumu pienācīgai veikšanai.

38. pants

Paziņojošo iestāžu pienākums informēt

1. Dalībvalstis informē Komisiju par atbilstības novērtēšanas struktūru novērtēšanas un paziņošanas procedūrām un paziņoto struktūru uzraudzības procedūrām, kā arī par visām izmaiņām šajā informācijā.

2. Komisija 1. punktā minēto informāciju dara publiski pieejamu.

39. pants

Prasības paziņotajām struktūrām

1. Paziņošanas nolūkos atbilstības novērtēšanas struktūra atbilst 2. līdz 12. punkta prasībām.

2. Atbilstības novērtēšanas struktūru izveido saskaņā ar valsts tiesību aktiem, un tā ir juridiska persona.

3. Atbilstības novērtēšanas struktūra ir trešā persona, kas ir neatkarīga no organizācijas vai produkta ar digitāliem elementiem, ko tā novērtē.

Struktūra, kas pieder uzņēmumu apvienībai vai profesionālajai federācijai, kura pārstāv uzņēmumus, kas iesaistīti novērtējamo produktu ar digitāliem elementiem projektēšanā, izstrādē, ražošanā, piegādē, uzstādīšanā, lietošanā vai uzturēšanā, ar nosacījumu, ka ir pierādīta tās neatkarība un interešu konflikta neesamība, tiek uzskatīta par šādu trešo personu

4. Atbilstības novērtēšanas struktūra, tās augstākā vadība un darbinieki, kas ir atbildīgi par atbilstības novērtēšanas uzdevumu veikšanu, nav vērtējamo produktu ar digitāliem elementiem projektētāji, izstrādātāji, ražotāji, piegādātāji, importētāji, izplatītāji, instalētāji, pircēji, īpašnieki, lietotāji vai uzturētāji, ne arī to pilnvaroti pārstāvji. Tas neliedz izmantot novērtētos produktus, kas ir vajadzīgi atbilstības novērtēšanas struktūras darbībai, vai izmantot šādus produktus personiskiem mērķiem.

Atbilstības novērtēšanas struktūra, tās augstākā vadība un darbinieki, kas ir atbildīgi par atbilstības novērtēšanas uzdevumu veikšanu, nav tieši saistīti ar produktu ar digitāliem elementiem, ko tie novērtē, projektēšanu, izstrādi, ražošanu, importu, izplatīšanu, tirdzniecību, instalēšanu, lietošanu vai uzturēšanu un nepārstāv šajās darbībās iesaistītās personas. Tā neiesaistās darbībās, kas var būt pretrunā viņu lēmuma neatkarībai vai integritātei attiecībā uz tām novērtēšanas darbībām, kuru dēļ tā ir paziņotā struktūra. Tas jo īpaši attiecas uz konsultāciju pakalpojumiem.

Atbilstības novērtēšanas struktūras nodrošina, lai to meitasuzņēmumu vai apakšlīgumu slēdzēju darbības neietekmētu atbilstības novērtēšanas darbību konfidencialitāti, objektivitāti vai taisnīgumu.

5. Atbilstības novērtēšanas struktūras un to darbinieki veic atbilstības novērtēšanas darbības ar visaugstāko profesionālo godprātību un vajadzīgo tehnisko kompetenci konkrētajā jomā bez spiediena un pamudinājumiem, arī finansiāliem, kas varētu ietekmēt viņu lēmumu vai atbilstības novērtēšanas darbību rezultātus, īpaši attiecībā uz personām vai personu grupām, kuras ir ieinteresētas šo darbību rezultātos.

6. Atbilstības novērtēšanas struktūra ir spējīga veikt visus atbilstības novērtēšanas uzdevumus, kuri minēti VIII pielikumā un kuru dēļ tā ir paziņotā struktūra, neatkarīgi no tā, vai šos uzdevumus veic pati atbilstības novērtēšanas struktūra vai tie tiek veikti tās vārdā un uz tās atbildību.

Atbilstības novērtēšanas struktūrai vienmēr un par visām atbilstības novērtēšanas procedūrām un produktu ar digitāliem elementiem veidiem un kategorijām, saistībā ar ko tā ir paziņotā struktūra, ir vajadzīgie:

a) personāls ar tehniskajām zināšanām un pietiekamu un piemērotu pieredzi atbilstības novērtēšanas uzdevumu veikšanai;

b) attiecīgs to procedūru apraksts, saskaņā ar kurām ir jāveic atbilstības izvērtēšana, nodrošinot pārredzamību un to, ka šīs procedūras ir iespējams piemērot. Tai ir izstrādāta pienācīga politika un procedūras, ar ko uzdevumi, ko tā veic kā paziņotā struktūra, ir nodalīti no citām darbībām;

c) procedūras darbību veikšanai, kurās pienācīgi ņem vērā uzņēmuma lielumu, nozari, kurā tas darbojas, tā struktūru, attiecīgās produkta tehnoloģijas sarežģītības pakāpi un to, vai ražošanas process ir masveida vai sērijveida.

Atbilstības novērtēšanas struktūrai ir nepieciešamie līdzekļi, lai pienācīgi veiktu tehniskos un administratīvos uzdevumus saistībā ar atbilstības novērtēšanas darbībām, un ir piekļuve visam nepieciešamajam aprīkojumam un iekārtām.

7. Personālam, kas atbildīgs par atbilstības novērtēšanas darbību veikšanu, ir:

a) pienācīga tehniskā un profesionālā apmācība, kas aptver visas atbilstības novērtēšanas darbības, kuru dēļ atbilstības novērtēšanas struktūra ir paziņotā struktūra;

b) pietiekamas zināšanas par prasībām attiecībā uz veicamo novērtēšanu un atbilstīgas pilnvaras veikt šo novērtēšanu;

c) attiecīgas zināšanas un izpratne par I pielikumā izklāstītajām kiberdrošības pamatprasībām, piemērojamajiem saskaņotajiem standartiem, kopīgajām specifikācijām un attiecīgajiem noteikumiem Savienības saskaņošanas tiesību aktos un īstenošanas aktos;

d) māka sastādīt sertifikātus, dokumentāciju un ziņojumus, kas apliecina, ka ir veikta novērtēšana.

8. Tiek garantēta atbilstības novērtēšanas struktūru, tās augstākā līmeņa vadības un personāla, kas veic novērtēšanu, objektivitāte.

Atalgojums, ko saņem atbilstības novērtēšanas struktūras augstākā līmeņa vadība un personāls, kas veic novērtēšanu, nav atkarīgs no veikto novērtējumu skaita vai to rezultātiem.

9. Atbilstības novērtēšanas struktūrām ir apdrošināta civiltiesiskā atbildība, ja vien atbildību neuzņemas attiecīgo struktūru dalībvalsts saskaņā ar valsts tiesību aktiem vai ja dalībvalsts pati nav tieši atbildīga par atbilstības novērtēšanu.

10. Atbilstības novērtēšanas struktūras personāls glabā dienesta noslēpumus attiecībā uz visu informāciju, kas iegūta, veicot pienākumus, uz kuriem attiecas VIII pielikums vai valstu tiesību aktu noteikumi, kas to īsteno, izņemot attiecībā uz tās dalībvalsts tirgus uzraudzības iestādēm, kurā darbības tiek veiktas. Īpašumtiesības ir aizsargātas. Atbilstības novērtēšanas struktūrai ir dokumentētas procedūras, kas nodrošina atbilstību šim punktam.

11. Atbilstības novērtēšanas struktūras nodrošina, ka personāls, kas ir atbildīgs par atbilstības novērtēšanas uzdevumu veikšanu, ir informēts par attiecīgajām standartizācijas darbībām un saskaņā ar 51. pantu izveidotās paziņoto struktūru koordinācijas grupas darbībām, vai pašas piedalās šo darbību veikšanā un piemēro kā pamatnostādnes šīs darba grupas administratīvos lēmumus un sagatavotos dokumentus.

12. Atbilstības novērtēšanas struktūras darbojas saskaņā ar konsekventiem, taisnīgiem, samērīgiem un saprātīgiem noteikumiem, vienlaikus izvairoties no nevajadzīga sloga radīšanas uzņēmējiem, un attiecībā uz maksām jo īpaši ņem vērā mikrouzņēmumu un mazo un vidējo uzņēmumu intereses.

40. pants

Pieņēmums par paziņoto struktūru atbilstību

Ja atbilstības novērtēšanas struktūra pierāda savu atbilstību kritērijiem, kas noteikti attiecīgajos saskaņotajos standartos vai to daļās, uz kuriem atsauces publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, to uzskata par atbilstīgu 39. panta prasībām, ciktāl piemērojamie saskaņotie standarti attiecas uz minētajām prasībām.

41. pants

Paziņoto struktūru meitasuzņēmumi un apakšlīgumu slēgšana

1. Ja paziņotā struktūra slēdz apakšlīgumus par konkrētu uzdevumu veikšanu saistībā ar atbilstības novērtēšanu vai izmanto meitasuzņēmumu, tā pārliecinās, ka apakšuzņēmējs vai meitasuzņēmums atbilst 39. panta prasībām, un attiecīgi informē paziņojošo iestādi.

2. Paziņotās struktūras uzņemas pilnu atbildību par apakšuzņēmēju vai meitasuzņēmumu veiktajiem uzdevumiem neatkarīgi no tā, kur tie iedibināti.

3. Par darbībām var slēgt apakšlīgumu vai tās var veikt meitasuzņēmums tikai tad, ja ražotājs tam piekrīt.

4. Paziņotās struktūras glabā paziņojošajai iestādei pieejamus attiecīgos dokumentus par apakšuzņēmēja vai meitasuzņēmuma kvalifikāciju novērtēšanu un to veikto darbu saskaņā ar šo regulu.

42. pants

Paziņošanas pieteikums

1. Atbilstības novērtēšanas struktūra iesniedz paziņošanas pieteikumu tās dalībvalsts paziņojošajai iestādei, kur tā veic darbību.

2. Minētajam pieteikumam pievieno aprakstu par atbilstības izvērtēšanas darbībām, atbilstības izvērtēšanas procedūru vai procedūrām un produktu vai produktiem ar digitāliem elementiem, attiecībā uz kuriem struktūra sevi piesaka par kompetentu, kā arī attiecīgā gadījumā akreditācijas sertifikātu, ja tāds ir, ko izsniegusi valsts akreditācijas struktūra, apliecinot, ka atbilstības izvērtēšanas struktūra atbilst 39. panta prasībām.

3. Ja attiecīgajai atbilstības novērtēšanas struktūrai nav akreditācijas sertifikāta, tā paziņojošajai iestādei iesniedz visus dokumentāros pierādījumus, kas nepieciešami, lai verificētu, atzītu un regulāri uzraudzītu tās atbilstību 39. panta prasībām

43. pants

Paziņošanas procedūra

1. Paziņojošās iestādes paziņo tikai tās atbilstības novērtēšanas struktūras, kas atbilst 39. pantā noteiktajām prasībām.

2. Paziņojošā iestāde Komisiju un pārējās dalībvalstis informē, izmantojot atbilstīgi jaunajai pieejai paziņoto un izraudzīto organizāciju informācijas sistēmu, ko ir izveidojusi un pārvalda Komisija.

3. Paziņojumā iekļauj sīku informāciju par atbilstības novērtēšanas darbībām, atbilstības novērtēšanas moduli vai moduļiem, attiecīgo produktu vai produktiem ar digitāliem elementiem un attiecīgo kompetences apliecinājumu.

4. Ja paziņošana ir veikta, neizmantojot 42. panta 2. punktā minēto akreditācijas sertifikātu, paziņojošā iestāde iesniedz Komisijai un pārējām dalībvalstīm dokumentārus pierādījumus, kuri apliecina atbilstības novērtēšanas struktūras kompetenci un veiktos pasākumus, ar ko nodrošina, ka minētā struktūra tiek regulāri uzraudzīta un ka tā joprojām atbilst 39. panta prasībām.

5. Attiecīgā struktūra drīkst veikt paziņotās struktūras darbības tikai tad, ja divu nedēļu laikā pēc paziņošanas Komisija vai pārējās dalībvalstis nav izteikušas iebildumus, ja tiek izmantots akreditācijas sertifikāts vai ja divu mēnešu laikā no paziņošanas nav izmantota akreditācijas procedūra.

   Šajā regulā tikai šādu struktūru uzskata par paziņoto struktūru.

6. Komisijai un pārējām dalībvalstīm paziņo par attiecīgām turpmākām izmaiņām paziņojumā.

44. pants

Paziņoto struktūru identifikācijas numuri un saraksti

1. Komisija paziņotajai struktūrai piešķir identifikācijas numuru.

   Tā piešķir tikai vienu šādu numuru arī tad, ja struktūra ir paziņota atbilstīgi vairākiem Savienības tiesību aktiem.

2. Komisija dara publiski pieejamu to struktūru sarakstu, kas paziņotas saskaņā ar šo regulu, ieskaitot tām piešķirtos identifikācijas numurus un darbības, kuru dēļ tās ir paziņotās struktūras.

   Komisija nodrošina minētā saraksta atjaunināšanu.

45. pants

Izmaiņas paziņojumos

1. Ja paziņojošā iestāde ir noskaidrojusi vai tikusi informēta par to, ka paziņotā struktūra vairs neatbilst 39. panta prasībām vai nepilda savus pienākumus, vajadzības gadījumā paziņojošā iestāde attiecīgi ierobežo, aptur vai atsauc paziņojumu atkarībā no tā, kādā ziņā attiecīgā struktūra nav spējusi nodrošināt atbilstību minētajām prasībām vai pildīt minētos pienākumus. Tā nekavējoties par to attiecīgi informē Komisiju un pārējās dalībvalstis.

2. Ja paziņojums ir ierobežots, apturēts vai anulēts vai ja paziņotā struktūra ir beigusi darbību, paziņojošā dalībvalsts veic atbilstīgus pasākumus, lai nodrošinātu, ka minētās struktūras dokumentus vai nu apstrādā cita paziņotā struktūra, vai arī tie pēc pieprasījuma ir pieejami atbildīgajām paziņojošajām un tirgus uzraudzības iestādēm.

46. pants

Paziņoto struktūru kompetences apšaubīšana

1. Komisija izmeklē visus gadījumus, kad tai ir radušās šaubas vai kad tai ir ziņots par šaubām attiecībā uz kādas paziņotās struktūras kompetenci vai tās spēju joprojām pildīt tai piemērojamās prasības un pienākumus.

2. Paziņotāja dalībvalsts pēc pieprasījuma sniedz Komisijai visu informāciju saistībā ar attiecīgās struktūras paziņošanas pamatojumu vai tās kompetences saglabāšanu.

3. Komisija nodrošina, lai visa sensitīvā informācija, kas saņemta izmeklēšanas gaitā, tiktu apstrādāta kā konfidenciāla informācija.

4. Ja Komisija noskaidro, ka paziņotā struktūra neatbilst vai vairs neatbilst paziņošanas prasībām, tā par to informē paziņotāju dalībvalsti un lūdz tai veikt nepieciešamos korektīvos pasākumus, ieskaitot – vajadzības gadījumā – paziņojuma atsaukšanu.

47. pants

Paziņoto struktūru darba pienākumi

1. Paziņotās struktūras veic atbilstības novērtēšanu saskaņā ar 32. pantā un VIII pielikumā paredzētajām atbilstības novērtēšanas procedūrām.

2. Atbilstības novērtēšanu veic samērīgi, neradot lieku slogu uzņēmējiem. Atbilstības novērtēšanas struktūras īsteno savu darbību, pienācīgi ņemot vērā uzņēmuma lielumu, jo īpaši attiecībā uz mikrouzņēmumiem un maziem un vidējiem uzņēmumiem, nozari, kurā tie darbojas, to struktūru, to sarežģītības pakāpi, attiecīgo produktu ar digitāliem elementiem kiberdrošības riska līmeni un attiecīgo tehnoloģiju, kā arī to, vai ražošanas process ir masveidīgs vai sērijveida.

3. Paziņotās struktūras tomēr ievēro tādu stingrību un aizsardzības līmeni, kāds vajadzīgs, lai produkti ar digitāliem elementiem atbilstu šīs regulas noteikumiem.

4. Ja paziņotā struktūra konstatē, ka ražotājs nav izpildījis I pielikumā vai atbilstīgajos saskaņotajos standartos, vai 27. pantā minētajās kopīgajās specifikācijās noteiktās prasības, tā pieprasa, lai ražotājs veiktu attiecīgus korektīvos pasākumus, un neizdod atbilstības sertifikātu.

5. Ja, uzraugot atbilstību pēc sertifikāta izdošanas, paziņotā struktūra atklāj, ka kāds produkts ar digitāliem elementiem vairs nav atbilstīgs šajā regulā noteiktajām prasībām, tā pieprasa, lai ražotājs veiktu attiecīgus korektīvos pasākumus, un vajadzības gadījumā sertifikātu aptur vai atsauc.

6. Ja korektīvie pasākumi netiek veikti vai tie nedod vēlamo rezultātu, paziņotā struktūra attiecīgos sertifikātus attiecīgi ierobežo, aptur vai atsauc.

48. pants

Paziņoto struktūru lēmumu apstrīdēšana

Dalībvalstis nodrošina, ka ir pieejama paziņoto struktūru lēmumu apstrīdēšanas procedūra.

49. pants

Paziņoto struktūru pienākums informēt

1. Paziņotās struktūras informē paziņojošo iestādi par:

   a) sertifikāta atteikšanu, ierobežošanu, apturēšanu vai atsaukšanu;

   b) apstākļiem, kas ietekmē paziņojuma darbības jomu un nosacījumus;

c) visiem informācijas pieprasījumiem par atbilstības novērtēšanas darbībām, ko tās saņēmušas no tirgus uzraudzības iestādēm;

d) atbilstības novērtēšanas darbībām, kas veiktas paziņojuma darbības jomā, un visām citām veiktajām darbībām, arī pārrobežu darbībām un apakšlīgumu slēgšanu – pēc pieprasījuma.

2. Paziņotās struktūras pārējām struktūrām, kas paziņotas atbilstīgi šai regulai un kas veic līdzīgas atbilstības novērtēšanas darbības, kuras attiecas uz tiem pašiem produktiem ar digitāliem elementiem, sniedz attiecīgu informāciju par jautājumiem saistībā ar negatīviem un, pēc pieprasījuma, arī pozitīviem atbilstības novērtēšanas rezultātiem.

50. pants

Pieredzes apmaiņa

Komisija gādā, lai starp dalībvalstu iestādēm, kas ir atbildīgas par paziņošanas politiku, tiktu organizēta pieredzes apmaiņa.

51. pants

Paziņoto struktūru koordinācija

1. Komisija nodrošina to, lai starp paziņotajām struktūrām tiktu izveidota attiecīga koordinācija un sadarbība un lai tā tiktu pienācīgi īstenota paziņoto struktūru starpnozaru grupas veidā.

2. Dalībvalstis nodrošina, lai to paziņotās struktūras tieši vai ar ieceltu pārstāvju palīdzību piedalītos minētās grupas darbā.

V nodaļa

Tirgus uzraudzība un izpildes panākšana

52. pants

Tirgus uzraudzība un produktu ar digitāliem elementiem kontrole Savienības tirgū

1. Produktiem ar digitāliem elementiem, kas ietilpst šīs regulas darbības jomā, piemēro Regulu (ES) 2019/1020.

2. Katra dalībvalsts izraugās vienu vai vairākas tirgus uzraudzības iestādes, lai nodrošinātu šīs regulas efektīvu īstenošanu. Dalībvalstis var izraudzīties esošu vai jaunu iestādi, lai tā darbotos kā tirgus uzraudzības iestāde saistībā ar šo regulu.

3. Tirgus uzraudzības iestādes, kas izraudzītas saskaņā ar šā panta 2. punktu, ir atbildīgas arī par tirgus uzraudzības darbību veikšanu saistībā ar 24. pantā noteiktajiem atvērtā pirmkoda programmatūras pārziņu pienākumiem. Ja tirgus uzraudzības iestāde konstatē, ka atvērtā pirmkoda programmatūras pārzinis nepilda minētajā pantā noteiktos pienākumus, tā pieprasa atvērtā pirmkoda programmatūras pārzinim nodrošināt, ka tiek veikti visi vajadzīgie korektīvie pasākumi. Atklātā pirmkoda programmatūras pārziņi nodrošina, ka tiek veikti visi vajadzīgie korektīvie pasākumi attiecībā uz pienākumiem, kas tiem noteikti šajā regulā.

4. Attiecīgā gadījumā tirgus uzraudzības iestādes sadarbojas ar valsts kiberdrošības sertifikācijas iestādēm, kas izraudzītas, ievērojot Regulas (ES) 2019/881 58. pantu, kā arī regulāri apmainās ar informāciju. Izraudzītās tirgus uzraudzības iestādes attiecībā uz šīs regulas 14. pantā noteikto ziņošanas pienākumu īstenošanas uzraudzību sadarbojas un veic regulāru informācijas apmaiņu ar *CSIRT*, kas izraudzītas par koordinatoriem, un ar *ENISA*.

5. Tirgus uzraudzības iestādes var pieprasīt par koordinatoru izraudzītajai *CSIRT* vai *ENISA* sniegt tehniskas konsultācijas jautājumos, kuri saistīti ar šīs regulas īstenošanu un izpildi. Veicot izmeklēšanu saskaņā ar 54. pantu, tirgus uzraudzības iestādes var pieprasīt par koordinatoru izraudzītajai *CSIRT* vai *ENISA* sniegt analīzi, kas palīdz sagatavot produktu ar digitāliem elementiem atbilstības novērtējumus.

6. Vajadzības gadījumā tirgus uzraudzības iestādes sadarbojas ar citām tirgus uzraudzības iestādēm, kas izraudzītas, pamatojoties uz Savienības saskaņošanas tiesību aktiem, kas nav šī regula, kā arī regulāri apmainās ar informāciju.

7. Tirgus uzraudzības iestādes attiecīgā gadījumā sadarbojas ar iestādēm, kas uzrauga Savienības datu aizsardzības tiesību aktus. Šāda sadarbība ietver minēto iestāžu informēšanu par visiem konstatējumiem, kas ir būtiski to kompetences īstenošanai, tostarp, kad tiek sniegti norādījumi un padomi, ievērojot šā panta 10. punktu, ja šādi norādījumi un padomi attiecas uz personas datu apstrādi.

   Iestādes, kas uzrauga Savienības datu aizsardzības tiesību aktus, ir pilnvarotas pieprasīt dokumentāciju, kas izveidota vai tiek uzturēta saskaņā ar šo regulu, un tai piekļūt, ja piekļuve minētajai dokumentācijai ir nepieciešama to uzdevumu izpildei. Tās informē attiecīgās dalībvalsts izraudzītās tirgus uzraudzības iestādes par jebkuru šādu pieprasījumu.

8. Dalībvalstis nodrošina, ka izraudzītajām tirgus uzraudzības iestādēm tiek sniegti atbilstoši finanšu resursi un tehniskie resursi, tostarp vajadzības gadījumā automatizētas apstrādes rīki, kā arī cilvēkresursi ar nepieciešamajām kiberdrošības prasmēm, lai tās varētu pildīt uzdevumus, kas tām noteikti šajā regulā.

9. Komisija mudina apmainīties ar pieredzi un veicina pieredzes apmaiņu starp izraudzītajām tirgus uzraudzības iestādēm.

10. Tirgus uzraudzības iestādes ar Komisijas un vajadzības gadījumā ar *CSIRT* un *ENISA* atbalstu var sniegt uzņēmējiem norādījumus un padomus par šīs regulas īstenošanu.

11. Tirgus uzraudzības iestādes saskaņā ar Regulas (ES) 2019/1020 11. pantu sniedz patērētājiem informāciju par to, kur iesniegt sūdzības par iespējamu neatbilstību šai regulai, un par to, kur un kā piekļūt mehānismiem, kas atvieglotu ziņošanu par ievainojamībām, incidentiem un kiberdraudiem, kuri var ietekmēt produktus ar digitāliem elementiem.

12. Tirgus uzraudzības iestādes attiecīgā gadījumā veicina sadarbību ar ieinteresētajam personām, tostarp zinātnes, pētniecības un patērētāju organizācijām.

13. Tirgus uzraudzības iestādes katru gadu ziņo Komisijai par attiecīgo tirgus uzraudzības darbību rezultātiem. Izraudzītās tirgus uzraudzības iestādes nekavējoties ziņo Komisijai un attiecīgajām valsts konkurences iestādēm par visu tirgus uzraudzības darbībās identificēto informāciju, kas varētu tās interesēt Savienības konkurences tiesību normu piemērošanā.

14. Produktiem ar digitāliem elementiem, kas ietilpst šīs regulas darbības jomā un ir klasificēti kā augsta riska MI sistēmas, ievērojot Regulas (ES) 2024/1689 6. pantu, tirgus uzraudzības iestādes, kas izraudzītas Regulas (ES) 2024/1689 vajadzībām, ir iestādes, kas atbild par šajā regulā noteiktajām tirgus uzraudzības darbībām. Atbilstīgi Regulai (ES) 2024/1689 izraudzītās tirgus uzraudzības iestādes attiecīgā gadījumā sadarbojas ar atbilstīgi šai regulai izraudzītajām tirgus uzraudzības iestādēm un – attiecībā uz šīs regulas 14. pantā noteikto ziņošanas pienākumu īstenošanas uzraudzību – ar *CSIRT*, kas izraudzītas par koordinatoriem, un *ENISA*. Tirgus uzraudzības iestādes, kas izraudzītas, ievērojot Regulu (ES) 2024/1689, jo īpaši informē tirgus uzraudzības iestādes, kas izraudzītas saskaņā ar šo regulu, par visiem konstatējumiem, kas ir būtiski to uzdevumu izpildei, kas tām noteikti saistībā ar šīs regulas īstenošanu.

15. Šīs regulas vienotai piemērošanai izveido *ADCO*, ievērojot Regulas (ES) 2019/1020 30. panta 2. punktu. *ADCO* sastāvā ir izraudzīto tirgus uzraudzības iestāžu pārstāvji un attiecīgā gadījumā arī vienoto sadarbības biroju pārstāvji. *ADCO* risina arī konkrētus jautājumus, kas attiecas uz tirgus uzraudzības darbībām, kuras ir saistītas ar atvērtā pirmkoda programmatūras pārziņiem uzticētajiem pienākumiem.

16. Tirgus uzraudzības iestādes uzrauga, kā ražotāji, nosakot atbalsta periodu saviem produktiem ar digitāliem elementiem, ir piemērojuši 13. panta 8. punktā minētos kritērijus.

ADCO publiski pieejamā un lietotājdraudzīgā veidā publicē attiecīgu statistiku par produktu ar digitāliem elementiem kategorijām, tostarp vidējos atbalsta periodus, ko ražotājs noteicis, ievērojot 13. panta 8. punktu, kā arī sniedz norādījumus, kas ietver indikatīvus atbalsta periodus produktu ar digitāliem elementiem kategorijām.

Ja dati liecina, ka konkrētām produktu ar digitāliem elementiem kategorijām atbalsta periodi nav pietiekami, *ADCO* var izdot ieteikumus tirgus uzraudzības iestādēm, lai tās rūpīgāk pievērstos attiecīgajām produktu ar digitāliem elementiem kategorijām.

53. pants

Piekļuve datiem un dokumentācijai

Ja tas nepieciešams, lai novērtētu produktu ar digitāliem elementiem un to ražotāju ieviesto procesu atbilstību I pielikumā izklāstītajām kiberdrošības pamatprasībām, tirgus uzraudzības iestādēm pēc pamatota pieprasījuma un tām viegli saprotamā valodā piešķir piekļuvi šādu produktu projektēšanas, izstrādes, ražošanas un ievainojamību novēršanas izvērtēšanai vajadzīgajiem datiem, ieskaitot attiecīgā uzņēmēja saistīto iekšējo dokumentāciju.

54. pants

Valsts līmeņa procedūra attiecībā uz produktiem ar digitāliem elementiem, kas rada būtisku kiberdrošības risku

1. Ja dalībvalsts tirgus uzraudzības iestādei ir pietiekams iemesls uzskatīt, ka produkts ar digitāliem elementiem, ieskaitot ievainojamību novēršanu, rada būtisku kiberdrošības risku, tā, lieki nekavējoties un vajadzības gadījumā sadarbojoties ar attiecīgo *CSIRT*, veic attiecīgā produkta ar digitāliem elementiem izvērtēšanu attiecībā uz tā atbilstību visām šajā regulā noteiktajām prasībām. Attiecīgie uzņēmēji pēc vajadzības sadarbojas ar tirgus uzraudzības iestādi.

Ja izvērtēšanā tirgus uzraudzības iestāde konstatē, ka produkts ar digitāliem elementiem neatbilst šajā regulā noteiktajām prasībām, tā nekavējoties pieprasa attiecīgajam uzņēmējam veikt visus attiecīgos korektīvos pasākumus, kas vajadzīgi, lai panāktu šā produkta ar digitāliem elementiem atbilstību vai lai samērīgi kiberdrošības riskam to izņemtu no tirgus vai atsauktu tirgus uzraudzības iestādes noteiktā pienācīgā termiņā.

Tirgus uzraudzības iestāde attiecīgi informē attiecīgo paziņoto struktūru. Korektīvajiem pasākumiem piemēro Regulas (ES) 2019/1020 18. pantu.

2. Nosakot šā panta 1. punktā minētā kiberdrošības riska nozīmīgumu, tirgus uzraudzības iestādes ņem vērā arī netehniskos riska faktorus, jo īpaši tos, kas identificēti, saskaņā ar Direktīvas (ES) 2022/2555 22. pantu veicot kritisko piegādes ķēžu koordinēto drošības riska novērtējumus. Ja tirgus uzraudzības iestādei ir pamatots iemesls uzskatīt, ka, ņemot vērā netehniskos riska faktorus, produkts ar digitāliem elementiem rada būtisku kiberdrošības risku, tā informē saskaņā ar Direktīvas (ES) 2022/2555 8. pantu izraudzītās vai izveidotās kompetentās iestādes un pēc vajadzības sadarbojas ar šīm iestādēm.

3. Ja tirgus uzraudzības iestāde uzskata, ka neatbilstība ir vērojama ne tikai tās valsts teritorijā, tā informē Komisiju un pārējās dalībvalstis par izvērtēšanas rezultātiem un par pasākumiem, ko tā pieprasījusi veikt uzņēmējam.

4. Uzņēmējs nodrošina, ka visi piemērotie korektīvie pasākumi tiek veikti attiecībā uz visiem attiecīgajiem produktiem ar digitāliem elementiem, ko tas darījis pieejamus tirgū visā Savienībā.

5. Ja uzņēmējs neveic pienācīgus korektīvus pasākumus 1. punkta otrajā daļā noteiktajā termiņā, tirgus uzraudzības iestāde veic visus vajadzīgos pagaidu pasākumus, lai aizliegtu vai ierobežotu to, ka minētais produkts ar digitāliem elementiem tiek darīts pieejams tās valsts tirgū, izņemtu to no minētā tirgus vai atsauktu to.

   Par šiem pasākumiem šī iestāde nekavējoties paziņo Komisijai un pārējām dalībvalstīm.

6. Šā panta 5. punktā minētajā informācijā ietver visas pieejamās ziņas, jo īpaši datus neatbilstīgā produkta ar digitāliem elementiem identificēšanai, datus par attiecīgā produkta ar digitāliem elementiem izcelsmi, attiecīgo neatbilstības veidu un ar to saistīto apdraudējumu, veikto valsts pasākumu veidu un ilgumu, kā arī attiecīgā uzņēmēja viedokli. Tirgus uzraudzības iestāde īpaši norāda, vai neatbilstība ir saistīta ar vienu vai vairākiem šādiem aspektiem:

   a) produkta ar digitāliem elementiem vai ražotāja ieviesto procesu neatbilstība I pielikumā izklāstītajām kiberdrošības pamatprasībām;

   b) trūkumi saskaņotajos standartos, Eiropas kiberdrošības sertifikācijas shēmās vai kopīgajās specifikācijās, kā minēts 27. pantā.

7. Dalībvalstu tirgus uzraudzības iestādes, kas nav procedūru sākušās dalībvalsts tirgus uzraudzības iestādes, nekavējoties informē Komisiju un pārējās dalībvalstis par visiem pieņemtajiem pasākumiem un visu savā rīcībā esošo papildu informāciju par attiecīgā produkta ar digitāliem elementiem neatbilstību un – ja tās nepiekrīt paziņotajam valsts pasākumam – par saviem iebildumiem.

8. Ja triju mēnešu laikā pēc šā panta 5. punktā minētā paziņojuma saņemšanas neviena dalībvalsts vai Komisija nav cēlusi iebildumus pret kādas dalībvalsts veiktu pagaidu pasākumu, minēto pasākumu uzskata par pamatotu. Tas neskar attiecīgā uzņēmēja procesuālās tiesības saskaņā ar Regulas (ES) 2019/1020 18. pantu.

9. Visu dalībvalstu tirgus uzraudzības iestādes nodrošina, ka attiecībā uz attiecīgo produktu ar digitāliem elementiem nekavējoties tiek veikti atbilstoši ierobežojoši pasākumi, piemēram, attiecīgo produktu izņem no to tirgus.

55. pants

Savienības drošības procedūra

1. Ja triju mēnešu laikā pēc 54. panta 5. punktā minētā paziņojuma saņemšanas dalībvalsts ceļ iebildumus par citas dalībvalsts veiktu pasākumu vai ja Komisija uzskata, ka pasākums ir pretrunā Savienības tiesību aktiem, Komisija nekavējoties uzsāk apspriešanos ar attiecīgo dalībvalsti un uzņēmēju vai uzņēmējiem un izvērtē valsts pasākumu. Pamatojoties uz šā izvērtējuma rezultātiem, Komisija deviņu mēnešu laikā pēc 54. panta 5. punktā minētā paziņojuma saņemšanas izlemj, vai valsts pasākums ir vai nav pamatots, un attiecīgo lēmumu dara zināmu attiecīgajai dalībvalstij.

2. Ja valsts pasākums tiek uzskatīts par pamatotu, visas dalībvalstis veic nepieciešamos pasākumus, lai nodrošinātu neatbilstīgā produkta ar digitāliem elementiem izņemšanu no sava tirgus, un par to attiecīgi informē Komisiju. Ja valsts pasākums tiek uzskatīts par nepamatotu, attiecīgā dalībvalsts atsauc šo pasākumu.

3. Ja valsts pasākums tiek uzskatīts par pamatotu un produkta ar digitāliem elementiem neatbilstība tiek saistīta ar trūkumiem saskaņotajos standartos, Komisija piemēro Regulas (ES) Nr. 1025/2012 11. pantā paredzēto procedūru.

4. Ja valsts pasākums tiek uzskatīts par pamatotu un produkta ar digitāliem elementiem neatbilstība tiek saistīta ar trūkumiem 27. pantā minētajā Eiropas kiberdrošības sertifikācijas shēmā, Komisija apsver, vai grozīt vai atcelt kādu deleģēto aktu, kas pieņemts, ievērojot 27. panta 9. punktu, un kas attiecībā uz šo sertifikācijas shēmu precizē pieņēmumu par atbilstību.

5. Ja valsts pasākums tiek uzskatīts par pamatotu un produkta ar digitāliem elementiem neatbilstība tiek saistīta ar trūkumiem 27. pantā minētajās kopīgajās specifikācijās, Komisija apsver, vai grozīt vai atcelt jebkuru saskaņā ar 27. panta 2. punktu pieņemto īstenošanas aktu, kurā izklāstītas šīs kopīgās specifikācijas.

56. pants

Savienības līmeņa procedūra attiecībā uz produktiem ar digitāliem elementiem, kas rada būtisku kiberdrošības risku

1. Ja Komisijai, pamatojoties uz *ENISA* sniegto informāciju, ir pietiekams iemesls uzskatīt, ka produkts ar digitāliem elementiem, kas rada būtisku kiberdrošības risku, neatbilst šajā regulā noteiktajām prasībām, tā informē attiecīgās tirgus uzraudzības iestādes. Kad tirgus uzraudzības iestādes izvērtē attiecīgā produkta ar digitāliem elementiem, kas var radīt būtisku kiberdrošības risku, atbilstību šajā regulā noteiktajām prasībām, tās piemēro 54. un 55. pantā minētās procedūras.

2. Ja Komisijai ir pamatots iemesls uzskatīt, ka produkts ar digitāliem elementiem, ņemot vērā netehniskos riska faktorus, rada būtisku kiberdrošības risku, tā informē tirgus uzraudzības iestādes un attiecīgā gadījumā saskaņā ar Direktīvas (ES) 2022/2555 8. pantu izraudzītās vai izveidotās kompetentās iestādes un pēc vajadzības sadarbojas ar šīm iestādēm. Komisija arī apsver, cik būtiski ir identificētie minētā produkta ar digitāliem elementiem riski, ņemot vērā savus uzdevumus attiecībā uz Savienības līmenī koordinētiem kritisko piegādes ķēžu drošības riska novērtējumiem, kas paredzēti Direktīvas (ES) 2022/2555 22. pantā, un vajadzības gadījumā apspriežas ar sadarbības grupu, kas izveidota, ievērojot Direktīvas (ES) 2022/2555 14. pantu, un ar *ENISA*.

3. Apstākļos, kas pamato tūlītēju intervenci ar mērķi saglabāt iekšējā tirgus pienācīgu darbību, un ja Komisijai ir pietiekams pamats uzskatīt, ka 1. punktā minētais produkts ar digitāliem elementiem joprojām neatbilst šajā regulā noteiktajām prasībām un attiecīgās tirgus uzraudzības iestādes nav veikušas efektīvus pasākumus, Komisija veic atbilstības novērtējumu un var pieprasīt *ENISA* sniegt analīzi, kas palīdzētu izvērtēšanā. Komisija attiecīgi informē attiecīgās tirgus uzraudzības iestādes. Attiecīgie uzņēmēji pēc vajadzības sadarbojas ar *ENISA*.

4. Pamatojoties uz 3. punktā minēto izvērtējumu, Komisija var noteikt, ka ir nepieciešams korektīvs vai ierobežojošs pasākums Savienības līmenī. Šajā nolūkā tā nekavējoties apspriežas ar attiecīgajām dalībvalstīm un attiecīgo uzņēmēju vai uzņēmējiem.

5. Pamatojoties uz šā panta 4. punktā minēto apspriešanos, Komisija var pieņemt īstenošanas aktus, lai paredzētu korektīvus vai ierobežojošus pasākumus Savienības līmenī, tajā skaitā pieprasot pienācīgā termiņā, kas ir samērīgs ar risku, attiecīgos produktus ar digitāliem elementiem izņemt no tirgus vai tos atsaukt. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 62. panta 2. punktā.

6. Komisija nekavējoties informē attiecīgo uzņēmēju vai uzņēmējus par 5. punktā minētajiem īstenošanas aktiem. Dalībvalstis nekavējoties īsteno minētos īstenošanas aktus un attiecīgi informē Komisiju.

7. Šā panta 3. līdz 5. punktu piemēro uz laiku, kamēr ir spēkā ārkārtas situācija, kas ir pamatojusi Komisijas intervenci, ja vien nav panākta attiecīgā produkta ar digitāliem elementiem atbilstība šai regulai.

57. pants

Atbilstīgi produkti ar digitāliem elementiem, kas rada būtisku kiberdrošības risku

1. Dalībvalsts tirgus uzraudzības iestāde pieprasa uzņēmējam veikt visus piemērotos pasākumus, ja tā pēc 54. pantā minētās izvērtēšanas konstatē, ka, neraugoties uz to, ka produkts ar digitāliem elementiem un ražotāja ieviestie procesi atbilst šai regulai, attiecīgais produkts tomēr rada būtisku kiberdrošības risku, kā arī risku, kas saistīts ar:

   a) cilvēka veselību vai drošību;

   b) atbilstību Savienības vai valstu tiesību aktos noteiktajiem pienākumiem, kuru mērķis ir aizsargāt pamattiesības;

c) tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus, izmantojot elektronisko informācijas sistēmu, piedāvā būtiskās vienības, kā minēts Direktīvas (ES) 2022/2555 3. panta 1. punktā; vai

d) citiem sabiedrības interešu aizsardzības aspektiem.

Pirmajā daļā minētie pasākumi var ietvert pasākumus, ar kuriem nodrošina, lai attiecīgais produkts ar digitāliem elementiem un ražotāja ieviestie procesi vairs neradītu konkrētos riskus brīdī, kad attiecīgo produktu ar digitāliem elementiem dara pieejamu tirgū, izņem no tirgus vai atsauc, un minētajiem pasākumiem jābūt samērīgiem ar šo risku būtību.

2. Ražotājs vai citi attiecīgie uzņēmēji nodrošina, ka termiņā, ko noteikusi 1. punktā minētā dalībvalsts tirgus uzraudzības iestāde, tiek veikti korektīvi pasākumi attiecībā uz attiecīgajiem produktiem ar digitāliem elementiem, ko tie darījuši pieejamus tirgū visā Savienībā.

3. Dalībvalsts nekavējoties informē Komisiju un pārējās dalībvalstis par saskaņā ar 1. punktu veiktajiem pasākumiem. Informācijā ietver visas pieejamās ziņas, jo īpaši datus, kas nepieciešami attiecīgo produktu ar digitāliem elementiem identificēšanai, datus par šo produktu ar digitāliem elementiem izcelsmi un piegādes ķēdi, konkrētā riska veidu un veikto valsts pasākumu veidu un ilgumu.

4. Komisija nekavējoties sāk apspriešanos ar dalībvalstīm un attiecīgo uzņēmēju un izvērtē valsts veiktos pasākumus. Pamatojoties uz minētā izvērtējuma rezultātiem, Komisija pieņem lēmumu par to, vai pasākums ir vai nav pamatots, un attiecīgā gadījumā ierosina pienācīgus pasākumus.

5. Šā panta 4. punktā minēto lēmumu Komisija adresē dalībvalstīm.

6. Ja Komisijai, arī pamatojoties uz *ENISA* sniegto informāciju, ir pietiekams iemesls uzskatīt, ka, lai gan produkts ar digitāliem elementiem atbilst šai regulai, tas rada šā panta 1. punktā minētos riskus, Komisija informē attiecīgo tirgus uzraudzības iestādi vai iestādes un var pieprasīt attiecīgajai iestādei veikt izvērtēšanu un rīkoties atbilstoši 54. pantā un šā panta 1., 2. un 3. punktā minētajām procedūrām.

7. Apstākļos, kas pamato tūlītēju intervenci ar mērķi saglabāt iekšējā tirgus pienācīgu darbību, un ja Komisijai ir pietiekams iemesls uzskatīt, ka 6. punktā minētais produkts ar digitāliem elementiem joprojām rada 1. punktā minētos riskus un attiecīgās valsts tirgus uzraudzības iestādes nav veikušas efektīvus pasākumus, Komisija veic minētā produkta ar digitāliem elementiem radīto risku izvērtēšanu un var pieprasīt *ENISA* sniegt analīzi, kas palīdzētu izvērtēšanā, un atbilstīgi informē attiecīgās tirgus uzraudzības iestādes. Attiecīgie uzņēmēji pēc vajadzības sadarbojas ar *ENISA*.

8. Pamatojoties uz 7. punktā minēto *ENISA* izvērtējumu, Komisija var noteikt, ka ir nepieciešams korektīvs vai ierobežojošs pasākums Savienības līmenī. Šajā nolūkā tā nekavējoties apspriežas ar attiecīgajām dalībvalstīm un attiecīgo uzņēmēju vai uzņēmējiem.

9. Pamatojoties uz šā panta 8. punktā minēto apspriešanos, Komisija var pieņemt īstenošanas aktus, lai lemtu par korektīviem vai ierobežojošiem pasākumiem Savienības līmenī, tajā skaitā pieprasīt attiecīgā produkta ar digitāliem elementiem izņemšanu no tirgus vai atsaukšanu pienācīgā termiņā, kas ir samērīgs ar risku. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 62. panta 2. punktā.

10. Komisija nekavējoties informē attiecīgo uzņēmēju vai uzņēmējus par 9. punktā minētajiem īstenošanas aktiem. Dalībvalstis nekavējoties īsteno minētos īstenošanas aktus un attiecīgi informē Komisiju.

11. Šā panta 6. līdz 10. punktu piemēro uz laiku, kamēr ir spēkā ārkārtas situācija, kas ir pamatojusi Komisijas intervenci, un tik ilgi, kamēr attiecīgais produkts ar digitāliem elementiem turpina radīt 1. punktā minētos riskus.

58. pants

Formāla neatbilstība

1. Ja dalībvalsts tirgus uzraudzības iestāde konstatē kādu no tālāk norādītajām problēmām, tā pieprasa, lai attiecīgais ražotājs novērš attiecīgo neatbilstību:

a) CE zīme ir uzlikta, pārkāpjot 29. un 30. pantu;

b) CE zīme nav uzlikta;

c) nav sagatavota EK atbilstības deklarācija;

d) ES atbilstības deklarācija ir sagatavota nepareizi;

e) attiecīgā gadījumā nav norādīts tās paziņotās struktūras identifikācijas numurs, kura ir iesaistīta atbilstības novērtēšanas procedūrā;

f) tehniskā dokumentācija nav pieejama vai ir nepilnīga.

2. Ja 1. punktā minētā neatbilstība saglabājas, attiecīgā dalībvalsts veic visus atbilstīgos pasākumus, lai ierobežotu vai aizliegtu produktu ar digitāliem elementiem darīt pieejamu tirgū vai nodrošinātu tās atsaukšanu vai izņemšanu no tirgus.

59. pants

Tirgus uzraudzības iestāžu kopīgās darbības

1. Tirgus uzraudzības iestādes var vienoties ar citām attiecīgajām iestādēm par tādu kopīgu darbību veikšanu, kuru mērķis ir nodrošināt kiberdrošību un patērētāju aizsardzību attiecībā uz konkrētiem produktiem ar digitāliem elementiem, kas tiek laisti tirgū vai darīti pieejami tirgū, jo īpaši produktiem ar digitāliem elementiem, par kuriem bieži konstatēts, ka tie rada kiberdrošības riskus.

2. Komisija vai *ENISA* nolūkā pārbaudīt atbilstību šai regulai ierosina kopīgas darbības, kas jāveic tirgus uzraudzības iestādēm, pamatojoties uz norādēm vai informāciju par to, ka produkti ar digitāliem elementiem, kuri ietilpst šīs regulas darbības jomā, varētu neatbilst šajā regulā noteiktajām prasībām vairākās dalībvalstīs.

3. Tirgus uzraudzības iestādes un attiecīgā gadījumā Komisija nodrošina, ka vienošanās par kopīgu darbību veikšanu nerada negodīgu konkurenci starp uzņēmējiem un nelabvēlīgi neietekmē vienošanās pušu objektivitāti, neatkarību un neitralitāti.

4. Tirgus uzraudzības iestāde var izmantot jebkādu informāciju, kas iegūta kopīgajās darbībās, ko veic kā daļu no attiecīgās izmeklēšanas.

5. Attiecīgā tirgus uzraudzības iestāde un attiecīgā gadījumā Komisija publisko vienošanos par kopīgām darbībām, arī iesaistīto pušu nosaukumus.

60. pants

Kontrolreidi

1. Tirgus uzraudzības iestādes veic vienlaicīgas koordinētas kontroles darbības (“kontrolreidi”) attiecībā uz konkrētiem produktiem ar digitāliem elementiem vai to kategorijām, lai pārbaudītu atbilstību šai regulai vai konstatētu pārkāpumus. Šādi kontrolreidi var ietvert produktu ar digitāliem elementiem pārbaudes, kuru veicēja identitāte netiek izpausta.

2. Izņemot gadījumus, kad iesaistītās tirgus uzraudzības iestādes vienojas citādi, kontrolreidus koordinē Komisija. Kontrolreida koordinators attiecīgā gadījumā publisko apkopotos rezultātus.

3. Ja *ENISA*, veicot savus uzdevumus, tostarp tos, kuru pamatā ir paziņojumi, kas saņemti, ievērojot 14. panta 1. un 3. punktu, identificē produktu ar digitāliem elementiem kategorijas, attiecībā uz kurām var organizēt kontrolreidus, tā priekšlikumu par kontrolreidiem iesniedz šā panta 2. punktā minētajam koordinatoram izskatīšanai tirgus uzraudzības iestādēs.

4. Veicot kontrolreidus, iesaistītās tirgus uzraudzības iestādes var izmantot 52. līdz 58. pantā noteiktās izmeklēšanas pilnvaras un jebkādas citas pilnvaras, kas tām piešķirtas ar valsts tiesību aktiem.

5. Tirgus uzraudzības iestādes var uzaicināt Komisijas amatpersonas un citas pavadošās personas, ko pilnvarojusi Komisija, piedalīties kontrolreidos.

VI nodaļa

Deleģētās pilnvaras un komiteju procedūra

61. pants

Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šajā pantā izklāstītos nosacījumus.

2. Pilnvaras pieņemt 2. panta 5. punkta otrajā daļā, 7. panta 3. punktā, 8. panta 1. un 2. punktā, 13. panta 8. punkta ceturtajā daļā, 14. panta 9. punktā, 25. pantā, 27. panta 9. punktā, 28. panta 5. punktā un 31. panta 5. punktā minētos deleģētos aktus piešķir Komisijai uz piecu gadu laikposmu no ... [šīs regulas spēkā stāšanās diena]. Komisija sagatavo ziņojumu par pilnvaru deleģēšanu vēlākais deviņus mēnešus pirms piecu gadu laikposma beigām. Pilnvaru deleģēšana tiek automātiski pagarināta uz tāda paša ilguma laikposmiem, ja vien Eiropas Parlaments vai Padome neiebilst pret šādu pagarinājumu vēlākais trīs mēnešus pirms katra laikposma beigām.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 2. panta 5. punkta otrajā daļā, 7. panta 3. punktā, 8. panta 1. un 2. punktā, 13. panta 8. punkta ceturtajā daļā, 14. panta 9. punktā, 25. pantā, 27. panta 9. punktā, 28. panta 5. punktā un 31. panta 5. punktā minēto pilnvaru deleģēšanu. Ar lēmumu par atsaukšanu izbeidz tajā norādīto pilnvaru deleģēšanu. Lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* vai vēlākā dienā, kas tajā norādīta. Tas neskar jau spēkā esošos deleģētos aktus.

4. Pirms deleģētā akta pieņemšanas Komisija apspriežas ar katras dalībvalsts ieceltajiem ekspertiem saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu.

5. Tiklīdz Komisija pieņem deleģēto aktu, tā par to paziņo vienlaikus Eiropas Parlamentam un Padomei.

6. Saskaņā ar 2. panta 5. punkta otro daļu, 7. panta 3. punktu, 8. panta 1. un 2. punktu, 13. panta 8. punkta ceturto daļu, 14. panta 9. punktu, 25. pantu, 27. panta 9. punktu, 28. panta 5. punktu un 31. panta 5. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja divos mēnešos no dienas, kad minētais akts paziņots Eiropas Parlamentam un Padomei, ne Eiropas Parlaments, ne Padome nav izteikuši iebildumus vai ja pirms minētā laikposma beigām gan Eiropas Parlaments, gan Padome ir informējuši Komisiju par savu nodomu neizteikt iebildumus. Pēc Eiropas Parlamenta vai Padomes iniciatīvas šo laikposmu pagarina par diviem mēnešiem.

62. pants

Komiteju procedūra

1. Komisijai palīdz komiteja. Minētā komiteja ir komiteja Regulas (ES) Nr. 182/2011 nozīmē.

2. Ja ir atsauce uz šo punktu, piemēro Regulas (ES) Nr. 182/2011 5. pantu.

3. Ja komitejas atzinums jāsaņem rakstiskā procedūrā, minēto procedūru izbeidz, nepanākot rezultātu, ja atzinuma sniegšanas termiņā tā nolemj komitejas priekšsēdētājs vai to pieprasa kāds no komitejas locekļiem.

VII nodaļa
Konfidencialitāte un sankcijas

63. pants

Konfidencialitāte

1. Visas puses, kas ir iesaistītas šīs regulas piemērošanā, ievēro savu uzdevumu un darbību veikšanā iegūtās informāciju un datu konfidencialitāti tādā veidā, lai jo īpaši aizsargātu:

   a) intelektuālā īpašuma tiesības un fiziskas vai juridiskas personas konfidenciālu uzņēmējdarbības informāciju vai komercnoslēpumus, ieskaitot pirmkodu, izņemot gadījumus, kas minēti Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/943[36] 5. pantā;

   b) šīs regulas efektīvu īstenošanu, jo īpaši pārbaužu, izmeklēšanas vai revīzijas nolūkos;

   c) sabiedrības un valsts drošības intereses;

   d) kriminālprocesu vai administratīvo procesu neaizskaramību.

[36] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/943 (2016. gada 8. jūnijs) par zinātības un darījumdarbības neizpaužamas informācijas (komercnoslēpumu) aizsardzību pret nelikumīgu iegūšanu, izmantošanu un izpaušanu (OV L 157, 15.6.2016., 1. lpp.).

2. Neskarot 1. punktu, informācija, ar ko konfidenciāli savā starpā apmainās tirgus uzraudzības iestādes, kā arī tirgus uzraudzības iestādes un Komisija, netiek izpausta bez iepriekšējas vienošanās ar informācijas izcelsmes tirgus uzraudzības iestādi.

3. Šā panta 1. un 2. punkts neskar Komisijas, dalībvalstu un paziņoto struktūru tiesības un pienākumus attiecībā uz informācijas apmaiņu un brīdinājumu izplatīšanu, ne arī attiecīgo personu pienākumus sniegt informāciju saskaņā ar dalībvalstu krimināltiesībām.

4. Vajadzības gadījumā Komisija un dalībvalstis var apmainīties ar sensitīvu informāciju ar attiecīgajām trešo valstu iestādēm, ar kurām tās ir noslēgušas divpusējus vai daudzpusējus konfidencialitātes nolīgumus, kas garantē pietiekamu konfidencialitātes līmeni.

64. pants

Sodi

1. Dalībvalstis paredz noteikumus par sodiem, ko piemēro par šīs regulas pārkāpumiem, un veic visus vajadzīgos pasākumus, lai nodrošinātu to īstenošanu. Paredzētie sodi ir efektīvi, samērīgi un atturoši. Dalībvalstis attiecīgos noteikumus un pasākumus nekavējoties dara zināmus Komisijai un nekavējoties paziņo tai par jebkādiem turpmākiem grozījumiem, kas tos ietekmē.

2. Par neatbilstību I pielikumā noteiktajām kiberdrošības pamatprasībām un 13. un 14. pantā noteiktajiem pienākumiem piemēro administratīvos naudas sodus līdz 15 000 000 EUR vai, ja pārkāpējs ir uzņēmums, līdz 2,5 % no tā kopējā globālā apgrozījuma iepriekšējā finanšu gadā, atkarībā no tā, kura no šīm summām ir lielāka.

3. Par 18. līdz 23. pantā, 28. pantā, 30. panta 1. līdz 4. punktā, 31. panta 1. līdz 4. punktā, 32. panta 1., 2. un 3. punktā, 33. panta 5. punktā un 39., 41., 47., 49. un 53. pantā noteikto pienākumu neizpildi piemēro administratīvos naudas sodus līdz 10 000 000 EUR vai, ja pārkāpējs ir uzņēmums, līdz 2 % no tā kopējā globālā apgrozījuma iepriekšējā finanšu gadā, atkarībā no tā, kura no šīm summām ir lielāka.

4. Par nepareizas, nepilnīgas vai maldinošas informācijas sniegšanu paziņotajām struktūrām un tirgus uzraudzības iestādēm atbildē uz pieprasījumu piemēro administratīvos naudas sodus līdz 5 000 000 EUR vai, ja pārkāpējs ir uzņēmums, līdz 1 % no tā kopējā globālā apgrozījuma iepriekšējā finanšu gadā, atkarībā no tā, kura no šīm summām ir lielāka.

5. Lemjot par administratīvā naudas soda apmēru, katrā atsevišķā gadījumā ņem vērā visus īpašos konkrētās situācijas apstākļus un rūpīgi izvērtē šādus elementus:

   a) pārkāpuma un tā seku raksturu, smagumu un ilgumu;

   b) to, vai tās pašas vai citas tirgus uzraudzības iestādes jau ir piemērojušas administratīvos naudas sodus tam pašam uzņēmējam par līdzīgu pārkāpumu;

   c) uzņēmēja, jo īpaši attiecībā uz mikrouzņēmumiem, maziem un vidējiem uzņēmumiem, tostarp jaunuzņēmumiem, kurš veicis pārkāpumu, lielumu un tirgus daļu.

6. Tirgus uzraudzības iestādes, kas piemēro administratīvos naudas sodus, sniedz informāciju par piemērotajiem sodiem citu dalībvalstu tirgus uzraudzības iestādēm, izmantojot Regulas (ES) 2019/1020 34. pantā minēto informācijas un saziņas sistēmu.

7. Katra dalībvalsts pieņem noteikumus par to, vai šīs dalībvalsts publiskā sektora iestādēm un publiskā sektora struktūrām var uzlikt administratīvos naudas sodus un cik lielā apmērā.

8. Atkarībā no dalībvalstu tiesību sistēmas noteikumus par administratīvajiem naudas sodiem var piemērot tādā veidā, ka naudas sodus uzliek kompetentās valsts tiesas vai citas struktūras saskaņā ar kompetenci, kas šajās dalībvalstīs noteikta valsts līmenī. Šādu noteikumu piemērošanai šajās dalībvalstīs ir līdzvērtīga ietekme.

9. Administratīvos naudas sodus atkarībā no katra atsevišķā gadījuma apstākļiem var uzlikt papildus jebkādiem citiem korektīviem vai ierobežojošiem pasākumiem, kurus tirgus uzraudzības iestādes piemēro attiecībā uz to pašu pārkāpumu.

10. Atkāpjoties no 3. līdz 9. punkta, minētajos punktos norādītos administratīvos naudas sodus nepiemēro:

a) attiecībā uz 14. panta 2. punkta a) apakšpunktā vai 14. panta 4. punkta a) apakšpunktā minētā termiņa neievērošanu – ražotājiem, kuri ir mikrouzņēmumi vai mazie uzņēmumi;

b) par jebkuru šīs regulas pārkāpumu, ko izdarījis atvērtā pirmkoda programmatūras pārzinis.

65. pants

Pārstāvības prasības

Direktīvu (ES) 2020/1828 piemēro pārstāvības prasībām, kuras celtas par uzņēmēju izdarītiem šīs regulas noteikumu pārkāpumiem, kas kaitē vai var kaitēt patērētāju kolektīvajām interesēm.

VIII nodaļa

Pārejas un nobeiguma noteikumi

66. pants

Grozījums Regulā (ES) 2019/1020

Regulas (ES) 2019/1020 I pielikumā pievieno šādu punktu:

"XX[+]. Eiropas Parlamenta un Padomes Regula (ES) 2024/...[*++].

---

* Eiropas Parlamenta un Padomes Regula (ES) 2024/... (... gada ...) par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulu (ES) Nr. 168/2013, Regulu (ES) 2019/1020 un Direktīvu (ES) 2020/1828 (Kibernoturības akts) ... (OV ..., ELI: ...).".

[+] OV: lūgums ievietot tekstā nākamo kārtas numuru Regulas (ES) 2019/1020 I pielikumā iekļautajā sarakstā.

[++] OV: lūgums ievietot dokumentā PE-CONS 100/23 (2022/0272(COD)) ietvertās regulas numuru un zemsvītras piezīmē ievietot minētās regulas numuru, datumu un OV atsauci.

67. pants

Grozījums Direktīvā (ES) 2020/1828

Direktīvas (ES) 2020/1828 I pielikumā pievieno šādu punktu:

"(XX[+]) Eiropas Parlamenta un Padomes Regula (ES) 2024/...[*++]."

---

[*] Eiropas Parlamenta un Padomes Regula (ES) 2024/... (... gada ...) par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulu (ES) Nr. 168/2013, Regulu (ES) 2019/1020 un Direktīvu (ES) 2020/1828 (Kibernoturības akts) ... (OV ..., ELI: ...).".

[+] OV: Lūgums ievietot tekstā nākamo kārtas numuru Regulas (ES) 2020/1828 I pielikumā iekļautajā sarakstā.

[++] OV: ievietot dokumentā PE-CONS 100/23 (2022/0272(COD)) ietvertās regulas numuru un zemsvītras piezīmē ievietot minētās regulas numuru, datumu un OV atsauci.

68. pants

Grozījums Regulā (ES) Nr. 168/2013

Eiropas Parlamenta un Padomes Regulas (ES) Nr. 168/2013[37] II pielikumu groza šādi:

tabulas C1 sadaļā iekļauj šādu ierakstu:

“

XX+	18	Transportlīdzekļa aizsardzība pret kiberuzbrukumiem		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

”.

---

37 Eiropas Parlamenta un Padomes Regula (ES) Nr. 168/2013 (2013. gada 15. janvāris) par divu riteņu vai trīs riteņu transportlīdzekļu un kvadriciklu apstiprināšanu un tirgus uzraudzību (OV L 60, 2.3.2013., 52. lpp.).

\+ OV: Lūgums ievietot tekstā nākamo kārtas numuru Regulas (ES) 168/2013 I pielikuma C1 sadaļā iekļautajā sarakstā.

69. pants

Pārejas noteikumi

1. ES tipa pārbaudes sertifikāti un apstiprinājuma lēmumi, kas izdoti attiecībā uz kiberdrošības prasībām par produktiem ar digitāliem elementiem, uz kuriem attiecas Savienības saskaņošanas tiesību akti, kas nav šī regula, paliek spēkā līdz ... [42 mēneši no šīs regulas spēkā stāšanās dienas], ja vien to derīguma termiņš nav beidzies pirms minētās dienas vai ja šādos citos Savienības saskaņošanas tiesību aktos nav noteikts citādi, un tādā gadījumā tie paliek spēkā termiņā, kas norādīts minētajos Savienības tiesību aktos.

2. Uz produktiem ar digitāliem elementiem, kas laisti tirgū pirms [36 mēneši no šīs regulas spēkā stāšanās dienas], šīs regulas prasības attiecas tikai tad, ja no minētās dienas šajos produktos notikušas būtiskas modifikācijas.

3. Atkāpjoties no šā panta 2. punkta, pienākumus, kas noteikti 14. pantā, piemēro visiem šīs regulas darbības jomā ietilpstošajiem produktiem ar digitāliem elementiem, kuri laisti tirgū pirms ... [36 mēneši no šīs regulas spēkā stāšanās dienas].

70. pants

Izvērtēšana un pārskatīšana

1. Līdz ... [72 mēneši no šīs regulas piemērošanas dienas] un pēc tam ik pēc četriem gadiem Komisija iesniedz Eiropas Parlamentam un Padomei ziņojumu par šīs regulas izvērtēšanu un pārskatīšanu. Minētos ziņojumus publisko.

2. Līdz ... [45 mēneši no šīs regulas spēkā stāšanās dienas] Komisija pēc apspriešanās ar *ENISA* un *CSIRT* tīklu iesniedz Eiropas Parlamentam un Padomei ziņojumu, kurā izvērtē 16. pantā izklāstītās vienotās ziņošanas platformas efektivitāti, kā arī 16. pantā minēto ar kiberdrošību saistīto iemeslu piemērošanas ietekmi uz vienotās ziņošanas platformas efektivitāti attiecībā uz saņemto paziņojumu savlaicīgu izplatīšanu citām attiecīgajām *CSIRT*.

71. pants

Stāšanās spēkā un piemērošana

1. Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

2. Šo regulu piemēro no ... [36 mēneši no šīs regulas spēkā stāšanās dienas].

   Tomēr 14. pantu piemēro no ... [21 mēnesis no šīs regulas spēkā stāšanās dienas] un IV nodaļu (35. līdz 51. pants) piemēro no ... [18 mēneši no šīs regulas spēkā stāšanās dienas].

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

...,

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētāja	*priekšsēdētājs / priekšsēdētāja*

I PIELIKUMS

KIBERDROŠĪBAS PAMATPRASĪBAS

I daļa Kiberdrošības prasības, kas attiecas uz produktu ar digitāliem elementiem raksturlielumiem

1) Produktus ar digitāliem elementiem projektē, izstrādā un ražo tā, lai tie nodrošinātu atbilstošu kiberdrošības līmeni, pamatojoties uz riskiem.

2) Pamatojoties uz 13. panta 2. punktā minēto kiberdrošības riska novērtējumu, un attiecīgā gadījumā produkti ar digitāliem elementiem:

   a) tiek darīti pieejami tirgū bez zināmām izmantojamām ievainojamībām;

   b) tiek darīti pieejami tirgū ar drošu pēc noklusējuma konfigurāciju, ja vien attiecībā uz individuāli pielāgotu produktu ar digitāliem elementiem ražotājs un komerciālais lietotājs nav vienojušies citādi, ieskaitot iespēju atiestatīt produktu tā sākotnējā stāvoklī;

   c) nodrošina, ka ievainojamības var novērst ar drošības atjauninājumiem, tostarp attiecīgā gadījumā izmantot atbilstīgā termiņā iestatītus un pēc noklusējuma iespējotus automātiskus drošības atjauninājumus ar viegli lietojamu atteikšanās mehānismu, un lietotājiem sniedz paziņojumus par pieejamajiem atjauninājumiem, ko uz laiku var atlikt;

d) nodrošina aizsardzību pret nesankcionētu piekļuvi, izmantojot atbilstošus kontroles mehānismus, tajā skaitā, bet ne tikai, autentifikācijas, identitātes vai piekļuves pārvaldības sistēmas, un ziņo par iespējamu nesankcionētu piekļuvi;

e) aizsargā uzglabāto, pārsūtīto vai citādi apstrādāto personas vai citu datu konfidencialitāti, piemēram, šifrējot attiecīgos datus miera stāvoklī vai tranzītā, izmantojot mūsdienīgus mehānismus un citus tehniskos līdzekļus;

f) aizsargā uzkrāto, pārsūtīto vai citādi apstrādāto personas vai citu datu, komandu, programmu un konfigurācijas integritāti pret jebkādām manipulācijām vai modifikācijām, kuras nav atļāvis lietotājs, un ziņo par bojājumiem;

g) apstrādā tikai tādus personas vai citus datus, kas ir atbilstīgi, būtiski un ierobežoti līdz tam, kas nepieciešams produkta ar digitāliem elementiem paredzētajam nolūkam ("datu minimizēšana");

h) aizsargā būtisku un pamata funkciju pieejamību, tostarp pēc incidenta, arī izmantojot pasākumus, ar ko nodrošina noturību pret pakalpojuma atteikuma uzbrukumiem un mazina to ietekmi;

i) samazina pašu produktu vai savienoto ierīču negatīvo ietekmi uz citu ierīču vai tīklu sniegto pakalpojumu pieejamību;

j) ir projektēti, izstrādāti un ražoti tā, lai ierobežotu uzbrukuma laukumus, ieskaitot ārējās saskarnes;

k) ir projektēti, izstrādāti un ražoti tā, lai samazinātu incidenta ietekmi, izmantojot atbilstošus izmantošanas ietekmes mazināšanas mehānismus un paņēmienus;

l) nodrošina ar drošību saistītu informāciju, reģistrējot un uzraugot attiecīgo iekšējo darbību, tostarp piekļuvi datiem, pakalpojumiem vai funkcijām vai to modificēšanu, un nodrošina lietotājam viegli lietojamu atteikšanās mehānismu;

m) nodrošina lietotājiem iespēju droši un viegli dzēst visus datus un iestatījumus un, ja šādus datus var pārsūtīt uz citiem produktiem vai sistēmām, nodrošina, ka to var izdarīt drošā veidā.

II daļa Ievainojamību novēršanas prasības

Produktu ar digitāliem elementiem ražotāji:

1) identificē un dokumentē produkta ar digitāliem elementiem ievainojamības un komponentus, arī sastādot programmatūras materiālu komplektu plaši izmantotā un mašīnlasāmā formātā, kas aptver vismaz produkta augstākā līmeņa atkarības;

2) saistībā ar riskiem, kam pakļauti produkti ar digitāliem elementiem, nekavējoties pievēršas ievainojamībām un tās novērš, arī nodrošinot drošības atjauninājumus; ja vien tehniski iespējams, jaunus drošības atjauninājumus nodrošina atsevišķi no funkcionalitātes atjauninājumiem;

3) veic efektīvas un regulāras produkta ar digitāliem elementiem drošības pārbaudes un pārskatus;

4) kad drošības atjauninājums ir darīts pieejams, publiski atklāj un apmainās ar informāciju par novērstajām ievainojamībām, ieskaitot ievainojamību aprakstu, informāciju, kas lietotājiem ļauj identificēt produktu ar ietekmētajiem digitāliem elementiem, ievainojamību ietekmi, to nopietnību, un skaidru un pieejamu informāciju, kas palīdz lietotājiem novērst ievainojamības; pienācīgi pamatotos gadījumos, ja ražotāji uzskata, ka publicēšanas radītie drošības riski pārsniedz drošības ieguvumus, ražotāji var atlikt informācijas par novērstās ievainojamības publiskošanu līdz brīdim, kad lietotājiem ir dota iespēja piemērot attiecīgo ielāpu;

5) ievieš un īsteno politiku par koordinētu informācijas par ievainojamībām izpaušanu;

6) veic pasākumus, lai veicinātu informācijas apmaiņu par iespējamām sava produkta ar digitāliem elementiem ievainojamībām, kā arī trešo personu komponentiem, kas iekļauti attiecīgajā produktā, arī norādot kontaktadresi ziņošanai par ievainojamībām, kas atklātas produktā ar digitāliem elementiem;

7) nodrošina mehānismus, ar ko droši izplatīt produktu ar digitāliem elementiem atjauninājumus, lai nodrošinātu, ka ievainojamības tiek savlaicīgi novērstas vai mazinātas, un attiecīgā gadījumā nodrošina automātiskus drošības atjauninājumus;

8) nodrošina, ka gadījumos, kad ir pieejami drošības atjauninājumi, tie tiek nekavējoties un, ja vien saistībā ar attiecīgo individuāli pielāgoto produktu ar digitāliem elementiem ražotājs un komerciālais lietotājs nav vienojušies citādi, bez maksas izplatīti kopā ar ieteikuma ziņojumiem, kuros lietotājiem sniegta atbilstoša informācija, ieskaitot informāciju par iespējamām veicamām darbībām.

II PIELIKUMS

INFORMĀCIJA UN NORĀDĪJUMI LIETOTĀJIEM

Produktam ar digitāliem elementiem jāpievieno vismaz:

1. ražotāja nosaukums, reģistrētais tirdzniecības nosaukums vai reģistrētā preču zīme, e-pasta adrese vai cita digitāla kontaktinformācija, kā arī attiecīgā gadījumā tīmekļa vietne, kurā sazināties ar ražotāju;

2. vienotais kontaktpunkts, kur var ziņot par produkta ar digitāliem elementiem kiberdrošības ievainojamībām, un vietne, kur atrast ražotāja politiku par koordinētu informācijas par ievainojamībām izpaušanu;

3. nosaukums, tips un jebkāda papildu informācija, kas ļauj unikāli identificēt produktu ar digitāliem elementiem;

4. paredzētais produkta ar digitāliem elementiem nolūks, tai skaitā ražotāja nodrošinātā drošības vide, kā arī produkta ar digitāliem elementiem būtiskā funkcionalitāte un informācija par drošības īpašībām;

5. visi zināmie vai paredzamie apstākļi, kas saistīti ar produkta ar digitāliem elementiem izmantošanu atbilstoši tā paredzētajam nolūkam vai citos pamatoti paredzama nepareiza lietojuma apstākļos, kas var radīt būtiskus kiberdrošības riskus;

6. attiecīgā gadījumā interneta adrese, kurā var piekļūt ES atbilstības deklarācijai;

7. ražotāja piedāvātā drošības tehniskā atbalsta veids, norādot atbalsta perioda galīgo termiņu, līdz kuram lietotāji var sagaidīt, ka ievainojamības tiks novērstas un tiks saņemti drošības atjauninājumi;

8. sīki izklāstīti norādījumi vai interneta adrese, kurā sniegta atsauce uz šādiem sīki izklāstītiem norādījumiem un informācija par:

   a) pasākumiem, kas jāveic, īstenojot sākotnējo nodošanu ekspluatācijā, un visā produkta ar digitāliem elementiem lietošanas laikā, lai nodrošinātu tā drošu lietošanu;

   b) to, kā produkta ar digitāliem elementiem izmaiņas var ietekmēt datu drošību;

   c) to, kā var instalēt ar drošību saistītus atjauninājumus;

   d) drošu produkta ar digitāliem elementiem ekspluatācijas pārtraukšanu, ieskaitot informāciju par to, kā var droši dzēst lietotāja datus;

   e) to, kā atiestatīt pēc noklusējuma instalēto iestatījumu, kas ļauj automātiski instalēt drošības atjauninājumus, kā prasīts I pielikuma I daļas 2. punkta c) apakšpunktā;

   f) ja produktu ar digitāliem elementiem paredzēts integrēt citos produktos ar digitāliem elementiem – informāciju, kas integrētājam nepieciešama, lai izpildītu I pielikumā izklāstītās kiberdrošības pamatprasības un VII pielikumā izklāstītās dokumentācijas prasības.

9. Ja ražotājs nolemj lietotājam darīt pieejamu programmatūras materiālu sarakstu, sniedz informāciju par to, kur var piekļūt programmatūras materiālu sarakstam.

III PIELIKUMS

NOZĪMĪGI PRODUKTI AR DIGITĀLIEM ELEMENTIEM

I klase

1. Identitātes pārvaldības sistēmas un privileģētas piekļuves pārvaldības programmatūra un aparatūra, arī autentifikācijas un piekļuves kontroles lasītāji, tostarp biometriskie lasītāji

2. Atsevišķas un iegultas pārlūkprogrammas

3. Paroļu pārvaldnieki

4. Programmatūra, kas meklē, dzēš vai ievieto karantīnā ļaunprogrammatūru

5. Produkti ar digitāliem elementiem ar virtuālā privātā tīkla (*VPN*) funkciju

6. Tīkla pārvaldības sistēmas

7. Drošības informācijas un notikumu pārvaldības (*SIEM*) sistēmas

8. Palaišanas pārvaldnieki

9. Publiskās atslēgas infrastruktūra un digitālo sertifikātu izsniegšanas programmatūra

10. Fiziskā un virtuālā tīkla saskarnes

11. Operētājsistēmas

12. Maršrutētāji, modemi, kas paredzēti savienojumam ar internetu, un slēdži

13. Mikroprocesori ar funkcijām, kas saistītas ar drošību

14. Mikrokontrolleri ar funkcijām, kas saistītas ar drošību

15. Lietojumam pielāgotas integrētās shēmas (*ASIC*) un lauka programmējamās ventiļu matricas (*FPGA*) ar funkcijām, kas saistītas ar drošību

16. Vispārēja lietojuma viedmāju virtuālie asistenti

17. Viedmāju produkti ar drošības funkcijām, tostarp vieddurvju slēdzenes, videonovērošanas kameras, bērnu uzraudzības sistēmas un signalizācijas sistēmas

18. Internetam pieslēgtas rotaļlietas, uz kurām attiecas Eiropas Parlamenta un Padomes Direktīva 2009/48/EK[1] un kurām ir interaktīvas sociālas funkcijas (piemēram, runas vai filmēšanas funkcijas) vai kurām ir atrašanās vietas izsekošanas funkcijas

19. Izstrādājumi personiskai valkāšanai, kurus paredzēts valkāt vai nēsāt uz cilvēka ķermeņa, kuri veic veselības monitorēšanas (piemēram, datu reģistratora) funkciju un uz kuriem neattiecas Regula (ES) 2017/745 vai Regula (ES) 2017/746, vai izstrādājumi personiskai valkāšanai, kuri paredzēti bērniem un kurus lieto bērni.

II klase

1. Virtuālo mašīnu pārraugi un konteineru izpildlaika sistēmas, kas atbalsta operētājsistēmu un līdzīgas vides virtualizētu izpildi;

2. Ugunsmūri, ielaušanās atklāšanas un novēršanas sistēmas;

3. Pret iejaukšanos droši mikroprocesori;

4. Pret iejaukšanos droši mikrokontrolleri.

---

[1] Eiropas Parlamenta un Padomes Direktīva 2009/48/EK (2009. gada 18. jūnijs) par rotaļlietu drošumu (OV L 170, 30.6.2009., 1. lpp.).

IV PIELIKUMS

KRITISKI SVARĪGI PRODUKTI AR DIGITĀLIEM ELEMENTIEM

1. Aparatūras ierīces ar drošības blokiem

2. Viedās skaitītāju vārtejas, kas ir daļa no viedām uzskaites sistēmām, kas definētas Eiropas Parlamenta un Padomes Direktīvas (ES) 2019/944[1] 2. panta 23. punktā, un citas ierīces augstas drošības nolūkiem, tostarp drošai kriptoapstrādei

3. Viedkartes vai līdzīgas ierīces, ieskaitot to drošības elementus

---

[1] Eiropas Parlamenta un Padomes Direktīva (ES) 2019/944 (2019. gada 5. jūnijs) par kopīgiem noteikumiem attiecībā uz elektroenerģijas iekšējo tirgu un ar ko groza Direktīvu 2012/27/ES (OV L 158, 14.6.2019., 125. lpp.).

V PIELIKUMS

ES ATBILSTĪBAS DEKLARĀCIJA

ES atbilstības deklarācijā, kas minēta 28. pantā, ietilpst šāda informācija:

1. Nosaukums un tips, kā arī jebkāda papildu informācija, kas ļauj unikāli identificēt produktu ar digitāliem elementiem

2. Ražotāja vai tā pilnvarotā pārstāvja vārds vai nosaukums un adrese

3. Paziņojums par to, ka šo atbilstības deklarāciju izdod tikai un vienīgi uz ražotāja atbildību

4. Deklarācijas priekšmets (produkta ar digitāliem elementiem identifikācija, kas nodrošina tā izsekojamību. Attiecīgā gadījumā var būt iekļauta fotogrāfija)

5. Paziņojums, ka iepriekš aprakstītais deklarācijas priekšmets atbilst attiecīgajam Savienības saskaņošanas tiesību aktam

6. Norādes uz attiecīgajiem piemērojamajiem saskaņotajiem standartiem, citām kopējām specifikācijām vai kiberdrošības sertifikāciju, attiecībā uz ko tiek deklarēta atbilstība

7. Attiecīgā gadījumā paziņotās struktūras nosaukums un numurs, veiktās atbilstības novērtēšanas procedūras apraksts un izdotā sertifikāta identifikācija

8. Papildu informācija:

Parakstīts šādas personas vārdā: .....

(izdošanas vieta un datums):

(vārds, uzvārds, amats) (paraksts):

VI PIELIKUMS

VIENKĀRŠOTĀ ES ATBILSTĪBAS DEKLARĀCIJA

Vienkāršoto ES atbilstības deklarāciju, kas minēta 13. panta 20. punktā, sniedz šādi:

Ar šo [ražotāja nosaukums] apliecina, ka produkta ar digitāliem elementiem tips [produkta ar digitāliem elementiem tipa nosaukums] atbilst Eiropas Parlamenta un Padomes Regulai (ES) .../...[1].

Pilns ES atbilstības deklarācijas teksts ir pieejams šādā interneta vietnē:

---

[1] OV: tekstā ievietot dokumentā PE-CONS Nr./GG (2022/0272(COD)) ietvertās regulas numuru.

VII PIELIKUMS

TEHNISKĀS DOKUMENTĀCIJAS SATURS

Tehniskajā dokumentācijā, kas minēta 31. pantā, norāda vismaz tālāk uzskaitīto informāciju, ja tā ir attiecināma uz konkrēto produktu ar digitāliem elementiem:

1. vispārīgu produkta ar digitāliem elementiem aprakstu, ieskaitot:

   a) tam paredzēto nolūku;

   b) programmatūras versijas, kas ietekmē atbilstību kiberdrošības pamatprasībām;

   c) ja produkts ar digitāliem elementiem ir aparatūras produkts, fotogrāfijas vai ilustrācijas, kas ilustrē ārējās funkcijas, marķējumu un iekšējo izkārtojumu;

   d) informāciju un norādījumus, kā noteikts II pielikumā;

2. produkta ar digitāliem elementiem projektēšanas, izstrādes un ražošanas, kā arī ievainojamību novēršanas procesu aprakstu, ieskaitot:

   a) nepieciešamo informāciju par produkta ar digitāliem elementiem projektēšanu un izstrādi, attiecīgā gadījumā arī rasējumus un shēmas un/vai sistēmas arhitektūras aprakstu, kurā paskaidrots, kā programmatūras komponenti balstās viens uz otru vai papildina viens otru un ir integrēti kopējā apstrādē;

b) nepieciešamo informāciju un specifikācijas par ražotāja ieviestajiem ievainojamību novēršanas procesiem, ieskaitot programmatūras materiālu sarakstu, politiku par koordinētu informācijas par ievainojamībām izpaušanu, pierādījumus par kontaktadreses norādīšanu ziņošanai par ievainojamībām un drošai atjauninājumu izplatīšanai izvēlēto tehnisko risinājumu aprakstu;

c) nepieciešamo informāciju par produkta ar digitāliem elementiem ražošanas un uzraudzības procesiem, šo procesu specifikācijām un validāciju;

3. novērtējumu par kiberdrošības riskiem, pret kuriem produkts ar digitāliem elementiem ir projektēts, izstrādāts, ražots, piegādāts un uzturēts, ievērojot 13. pantu, tostarp par to, kā ir piemērojamas I pielikuma I daļā izklāstītās kiberdrošības pamatprasības;

4. attiecīgā informācija, kas ņemta vērā, lai produktam ar digitāliem elementiem noteiktu atbalsta periodu, ievērojot 13. panta 8. punktu;

5. to pilnībā vai daļēji piemēroto saskaņoto standartu sarakstu, uz kuriem ir publicētas atsauces *Eiropas Savienības Oficiālajā Vēstnesī*, kopējās specifikācijas, kas paredzētas šīs regulas 27. pantā vai Eiropas kiberdrošības sertifikācijas shēmās, kuras pieņemtas, ievērojot Regulu (ES) 2019/881 un atbilstīgi šīs regulas 27. panta 8. punktam, un, ja minētie saskaņotie standarti, kopējās specifikācijas vai Eiropas kiberdrošības sertifikācijas shēmas nav piemērotas, to risinājumu aprakstus, kas pieņemti, lai atbilstu I pielikuma I un II daļā izklāstītajām kiberdrošības pamatprasībām, ietverot citu attiecīgo piemēroto tehnisko specifikāciju sarakstu. Ja saskaņotie standarti, kopējās specifikācijas vai Eiropas kiberdrošības sertifikācijas shēmas ir piemērotas daļēji, tehniskajā dokumentācijā norāda piemērotās daļas;

6. ziņojumus par testiem, kas veikti, lai pārbaudītu produkta ar digitāliem elementiem atbilstību un ievainojamību novēršanas procesu atbilstību piemērojamajām kiberdrošības pamatprasībām, kā noteikts I pielikuma I un II daļā;

7. ES atbilstības deklarācijas kopiju;

8. attiecīgā gadījumā programmatūras materiālu sarakstu pēc tirgus uzraudzības iestādes pamatota pieprasījuma, ja tas ir nepieciešams, lai šī iestāde varētu pārbaudīt atbilstību I pielikumā noteiktajām kiberdrošības pamatprasībām.

VIII PIELIKUMS

ATBILSTĪBAS NOVĒRTĒŠANAS PROCEDŪRAS

I daļa Atbilstības novērtēšanas procedūra, kas balstās uz iekšējo kontroli (pamatojoties uz A moduli)

1. Iekšējā kontrole ir atbilstības novērtēšanas procedūra, ar kuru ražotājs izpilda šīs daļas 2., 3. un 4. punktā noteiktos pienākumus un nodrošina un paziņo uz savu atbildību, ka attiecīgie produkti ar digitāliem elementiem atbilst visām I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām un ka ražotājs atbilst I pielikuma II daļā noteiktajām kiberdrošības pamatprasībām.

2. Ražotājs sagatavo VII pielikumā aprakstīto tehnisko dokumentāciju.

3. Produktu ar digitāliem elementiem projektēšana, izstrāde, ražošana un ievainojamību novēršana

Ražotājs veic visus vajadzīgos pasākumus, lai projektēšanas, izstrādes, ražošanas un ievainojamību novēršanas procesi un to uzraudzība nodrošinātu izgatavoto vai izstrādāto produktu ar digitāliem elementiem un ražotāja ieviesto procesu atbilstību I pielikuma I un II daļā noteiktajām kiberdrošības pamatprasībām.

4. Atbilstības zīme un atbilstības deklarācija

4.1. Ražotājs uzliek CE zīmi katram atsevišķam produktam ar digitāliem elementiem, kurš atbilst piemērojamajām prasībām, kas noteiktas šajā regulā.

4.2. Ražotājs saskaņā ar 28. pantu sagatavo katram produktam ar digitāliem elementiem ES atbilstības deklarāciju un to glabā kopā ar tehnisko dokumentāciju, lai tā būtu valsts iestāžu rīcībā 10 gadus pēc produkta ar digitāliem elementiem laišanas tirgū vai atbalsta periodā (atkarībā no tā, kurš termiņš ir ilgāks). ES atbilstības deklarācijā identificē produktu ar digitāliem elementiem, kam šī deklarācija ir sagatavota. ES atbilstības deklarācijas kopija pēc pieprasījuma ir pieejama visām attiecīgajām iestādēm.

5. Pilnvarotie pārstāvji

Ražotāja pienākumus, kas noteikti 4. punktā, tā uzdevumā un uz tā atbildību drīkst pildīt tā pilnvarotais pārstāvis ar noteikumu, ka attiecīgie pienākumi ir precizēti pilnvarojumā.

II daļa ES tipa pārbaude (pamatojoties uz B moduli)

1. ES tipa pārbaude ir atbilstības novērtēšanas procedūras daļa, kurā paziņotā struktūra pārbauda produkta ar digitāliem elementiem tehnisko projektu un izstrādi, kā arī ražotāja ieviestos ievainojamību novēršanas procesus un apliecina, ka produkts ar digitāliem elementiem atbilst I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām un ka ražotājs atbilst I pielikuma II daļā noteiktajām kiberdrošības pamatprasībām.

2. ES tipa pārbaudi veic ar produkta ar digitāliem elementiem tehniskā projekta un izstrādes atbilstības novērtējumu, pārbaudot 3. punktā minēto tehnisko dokumentāciju un apstiprinošos pierādījumus, kā arī pārbaudot produkta vienas vai vairāku būtisku daļu paraugus (ražošanas tipa un projekta tipa kombinācija).

3. Ražotājs iesniedz ES tipa pārbaudes pieteikumu vienai paziņotajai struktūrai pēc savas izvēles.

   Pieteikumā iekļauj:

   3.1. ražotāja nosaukumu un adresi, kā arī, ja pieteikumu iesniedz ražotāja pilnvarotais pārstāvis, – tā vārdu vai nosaukumu un adresi;

3.2. rakstisku paziņojumu, ka šāds pieteikums nav iesniegts nevienā citā paziņotajā struktūrā;

3.3. tehnisko dokumentāciju, kura ļauj novērtēt produkta ar digitāliem elementiem atbilstību piemērojamajām I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām un I pielikuma II daļā noteiktajiem ražotāja ievainojamību novēršanas procesiem, un ietver atbilstošu analīzi un risku novērtējumu. Tehniskajā dokumentācijā norāda piemērojamās prasības, un, ciktāl tas nepieciešams novērtēšanai, tā aptver produkta ar digitāliem elementiem projektēšanu, ražošanu un darbību. Tehniskajā dokumentācijā attiecīgā gadījumā iekļauj vismaz VII pielikumā izklāstītos elementus;

3.4. pierādījumus, kas apstiprina tehniskā projekta, izstrādes risinājumu un ievainojamību novēršanas procesu atbilstību. Šajos pierādījumos norāda visus izmantotos dokumentus, jo īpaši tad, ja attiecīgie harmonizētie standarti vai tehniskās specifikācijas netiek piemēroti pilnībā. Pierādījumos vajadzības gadījumā iekļauj to testu rezultātus, kurus ražotāja vārdā un uz ražotāja atbildību veikusi ražotāja atbilstīgā laboratorija vai cita testēšanas laboratorija.

4. Paziņotā struktūra:

4.1. pārbauda tehnisko dokumentāciju un apstiprinošos pierādījumus, lai novērtētu produkta ar digitāliem elementiem tehniskā projekta un izstrādes atbilstību I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām un ražotāja ieviesto ievainojamību novēršanas procesu atbilstību I pielikuma II daļā noteiktajām kiberdrošības pamatprasībām;

4.2. verificē, ka paraugi ir izstrādāti vai ražoti atbilstīgi minētajai tehniskajai dokumentācijai, un noskaidro, kuri elementi ir projektēti saskaņā ar atbilstīgo harmonizēto standartu un/vai tehnisko specifikāciju piemērojamajiem noteikumiem, kā arī to, kuri elementi ir projektēti un izstrādāti, nepiemērojot šo standartu attiecīgos noteikumus;

4.3. veic atbilstīgas pārbaudes un testus vai nodrošina to veikšanu, lai pārbaudītu, vai gadījumos, kad ražotājs izvēlējies piemērot attiecīgajos saskaņotajos standartos vai tehniskajās specifikācijās paredzētos risinājumus attiecībā uz prasībām, kas noteiktas I pielikumā, tie piemēroti pareizi;

4.4. veic atbilstīgas pārbaudes un testus vai nodrošina to veikšanu, lai pārbaudītu, vai gadījumos, kad nav piemēroti attiecīgie saskaņotajos standartos vai tehniskajās specifikācijās paredzētie risinājumi attiecībā uz prasībām, kas noteiktas I pielikumā, ražotāja īstenotie risinājumi atbilst attiecīgajām kiberdrošības pamatprasībām;

4.5. vienojas ar ražotāju par vietu, kur tiks veiktas šīs pārbaudes un testi.

5. Paziņotā struktūra sagatavo izvērtēšanas ziņojumu, kurā norāda pasākumus, kas veikti saskaņā ar 4. punktu, un šo pasākumu rezultātus. Neskarot savus pienākumus pret paziņojošajām iestādēm, paziņotā struktūra pilnīgi vai daļēji izpauž minētā ziņojuma saturu tikai ar ražotāja piekrišanu.

6. Ja tips un ievainojamību novēršanas procesi atbilst I pielikumā noteiktajām kiberdrošības pamatprasībām, paziņotā struktūra izsniedz ražotājam ES tipa pārbaudes sertifikātu. Sertifikātā iekļauj ražotāja vārdu vai nosaukumu un adresi, secinājumus pēc pārbaudes, sertifikāta derīguma nosacījumus (ja tādi ir) un datus, kas vajadzīgi apstiprinātā tipa un ievainojamību novēršanas procesu identifikācijai. Sertifikātam var būt viens vai vairāki pielikumi.

Sertifikātā un tā pielikumos ietver visu attiecīgo informāciju, kas vajadzīga, lai varētu novērtēt izgatavoto vai izstrādāto produktu ar digitāliem elementiem atbilstību pārbaudītajam tipam un ievainojamību novēršanas procesiem, lai varētu veikt pārbaudi lietošanas laikā.

Ja tips un ievainojamību novēršanas procesi neatbilst piemērojamajām I pielikumā noteiktajām kiberdrošības pamatprasībām, paziņotā struktūra atsakās izsniegt ES tipa pārbaudes sertifikātu un attiecīgi informē pieteikuma iesniedzēju, atteikumu detalizēti pamatojot.

7. Paziņotā struktūra pastāvīgi apzina visas izmaiņas vispāratzītajos jaunākajos tehnikas sasniegumos, kas norāda, ka apstiprinātais tips un ievainojamību novēršanas procesi varētu vairs neatbilst piemērojamajām I pielikumā noteiktajām kiberdrošības pamatprasībām, un nosaka, vai šādu izmaiņu dēļ ir nepieciešama sīkāka izmeklēšana. Ja šāda izmeklēšana ir nepieciešama, paziņotā struktūra par to informē ražotāju.

Ražotājs informē paziņoto struktūru, kura glabā tehnisko dokumentāciju, kas saistīta ar ES tipa pārbaudes sertifikātu, par visām apstiprinātā tipa un ievainojamību novēršanas procesu modifikācijām, kas var ietekmēt atbilstību piemērojamajām I pielikumā noteiktajām kiberdrošības pamatprasībām, vai minētā sertifikāta derīguma nosacījumus. Šādas modifikācijām paredz papildu apstiprinājumu, ko pievieno kā papildinājumu sākotnējam ES tipa pārbaudes sertifikātam.

8. Paziņotā struktūra periodiski veic revīzijas, lai nodrošinātu, ka I pielikuma II daļā izklāstītie ievainojamības novēršanas procesi tiek pienācīgi īstenoti.

9. Katra paziņotā struktūra informē paziņojušās iestādes par izdotajiem un atsauktajiem ES tipa pārbaudes sertifikātiem un to papildinājumiem un periodiski vai pēc pieprasījuma iesniedz paziņojušajām iestādēm tādu sertifikātu un to papildinājumu sarakstu, kuri ir noraidīti vai kuru darbība ir pārtraukta vai citādi ierobežota.

Katra paziņotā struktūra informē pārējās paziņotās struktūras par tiem ES tipa pārbaudes sertifikātiem un to papildinājumiem, kurus šī struktūra ir atteikusi, atsaukusi, kuru darbību tā ir apturējusi vai citādi ierobežojusi, un pēc pieprasījuma arī par tiem sertifikātiem un to papildinājumiem, kurus tā ir izsniegusi.

Komisija, dalībvalstis un pārējās paziņotās struktūras, iesniedzot pieprasījumu, var saņemt ES tipa pārbaudes sertifikātu un to papildinājumu kopijas. Pēc pieprasījuma Komisija un dalībvalstis var saņemt tehniskās dokumentācijas un paziņotās struktūras veikto pārbaužu rezultātu kopijas. Paziņotā struktūra glabā ES tipa pārbaudes sertifikāta, tā pielikumu un papildinājumu, tehniskās dokumentācijas, tai skaitā arī ražotāja iesniegtās dokumentācijas, kopiju līdz sertifikāta derīguma beigām.

10. Ražotājs ES tipa pārbaudes sertifikāta, tā pielikumu un papildinājumu kopiju kopā ar tehnisko dokumentāciju glabā tā, ka tie ir pieejami valsts iestādēm 10 gadus pēc produkta ar digitāliem elementiem laišanas tirgū vai atbalsta periodā (atkarībā no tā, kurš termiņš ir ilgāks).

11. Ražotāja pilnvarotais pārstāvis var iesniegt 3. punktā minēto pieteikumu un pildīt pienākumus, kas izklāstīti 7. un 9. punktā, ar noteikumu, ka attiecīgie pienākumi ir precizēti pilnvarojumā.

III daļa Atbilstība tipam, balstoties uz ražošanas iekšējo kontroli (pamatojoties uz C moduli)

1. Atbilstība tipam, pamatojoties uz iekšējo ražošanas kontroli, ir atbilstības novērtēšanas procedūras daļa, ar kuru ražotājs izpilda šīs daļas 2. un 3. punktā noteiktos pienākumus un nodrošina un paziņo, ka attiecīgie produkti ar digitāliem elementiem atbilst ES tipa pārbaudes sertifikātā aprakstītajam tipam un piemērojamajām I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām un ka ražotājs ir izpildījis I pielikuma II daļā izklāstītās kiberdrošības pamatprasības.

2. Ražošana

Ražotājs veic visus pasākumus, kas vajadzīgi, lai ražošana un tās uzraudzība nodrošinātu izgatavotā produkta ar digitāliem elementiem atbilstību ES tipa pārbaudes sertifikātā aprakstītajam apstiprinātajam tipam un piemērojamām I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām un lai nodrošinātu, ka ražotājs ir izpildījis I pielikuma II daļā izklāstītās kiberdrošības pamatprasības.

3. Atbilstības zīme un atbilstības deklarācija

3.1. Ražotājs uzliek CE zīmi katram atsevišķam produktam ar digitāliem elementiem, kurš atbilst ES tipa pārbaudes sertifikātā aprakstītajam tipam un ievēro tiesību aktā noteiktās piemērojamās prasības.

3.2. Ražotājs rakstiski sastāda produkta modeļa atbilstības deklarāciju un glabā to kopā ar tehnisko dokumentāciju valsts iestāžu vajadzībām vismaz 10 gadus pēc produkta ar digitāliem elementiem laišanas tirgū vai atbalsta periodā (atkarībā no tā, kurš termiņš ir ilgāks). Atbilstības deklarācijā identificē produkta modeli, kam šī deklarācija ir sagatavota. Atbilstības deklarācijas kopiju pēc pieprasījuma dara pieejamu visām attiecīgajām iestādēm.

4. Pilnvarotais pārstāvis

Ražotāja pienākumus, kas noteikti 3. punktā, tā uzdevumā un uz tā atbildību drīkst pildīt tā pilnvarotais pārstāvis ar noteikumu, ka attiecīgie pienākumi ir precizēti pilnvarojumā.

IV daļa Atbilstība, balstoties uz visaptverošu kvalitātes nodrošināšanu (pamatojoties uz H moduli)

1. Atbilstība, pamatojoties uz visaptverošu kvalitātes nodrošināšanu, ir atbilstības novērtēšanas procedūra, ar kuru ražotājs izpilda šīs daļas 2. un 5. punktā noteiktos pienākumus un nodrošina un paziņo uz savu atbildību, ka attiecīgie produkti ar digitāliem elementiem vai produktu kategorijas atbilst I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām un ka ražotāja ieviestie ievainojamību novēršanas procesi atbilst I pielikuma II daļā noteiktajām prasībām.

2. Produktu ar digitāliem elementiem projektēšana, izstrāde, ražošana un ievainojamību novēršana

Ražotājs izmanto apstiprinātu attiecīgo produktu ar digitāliem elementiem projektēšanas, izstrādes un galīgās produkta pārbaudes un testēšanas, kā arī ievainojamību novēršanas kvalitātes sistēmu, kā norādīts 3. punktā, saglabā tās efektivitāti visā attiecīgo produktu atbalsta periodā un uzrauga to, kā norādīts 4. punktā.

3. Kvalitātes sistēma

3.1. Ražotājs iesniedz paša izvēlētajai paziņotajai struktūrai pieteikumu novērtēt attiecīgo produktu ar digitāliem elementiem kvalitātes nodrošināšanas sistēmu.

Pieteikumā iekļauj:

– ražotāja nosaukumu un adresi, kā arī, ja pieteikumu iesniedz ražotāja pilnvarotais pārstāvis, – tā vārdu vai nosaukumu un adresi;

– tehnisko dokumentāciju vienam modelim no katras ražošanai vai izstrādei paredzētās produktu ar digitāliem elementiem kategorijas. Tehniskajā dokumentācijā attiecīgā gadījumā iekļauj vismaz VII pielikumā izklāstītos elementus;

– kvalitātes nodrošināšanas sistēmas dokumentāciju; kā arī

– rakstisku paziņojumu, ka viens un tas pats pieteikums nav iesniegts nevienā citā paziņotajā struktūrā.

3.2. Kvalitātes nodrošināšanas sistēma garantēs produktu ar digitāliem elementiem atbilstību I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām un ražotāja ieviesto ievainojamību novēršanas procesu atbilstību I pielikuma II daļā noteiktajām pamatprasībām.

Visi elementi, prasības un noteikumi, ko pieņēmis ražotājs, ir sistemātiski un strukturēti dokumentēti rakstisku nostādņu, procedūru un norādījumu veidā. Kvalitātes nodrošināšanas sistēmas dokumentācija rada iespēju konsekventi interpretēt kvalitātes nodrošināšanas programmas, plānus, rokasgrāmatas un dokumentāciju.

Tajā jo īpaši ietver atbilstošu aprakstu par:

– kvalitātes nodrošināšanas mērķiem, kā arī vadības organizatorisko struktūru, pienākumiem un pilnvarām saistībā ar projektēšanu, izstrādi, produktu kvalitāti un ievainojamību novēršanu;

– izmantojamajām tehnisko projektu un izstrādes specifikācijām, ieskaitot standartus, un, ja attiecīgie saskaņotie standarti vai tehniskās specifikācijas netiek piemērotas pilnībā, izmantojamiem paņēmieniem, ar kādiem tiks nodrošināta produktu ar digitāliem elementiem atbilstība attiecīgajām I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām;

– izmantojamajām procedūru specifikācijām, ieskaitot standartus, un, ja attiecīgie saskaņotie standarti vai tehniskās specifikācijas netiek piemērotas pilnībā, izmantojamiem paņēmieniem, ar kādiem tiks nodrošināta produktu atbilstība I pielikuma II daļā noteiktajām kiberdrošības pamatprasībām, kas attiecas uz ražotāju;

– projektēšanas un izstrādes kontroli, kā arī projektēšanas un izstrādes pārbaudes paņēmieniem, procesiem un sistemātiskām darbībām, kas tiks izmantotas, projektējot un izstrādājot attiecīgās produktu ar digitāliem elementiem kategorijas;

– attiecīgajiem ražošanas, kvalitātes kontroles un kvalitātes nodrošināšanas paņēmieniem, procesiem un sistemātiskām darbībām, kas tiks izmantotas;

– pārbaudēm un testiem, ko veiks pirms ražošanas, tās laikā un pēc tās, un biežumu, kādā tos veiks;

– datus par kvalitāti, piemēram, inspekcijas ziņojumus un testu datus, kalibrēšanas datus un ziņojumus par attiecīgā personāla kvalifikāciju.

– projekta un produkta vajadzīgās kvalitātes sasniegšanas un kvalitātes nodrošināšanas sistēmas efektīvas darbības uzraudzības līdzekļiem.

3.3. Paziņotā struktūra novērtē kvalitātes nodrošināšanas sistēmu, lai noteiktu, vai tā atbilst 3.2. punktā minētajām prasībām.

Tā pieņem, ka šīm prasībām atbilst tie kvalitātes nodrošināšanas sistēmas elementi, kas atbilst attiecīgajām valsts standarta specifikācijām, ar kurām īstenots attiecīgais saskaņotais standarts vai tehniskā specifikācija.

Papildus pieredzei kvalitātes vadības sistēmu jomā vismaz vienam revīzijas grupas loceklim ir jābūt pieredzei attiecīgās produktu jomas un ražošanas tehnoloģijas novērtēšanā un zināšanām par šajā regulā noteiktajām piemērojamajām prasībām. Revīzija ietver novērtēšanas apmeklējumu ražotāja telpās, ja šādas telpas ir. Revīzijas grupa izskata 3.1. punkta otrajā ievilkumā minēto tehnisko dokumentāciju, lai pārliecinātos par ražotāja spēju konstatēt šajā regulā noteiktās piemērojamās prasības un veikt nepieciešamās pārbaudes nolūkā nodrošināt produkta ar digitāliem elementiem atbilstību minētajām prasībām.

Lēmumu paziņo ražotājam vai viņa pilnvarotajam pārstāvim.

Paziņojumā iekļauj revīzijas secinājumus un argumentētu novērtējuma lēmumu.

3.4. Ražotājs apņemas pildīt pienākumus, kas izriet no apstiprinātās kvalitātes nodrošināšanas sistēmas, un nodrošināt tās atbilstīgu un efektīvu darbu.

3.5. Ražotājs informē paziņoto struktūru, kas apstiprinājusi kvalitātes nodrošināšanas sistēmu, par visām plānotajām kvalitātes nodrošināšanas sistēmas izmaiņām.

Paziņotā struktūra izvērtē visas ierosinātās izmaiņas un lemj, vai mainītā kvalitātes nodrošināšanas sistēma joprojām atbildīs prasībām, kas minētas 3.2. punktā, vai arī ir nepieciešams pārvērtējums.

Tā savu lēmumu paziņo ražotājam. Paziņojumā ietver pārbaudes secinājumus un argumentētu novērtējuma lēmumu.

4. Uzraudzība, par kuru atbild paziņotā struktūra

4.1. Uzraudzības nolūks ir pārliecināties, ka ražotājs pienācīgi pilda pienākumus, ko paredz apstiprinātā kvalitātes nodrošināšanas sistēma.

4.2. Ražotājs nodrošina paziņotās struktūras pārstāvjiem pieeju projektēšanas, izstrādes, ražošanas, inspicēšanas, testēšanas un noliktavu telpām novērtēšanas vajadzībām un sniedz visu vajadzīgo informāciju, jo īpaši:

– kvalitātes nodrošināšanas sistēmas dokumentāciju;

– datus par kvalitāti, piemēram, analīžu, aprēķinu un testu rezultātus, kā to paredz sistēma projektēšanas kvalitātes nodrošināšanai;

– datus par kvalitāti, piemēram, inspekcijas ziņojumus un testēšanas datus, kalibrēšanas datus un ziņojumus par attiecīgā personāla kvalifikāciju, kā to paredz sistēma ražošanas kvalitātes nodrošināšanai.

4.3. Paziņotā struktūra periodiski veic revīzijas, lai pārliecinātos, ka ražotājs uztur un izmanto kvalitātes nodrošināšanas sistēmu, un iesniedz ražotājam revīzijas ziņojumu.

5. Atbilstības zīme un atbilstības deklarācija

5.1. Ražotājs uzliek CE zīmi un uz 3.1. punktā minētās paziņotās struktūras atbildību arī šīs struktūras identifikācijas numuru katram atsevišķam produktam ar digitāliem elementiem, kas atbilst šīs regulas I pielikuma I daļā noteiktajām prasībām.

5.2. Ražotājs rakstiski sastāda produkta modeļa atbilstības deklarāciju un glabā to kopā ar tehnisko dokumentāciju valsts iestāžu vajadzībām vismaz 10 gadus pēc produkta ar digitāliem elementiem laišanas tirgū vai atbalsta periodā (atkarībā no tā, kurš termiņš ir ilgāks). Atbilstības deklarācijā identificē produkta modeli, kam šī deklarācija ir sagatavota.

Atbilstības deklarācijas kopiju pēc pieprasījuma dara pieejamu visām attiecīgajām iestādēm.

6. Ražotājs vismaz 10 gadus pēc produkta ar digitāliem elementiem laišanas tirgū vai atbalsta periodā (atkarībā no tā, kurš termiņš ir ilgāks) glabā pieejamu valsts iestādēm:

6.1. 3.1. punktā minēto tehnisko dokumentāciju;

6.2. dokumentāciju par 3.1. punktā minēto kvalitātes nodrošināšanas sistēmu;

6.3. iepriekš 3.5. punktā minētās apstiprinātās izmaiņas;

6.4. paziņotās struktūras lēmumus un ziņojumus, kas minēti 3.5. un 4.3. punktā.

7. Katra paziņotā struktūra informē to paziņojošās iestādes par izsniegtajiem vai atsauktajiem kvalitātes nodrošināšanas sistēmas apstiprinājumiem un periodiski vai pēc pieprasījuma dara pieejamu to paziņojošām iestādēm tādu kvalitātes nodrošināšanas sistēmu apstiprinājumu sarakstu, kuri ir atteikti, kuru darbība ir apturēta vai citādi ierobežota.

Katra paziņotā struktūra informē pārējās paziņotās struktūras par tiem kvalitātes nodrošināšanas sistēmas apstiprinājumiem, kurus tā ir atteikusi, apturējusi vai atsaukusi, un pēc pieprasījuma arī par tiem kvalitātes nodrošināšanas sistēmas apstiprinājumiem, kurus tā ir izdevusi.

8. Pilnvarotais pārstāvis

Ražotāja pienākumus, kā noteikts 3.1., 3.5., 5. un 6. punktā, tā uzdevumā un uz tā atbildību var pildīt pilnvarotais pārstāvis ar noteikumu, ka attiecīgie pienākumi ir precizēti pilnvarojumā.

Par šo tiesību aktu ir sniegts viens paziņojums, un tas ir atrodams [lūgums OV birojam norādīt: OV C XXX, XX.XX.2024., XX. lpp.] un pēc šādas saites: [lūgums OV birojam iekļaut saiti uz paziņojumu].