Eiropas Savienības
Padome

Briselē, 2022. gada 16. septembrī
(OR. en)

12429/22

Starpiestāžu lieta:
2022/0272(COD)

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

PRIEKŠLIKUMS

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2022. gada 15. septembris
Saņēmējs:	Padomes Ģenerālsekretariāts
K-jas dok. Nr.:	COM(2022) 454 final
Temats:	Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULA par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulu (ES) 2019/1020

Pielikumā ir pievienots dokuments COM(2022) 454 *final*.

Pielikumā: COM(2022) 454 *final*

EIROPAS
KOMISIJA

Briselē, 15.9.2022.
COM(2022) 454 final

2022/0272 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulu (ES) 2019/1020

(Dokuments attiecas uz EEZ)

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

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

• Priekšlikuma pamatojums un mērķi

Pret aparatūras un programmatūras produktiem arvien biežāk tiek īstenoti sekmīgi kiberuzbrukumi, kuru dēļ kibernoziedzības radītās ikgadējās izmaksas pēc aplēsēm pasaulē 2021. gadā sasniedza 5,5 triljonus EUR. Šādus produktus skar divas lielas problēmas, kas rada papildu izmaksas lietotājiem un sabiedrībai: 1) zems kiberdrošības līmenis, ko atspoguļo plaši izplatītas ievainojamības un nepietiekama un nekonsekventa drošības atjauninājumu nodrošināšana to novēršanai, un 2) nepietiekama lietotāju izpratne un piekļuve informācijai, kas neļauj lietotājiem izvēlēties produktus ar atbilstošām kiberdrošības īpašībām vai tos izmantot drošā veidā. Savienotā vidē ar vienu produktu noticis kiberdrošības incidents var ietekmēt visu organizāciju vai visu piegādes ķēdi, bieži vien dažās minūtēs izplatoties pāri iekšējā tirgus robežām. Tas var izraisīt nopietnus ekonomiskās un sociālās darbības traucējumus vai pat apdraudēt dzīvības.

Produktu ar digitāliem elementiem kiberdrošībai ir izteikta pārrobežu dimensija, jo vienā valstī ražoti produkti bieži tiek lietoti visā iekšējā tirgū. Turklāt incidenti, kas sākotnēji ietekmē vienu vienību vai vienu dalībvalsti, bieži vien dažās minūtēs izplatās visā iekšējā tirgū.

Lai gan spēkā esošos iekšējā tirgus tiesību aktus piemēro noteiktiem produktiem ar digitāliem elementiem, uz lielāko daļu aparatūras un programmatūras produktu patlaban neattiecas neviens ES tiesību akts, ar kuru tiktu risināta šo produktu kiberdrošība. Konkrēti pašreizējais ES tiesiskais regulējums nerisina neiegultas programmatūras kiberdrošību, neskatoties uz to, ka uzbrukumi kiberdrošībai arvien vairāk tiek vērsti uz šo produktu ievainojamībām, radot būtiskas sociālās un ekonomiskās izmaksas. Ir vairāki tādu vērā ņemamu kiberuzbrukumu piemēri, kuri notikuši nepietiekamas produktu drošības rezultātā, piemēram, *WannaCry* izspiedējprogrammatūras tārps, kas 2017. gadā izmantoja *Windows* ievainojamību un skāra 200 000 datoru 150 valstīs, kā arī radīja zaudējumus vairāku miljardu USD apmērā; uzbrukums *Kaseya VSA* piegādes ķēdei, kurā tika izmantota *Kaseya* tīkla administrēšanas programmatūra, lai uzbruktu vairāk nekā 1000 uzņēmumiem un piespiestu lielveikalu ķēdi slēgt visus tās 500 veikalus Zviedrijā; vai daudzie incidenti, kuros nolūkā nozagt naudu labticīgiem patērētājiem tiek veikta banku lietojumprogrammu uzlaušana.

Tika noteikti šādi divi galvenie mērķi, kuri vērsti uz pareizas iekšējā tirgus darbības nodrošināšanu: 1) radīt apstākļus, lai tiktu izstrādāti droši produkti ar digitāliem elementiem, nodrošinot, ka aparatūras un programmatūras produkti tirgū tiek laisti ar mazāk ievainojamībām un ka ražotājiem ir nopietna attieksme pret drošību visā produkta aprites ciklā; un 2) radīt apstākļus, kas lietotājiem, izvēloties un lietojot produktus ar digitāliem elementiem, dod iespēju ņemt vērā kiberdrošību. Tika noteikti četri konkrētie mērķi: i) nodrošināt, ka ražotāji, sākot no projektēšanas un izstrādes posma, kā arī visā aprites ciklā uzlabo produktu ar digitāliem elementiem drošību; ii) nodrošināt saskaņotu kiberdrošības satvaru, sekmējot aparatūras un programmatūras ražotāju atbilstību; iii) uzlabot produktu ar digitāliem elementiem drošības īpašību pārredzamību un iv) sniegt iespēju uzņēmumiem un patērētājiem droši lietot produktus ar digitāliem elementiem.

Kiberdrošības izteiktais pārrobežu raksturs un pieaugošais to incidentu skaits, kuru ietekme izvēršas pāri robežām, starp dažādām nozarēm un produktiem, nozīmē, ka dalībvalstis vienas pašas nevar efektīvi sasniegt šos mērķus. Ņemot vērā produktu ar digitāliem elementiem tirgu

globālo raksturu, dalībvalstis savā teritorijā attiecībā uz vienu un to pašu produktu ar digitāliem elementiem saskaras ar vieniem un tiem pašiem riskiem. Jauns sadrumstalots regulējums, ko veido potenciāli atšķirīgi valstu noteikumi, rada risku, ka var tikt kavēts atvērts un konkurētspējīgs vienotais tirgus attiecībā uz produktiem ar digitāliem elementiem. Tāpēc, lai palielinātu lietotāju uzticēšanos un ES produktu ar digitāliem elementiem pievilcību, ir vajadzīga vienota rīcība ES līmenī. Tā nāktu par labu arī iekšējam tirgum, nodrošinot juridisko noteiktību un panākot vienlīdzīgus konkurences apstākļus produktu ar digitāliem elementiem pārdevējiem, kā tas uzsvērts arī konferences par Eiropas nākotni galīgajā ziņojumā, kurā pilsoņi aicina palielināt ES nozīmi cīņā pret kiberdrošības apdraudējumiem.

- **Mijiedarbība ar pašreizējiem noteikumiem konkrētajā politikas jomā**

ES regulējumā ir vairāki horizontālie tiesību akti, kas no dažādiem skatupunktiem (produkti, pakalpojumi, krīzes pārvarēšana un noziegumi) aptver noteiktus ar kiberdrošību saistītus aspektus. 2013. gadā stājās spēkā Direktīva par uzbrukumiem informācijas sistēmām[1], ar ko saskaņo krimināltiesību noteikšanu un sodus par vairākiem noziedzīgiem nodarījumiem, kas vērsti pret informācijas sistēmām. 2016. gada augustā stājās spēkā Direktīva (ES) 2016/1148 par tīklu un informācijas sistēmu drošību (TID direktīva)[2], kas ir pirmais ES mēroga tiesību akts kiberdrošības jomā. Tās pārskatīšana, kuras rezultātā ir izstrādāta Direktīva [Direktīva XXX/XXXX (TID2)], paaugstina ES kopējo mērķu vērienīgumu. 2019. gadā stājās spēkā ES Kiberdrošības akts[3], kura mērķis ir uzlabot IKT produktu, IKT pakalpojumu un IKT procesu drošību, ieviešot brīvprātīgu Eiropas kiberdrošības sertifikācijas satvaru[4].

Visas piegādes ķēdes kiberdrošība ir nodrošināta tikai tad, ja kiberdroši ir visi tās komponenti. Tomēr iepriekš minētajos ES tiesību aktos šajā ziņā ir būtiskas nepilnības, jo tajos nav ietvertas obligātās prasības attiecībā uz produktu ar digitāliem elementiem drošību.

Lai gan ierosinātais Kibernoturības akts attiecas uz tirgū laistiem produktiem ar digitāliem elementiem, Direktīvas [Direktīva XXX/XXX (TID2)] mērķis ir nodrošināt augstu kiberdrošības līmeni attiecībā uz būtisko un svarīgo vienību sniegtajiem pakalpojumiem. Direktīvā [Direktīva XXX/XXXX (TID2)] ir noteikts, ka dalībvalstīm jānodrošina, lai darbības jomā ietilpstošās būtiskās un svarīgās vienības, piemēram, veselības aprūpes vai mākoņdatošanas pakalpojumu sniedzēji un valsts pārvaldes vienības veiktu atbilstīgus un samērīgus tehniskos, operatīvos un organizatoriskos kiberdrošības pasākumus. Tas cita starpā ietver prasību nodrošināt drošību attiecībā uz tīklu un informācijas sistēmu iegādi, izstrādi un uzturēšanu, ieskaitot ievainojamību novēršanu un ievainojamības atklāšanu. Direktīvā [Direktīva XXX/XXXX (TID2)] ir noteikts, ka Komisijai 21 mēneša laikā pēc šīs direktīvas stāšanās spēkā ir jāpieņem īstenošanas akti, ar kuriem nosaka minēto pasākumu tehniskās un

---

1 Eiropas Parlamenta un Padomes Direktīva 2013/40/ES (2013. gada 12. augusts) par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI, OV L 218, 14.8.2013., 8.–14. lpp.

2 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194/1, 19.7.2016., 1. lpp.).

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 Kiberdrošības akts ļauj izstrādāt īpašas sertifikācijas shēmas. Katra shēma ietver atsauces uz attiecīgajiem standartiem, tehniskajām specifikācijām vai citām kiberdrošības prasībām, kas ir noteiktas shēmā. Lēmums par kiberdrošības sertifikācijas izstrādi ir balstīts uz risku.

metodiskās prasības attiecībā uz noteiktu veidu vienībām, piemēram, mākoņdatošanas pakalpojumu sniedzējiem. Attiecībā uz visām pārējām vienībām Komisija var pieņemt īstenošanas aktu, ar ko nosaka tehniskās un metodiskās prasības, kā arī nozaru prasības. Šis regulējums nodrošinās, ka tehniskās specifikācijas un pasākumi, kas līdzīgi Kibernoturības akta kiberdrošības pamatprasībām, tiek īstenoti arī attiecībā uz tādas programmatūras projektēšanu, izstrādi un ievainojamību novēršanu, kuru sniedz kā pakalpojumu (*Software-as-a-Service*). Piemēram, tas varētu būt līdzeklis, lai nodrošinātu augstu kiberdrošības līmeni tādos gadījumos kā, piemēram, e-veselības pacienta karšu (EVPK) sistēmas, tajā skaitā gadījumos, kad attiecīgo programmatūru sniedz kā pakalpojumu (*SaaS*) vai izstrādā uz vietas pašās veselības iestādēs saskaņā ar ierosināto [Eiropas veselības datu telpas regulu].

- **Mijiedarbība ar citām Savienības politikas jomām**

Kā izklāstīts paziņojumā "Eiropas digitālās nākotnes veidošana"[5], Eiropas Savienībai ir ļoti svarīgi izmantot visas digitālā laikmeta priekšrocības un stiprināt tās rūpniecības un inovācijas spējas, ievērojot drošas un ētiskas robežas. Eiropas Datu stratēģijā ir paredzēti četri pīlāri — datu aizsardzība, pamattiesības, drošums un kiberdrošība — kā būtiski priekšnoteikumi sabiedrībai, kam datu izmantošana sniedz iespējas.

Pašreizējā ES regulējumā[6], ko piemēro produktiem, kuriem var būt arī digitāli elementi, ietilpst vairāki tiesību akti, to vidū konkrētiem produktiem paredzēti ES tiesību akti, kas aptver ar drošumu saistītus aspektus, kā arī vispārējie tiesību akti produktatbildības jomā. Priekšlikums atbilst pašreizējam ar produktiem saistītajam ES tiesiskajam regulējumam, kā arī jaunākajiem tiesību aktu priekšlikumiem, piemēram, Komisijas priekšlikumam regulai [Mākslīgā intelekta (MI) regula][7].

Ierosinātā regula attiektos uz visām radioiekārtām, kas ietilpst Komisijas Deleģētās regulas (ES) 2022/30 darbības jomā. Turklāt šajā regulā noteiktās prasības ietver visus Direktīvas 2014/53/ES 3. panta 3. punkta d), e) un f) apakšpunktā minēto pamatprasību elementus, ieskaitot galvenos elementus, kas noteikti uz minētās deleģētās regulas pamata izdotajā [Komisijas Īstenošanas lēmumā XXX/2022 par standartizācijas pieprasījumu Eiropas standartizācijas organizācijām]. Lai izvairītos no regulējuma pārklāšanās, ir paredzēts, ka Komisija atcels vai grozīs deleģēto regulu attiecībā uz ierosinātajā regulā ietvertajām radioiekārtām, lai minētā regula uz tām attiektos, kad tā būs piemērojama.

Turklāt, lai izvairītos no darba dublēšanās, ir paredzēts, ka Komisija un Eiropas standartizācijas organizācijas ņem vērā standartizācijas darbu, kas saistībā ar Komisijas Īstenošanas lēmumu C(2022)5637 par standartizācijas pieprasījumu attiecībā uz Radioiekārtu direktīvas Deleģēto regulu 2022/30 veikts saskaņoto standartu sagatavošanā un izstrādē ar mērķi sekmēt regulas īstenošanu.

---

5 Komisijas 2020. gada 19. februāra paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Eiropas digitālās nākotnes veidošana" (COM(2020) 67 *final*).

6 Galvenokārt jaunā tiesiskā regulējuma (JTR) tiesību akti.

7 Priekšlikums Eiropas Parlamenta un Padomes regulai, kas nosaka saskaņotas normas mākslīgā intelekta jomā (Mākslīgā intelekta akts) un groza dažus Savienības leģislatīvos aktus, 2021. gada 21. aprīlis, COM(2021) 206 *final*.

2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

• Juridiskais pamats

Šā priekšlikuma juridiskais pamats ir Līguma par Eiropas Savienības darbību ("LESD") 114. pants, kurā noteikta pasākumu pieņemšana iekšējā tirgus izveides un darbības nodrošināšanai. Priekšlikuma mērķis ir visās dalībvalstīs saskaņot kiberdrošības prasības attiecībā uz produktiem ar digitāliem elementiem un novērst šķēršļus preču brīvai apritei.

LESD 114. pantu var izmantot par juridisko pamatu, lai novērstu šos šķēršļus, ko rada atšķirīgi valstu tiesību akti un pieejas attiecībā uz to, kā novērst juridisko nenoteiktību un spēkā esošo tiesisko regulējumu nepilnības[8]. Turklāt Tiesa ir atzinusi, ka neviendabīgu tehnisko prasību piemērošana varētu būt pamatots iemesls LESD 114. panta piemērošanai[9].

Patlaban spēkā esošais ES tiesiskais regulējums, ko piemēro produktiem ar digitāliem elementiem, pamatojas uz LESD 114. pantu un ietver vairākus tiesību aktus, to vidū aktus, kas paredzēti konkrētiem produktiem un ar drošumu saistītiem aspektiem, vai vispārējos tiesību aktus produktatbildības jomā. Tomēr tas aptver tikai noteiktus aspektus, kas ir saistīti ar materiālo digitālo produktu kiberdrošību un attiecīgā gadījumā šajos produktos iegulto programmatūru. Valsts līmenī dalībvalstis sāk veikt valsts pasākumus, ar kuriem digitālo produktu pārdevējiem tiek prasīts uzlabot savu kiberdrošību[10]. Tajā pašā laikā digitālo produktu kiberdrošībai ir īpaši izteikta pārrobežu dimensija, jo vienā valstī ražotus produktus bieži lieto organizācijas un patērētāji visā iekšējā tirgū. Incidenti, kas sākotnēji skar vienu vienību vai dalībvalsti, bieži vien dažās minūtēs izplatās starp organizācijām, nozarēm un vairākām dalībvalstīm.

ES un valstu līmenī līdz šim īstenotie dažādie tiesību akti un iniciatīvas tikai daļēji risina konstatētās problēmas un rada likumdošanas sadrumstalotības risku iekšējā tirgū, palielinot juridisko nenoteiktību gan šo produktu pārdevējiem, gan lietotājiem un radot nevajadzīgu slogu uzņēmumiem, lai tie izpildītu vairākas prasības attiecībā uz līdzīgiem produktu veidiem.

Ierosinātā regula saskaņotu un racionalizētu ES regulatīvo vidi, ieviešot kiberdrošības prasības attiecībā uz produktiem ar digitāliem elementiem, un novērstu no dažādiem tiesību aktiem izrietošu prasību pārklāšanos. Tas radītu lielāku juridisko noteiktību uzņēmējiem un lietotājiem visā Savienībā, kā arī Eiropas vienotā tirgus labāku saskaņošanu, radot labvēlīgākus apstākļus uzņēmējiem, kuru mērķis ir ienākt ES tirgū.

• Subsidiaritāte (neekskluzīvas kompetences gadījumā)

Kiberdrošības izteiktais pārrobežu raksturs kopumā un pieaugošais to risku un incidentu skaits, kuru ietekme izvēršas pāri robežām, starp dažādām nozarēm un produktiem, nozīmē, ka dalībvalstis vienas pašas nevar efektīvi sasniegt pašreizējās intervences mērķus. Valstu pieejas problēmu risināšanā un jo īpaši pieejas, ar kurām ievieš obligātas prasības, radīs papildu juridisko nenoteiktību un juridiskos šķēršļus. Uzņēmumiem varētu tikt liegta netraucēta darbības paplašināšana citās dalībvalstīs, atņemot lietotājiem šo uzņēmumu produktu sniegtos ieguvumus.

---

8 EST spriedums (virspalāta), 2019. gada 3. decembris, Čehijas Republika pret Eiropas Parlamentu un Eiropas Savienības Padomi, lieta C-482/17, 35. punkts.

9 EST spriedums (virspalāta), 2006. gada 2. maijs, Lielbritānijas un Ziemeļīrijas Apvienotā Karaliste pret Eiropas Parlamentu un Eiropas Savienības Padomi, lieta C-217/04, 62.–63. punkts.

10 Piemēram, Somija 2019. gadā, pamatojoties uz ETSI standartiem, ir izveidojusi lietu interneta ierīcēm, piemēram, viedtelevizoriem, viedtālruņiem un rotaļlietām paredzētu marķēšanas sistēmu. Vācija ir nesen ieviesusi patērētāju drošības marķējumu platjoslas maršrutētājiem, viedtelevizoriem, kamerām, skaļruņiem, rotaļlietām, kā arī tīrīšanas un dārzkopības robotiem.

Tādēļ, lai panāktu augstu uzticēšanās līmeni starp lietotājiem, ir vajadzīga vienota rīcība ES līmenī, palielinot ES produktu ar digitāliem elementiem pievilcību. Tas sniegtu ieguvumus arī digitālajam vienotajam tirgum un iekšējam tirgum kopumā, nodrošinot juridisko noteiktību un panākot vienlīdzīgus konkurences apstākļus produktu ar digitāliem elementiem ražotājiem.

Visbeidzot, Padomes 2022. gada 23. maija secinājumos par Eiropas Savienības kiberdrošības parametru izstrādi Komisija ir aicināta līdz 2022. gada beigām ierosināt kopīgas kiberdrošības prasības attiecībā uz savienotajām ierīcēm.

- **Proporcionalitāte**

Attiecībā uz ierosinātās regulas proporcionalitāti apsvērto politikas risinājumu pasākumi nepārsniegtu vispārējo un konkrēto mērķu sasniegšanai nepieciešamo apmēru, kā arī neradītu nesamērīgas izmaksas. Konkrētāk, aplūkotā intervence nodrošinātu, ka produkti ar digitāliem elementiem būtu pasargāti visā to aprites ciklā un proporcionāli riskiem, ar ko tie saskaras, izmantojot uz mērķi vērstas un tehnoloģiski neitrālas prasības, kas saglabā savu pamatotību un kopumā atbilst iesaistīto vienību interesēm.

Priekšlikumā ietverto kiberdrošības pamatprasību pamatā ir plaši izmantoti standarti, un turpmākajā standartizācijas procesā tiktu ņemtas vērā produktu tehniskās īpatnības. Tas nozīmē, ka drošības kontrole tiktu pielāgota, ja tas nepieciešams konkrētam riska līmenim. Turklāt paredzētie horizontālie noteikumi kritiski svarīgiem produktiem paredzētu tikai trešo personu veiktu novērtējumu. Tas ietvertu tikai nelielu tirgus daļu attiecībā uz produktiem ar digitāliem elementiem. Ietekme uz MVU būtu atkarīga no to klātbūtnes šo konkrēto kategoriju produktu tirgū.

Attiecībā uz atbilstības novērtēšanas izmaksu samērīgumu paziņotās struktūras, kas īsteno trešo personu veiktus novērtējumus, maksas noteikšanā ņemtu vērā uzņēmuma lielumu. Lai sagatavotos īstenošanai, tiktu nodrošināts arī saprātīgs 24 mēnešu pārejas laikposms, dodot attiecīgajiem tirgiem laiku sagatavoties, vienlaikus nodrošinot skaidru virzienu attiecībā uz ieguldījumiem pētniecībā un izstrādē. Atbilstības nodrošināšanas izmaksas uzņēmumiem atsvērtu ieguvumi, ko sniegtu augstāks drošības līmenis produktiem ar digitāliem elementiem un galu galā lielāka lietotāju uzticēšanās attiecībā uz šiem produktiem.

- **Juridiskā instrumenta izvēle**

Regulatīva intervence nozīmētu regulas, nevis direktīvas pieņemšanu. Tas ir tāpēc, ka attiecībā uz šo konkrēto produktu tiesību aktu veidu regula efektīvāk risinātu konstatētās problēmas un panāktu izvirzītos mērķus, jo šī ir intervence, kas nosaka ļoti plašas produktu kategorijas laišanu iekšējā tirgū. Transponēšanas process direktīvas gadījumā attiecībā uz šādu intervenci varētu atstāt pārāk lielu rīcības brīvību valsts līmenī, iespējams, izraisot noteiktu kiberdrošības pamatprasību vienotības trūkumu, juridisko nenoteiktību, turpmāku sadrumstalotību vai pat diskriminējošas pārrobežu situācijas, vēl jo vairāk ņemot vērā to, ka ietvertajiem produktiem varētu būt vairāki nolūki vai lietojumi un ka ražotāji var ražot vairākas šādu produktu kategorijas.

3. *EX POST* IZVĒRTĒJUMU, APSPRIEŠANOS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMU REZULTĀTI

- **Apspriešanās ar ieinteresētajām personām**

Komisija ir apspriedusies ar plašu ieinteresēto personu loku. Dalībvalstis un ieinteresētās personas tika aicinātas piedalīties atklātā sabiedriskajā apspriešanā, kā arī apsekojumos un darbsemināros, kas tika organizēti saistībā ar pētījumu, ko veica Komisijas ietekmes novērtējuma sagatavošanas darba atbalsta konsorcijs, proti, *Wavestone*, Eiropas politikas

pētījumu centrs (*CEPS*) un *ICF*. Starp ieinteresētajām personām, ar kurām notika apspriešanās, bija valstu tirgus uzraudzības iestādes, Savienības struktūras, kas nodarbojas ar kiberdrošību, aparatūras un programmatūras ražotāji, aparatūras un programmatūras importētāji un izplatītāji, arodasociācijas, patērētāju organizācijas un produktu ar digitāliem elementiem lietotāji, kā arī pilsoņi, pētnieki un akadēmiskās aprindas, paziņotās struktūras un akreditācijas struktūras, un kiberdrošības nozares speciālisti.

Notika šādi apspriešanās pasākumi:

- pirmais pētījums, ko veica *ICF*, *Wavestone*, *Carsa* un *CEPS* konsorcijs un kas tika publicēts 2021. gada decembrī[11]. Pētījumā tika konstatētas vairākas tirgus nepilnības un izvērtētas iespējamās regulatīvās intervences.
- Atklāta sabiedriskā apspriešana, kas bija vērsta uz iedzīvotājiem, ieinteresētajām personām un kiberdrošības ekspertiem. Tika iesniegtas 176 atbildes. Tās palīdzēja apkopot dažādus viedokļus un pieredzi no visām ieinteresēto personu grupām.
- Komisijas Kibernoturības akta sagatavošanas darba atbalsta pētījuma rīkotajos darbsemināros piedalījās aptuveni 100 pārstāvji no visām 27 dalībvalstīm, pārstāvot plašu ieinteresēto personu loku.
- Tika veiktas ekspertu intervijas, lai gūtu dziļāku izpratni par pašreizējām kiberdrošības problēmām saistībā ar produktiem ar digitāliem elementiem un lai apspriestu politikas risinājumus attiecībā uz iespējamo regulatīvo intervenci.
- Notika divpusējas diskusijas ar valstu kiberdrošības iestāžu, privātā sektora un patērētāju organizāciju līdzdalību.
- Tika mērķtiecīgi informētas galvenās MVU ieinteresētās personas.

- **Ekspertu atzinumu pieprasīšana un izmantošana**

Apspriešanās pasākumu mērķis bija, pamatojoties uz ES labāka regulējuma pamatnostādnēm, iegūt informāciju par pieciem galvenajiem vērtēšanas kritērijiem (lietderīgums, efektivitāte, būtiskums, saskaņotība, ES pievienotā vērtība), kā arī par iespējamo risinājumu potenciālo ietekmi nākotnē. Līgumslēdzējs ir ne vien vērsies pie ieinteresētajām personām, kuras tieši ietekmētu ierosinātā regula, bet arī apspriedies ar plašu kiberdrošības jomas ekspertu loku.

- **Ietekmes novērtējums**

Komisija veica šā priekšlikuma ietekmes novērtējumu, ko izskatīja Komisijas Regulējuma kontroles padome (RKP). Sanāksme ar RKP piedalīšanos notika 2022. gada 6. jūlijā, un tai sekoja pozitīvs atzinums. Ietekmes novērtējums tika koriģēts, lai ņemtu vērā RKP ieteikumus un piezīmes.

Komisija izskatīja dažādus politikas risinājumus, ar ko sasniegt priekšlikuma vispārējo mērķi:

- ieteikuma tiesību pieeja un brīvprātīgi pasākumi (1. risinājums) — šajā risinājumā nebūtu obligātas regulatīvās intervences. Tā vietā Komisija nāktu

[11] *Study on the need of Cybersecurity requirements for ICT products* (Pētījums par kiberdrošības prasību nepieciešamību attiecībā uz IKT produktiem) – Nr. 2020-0715, galīgais pētījuma ziņojums, pieejams vietnē https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

klajā ar paziņojumiem, norādījumiem, ieteikumiem un, iespējams, rīcības kodeksiem, lai veicinātu brīvprātīgos pasākumus. Lai kompensētu ES horizontālo noteikumu trūkumu, arī turpmāk tiktu izstrādātas brīvprātīgas vai obligātas valstu shēmas.

- *Ad hoc* regulatīvā intervence attiecībā uz materiālo produktu ar digitāliem elementiem un attiecīgās iegultās programmatūras kiberdrošību (2. risinājums) — šis risinājums ietvertu konkrētam produktam paredzētu *ad hoc* regulatīvo intervenci, kas aprobežotos ar kiberdrošības prasību pievienošanu un/vai grozīšanu jau spēkā esošajos tiesību aktos vai jaunu tiesību aktu ieviešanu jaunu risku rašanās gadījumā, tostarp, iespējams, attiecībā uz neiegultu programmatūru.

3. un 4. risinājums ietver horizontālu regulatīvu intervenci ar atšķirīgu darbības jomu, lielā mērā ievērojot jauno tiesisko regulējumu (JTR). Šis regulējums nosaka pamatprasības kā nosacījumu noteiktu produktu laišanai iekšējā tirgū. JTR parasti paredz arī atbilstības izvērtēšanu, t. i., procesu, ko veic ražotājs, lai pierādītu, vai ir izpildītas attiecībā uz produktu noteiktās prasības.

- Jaukta pieeja, kas ietver horizontālus obligātos noteikumus attiecībā uz materiālo produktu ar digitāliem elementiem un attiecīgās iegultās programmatūras kiberdrošību, kā arī vairāku posmu pieeju attiecībā uz neiegultu programmatūru (3. risinājums) — šis risinājums ietvertu regulu, ar ko attiecībā uz visiem materiālajiem produktiem ar digitāliem elementiem un tajos iegultu programmatūru tiktu ieviestas horizontālas kiberdrošības prasības kā nosacījums laišanai tirgū, un iekļautu divus apakšrisinājumus, proti, ar obligātu trešās personas veiktu novērtējumu un bez tā (3.i) un 3.ii)). Neiegultā programmatūra netiktu reglamentēta.

- Horizontāla regulatīvā intervence, ar ko ievieš kiberdrošības prasības plašam materiālo un nemateriālo produktu ar digitāliem elementiem klāstam, ieskaitot neiegultu programmatūru (4. risinājums). Šis risinājums līdzinās 3. risinājumam, izņemot darbības jomu. 4. risinājums ietvertu neiegultu programmatūru (ar diviem apakšrisinājumiem, attiecīgi potenciālās regulas darbības jomā iekļaujot tikai kritiski svarīgu programmatūru (4.a)) vai visu programmatūru (4.b)). Par katru apakšrisinājumu saistībā ar atbilstības novērtējumu tiktu apsvērti tie paši apakšrisinājumi, kas attiecībā uz 3. risinājumu.

4. risinājums (ar apakšrisinājumiem, kas aptver visu programmatūru un paredz obligātu trešo personu veiktu kritiski svarīgo produktu novērtējumu) tika atzīts par vēlamo risinājumu, pamatojoties uz novērtējumu par lietderīgumu attiecībā pret konkrētajiem mērķiem, kā arī izmaksu efektivitāti salīdzinājumā ar ieguvumiem. Šis risinājums nodrošinātu konkrētu horizontālās kiberdrošības prasību noteikšanu visiem produktiem ar digitāliem elementiem, kuri tiek laisti vai darīti pieejami iekšējā tirgū, un tas būtu vienīgais risinājums, kas aptvertu visu digitālās piegādes ķēdi. Uz neiegultu programmatūru, kas bieži ir pakļauta ievainojamībai, arī attiektos šāda regulatīvā intervence, tādējādi nodrošinot saskaņotu pieeju attiecībā uz visiem produktiem ar digitāliem elementiem un skaidru atbildības sadalījumu starp dažādiem uzņēmējiem.

Šis politikas risinājums arī rada pievienoto vērtību, ietverot rūpības pienākumu un visa aprites cikla aspektus pēc produktu ar digitāliem elementiem laišanas tirgū, lai cita starpā nodrošinātu atbilstīgu informāciju par drošības atbalstu un drošības atjauninājumu nodrošināšanu. Šis

politikas risinājums arī visefektīvāk papildinātu neseno TID regulējuma pārskatīšanu, nodrošinot priekšnosacījumus piegādes ķēdes drošības stiprināšanai.

Vēlamais risinājums sniegtu ievērojamu labumu dažādām ieinteresētajām personām. Uzņēmumiem tas novērstu atšķirīgus drošības noteikumus attiecībā uz produktiem ar digitāliem elementiem un samazinātu atbilstības nodrošināšanas izmaksas attiecībā uz saistītajiem kiberdrošības tiesību aktiem. Tas samazinātu kiberincidentu skaitu, incidentu risināšanas izmaksas un kaitējumu reputācijai. Tiek lēsts, ka visā ES šī iniciatīva uzņēmumus ietekmējošu incidentu radītās izmaksas varētu samazināt par aptuveni 180 līdz 290 miljardiem EUR gadā. Tas radītu apgrozījuma palielināšanos, jo pieaugtu pieprasījums pēc produktiem ar digitāliem elementiem. Tas uzlabotu uzņēmumu globālo reputāciju, kā rezultātā pieprasījums pieaugtu arī ārpus ES. Lietotājiem vēlamais risinājums uzlabotu drošības īpašību pārredzamību un sekmētu produktu ar digitāliem elementiem lietošanu. Patērētāji un iedzīvotāji iegūtu arī no tā, ka tiktu labāk aizsargātas viņu pamattiesības, piemēram, privātums un datu aizsardzība.

Kad sabiedriskās apspriešanas respondentiem tika lūgts novērtēt politikas intervences pasākumu efektivitāti, tie atzina, ka 4. risinājums būtu visefektīvākais pasākums (4,08 skalā no 1 līdz 5). To vidū ir patērētāju organizācijas (5,00), respondenti, kas sevi identificē kā lietotājus (4,22), paziņotās struktūras (4,17), tirgus uzraudzības iestādes (5,00) un produktu ar digitāliem elementiem ražotāji (3,85), to vidū mazie un vidējie ražotāji (4,05).

- **Normatīvā atbilstība un vienkāršošana**

Šajā priekšlikumā ir noteiktas prasības, kas attieksies uz programmatūras un aparatūras ražošanu. Ir jānodrošina juridiskā noteiktība un nedrīkst pieļaut, ka iekšējā tirgū turpina sadrumstaloties ar produktiem saistītu kiberdrošības prasību tirgus ; par šādu vajadzību liecina dažādu ieinteresēto personu paustais plašais atbalsts attiecībā uz horizontālo intervenci. Priekšlikums līdz minimumam samazinās regulatīvo slogu, ko ražotājiem ir radījuši vairāki produktu drošuma tiesību akti. Saskaņošana ar JTR nozīmē labāku intervences darbību un tās izpildes panākšanu. Priekšlikums racionalizē drošības procedūru procesu, iesaistot ražotājus un dalībvalstis, pirms tiek informēta Komisija. Liela daļa priekšlikuma darbības jomā ietverto ražotāju jau ir iepazinušies ar JTR darbību, kas sekmēs tā izpratni un īstenošanu. Attiecībā uz patērētājiem un uzņēmumiem šis priekšlikums veicinās uzticēšanos produktiem ar digitāliem elementiem.

- **Pamattiesības**

Paredzams, ka visi politikas risinājumi zināmā mērā uzlabos tādu pamattiesību un pamatbrīvību aizsardzību kā, piemēram, privātums, persondatu aizsardzība, darījumdarbības brīvība un īpašuma vai personas cieņas un integritātes aizsardzība. Šajā ziņā visefektīvākais jo īpaši būtu vēlamais 4. politikas risinājums, kas ietver horizontālas regulatīvās intervences pasākumus un plašu politikas darbības jomu, jo tas, visticamāk, palīdzētu samazināt incidentu, arī persondatu aizsardzības pārkāpumu, skaitu un nopietnības pakāpi. Tas arī palielinātu juridisko noteiktību un nodrošinātu vienlīdzīgus konkurences apstākļus uzņēmējiem, palielinātu lietotāju uzticēšanos un ES produktu ar digitāliem elementiem pievilcību kopumā, tādējādi aizsargājot īpašumu un uzņēmējiem uzlabojot darījumdarbības veikšanas apstākļus.

Horizontālās kiberdrošības prasības veicinātu persondatu drošību, aizsargājot konfidencialitāti, integritāti un informācijas pieejamību attiecībā uz produktiem ar digitāliem elementiem. Šo prasību ievērošana sekmēs atbilstību prasībai par persondatu apstrādes

drošību saskaņā ar Regulu (ES) 2016/679 par Vispārīgo datu aizsardzības regulu (VDAR)[12]. Priekšlikums uzlabotu pārredzamību un informācijas sniegšanu lietotājiem, arī tiem, kuriem varētu būt zemāks prasmju līmenis kiberdrošības jomā. Lietotāji arī būtu labāk informēti par riskiem, spējām un ierobežojumiem saistībā ar produktiem ar digitāliem elementiem, un tas ļautu viņiem labāk veikt nepieciešamos preventīvos un riska mazināšanas pasākumus atlikušo risku samazināšanas nolūkā.

4. IETEKME UZ BUDŽETU

Lai pildītu uzdevumus, kas saskaņā ar šo regulu uzticēti Eiropas Savienības Kiberdrošības aģentūrai (*ENISA*), *ENISA* būs jāpārdala resursi aptuveni 4,5 pilnslodzes ekvivalentu (FTE) apmērā. Komisijai, lai izpildītu savus pienākumus saistībā ar izpildes panākšanu atbilstīgi šai regulai, būtu jāpiešķir 7 FTE.

Sīki izstrādāts attiecīgo izmaksu pārskats ir sniegts ar šo priekšlikumu saistītajā "finanšu pārskatā".

5. CITI ELEMENTI

• Īstenošanas plāni un uzraudzīšanas, izvērtēšanas un ziņošanas kārtība

Lai novērtētu jauno noteikumu efektivitāti, Komisija uzraudzīs to īstenošanu, piemērošanu un atbilstību tiem. Komisijai regula būs jāizvērtē un jāpārskata un jāsniedz par to publisks ziņojums Eiropas Parlamentam un Padomei 36 mēnešos pēc piemērošanas dienas un pēc tam reizi četros gados.

• Detalizēts konkrētu priekšlikuma noteikumu skaidrojums

Vispārīgie noteikumi (I nodaļa)

Šī ierosinātā regula nosaka a) noteikumus par produktu ar digitāliem elementiem laišanu tirgū, lai nodrošinātu šādu produktu kiberdrošību; b) pamatprasības attiecībā uz produktu ar digitāliem elementiem projektēšanu, izstrādi un ražošanu, kā arī ar šiem produktiem saistītos uzņēmēju pienākumus attiecībā uz kiberdrošību; c) pamatprasības par ievainojamību novēršanas procesiem, ko ražotāji ieviesuši, lai attiecībā uz produktiem ar digitāliem elementiem nodrošinātu kiberdrošību visā aprites ciklā, kā arī ar šiem procesiem saistītos uzņēmēju pienākumus; d) noteikumus par tirgus uzraudzību un iepriekš minēto noteikumu un prasību izpildes panākšanu.

Ierosinātā regula attieksies uz visiem produktiem ar digitāliem elementiem, kuru paredzētais un pamatoti paredzamais lietojums ietver tiešu vai netiešu loģisku vai fizisku datu savienojumu ar ierīci vai tīklu.

Ierosinātā regula neattieksies uz produktiem ar digitāliem elementiem, kuri ietilpst Regulas (ES) 2017/745 [cilvēkiem paredzētas medicīniskas ierīces un šādu ierīču piederumi] un Regulas (ES) 2017/746 [cilvēkiem paredzētas in vitro diagnostikas medicīniskas ierīces un šādu ierīču piederumi] darbības jomā, jo abās regulās ir ietvertas prasības attiecībā uz ierīcēm, ieskaitot prasības attiecībā uz programmatūru, un vispārīgie ražotāju pienākumi, kas aptver visu produktu aprites ciklu, kā arī atbilstības novērtēšanas procedūras. Šī regula neattieksies

[12] 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.).

uz produktiem ar digitāliem elementiem, kuri sertificēti saskaņā ar Regulu 2018/1139 [augsts, vienveidīgs civilās aviācijas drošības līmenis], ne arī uz produktiem, kuriem piemēro Regulu (ES) 2019/2144 [par prasībām mehānisko transportlīdzekļu un to piekabju un šiem transportlīdzekļiem paredzētu sistēmu, komponentu un atsevišķu tehnisko vienību tipa apstiprināšanai].

Kritiski svarīgiem produktiem ar digitāliem elementiem piemēro īpašas atbilstības novērtēšanas procedūras, un tos, kā noteikts III pielikumā, iedala I klasē un II klasē, atspoguļojot to kiberdrošības riska līmeni, un II klasē ir produkti ar lielāku risku. Produkts ar digitāliem elementiem tiek uzskatīts par kritiski svarīgu un tādēļ iekļauts III pielikumā, ņemot vērā ietekmi, ko rada iespējamās kiberdrošības ievainojamības, kas ietvertas produktā ar digitāliem elementiem. Nosakot kiberdrošības risku, cita starpā tiek ņemta vērā ar kiberdrošību saistītā funkcionalitāte, kas piemīt produktam ar digitāliem elementiem, un paredzētais lietojums sensitīvās vidēs, piemēram, rūpnieciskajā vidē.

Komisija tiek arī pilnvarota pieņemt deleģētos aktus, lai papildinātu šo regulu, precizējot kategorijas ļoti kritiski svarīgiem produktiem ar digitāliem elementiem, attiecībā uz kurām ražotājiem ir jāsaņem Eiropas kiberdrošības sertifikāts saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu, lai pierādītu atbilstību I pielikumā vai tā daļās izklāstītajām pamatprasībām. Nosakot kategorijas šādiem ļoti kritiski svarīgiem produktiem ar digitāliem elementiem, Komisija ņem vērā kiberdrošības riska līmeni, kas saistīts ar produktu ar digitāliem elementiem kategoriju, ņemot vērā vienu vai vairākus kritērijus, kas tiek izvērtēti, lai III pielikumā iekļautu kritiski svarīgus produktus ar digitāliem elementiem, kā arī ņemot vērā novērtējumu par to, vai attiecīgo produktu kategoriju lieto vai uz to paļaujas Direktīvas [Direktīva XXX/XXXX (TID2)] pielikumā [I pielikums] minēto veidu būtiskās vienības, vai arī tai, iespējams, būs būtiska turpmākā nozīme šo vienību darbībās; vai tā attiecas uz produktu ar digitāliem elementiem vispārējās piegādes ķēdes noturību pret darbības traucējumiem.

Uzņēmēju pienākumi (II nodaļa)

Priekšlikumā ir ietverti ražotāju, importētāju un izplatītāju pienākumi, kas pamatoti uz Lēmumā Nr. 768/2008/EK paredzētajiem atsauces noteikumiem. Kiberdrošības pamatprasības un pienākumi nosaka, ka visus produktus ar digitāliem elementiem dara pieejamus tirgū tikai tad, ja — ar noteikumu, ka tie pienācīgi piegādāti, pareizi uzstādīti, uzturēti un lietoti paredzētajam nolūkam vai apstākļos, ko var pamatoti paredzēt, — tie atbilst šajā regulā izklāstītajām kiberdrošības pamatprasībām.

Pamatprasības un pienākumi noteiktu, ka ražotājiem jāņem vērā kiberdrošība, projektējot, izstrādājot un ražojot produktus ar digitāliem elementiem, jāveic drošības aspektu uzticamības pārbaude savu produktu projektēšanā un izstrādē, jānodrošina to kiberdrošības aspektu pārredzamība, kuri jādara zināmi klientiem, samērīgi jānodrošina drošības atbalsts (atjauninājumi) un jāievēro ievainojamību novēršanas prasības.

Attiecībā uz produktu ar digitāliem elementiem laišanu tirgū uzņēmējiem — sākot no ražotājiem, līdz pat izplatītājiem un importētājiem — tiktu noteikti pienākumi, kas atbilst viņu nozīmei un atbildībai piegādes ķēdē.

Produkta ar digitāliem elementiem atbilstība (III nodaļa)

Tiek pieņemts, ka produkts ar digitāliem elementiem, kas atbilst saskaņotajiem standartiem vai to daļām, uz kuriem atsauces ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, atbilst šajā ierosinātajā regulā noteiktajām pamatprasībām. Ja saskaņoto standartu nav vai tie nav pietiekami, vai ja standartizācijas procedūra ir nepamatoti aizkavējusies, vai ja Eiropas

standartizācijas organizācijas nav pieņēmušas Komisijas pieprasījumu, Komisija var pieņemt kopīgas specifikācijas, izmantojot īstenošanas aktus.

Turklāt produkti ar digitāliem elementiem, kas ir sertificēti vai par kuriem izdots ES atbilstības apliecinājums vai sertifikāts saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu atbilstīgi Regulai (ES) 2019/881 un attiecībā uz kuriem Komisija ar īstenošanas aktu ir norādījusi, ka tā var nodrošināt pieņēmumu par atbilstību šai regulai, ir uzskatāmi par atbilstīgiem šīs regulas vai tās daļu pamatprasībām, ciktāl ES atbilstības apliecinājums vai kiberdrošības sertifikāts vai tā daļas attiecas uz minētajām prasībām.

Turklāt, lai novērstu nevajadzīgu administratīvo slogu ražotājiem, Komisijai attiecīgā gadījumā būtu jāprecizē, vai saskaņā ar šādu Eiropas kiberdrošības sertifikācijas shēmu izdots kiberdrošības sertifikāts atceļ ražotāju pienākumu par trešās personas veiktu atbilstības novērtējumu, kā tas šajā regulā noteikts saistībā ar attiecīgajām prasībām.

Ražotājs veic atbilstības izvērtēšanu attiecībā uz produktu ar digitāliem elementiem un ieviestajiem ievainojamību novēršanas procesiem, lai pierādītu atbilstību I pielikumā noteiktajām pamatprasībām, ievērojot vienu no VI pielikumā izklāstītajām procedūrām. I un II klases kritiski svarīgo produktu ražotāji izmanto attiecīgos atbilstības nodrošināšanai nepieciešamos moduļus. II klases kritiski svarīgu produktu ražotājiem atbilstības novērtēšanā ir jāiesaista trešā persona.

Atbilstības novērtēšanas struktūru paziņošana (IV nodaļa)

Lai nodrošinātu augsta līmeņa kiberdrošību un panāktu visu ieinteresēto personu uzticēšanos jaunās pieejas sistēmai, ļoti svarīga ir paziņoto struktūru pienācīga darbība. Tādēļ, ņemot vērā Lēmumu 768/2008/EK, priekšlikumā ir izklāstītas prasības valstu iestādēm, kuras ir atbildīgas par atbilstības novērtēšanas struktūrām (paziņotajām struktūrām). Tajā galīgā atbildība par paziņoto struktūru izraudzīšanos un uzraudzību ir atstāta dalībvalstu ziņā. Dalībvalstis izraugās paziņojošo iestādi, kas ir atbildīga par tādu procedūru izveidi un veikšanu, kuras vajadzīgas, lai novērtētu un paziņotu atbilstības novērtēšanas struktūras un uzraudzītu paziņotās struktūras.

Tirgus uzraudzība un tās izpilde (V nodaļa)

Saskaņā ar Regulu (ES) 2019/1020 valstu tirgus uzraudzības iestādes veic tirgus uzraudzību attiecīgās dalībvalsts teritorijā. Dalībvalstis tirgus uzraudzības iestādes darbībai var izraudzīties jebkuru esošu vai jaunu iestādi, ieskaitot izveidotās valstu kompetentās iestādes, kas minētas Direktīvas [Direktīva XXX/XXXX (TID2)] pantā [X. pants], vai izraudzītās valsts kiberdrošības sertifikācijas iestādes, kas minētas Regulas (ES) 2019/881 58. pantā. Uzņēmēji tiek aicināti pilnībā sadarboties ar tirgus uzraudzības iestādēm un citām kompetentajām iestādēm.

Deleģētās pilnvaras un komiteju procedūras (VI nodaļa)

Nolūkā nodrošināt, ka vajadzības gadījumā tiesisko regulējumu var pielāgot, Komisijai saskaņā ar LESD 290. pantu tiek deleģētas pilnvaras pieņemt aktus attiecībā uz to, lai atjauninātu I un II klases kritiski svarīgo produktu sarakstu un precizētu šo produktu definīcijas; precizētu, vai ir nepieciešams ierobežojums vai izslēgšana attiecībā uz produktiem ar digitāliem elementiem, uz kuriem attiecas citi Savienības noteikumi, ar ko nosaka prasības, kas nodrošina tādu pašu aizsardzības līmeni kā šī regula; pilnvarotu noteiktu ļoti kritiski svarīgu produktu ar digitāliem elementiem sertificēšanu, pamatojoties uz šajā regulā noteiktajiem kritērijiem; precizētu ES atbilstības deklarācijas minimālo saturu un papildinātu tehniskajā dokumentācijā iekļaujamos elementus.

Komisija tiek arī pilnvarota pieņemt īstenošanas aktus, lai: precizētu ziņošanas pienākumu un programmatūras materiālu komplekta formātu vai elementus; norādītu Eiropas kiberdrošības sertifikācijas shēmas, kuras var izmantot, lai pierādītu atbilstību šajā regulā noteiktajām pamatprasībām vai to daļām; pieņemtu kopīgas specifikācijas; noteiktu *CE* zīmes uzlikšanas tehniskās specifikācijas; pieņemtu izņēmuma apstākļos Savienības līmenī veicamus korektīvus vai ierobežojošus pasākumus, kas pamato tūlītēju intervenci ar mērķi saglabāt iekšējā tirgus pareizu darbību.

Konfidencialitāte un sankcijas (VII nodaļa)

Visas puses, kas piemēro šo regulu, ievēro savu uzdevumu un darbību veikšanā iegūtās informāciju un datu konfidencialitāti.

Lai nodrošinātu šajā regulā noteikto pienākumu efektīvu izpildi, katrai tirgus uzraudzības iestādei vajadzētu būt pilnvarām uzlikt administratīvus naudas sodus vai pieprasīt to uzlikšanu. Tāpat ar šo regulu nosaka administratīvo naudas sodu maksimālos līmeņus, kas valstu tiesību aktos būtu jāparedz attiecībā uz šajā regulā noteikto pienākumu neizpildi.

Pārejas un nobeiguma noteikumi (VIII nodaļa)

Lai ražotājiem, paziņotajām struktūrām un dalībvalstīm dotu laiku pielāgoties jaunajām prasībām, ierosināto regulu sāks piemērot [24 mēnešus] pēc tās stāšanās spēkā, izņemot ražotājiem noteikto ziņošanas pienākumu, kas būtu piemērojams, sākot no [12 mēnešiem] pēc spēkā stāšanās dienas.

2022/0272 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulu (ES) 2019/1020

(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],

ņemot vērā Reģionu komitejas atzinumu[2],

saskaņā ar parasto likumdošanas procedūru,

tā kā:

(1) Ir 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 tirgū tiek laisti 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.

(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 [Direktīva XXX/XXXX (TID2)] un Eiropas Parlamenta un

[1] OV C , , . lpp.
[2] OV C , , . lpp.

Padomes Regula (ES) 2019/881[3], tieši neaptver produktu ar digitāliem elementiem drošības obligātās prasības.

(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, lai tie izpildītu vairākas prasības attiecībā uz līdzīgiem produktu veidiem. Šo produktu kiberdrošībai ir īpaši izteikta pārrobežu dimensija, jo vienā valstī ražotus produktus bieži izmanto organizācijas un patērētāji visā iekšējā tirgū. Tādēļ šī joma ir jāreglamentē Savienības līmenī. Savienības regulatīvā vide būtu jāsaskaņo, ieviešot kiberdrošības prasības attiecībā uz produktiem ar digitāliem elementiem. Turklāt būtu jānodrošina noteiktība attiecībā uz uzņēmējiem un lietotājiem visā Savienībā, kā arī vienotā tirgus labāka saskaņošana, radot labvēlīgākus apstākļus uzņēmējiem, kuru mērķis ir ienākt Savienības tirgū.

(5) Savienības līmenī dažādi programmatiski un politiski dokumenti (piemēram, ES kiberdrošības stratēģija digitālajai desmitgadei[4], Padomes 2020. gada 2. decembra un 2022. gada 23. maija secinājumi vai Eiropas Parlamenta 2021. gada 10. jūnija rezolūcija[5]) ir aicinājuši 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[6] pilsoņi aicināja "stiprināt ES lomu cīņā pret kiberdrošības apdraudējumiem".

(6) 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.

(7) 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 izmantot sānisko piekļuvi, lai pārvietotos starp sistēmām. Tāpēc ražotājiem būtu jānodrošina, ka visi savienojamie produkti ar digitāliem elementiem tiek projektēti un izstrādāti saskaņā ar šajā regulā noteiktajām pamatprasībām. Tas ietver gan produktus, kurus var fiziski savienot ar aparatūras saskarņu palīdzību, gan produktus, kuri ir loģiski savienoti, piemēram, izmantojot tīkla ligzdas, programmkanālus, datnes,

---

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

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

[6] *Konference par Eiropas nākotni, Ziņojums par galīgo rezultātu*, 2022. gada maijs, priekšlikums Nr. 28(2). Konference notika no 2021. gada aprīļa līdz 2022. gada maijam. Tas bija unikāls, pilsoņu vadīts Eiropas mēroga apspriešanās demokrātijas pasākums, kurā iesaistījās tūkstošiem Eiropas pilsoņu, kā arī politikas dalībnieki, sociālie partneri, pilsoniskās sabiedrības pārstāvji un galvenās ieinteresētās personas.

lietojumprogrammu saskarnes vai cita veida programmatūras saskarnes. Tā kā kiberdrošības apdraudējumi pirms noteikta mērķa sasniegšanas var izplatīties ar dažādiem produktiem ar digitāliem elementiem, piemēram, saķēdējot kopā vairākus ievainojamības izmantotājus, ražotājiem būtu arī jānodrošina to produktu kiberdrošība, kuri ir tikai netieši savienoti ar citām ierīcēm vai tīkliem.

(8) Nosakot kiberdrošības prasības produktu ar digitāliem elementiem laišanai tirgū, tiks uzlabota šo produktu kiberdrošība gan patērētājiem, gan uzņēmumiem. Tas ietver arī prasības tādu patēriņa preču ar digitāliem elementiem laišanai tirgū, kas paredzētas neaizsargātiem patērētājiem, piemēram, rotaļlietu un bērnu monitoru laišanai tirgū.

(9) Šī regula nodrošina augstu kiberdrošības līmeni produktiem ar digitāliem elementiem. Tā nereglamentē pakalpojumus, piemēram, programmatūras kā pakalpojuma sniegšanu (*SaaS*), izņemot attiecībā uz attālinātas datu apstrādes risinājumiem saistībā ar produktu ar digitāliem elementiem, to saprotot kā jebkādu attālinātu datu apstrādi, kurai programmatūru ir projektējis un izstrādājis vai par to ir bijis atbildīgs attiecīgā produkta ražotājs un kuras neesamība liegtu šādam produktam ar digitāliem elementiem pildīt kādu no savām funkcijām. [Direktīva XXX/XXXX (TID2)] ievieš kiberdrošības un incidentu paziņošanas prasības būtiskām un svarīgām vienībām, piemēram, kritiski svarīgai infrastruktūrai, lai palielinātu to sniegto pakalpojumu noturību. [Direktīva XXX/XXXX (TID2)] attiecas uz mākoņdatošanas pakalpojumiem un mākoņpakalpojumu modeļiem, piemēram, *SaaS*. Minētās direktīvas darbības jomā ietilpst visas vienības, kas Savienībā sniedz mākoņdatošanas pakalpojumus un kas ir sasniegušas vai pārsniedz robežvērtību attiecībā uz vidējiem uzņēmumiem.

(10) Lai nekavētu inovāciju vai pētniecību, šai regulai nebūtu jāattiecas uz bezmaksas un atklātā pirmkoda programmatūru, kas izstrādāta vai piegādāta, neveicot komercdarbību. Tas jo īpaši attiecas uz programmatūru, arī tās pirmkodu un modificētajām versijām, kas ir atklāti kopīgota un brīvi pieejama, izmantojama, maināma un pārdalāma. Programmatūras kontekstā komercdarbībai var būt raksturīga ne tikai cenas noteikšana par produktu, bet arī cenas noteikšana par tehniskā atbalsta pakalpojumiem, nodrošinot programmatūras platformu, ar kuras palīdzību ražotājs izsaka naudas izteiksmē citus pakalpojumus, vai persondatu izmantošana citu iemeslu dēļ, nevis tikai programmatūras drošības, savietojamības vai sadarbspējas uzlabošanai.

(11) Drošs internets ir neaizstājams kritiski svarīgās infrastruktūras darbībai un sabiedrībai kopumā. [Direktīvas XXX/XXXX (TID2)] mērķis ir nodrošināt augstu kiberdrošības līmeni pakalpojumiem, ko sniedz būtiskas un svarīgas vienības, to vidū digitālās infrastruktūras nodrošinātāji, kuri atbalsta atvērtā interneta pamatfunkcijas, nodrošina piekļuvi internetam un 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 XXX/XXXX (TID2)], 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.

(12) Eiropas Parlamenta un Padomes Regulā (ES) 2017/745[7] ir izklāstīti noteikumi par medicīniskajām ierīcēm, un Eiropas Parlamenta un Padomes Regulā (ES) 2017/746[8] – par *in vitro* diagnostikas medicīniskajām ierīcēm. Abas 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 pielikuma pamatprasības attiecībā uz kiberdrošību[9]. Tāpēc šai regulai nebūtu jāattiecas uz produktiem ar digitāliem elementiem, kam piemēro kādu no minētajām regulām.

(13) Eiropas Parlamenta un Padomes Regulā (ES) 2019/2144[10] 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 kiberriskiem, kas saistīti ar transportlīdzekļu, iekārtu un pakalpojumu visu aprites ciklu, saskaņā ar piemērojamajiem Apvienoto Nāciju Organizācijas noteikumiem par tehniskajām specifikācijām un kiberdrošību[11] un paredzot īpašas atbilstības novērtēšanas procedūras. 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

---

7 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.).

8 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.).

9 MDCG 2019-16, ko apstiprinājusi Medicīnisko ierīču koordinācijas grupa (*MDCG*), kas izveidota ar Regulas (ES) 2017/745 103. pantu.

10 Eiropas Parlamenta un Padomes Regula (ES) 2019/2144 (2019. gada 27. novembris) par prasībām mehānisko transportlīdzekļu un to piekabju un šiem transportlīdzekļiem paredzētu sistēmu, komponentu 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.).

11 ANO Noteikumi Nr. 155 – Vienoti noteikumi par transportlīdzekļu apstiprināšanu attiecībā uz kiberdrošību un kiberdrošības pārvaldības sistēmu [2021/387].

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.).

attiecībā uz lidojumderīgumu aeronavigācijas produktiem, daļām, ierīcēm, ieskaitot programmatūru, kurā ņemti vērā pienākumi aizsargāt pret informācijas drošības apdraudējumiem. Tāpēc uz produktiem ar digitāliem elementiem, kam piemēro Regulu (ES) 2019/2144, un uz šiem produktiem, kas sertificēti saskaņā ar Regulu (ES) 2018/1139, neattiecas šajā regulā noteiktās pamatprasības un atbilstības novērtēšanas procedūras. Saskaņā ar Regulu (EU) 2018/1139 noteiktais sertifikācijas process nodrošina tādu uzticamības līmeni, kas atbilst šīs regulas mērķim.

(14) 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 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 šīs regulas I pielikumā izklāstītās pamatprasības, var ierobežot vai izslēgt, ja šāds ierobežojums vai izslēgšana atbilst vispārējam tiesiskajam regulējumam, ko piemēro minētajiem produktiem, un ja nozares noteikumi nodrošina tādu pašu aizsardzības līmeni, kāds paredzēts šajā regulā. Komisija tiek pilnvarota pieņemt deleģētos aktus, lai grozītu 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.

(15) Deleģētajā regulā (ES) 2022/30 ir norādīts, ka Direktīvas 2014/53/ES 3. panta 3. punkta d) apakšpunktā (kaitējums tīklam un tīkla resursu pārmērīga izmantošana), e) apakšpunktā (persondati un privātums) un f) apakšpunktā (krāpšana) izklāstītās pamatprasības piemēro noteiktām radioiekārtām. [Komisijas Īstenošanas lēmumā XXX/2022 par standartizācijas pieprasījumu Eiropas standartizācijas organizācijām] ir noteiktas prasības īpašu standartu izstrādei, papildus precizējot, kā šīs trīs pamatprasības būtu jārisina. Šajā regulā noteiktās pamatprasības ietver visus Direktīvas 2014/53/ES 3. panta 3. punkta d), e) un f) apakšpunktā minēto pamatprasību elementus. Turklāt šajā regulā noteiktās pamatprasības ir saskaņotas ar minētajā standartizācijas pieprasījumā iekļauto īpašo standartu prasību mērķiem. Turklāt, ja 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 Komisijas Īstenošanas lēmumu C(2022)5637 par standartizācijas pieprasījumu attiecībā uz Radioiekārtu direktīvas Deleģēto regulu 2022/30, saskaņoto standartu sagatavošanā un izstrādē ar mērķi sekmēt šīs regulas īstenošanu.

(16) Direktīva 85/374/EEK[13] 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 šādu drošuma trūkumu veido drošības atjauninājumu trūkums pēc produkta laišanas tirgū un tas rada kaitējumu, varētu iestāties ražotāja atbildība. Šajā regulā būtu

[13] Padomes Direktīva 85/374/EEK (1985. gada 25. jūlijs) par dalībvalstu normatīvo un administratīvo aktu tuvināšanu attiecībā uz atbildību par produktiem ar trūkumiem (OV L 210, 7.8.85.).

jānosaka ražotāju pienākumi, kas attiecas uz šādu drošības atjauninājumu nodrošināšanu.

(17) Šai regulai nebūtu jāskar Eiropas Parlamenta un Padomes Regula (ES) 2016/679[14], ieskaitot noteikumus par 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 galvenie Regulas (ES) 2016/679 elementi. Aizsargājot patērētājus un organizācijas no kiberdrošības riskiem, šajā regulā noteiktajām kiberdrošības pamatprasībām ir arī jāpalīdz uzlabot persondatu 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 (EDAK) 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 aktus. Tām vajadzētu būt arī piekļuvei informācijai, kas ir būtiska tām paredzēto uzdevumu veikšanai.

(18) Eiropas digitālās identitātes maku izdevējiem, kas minēti attiecīgajā pantā [Regulas (ES) Nr. 910/2014, kurā grozījumi izdarīti ar priekšlikumu regulai, ar ko Regulu (ES) Nr. 910/2014 groza attiecībā uz Eiropas digitālās identitātes regulējuma izveidi, 6.a panta 2. punkts], ciktāl to produkti ietilpst šīs regulas darbības jomā, būtu jāievēro gan ar šo regulu noteiktās horizontālās pamatprasības, gan īpašās drošības prasības, kas noteiktas ar [Regulas (ES) Nr. 910/2014, kurā grozījumi izdarīti ar priekšlikumu regulai, ar ko Regulu (ES) Nr. 910/2014 groza attiecībā uz Eiropas digitālās identitātes regulējuma izveidi, 6.a pants] pantu. Lai sekmētu atbilstību, maku izdevējiem būtu jāspēj pierādīt Eiropas digitālās identitātes maku atbilstību abos tiesību aktos attiecīgi noteiktajām prasībām, sertificējot savus produktus saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu, kas izveidota atbilstīgi Regulai (ES) 2019/881 un attiecībā uz kuru Komisija ar īstenošanas aktu ir noteikusi pieņēmumu par atbilstību šai regulai, ciktāl sertifikāts vai tā daļas attiecas uz minētajām prasībām.

(19) Daži šajā regulā paredzētie uzdevumi būtu jāveic *ENISA* saskaņā ar Regulas (ES) 2019/881 3. panta 2. punktu. Konkrēti *ENISA* būtu jāsaņem ražotāju paziņojumi par aktīvi izmantotām ievainojamībām produktos ar digitāliem elementiem, kā arī par incidentiem, kuri ietekmē minēto produktu drošību. *ENISA* būtu arī jāpārsūta šie paziņojumi attiecīgajām datordrošības incidentu reaģēšanas vienībām (*CSIRT*) vai attiecīgi noteiktajiem dalībvalstu vienotajiem kontaktpunktiem, kas izraudzīti saskaņā ar Direktīvas [Direktīva XXX/XXXX (TID2)] pantu [X. pants], kā arī par paziņoto ievainojamību jāinformē attiecīgās tirgus uzraudzības iestādes. *ENISA*, pamatojoties uz savākto informāciju, reizi divos gados būtu jāsagatavo tehniskais ziņojums par jaunākajām tendencēm attiecībā uz kiberdrošības riskiem produktos ar

[14] 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.).

digitāliem elementiem, un tas jāiesniedz Direktīvā [Direktīva XXX/XXXX (TID2)] minētajai sadarbības grupai. Turklāt, ņemot vērā *ENISA* speciālās zināšanas un pilnvaras, tai būtu jāspēj atbalstīt šīs regulas īstenošanas procesu. Jo īpaši tai vajadzētu būt iespējai 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 vienlaicīgas koordinētas kontroles darbības. Izņēmuma apstākļos pēc Komisijas pieprasījuma *ENISA* vajadzētu būt iespējai 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.

(20) Produkti ar digitāliem elementiem būtu jāmarķē ar *CE* zīmi, kas 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.

(21) Lai nodrošinātu, ka ražotāji pirms savu produktu atbilstības novērtēšanas var izlaist programmatūru testēšanas vajadzībām, dalībvalstīm nevajadzētu liegt darīt pieejamu nepabeigtu programmatūru, piemēram, alfa versijas, beta versijas vai izlaišanas kandidātus, ja vien versija ir pieejama tikai uz laiku, kas nepieciešams tās testēšanai un atsauksmju vākšanai. 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 arī jāīsteno ievainojamību novēršanas prasības. Ražotājiem nevajadzētu piespiest lietotājus veikt jauninājumu uz versijām, kas ir izlaistas tikai testēšanas vajadzībām.

(22) Lai nodrošinātu, ka, laižot tirgū produktus ar digitāliem elementiem, tie nerada kiberdrošības riskus personām un organizācijām, šādiem produktiem būtu jānosaka pamatprasības. Ja šādi produkti pēc tam ar fiziskiem vai digitāliem līdzekļiem tiek modificēti tā, kā ražotājs nav paredzējis, un tas varētu nozīmēt, ka tie vairs neatbilst attiecīgajām pamatprasībām, modifikācija būtu jāuzskata par būtisku. Piemēram, programmatūras atjauninājumus vai labojumus varētu pielīdzināt uzturēšanas darbībām ar noteikumu, ka tie nemodificē jau tirgū laistu produktu tā, ka var tikt ietekmēta atbilstība piemērojamajām prasībām, vai ka var tikt mainīts paredzētais lietojums, attiecībā uz kuru produkts ir izvērtēts. Tāpat kā attiecībā uz fiziskiem labojumiem vai modifikācijām produkts ar digitāliem elementiem būtu jāuzskata par būtiski modificētu ar programmatūras izmaiņām, ja programmatūras atjauninājums modificē produkta sākotnējās paredzētās funkcijas, veidu vai veiktspēju un šīs izmaiņas nav bijušas paredzētas sākotnējā riska novērtējumā vai ja ir mainījies apdraudējuma veids vai paaugstinājies riska līmenis programmatūras atjaunināšanas dēļ.

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

(24) Produkta ar digitāliem elementiem atjaunošana, uzturēšana un labošana, kā noteikts Regulā [Ekodizaina regula], ne vienmēr izraisa produkta būtisku modifikāciju, piemēram, ja paredzētais lietojums un funkcijas netiek mainītas un netiek ietekmēts riska līmenis. Tomēr ražotāja veikta produkta jauninašana varētu izraisīt izmaiņas produkta projektēšanā un izstrādē un tādējādi varētu ietekmēt produkta paredzēto lietojumu un atbilstību šajā regulā noteiktajām prasībām.

(25) Produkti ar digitāliem elementiem būtu jāuzskata par kritiski svarīgiem, ja produkta iespējamo kiberdrošības ievainojamību izmantošanas negatīvā ietekme var būt būtiska, cita starpā ar kiberdrošību saistītas funkcionalitātes vai paredzētā lietojuma dēļ. Jo īpaši tādu produktu ar digitāliem elementiem ievainojamība, kam ir ar kiberdrošību saistīta funkcionalitāte, piemēram, drošie elementi, var izraisīt drošības problēmu izplatīšanos visā piegādes ķēdē. Kiberdrošības incidenta ietekmes nopietnības pakāpe varētu pieaugt arī, ja tiek ņemts vērā produkta paredzētais lietojums, piemēram, rūpnieciskajā vidē vai saistībā ar Direktīvas [Direktīva XXX/XXXX (TID2)] pielikumā [I pielikums] minēto veidu būtiskajām vienībām, vai attiecībā uz tādu kritiski svarīgu vai sensitīvu funkciju veikšanu kā, piemēram, persondatu apstrāde.

(26) Kritiski svarīgiem produktiem ar digitāliem elementiem būtu jāpiemēro stingrākas atbilstības novērtēšanas procedūras, vienlaikus saglabājot samērīgu pieeju. Šajā nolūkā kritiski svarīgi produkti ar digitāliem elementiem būtu jāiedala divās klasēs, kas atspoguļo ar šīm produktu kategorijām saistītā kiberdrošības riska līmeni. Iespējamam kiberincidentam, kurā iesaistīti II klases produkti, varētu būt lielāka negatīvā ietekme nekā incidentam, kurā iesaistīti I klases produkti, piemēram, attiecīgo produktu ar kiberdrošību saistītās funkcijas rakstura vai sensitīvā vidē paredzētā lietojuma dēļ, un tāpēc tam būtu jāpiemēro stingrāka atbilstības novērtēšanas procedūra.

(27) Šīs regulas III pielikumā minētās kritiski svarīgo produktu ar digitāliem elementiem kategorijas būtu jāsaprot kā produkti, kuru pamatfunkcijas veids ir ietverts šīs regulas III pielikumā sniegtajā sarakstā. Piemēram, šīs regulas III pielikumā ir uzskaitīti produkti, kas pēc to pamatfunkcijas ir noteikti kā vispārēja lietojuma mikroprocesori un ir ietverti II klasē. Tādējādi uz vispārēja lietojuma mikroprocesoriem attiecas obligāts trešās personas veikts atbilstības novērtējums. Tas neattiecas uz citiem produktiem, kuri nav skaidri norādīti šīs regulas III pielikumā un kuros var būt integrēts vispārēja lietojuma mikroprocesors. Komisijai [12 mēnešos no šīs regulas stāšanās spēkā] būtu jāpieņem deleģētie akti, lai precizētu I un II klases produktu kategoriju definīcijas, kā noteikts III pielikumā.

(28) Šī regula mērķtiecīgi pievēršas kiberdrošības riskiem. Tomēr produkti ar digitāliem elementiem var radīt citus drošības riskus, kas nav saistīti ar kiberdrošību. Minētie riski arī turpmāk būtu jāreglamentē ar citiem attiecīgiem Savienības tiesību aktiem par produktiem. Ja nav piemērojami citi Savienības saskaņošanas tiesību akti, uz tiem būtu jāattiecina Regula [Ražojumu vispārēja drošuma regula]. Tāpēc, ņemot vērā šīs regulas mērķtiecīgo raksturu, atkāpjoties no Regulas [Ražojumu vispārēja drošuma regula] 2. panta 1. punkta trešās daļas b) apakšpunkta, ja uz produktiem ar digitāliem elementiem neattiecas īpašas prasības, kas noteiktas citos Savienības saskaņošanas tiesību aktos [Ražojumu vispārēja drošuma regulas 3. panta 25. punkta] nozīmē, minētajiem produktiem attiecībā uz šajā regulā neietvertiem drošības riskiem būtu jāpiemēro Regulas [Ražojumu vispārēja drošuma regula] III nodaļas 1. iedaļu, V un VII nodaļu un IX–XI nodaļu.

(29) Produktiem ar digitāliem elementiem, kas klasificēti kā augsta riska MI sistēmas saskaņā ar Regulas[15] [MI regula] 6. pantu un kas ietilpst šīs regulas darbības jomā, būtu jāatbilst šajā regulā noteiktajām pamatprasībām. Ja šīs augsta riska MI sistēmas atbilst šīs regulas pamatprasībām, tās būtu jāuzskata par atbilstošām Regulas [MI regula] pantā [15. pants] noteiktajām kiberdrošības prasībām, ciktāl uz šīm prasībām attiecas ES atbilstības deklarācija vai tās daļas, kas izdotas atbilstīgi šai regulai. Attiecībā uz atbilstības novērtēšanas procedūrām, kas saistītas ar kiberdrošības pamatprasībām produktam ar digitāliem elementiem, uz kuru attiecas šī regula un kurš klasificēts kā augsta riska MI sistēma, šīs regulas attiecīgo noteikumu vietā parasti būtu jāpiemēro attiecīgie Regulas [MI regula] 43. panta noteikumi. Tomēr šā noteikuma piemērošanai nevajadzētu samazināt nepieciešamo uzticamības līmeni attiecībā uz šajā regulā ietvertajiem kritiski svarīgajiem produktiem ar digitāliem elementiem. Tāpēc, atkāpjoties no šā noteikuma, augsta riska MI sistēmām, kuras ietilpst Regulas [MI regula] darbības jomā un kuras saskaņā ar šo regulu arī tiek kvalificētas kā kritiski svarīgi produkti ar digitāliem elementiem, un uz kurām attiecas Regulas [MI regula] VI pielikumā minētā uz iekšējo kontroli pamatotā atbilstības novērtēšanas procedūra, būtu jāpiemēro šīs regulas atbilstības novērtēšanas noteikumi, ciktāl tas attiecas uz šīs regulas pamatprasībām. Šajā gadījumā attiecībā uz visiem pārējiem Regulā [MI regula] ietvertajiem aspektiem būtu jāpiemēro attiecīgie uz iekšējo kontroli pamatotas atbilstības izvērtēšanas noteikumi, kas izklāstīti Regulas [MI regula] VI pielikumā.

(30) Mašīnbūves izstrādājumi, kuri ietilpst Regulas [Mašīnu regulas priekšlikums] darbības jomā un kuri ir produkti ar digitāliem elementiem šīs regulas nozīmē, un par kuriem uz šīs regulas pamata ir izdota atbilstības deklarācija, būtu jāuzskata par atbilstīgiem veselības aizsardzības un drošības pamatprasībām, kas izklāstītas Regulas [Mašīnu regulas priekšlikums] [III pielikuma 1.1.9. un 1.2.1. iedaļā] attiecībā uz aizsardzību pret korupciju un vadības sistēmu drošumu un uzticamību, ciktāl atbilstību minētajām prasībām pierāda saskaņā ar šo regulu izdota ES atbilstības deklarācija.

(31) Regula [Eiropas veselības datu telpas regulas priekšlikums] papildina šajā regulā noteiktās pamatprasības. Tāpēc e-veselības pacienta karšu sistēmām ("EVPK sistēmas"), kuras ietilpst Regulas [Eiropas veselības datu telpas regulas priekšlikums] darbības jomā un kuras ir produkti ar digitāliem elementiem šīs regulas nozīmē, būtu jāatbilst arī šajā regulā noteiktajām pamatprasībām. To ražotājiem būtu jāpierāda atbilstība, kā tas noteikts Regulā [Eiropas veselības datu telpas regulas priekšlikums]. Lai sekmētu atbilstību, ražotāji var izstrādāt vienotu tehnisko dokumentāciju, kurā ietverti abos tiesību aktos prasītie elementi. Tā kā šī regula neattiecas uz *SaaS* kā tādu, EVPK sistēmas, kas tiek piedāvātas ar *SaaS* licencēšanas un piegādes modeļa starpniecību, neietilpst šīs regulas darbības jomā. Tāpat EVPK sistēmas, kas ir izstrādātas un tiek lietotas uz vietas, neietilpst šīs regulas darbības jomā, jo tās netiek laistas tirgū.

(32) Lai nodrošinātu, ka produkti ar digitāliem elementiem ir droši gan brīdī, kad tos laiž tirgū, gan visā to aprites ciklā, ir jānosaka ievainojamību novēršanas pamatprasības un kiberdrošības pamatprasības attiecībā uz produktu ar digitāliem elementiem īpašībām. Lai gan ražotājiem būtu jāievēro visas ar ievainojamību novēršanu saistītās pamatprasības un jānodrošina, ka visi viņu produkti tiek piegādāti bez zināmām izmantojamām ievainojamībām, tiem būtu jānosaka, kuras citas ar produktu īpašībām

[15] Regula [MI regula].

saistītas pamatprasības ir būtiskas attiecīgajam produktu veidam. Šajā nolūkā ražotājiem būtu jāveic ar produktu ar digitāliem elementiem saistīto kiberdrošības risku novērtējums, lai konstatētu attiecīgos riskus un attiecīgās pamatprasības, kā arī lai pienācīgi piemērotu atbilstošus saskaņotos standartus vai kopīgas specifikācijas.

(33) Lai uzlabotu drošību attiecībā uz produktiem ar digitāliem elementiem, kurus laiž iekšējā tirgū, ir jānosaka pamatprasības. Šīm pamatprasībām nebūtu jāskar kritiski svarīgo piegādes ķēžu ES koordinētie riska novērtējumi, kas noteikti Direktīvas [Direktīva XXX/XXXX(TID2)][16] [X. pantā], kuros tiek ņemti vērā gan tehniski, gan attiecīgā gadījumā netehniski riska faktori, piemēram, nepamatota trešās valsts ietekme uz piegādātājiem. Turklāt nebūtu jāskar dalībvalstu prerogatīvas noteikt papildu prasības, kurās augsta noturības līmeņa nodrošināšanai tiek ņemti vērā netehniski faktori, arī tie, kas noteikti Ieteikumā (ES) 2019/534, Savienības mēroga koordinētajā 5G tīklu drošības riska novērtējumā un ES rīkkopā par 5G kiberdrošību, kuru saskaņojusi TID sadarbības grupa, kā minēts [Direktīvā XXX/XXXX (TID2)].

(34) Lai nodrošinātu, ka valstu *CSIRT* un vienotajiem kontaktpunktiem, kas izraudzīti atbilstīgi Direktīvas [Direktīva XX/XXXX (TID2)] pantam [X. pants], tiek sniegta informācija, kas nepieciešama to uzdevumu izpildei un būtisko un svarīgo vienību vispārējā kiberdrošības līmeņa paaugstināšanai, un lai nodrošinātu tirgus uzraudzības iestāžu efektīvu darbību, produktu ar digitāliem elementiem ražotājiem būtu jāpaziņo *ENISA* par aktīvi izmantotām ievainojamībām. 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. Ražotājiem būtu arī jāapsver iespēja atklāt izlabotās ievainojamības Eiropas ievainojamību datubāzē, kas izveidota saskaņā ar Direktīvu [Direktīva XX/XXXX (TID2)] un ko pārvalda *ENISA*, vai saskaņā ar jebkuru citu publiski pieejamu ievainojamību datubāzi.

(35) Ražotājiem būtu arī jāziņo *ENISA* par jebkuru incidentu, kas ietekmē produkta ar digitāliem elementiem drošību. Neskarot Direktīvā [Direktīva XXX/XXXX (TID2)] būtiskām un svarīgām vienībām noteiktos pienākumus ziņot par incidentiem, ir ļoti svarīgi, lai *ENISA*, vienotie kontaktpunkti, ko dalībvalstis izraudzījušās saskaņā ar direktīvas [Direktīva XXX/XXXX (TID2)] pantu [X. pantu], un tirgus uzraudzības iestādes no produktu ar digitāliem elementiem ražotājiem saņemtu informāciju, kas ļautu tiem novērtēt minēto produktu drošību. Lai nodrošinātu, ka lietotāji var ātri reaģēt uz 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 riski to pamato, tiešā veidā vēršoties pie lietotājiem.

(36) Produktu ar digitāliem elementiem ražotājiem būtu jāievieš koordinēta ievainojamības atklāšanas politika, lai sekmētu personu vai vienību ziņošanu par ievainojamībām. 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

[16] Eiropas Parlamenta un Padomes Direktīva XXX ([datums]), [ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148 (OV L xx, datums, x. lpp.)].

darīta zināma trešām personām vai sabiedrībai. 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 (tā dēvētās "atlīdzības par kļūdām programmas").

(37) Lai sekmētu ievainojamības analīzi, ražotājiem būtu jāidentificē un jādokumentē produktu ar digitāliem elementiem komponenti, arī sagatavojot programmatūras materiālu komplektu. Tiem, kas ražo, pērk un ekspluatē programmatūru, programmatūras materiālu komplekts 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 risku izsekošanu. Ražotājiem ir īpaši svarīgi nodrošināt, ka viņu produkti nesatur trešo personu izstrādātus neaizsargātus komponentus.

(38) 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 šīs regulas pamatprasības pārveidotas sīki izstrādātās tehniskajās specifikācijās un kuri tiek pieņemti saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1025/2012[17]. Regulā (ES) Nr. 1025/2012 paredzēta kārtība iebildumu iesniegšanai par saskaņotajiem standartiem, ja minētie standarti pilnībā neatbilst šīs regulas prasībām.

(39) Ar Regulu (ES) 2019/881 ir izveidots brīvprātīgs Eiropas kiberdrošības sertifikācijas satvars IKT produktiem, procesiem un pakalpojumiem. Eiropas kiberdrošības sertifikācijas shēmas var attiekties uz tiem produktiem ar digitāliem elementiem, kuri ietverti šajā regulā. 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 kiberdrošības shēmu atbilstīgi Regulai (ES) 2019/881 un kurus Komisija identificējusi īstenošanas aktā, atbilst šīs regulas pamatprasībām, ciktāl 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. Šādās turpmākās Eiropas kiberdrošības sertifikācijas shēmās, kas attiecas uz produktiem ar digitāliem elementiem, būtu jāņem vērā šajā regulā noteiktās pamatprasības, un tām būtu jāsekmē atbilstība šai regulai. Komisija būtu jāpilnvaro ar īstenošanas aktiem precizēt Eiropas kiberdrošības sertifikācijas shēmas, kuras var izmantot, lai pierādītu atbilstību šajā regulā noteiktajām pamatprasībām. Turklāt, lai novērstu nevajadzīgu administratīvo slogu ražotājiem, Komisijai attiecīgā gadījumā būtu jāprecizē, vai saskaņā ar šādām Eiropas kiberdrošības sertifikācijas shēmām izdots kiberdrošības sertifikāts atceļ ražotāju pienākumu par trešās personas veiktu atbilstības novērtējumu, kā tas šajā regulā noteikts saistībā ar attiecīgajām prasībām.

---

[17] 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.).

(40) Stājoties spēkā īstenošanas aktam, ar ko nosaka [Komisijas Īstenošanas regulu (ES) Nr. .../... (XXX) par Eiropas uz kopējiem kritērijiem pamatotu kiberdrošības sertifikācijas shēmu] (*EUCC*), kas attiecas uz šajā regulā ietvertajiem aparatūras produktiem, piemēram, aparatūras drošības moduļiem un mikroprocesoriem, Komisija ar īstenošanas aktu var precizēt, kā *EUCC* izdara pieņēmumu par atbilstību šīs regulas I pielikumā vai tā daļās minētajām pamatprasībām. Turklāt šādā īstenošanas aktā var precizēt veidu, kā atbilstīgi *EUCC* izdots sertifikāts atceļ ražotāju pienākumu nodrošināt trešās personas veiktu novērtējumu, kas attiecībā uz atbilstošajām prasībām noteikts regulā.

(41) Ja saskaņotie standarti netiek pieņemti vai ja saskaņotajos standartos nav pietiekami ņemtas vērā šīs regulas pamatprasības, Komisijai vajadzētu būt iespējai ar īstenošanas aktiem pieņemt kopīgas specifikācijas. Iemesli tam, lai izstrādātu šādas kopīgas specifikācijas, nevis paļautos uz saskaņotajiem standartiem, varētu būt jebkuras Eiropas standartizācijas organizācijas atteikums attiecībā uz standartizācijas pieprasījumu, nepamatota kavēšanās atbilstīgu saskaņoto standartu izveidē vai izstrādāto standartu neatbilstība šīs regulas prasībām vai Komisijas pieprasījumam. Lai sekmētu novērtējumu par atbilstību šajā regulā noteiktajām 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 sīki izstrādātas minēto prasību tehniskās specifikācijas.

(42) Ražotājiem būtu jāsagatavo ES atbilstības deklarācija, tajā sniedzot šajā regulā prasīto informāciju par produktu ar digitāliem elementiem atbilstību šīs regulas pamatprasībām un vajadzības gadījumā prasībām, kas noteiktas citos attiecīgos Savienības saskaņošanas tiesību aktos, kuros ietverts konkrētais produkts. 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.

(43) *CE* zīme, kas norāda uz produkta atbilstību, ir redzamais rezultāts veselam procesam, kas plašākā nozīmē ietver arī atbilstības novērtējumu. Vispārējie principi, kas reglamentē *CE* zīmi, ir izklāstīti Eiropas Parlamenta un Padomes Regulā (EK) Nr. 765/2008[18]. 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 šīs regulas prasībām.

(44) Lai uzņēmēji varētu pierādīt atbilstību šajā regulā noteiktajām pamatprasībām 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[19] 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 procedūras, kas piemērotas

---

18 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.).

19 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.).

tam, lai verificētu produktu atbilstību šajā regulā noteiktajām pamatprasībām, ir pamatotas 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 plānošanu, projektēšanu, izstrādi vai ražošanu, testēšanu un uzturēšanu.

(45) Atbilstības novērtēšana attiecībā uz produktiem ar digitāliem elementiem parasti būtu jāveic ražotājam uz savu atbildību, ievērojot procedūru, kas pamatota uz Lēmuma 768/2008/EK A moduli. Ražotājam būtu jāsaglabā rīcības brīvība izvēlēties stingrāku atbilstības novērtēšanas procedūru, kurā tiktu iesaistīta trešā persona. Ja produkts ir klasificēts kā I klases kritiski svarīgs produkts, ir vajadzīga papildu garantija, lai pierādītu atbilstību šajā regulā noteiktajām pamatprasībām. Ražotājam, ja tas vēlas veikt atbilstības novērtēšanu uz savu atbildību (A modulis), būtu jāpiemēro saskaņotie standarti, kopīgās specifikācijas vai Regulā (ES) 2019/881 noteiktās kiberdrošības sertifikācijas shēmas, ko Komisija ir identificējusi īstenošanas aktā. Ja ražotājs nepiemēro šādus saskaņotos standartus, kopīgās specifikācijas vai kiberdrošības sertifikācijas shēmas, ražotājam būtu jāveic atbilstības novērtēšana, kurā tiek iesaistīta trešā persona. 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 kritiski svarīgu produktu atbilstību digitālajiem elementiem kā vispiemērotākās ir izvēlētas atbilstības novērtēšanas procedūras, kas attiecīgi pamatojas uz Lēmuma 768/2008/EK B+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 produktu lietošanu, kuri klasificēti kā II klases kritiski svarīgie produkti, atbilstības izvērtēšanā vienmēr būtu jāiesaista trešā persona.

(46) 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 šīs regulas pamatprasībām visos projektēšanas, izstrādes un ražošanas posmos, šīs darbības būtu jāuzskata par ražošanu veidojošām darbībām.

(47) 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.

(48) 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.

(49) 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 normatīvajām prasībām.

(50) Atbilstības novērtēšanas struktūras bieži piešķir apakšlīgumus par kādām to darbības daļām saistībā ar atbilstības novērtēšanu vai izmanto meitasuzņēmumus. 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.

(51) 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.

(52) 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.

(53) Konkurētspējai 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 tehniskā piemērošanā. Vislabāk to var panākt ar atbilstīgu koordinēšanu un sadarbību starp paziņotajām struktūrām.

(54) 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[20] paredzētos noteikumus par Savienības tirgus uzraudzību un kontroli attiecībā uz produktiem, ko ieved Savienības tirgū, piemēro produktiem ar digitāliem elementiem, uz kuriem attiecas šī regula.

(55) Saskaņā ar Regulu (ES) 2019/1020 tirgus uzraudzības iestādes veic tirgus uzraudzību attiecīgās dalībvalsts teritorijā. Šai regulai nebūtu jāliedz dalībvalstīm izraudzīties kompetentās iestādes minēto uzdevumu veikšanai. Katrai dalībvalstij savā teritorijā būtu jāizraugās viena vai vairākas tirgus uzraudzības iestādes. Dalībvalstis tirgus uzraudzības iestādes darbībai var izraudzīties jebkuru esošu vai jaunu iestādi, to vidū valsts kompetentās iestādes, kas minētas Direktīvas [Direktīva XXX/XXXX (TID2)] pantā [X. pants], vai izraudzītās valsts kiberdrošības sertifikācijas iestādes, kas minētas Regulas (ES) 2019/881 58. pantā. Uzņēmējiem būtu pilnībā jāsadarbojas ar tirgus uzraudzības iestādēm un citām kompetentajām iestādēm. Katrai dalībvalstij būtu

[20] 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.).

jāinformē Komisija un pārējās dalībvalstis par savām tirgus uzraudzības iestādēm un par katras minētās iestādes kompetences jomu un jānodrošina ar šo regulu saistīto 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.

(56) Šīs regulas vienotai piemērošanai būtu jāizveido īpaša administratīvās sadarbības grupa (*ADCO*), ievērojot Regulas (ES) 2019/1020 30. panta 2. punktu. Šīs *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, pamatojoties uz Regulas (ES) 2019/1020 29. pantu, un kurā piedalās pārstāvji no katras dalībvalsts, to vidū pārstāvis no katra vienotā sadarbības biroja, kas minēts Regulas (ES) 2019/1020 10. pantā, kā arī fakultatīvs valsts eksperts, *ADCO* priekšsēdētāji un Komisijas pārstāvji. Komisijai būtu jāpiedalās minētā tīkla, tā apakšgrupu un attiecīgās *ADCO* sanāksmēs. Tai arī būtu jāpalīdz šai *ADCO*, izmantojot izpildsekretariātu, kas sniedz tehnisko un loģistikas atbalstu.

(57) Lai nodrošinātu savlaicīgus, samērīgus un efektīvus pasākumus attiecībā uz produktiem ar digitāliem elementiem, kas rada būtisku kiberdrošības risku, būtu jāparedz 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 turpmāk nebūtu jāiesaistās, izņemot gadījumus, kad neatbilstība var būt izskaidrojama ar saskaņotā standarta nepilnībām.

(58) Noteiktos gadījumos produkts ar digitāliem elementiem, kas atbilst šai regulai, tomēr var radīt būtisku kiberdrošības risku vai izraisīt risku personu 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 [Direktīvas XXX/XXXX (TID2) I pielikumā] minēto veidu būtiskās vienības, 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 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, 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, Komisija var arī apsvērt iespēju pieņemt priekšlikumus attiecīgo Savienības tiesību aktu pārskatīšanai.

(59) 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,

kuri atbilst šai regulai, bet rada citus nozīmīgus riskus, piemēram, riskus cilvēku veselībai vai drošībai, pamattiesībām vai tādu pakalpojumu sniegšanai, ko veic [Direktīvas XXX/XXXX (TID2) I pielikumā] minēto veidu būtiskās vienības, Komisija var pieprasīt *ENISA* veikt izvērtēšanu. Pamatojoties uz minēto izvērtējumu, Komisija ar īstenošanas aktiem var pieņemt korektīvus vai ierobežojošus pasākumus Savienības līmenī, arī uzdot attiecīgos produktus izņemt no tirgus vai atsaukt pienācīgā termiņā, kas samērīgs ar risku. Komisija var izmantot šādu intervenci tikai izņēmuma apstākļos, kas attaisno tūlītēju intervenci, lai saglabātu pareizu iekšējā tirgus darbību, un tikai tādā gadījumā, ja uzraudzības iestādes nav veikušas efektīvus pasākumus situācijas risināšanai. Šādi izņēmuma apstākļi var būt ārkārtas situācijas, kad, piemēram, ražotājs neatbilstīgu produktu ir darījis plaši pieejamu vairākās dalībvalstīs, to arī galvenajās nozarēs lieto vienības, kas ietilpst [Direktīvas XXX / XXXX (TID2)] darbības jomā, lai gan tam ir zināmas ievainojamības, kuras izmanto ļaundari un attiecībā uz kurām ražotājs nenodrošina pieejamus programmatūras ielāpus. Komisija šādās ārkārtas situācijās var iejaukties tikai uz laiku, kamēr pastāv izņēmuma apstākļi, un ja neatbilstība šai regulai vai radītie nozīmīgie riski saglabājas.

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

(61) Vienlaicīgas koordinētas kontroles darbības (“kontrolreidi”) ir tirgus uzraudzības iestāžu 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 kategorijas. *ENISA* būtu jāiesniedz tirgus uzraudzības iestādēm priekšlikumi par produktu kategorijām, attiecībā uz kurām varētu rīkot kontrolreidus, cita starpā pamatojoties tās saņemtajiem paziņojumiem par produktu ievainojamībām un incidentiem.

(62) Nolūkā nodrošināt, ka vajadzības gadījumā tiesisko regulējumu var pielāgot, saskaņā ar Līguma 290. pantu pilnvaras pieņemt aktus attiecībā uz III pielikumā sniegto kritiski svarīgo produktu saraksta atjaunināšanu un šo produktu kategoriju definīciju precizēšanu būtu jādeleģē Komisijai. 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 noteiktu ļoti kritiski svarīgu produktu ar digitāliem elementiem iespējamo sertificēšanas pilnvarojumu, pamatojoties uz kritiskuma kritērijiem, kas izklāstīti šajā regulā, kā arī attiecībā uz ES atbilstības deklarācijas minimālā satura noteikšanu un tehniskajā dokumentācijā iekļaujamo elementu papildināšanu. Ir īpaši būtiski, lai Komisija, veicot sagatavošanas darbus, rīkotu atbilstīgas apspriešanās, arī ekspertu līmenī, un lai minētās apspriešanās tiktu rīkotas saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu[21]. Jo īpaši, lai deleģēto aktu sagatavošanā nodrošinātu vienādu dalību, Eiropas Parlaments un Padome visus dokumentus saņem vienlaicīgi ar dalībvalstu ekspertiem, un minēto

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

iestāžu ekspertiem ir sistemātiska piekļuve Komisijas ekspertu grupu sanāksmēm, kurās notiek deleģēto aktu sagatavošana.

(63) Lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, īstenošanas pilnvaras būtu jāpiešķir Komisijai, lai precizētu programmatūras materiālu komplekta formātu un elementus, papildus precizētu informācijas veidu, formātu un procedūru attiecībā uz tiem paziņojumiem par aktīvi izmantotām ievainojamībām un incidentiem, ko ražotāji iesniedz *ENISA*, precizētu atbilstīgi Regulai (ES) 2019/881 pieņemtās Eiropas kiberdrošības sertifikācijas shēmas, kuras var izmantot, lai pierādītu atbilstību šīs regulas I pielikumā izklāstītajām pamatprasībām vai to daļām, pieņemtu kopīgas specifikācijas attiecībā uz I pielikumā izklāstītajām pamatprasībām, noteiktu tehniskās specifikācijas piktogrammām vai citām zīmēm, kas saistītas ar produktu ar digitāliem elementiem drošību, un mehānismus to lietošanas veicināšanai, lemtu par korektīviem vai ierobežojošiem pasākumiem Savienības līmenī izņēmuma apstākļos, kas pamato tūlītēju intervenci ar mērķi saglabāt pareizu iekšējā tirgus darbību. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011[22].

(64) 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.

(65) 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, arī tas, vai citas tirgus uzraudzības iestādes tam pašam uzņēmējam jau ir piemērojušas administratīvos naudas sodus par līdzīgiem pārkāpumiem. Šādi apstākļi var 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.

(66) 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.

(67) Eiropas Savienība attiecībās ar trešām valstīm *inter alia* cenšas veicināt reglamentēto produktu starptautisku tirdzniecību. Lai sekmētu tirdzniecību, var piemērot plašu

[22] 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.).

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 šiem 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 spēkā esoši SAN ir attiecībā uz vairākām valstīm. Šie nolīgumi attiecas uz vairākām konkrētām nozarēm, kas dažādās 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 partnervalstīm, lai stiprinātu kibernoturību visā pasaulē, jo ilgtermiņā tā sekmēs kiberdrošības satvara stiprināšanu gan Eiropas Savienībā, gan ārpus tās.

(68) Komisijai, apspriežoties ar ieinteresētajām personām, būtu periodiski jāpārskata šī regula, jo īpaši lai noteiktu izmaiņu veikšanas nepieciešamību, ņemot vērā izmaiņas sociālajos, politiskajos, tehnoloģiskajos vai tirgus apstākļos.

(69) Jādod uzņēmējiem pietiekami daudz laika, lai tie varētu pielāgoties šīs regulas prasībām. Šī regula būtu jāsāk piemērot [24 mēnešus] no tās spēkā stāšanās dienas, izņemot ziņošanas pienākumus attiecībā uz aktīvi izmantotām ievainojamībām un incidentiem, kuri būtu jāsāk piemērot [12 mēnešus] no šīs regulas spēkā stāšanās dienas.

(70) Ņemot vērā to, ka šīs regulas mērķi nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet rīcības ietekmes dēļ tos 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 norādītā mērķa sasniegšanai.

(71) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725[23] 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas […] sniedza atzinumu,

IR PIEŅĒMUŠI ŠO REGULU.

I NODAĻA

VISPĀRĪGIE NOTEIKUMI

1. pants

Priekšmets

Šī regula nosaka:

[23] 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.).

(a) noteikumus par produktu ar digitāliem elementiem laišanu tirgū, lai nodrošinātu šādu produktu kiberdrošību;

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

(c) pamatprasības par ievainojamību novēršanas procesiem, ko ražotāji ieviesuši, lai attiecībā uz produktiem ar digitāliem elementiem nodrošinātu kiberdrošību visā aprites ciklā, kā arī ar šiem procesiem saistītos uzņēmēju pienākumus;

(d) noteikumus par tirgus uzraudzību un iepriekš minēto noteikumu un prasību izpildes panākšanu.

2. pants

Darbības joma

1. Šo regulu piemēro produktiem ar digitāliem elementiem, kuru paredzētais 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. 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 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.

   Komisija saskaņā ar 50. pantu tiek pilnvarota pieņemt deleģētos aktus nolūkā grozīt šo regulu, norādot, vai šāda ierobežošana vai izslēgšana ir nepieciešama, attiecīgos produktus un noteikumus, kā arī attiecīgā gadījumā ierobežojuma darbības jomu.

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

3. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

(1) “produkts ar digitāliem elementiem” ir jebkurš programmatūras vai aparatūras produkts un tā attālinātās datu apstrādes risinājumi, ieskaitot programmatūras vai aparatūras komponentus, kas laižami tirgū atsevišķi;

(2) “attālināta datu apstrāde” ir jebkura 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) “kritiski svarīgs produkts ar digitāliem elementiem” ir produkts ar digitāliem elementiem, kurš rada kiberdrošības risku saskaņā ar 6. panta 2. punktā noteiktajiem kritērijiem un kura pamatfunkcija ir izklāstīta III pielikumā;

(4) “ļoti kritiski svarīgs produkts ar digitāliem elementiem” ir produkts ar digitāliem elementiem, kurš rada kiberdrošības risku saskaņā ar 6.panta 5. punktā noteiktajiem kritērijiem;

(5) “operacionālā tehnoloģija” ir programmējamas digitālas sistēmas vai ierīces, kas mijiedarbojas ar fizisko vidi vai pārvalda ierīces, kuras mijiedarbojas ar fizisko vidi;

(6) “programmatūra” ir elektroniskās informācijas sistēmas daļa, kura sastāv no datora koda;

(7) “aparatūra” ir fiziska elektroniskā informācijas sistēma vai tās daļas, kas spēj apstrādāt, uzglabāt vai pārraidīt digitālos datus;

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

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

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

(11) “fiziskais savienojums” ir jebkāds savienojums starp elektroniskām informācijas sistēmām vai komponentiem, ko īsteno, izmantojot fiziskos līdzekļus, to vidū elektriskās vai mehāniskās saskarnes, vadus vai radioviļņus;

(12) “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;

(13) “privilēģija” ir piekļuves tiesības, kas piešķirtas konkrētiem lietotājiem vai programmām, lai elektroniskajā informācijas sistēmā veiktu ar drošību saistītas darbības;

(14) “paaugstināta privilēģija” ir piekļuves tiesības, kas piešķirtas konkrētiem lietotājiem vai programmām, lai elektroniskajā informācijas sistēmā veiktu paplašinātu ar drošību saistītu darbību kopumu, un kas nepareizas lietošanas vai apdraudējuma gadījumā varētu ļaut ļaundarim iegūt plašāku piekļuvi sistēmas vai organizācijas resursiem;

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

(16) “tīklošanas vai datošanas resursi” ir datu, aparatūras vai programmatūras funkcionalitāte, kas pieejama vai nu lokāli, vai ar tīkla vai citas pievienotas ierīces starpniecību;

(17) “ uzņēmējs” ir ražotājs, pilnvarotais pārstāvis, importētājs, izplatītājs vai jebkura cita fiziska vai juridiska persona, uz kuru attiecas šajā regulā noteiktie pienākumi;

(18) “ražotājs” ir jebkura 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 vai bez tās;

(19) “pilnvarotais pārstāvis” ir jebkura fiziska vai juridiska persona, kas veic uzņēmējdarbību Savienībā un ir saņēmusi rakstisku ražotāja pilnvarojumu rīkoties tā vārdā attiecībā uz konkrētiem uzdevumiem;

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

(21) “izplatītājs” ir jebkura 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;

(22) “laist tirgū” ir produktu ar digitāliem elementiem pirmo reizi darīt pieejamu Savienības tirgū;

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

(24) “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;

(25) “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;

(26) “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;

(27) “paziņojošā iestāde” ir valsts iestāde, kas atbild par to procedūru izveidi un izpildi, kuras nepieciešamas atbilstības novērtēšanas struktūru novērtēšanai, izraudzīšanai un paziņošanai, kā arī to uzraudzībai;

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

(29) “atbilstības novērtēšanas struktūra” ir Regulas (ES) Nr. 765/2008 2. panta 13. punktā noteiktā struktūra;

(30) “paziņotā struktūra” ir atbilstības novērtēšanas struktūra, kas izraudzīta saskaņā ar šīs regulas 33. pantu un citiem attiecīgajiem Savienības saskaņošanas tiesību aktiem;

(31) “būtiska modifikācija” ir produkta ar digitāliem elementiem tādas izmaiņas pēc laišanas tirgū, kas ietekmē produkta atbilstību I pielikuma 1. iedaļā izklāstītajām

pamatprasībām vai izraisa modifikāciju attiecībā uz paredzēto lietojumu, par kuru ir saņemts produkta ar digitāliem elementiem novērtējums;

(32) "*CE* zīme" ir marķējums, ar ko ražotājs norāda, ka produkts ar digitāliem elementiem un ražotāja ieviestie procesi atbilst I pielikumā izklāstītajām pamatprasībām un citiem piemērojamiem Savienības tiesību aktiem, ar kuriem saskaņo produktu tirdzniecības nosacījumus ("Savienības saskaņošanas tiesību akti") un kuros noteikta šādas zīmes uzlikšana;

(33) "tirgus uzraudzības iestāde" ir iestāde, kas definēta Regulas (ES) 2019/1020 3. panta 4. punktā;

(34) "saskaņotais standarts" ir saskaņots standarts, kas definēts Regulas (ES) Nr. 1025/2012 2. panta 1. punkta c) apakšpunktā;

(35) "kiberdrošības risks" ir risks, kas definēts Direktīvas [Direktīva XXX/XXXX (TID2)] pantā [X. pants];

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

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

(38) "ievainojamība" ir ievainojamība, kas definēta Direktīvas [Direktīva XXX/XXXX (TID2)] pantā [X. pants];

(39) "aktīvi izmantota ievainojamība" ir ievainojamība, par kuru ir ticami pierādījumi, ka kāds sistēmas dalībnieks bez sistēmas īpašnieka atļaujas ir veicis ļaunprātīga koda izpildi;

(40) "persondati" ir dati, kas definēti Regulas (ES) 2016/679 4. panta 1. punktā.

4. pants

Brīva aprite

1. Dalībvalstis saistībā ar šīs regulas aptvertajiem aspektiem nekavē darīt pieejamus tirgū produktus ar digitāliem elementiem, kas atbilst šai regulai.

2. Tirdzniecības gadatirgos, izstādēs un demonstrācijās vai līdzīgos pasākumos dalībvalstis neliedz piedāvāt un izmantot produktu ar digitāliem elementiem, kas neatbilst šai regulai.

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

5. pants

Prasības produktiem ar digitāliem elementiem

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

(1) tie atbilst I pielikuma 1. iedaļā izklāstītajām pamatprasībām ar nosacījumu, ka tie ir pareizi uzstādīti, uzturēti, lietoti tiem paredzētajā nolūkā vai apstākļos, kurus var pamatoti paredzēt, un vajadzības gadījumā atjaunināti, un

(2) ražotāja ieviestie procesi atbilst I pielikuma 2. iedaļā izklāstītajām pamatprasībām.

6. pants

Kritiski svarīgi produkti ar digitāliem elementiem

1. Produktus ar digitāliem elementiem, kas pieder III pielikumā uzskaitītajai kategorijai, uzskata par kritiski svarīgiem produktiem ar digitāliem elementiem. Produkti, kuriem ir tādas kategorijas pamatfunkcija, kas uzskaitīta šīs regulas III pielikumā, ir uzskatāmi par produktiem, kas ietilpst minētajā kategorijā. Kā norādīts III pielikumā, kritiski svarīgu produktu ar digitāliem elementiem kategorijas iedala I un II klasē, kas atspoguļo ar šiem produktiem saistītā kiberdrošības riska līmeni.

2. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 50. pantu, lai grozītu III pielikumu, kritiski svarīgo produktu ar digitāliem elementiem kategoriju sarakstā iekļaujot jaunu kategoriju vai svītrojot no minētā saraksta tajā esošu kategoriju. Izvērtējot vajadzību grozīt III pielikuma sarakstu, Komisija ņem vērā kiberdrošības riska līmeni, kas saistīts ar produktu ar digitāliem elementiem kategorijām. Nosakot kiberdrošības riska līmeni, ņem vērā vienu vai vairākus šādus kritērijus:

   (a) ar kiberdrošību saistīto funkcionalitāti, kas piemīt produktam ar digitāliem elementiem, un to, vai produktam ar digitāliem elementiem ir vismaz viena no šādām īpašībām:

      (i) tas ir paredzēts paaugstinātas privilēģijas darbībai vai privilēģiju pārvaldībai;

      (ii) tam ir tieša vai privileģēta piekļuve tīklošanas vai datošanas resursiem;

      (iii) tas ir paredzēts, lai kontrolētu piekļuvi datiem vai operacionālajai tehnoloģijai;

      (iv) tas veic funkciju, kas ir kritiski svarīga attiecībā uz uzticamību, jo īpaši drošības funkcijas, piemēram, tīkla vadību, galapunkta drošību un tīkla aizsardzību;

   (b) paredzēto lietojumu sensitīvā vidē, arī rūpnieciskajā vidē vai tāda veida būtiskajās vienībās, kas minētas Direktīvas [Direktīva XXX/XXXX (TID2)] pielikumā [I pielikums];

   (c) paredzēto lietojumu kritiski svarīgu vai sensitīvu funkciju izpildei, piemēram, persondatu apstrādei;

   (d) nelabvēlīgas ietekmes iespējamo apmēru, jo īpaši attiecībā uz tās intensitāti un spēju ietekmēt daudzas personas;

   (e) to, kādā mērā produktu ar digitāliem elementiem izmantošana jau ir radījusi materiālus vai nemateriālus zaudējumus vai traucējumus vai izraisījusi nopietnas bažas saistībā ar nelabvēlīgas ietekmes iestāšanos.

3. Komisija tiek pilnvarota pieņemt deleģēto aktu saskaņā ar 50. pantu, lai papildinātu šo regulu, precizējot III pielikumā izklāstītās I un II klases produktu kategoriju definīcijas. Deleģēto aktu pieņem [12 mēnešos no šīs regula stāšanās spēkā].

4. Uz kritiski svarīgajiem produktiem ar digitāliem elementiem attiecas 24. panta 2. un 3. punktā minētās atbilstības novērtēšanas procedūras.

5. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 50. pantu, lai papildinātu šo regulu, precizējot kategorijas attiecībā uz ļoti kritiski svarīgiem produktiem ar digitāliem elementiem, attiecībā uz kurām ražotājiem ir jāsaņem Eiropas kiberdrošības sertifikāts saskaņā ar Regulā (ES) 2019/881 noteikto Eiropas kiberdrošības sertifikācijas shēmu, lai pierādītu atbilstību I pielikumā vai tā daļās izklāstītajām pamatprasībām. Nosakot šādas ļoti kritiski svarīgu produktu ar digitāliem elementiem kategorijas, Komisija ņem vērā kiberdrošības riska līmeni, kas saistīts ar produktu ar digitāliem elementiem kategoriju, ņemot vērā vienu vai vairākus no 2. punktā uzskaitītajiem kritērijiem, kā arī ņemot vērā novērtējumu par to, vai minēto produktu kategorija:

   (a) tiek lietota vai uz to paļaujas tādas būtiskās vienības, kuru veids minēts Direktīvas [Direktīva XXX/XXXX (TID2)] pielikumā [I pielikums], vai arī tai, iespējams, būs būtiska turpmākā nozīme šo vienību darbībās; vai

   (b) attiecas uz produktu ar digitāliem elementiem vispārējās piegādes ķēdes noturību pret darbības traucējumiem.

7. pants

Produktu vispārējais drošums

Atkāpjoties no Regulas [Ražojumu vispārēja drošuma regula] 2. panta 1. punkta trešās daļas b) apakšpunkta, ja uz produktiem ar digitāliem elementiem neattiecas īpašas prasības, kas noteiktas citos Savienības saskaņošanas tiesību aktos [Ražojumu vispārēja drošuma regulas 3. panta 25. punkta] nozīmē, minētajiem produktiem attiecībā uz šajā regulā neietvertiem drošības riskiem piemēro Regulas [Ražojumu vispārēja drošuma regulas] III nodaļas 1. iedaļu, V un VII nodaļu un IX–XI nodaļu.

8. pants

Augsta riska MI sistēmas

1. Produktus ar digitāliem elementiem, kuri saskaņā ar Regulas [MI regula] pantu [6. pants] klasificēti kā augsta riska MI sistēmas, kas ietilpst šīs regulas darbības jomā un atbilst šīs regulas I pielikuma 1. iedaļā noteiktajām pamatprasībām, un ja ražotāja ieviestie procesi atbilst I pielikuma 2. iedaļā noteiktajām pamatprasībām, uzskata par atbilstīgiem Regulas [MI regula] pantā [15. pants] noteiktajām ar kiberdrošību saistītajām prasībām, neskarot citas prasības attiecībā uz precizitāti un robustumu, kas iekļautas iepriekš minētajā pantā, un ciktāl ar minētajām prasībām noteiktā aizsardzības līmeņa panākšanu pierāda ES atbilstības deklarācija, kas izdota saskaņā ar šo regulu.

2. Attiecībā uz 1. punktā minētajiem produktiem un kiberdrošības prasībām piemēro attiecīgo atbilstības novērtēšanas procedūru, kas noteikta Regulas [MI regula] pantā [43. pants]. Minētās novērtēšanas nolūkā paziņotās struktūras, kurām saskaņā ar Regulu [MI regula] ir tiesības kontrolēt augsta riska MI sistēmu atbilstību, ir arī tiesīgas kontrolēt šīs regulas darbības jomā ietverto augsta riska MI sistēmu atbilstību šīs regulas I pielikumā izklāstītajām prasībām ar noteikumu, ka minēto paziņoto struktūru atbilstība šīs regulas 29. pantā noteiktajām prasībām ir izvērtēta saistībā ar Regulā [MI regula] noteikto paziņošanas procedūru.

3. Atkāpjoties no 2. punkta, šīs regulas III pielikumā uzskaitītajiem kritiski svarīgiem produktiem ar digitāliem elementiem, kuriem jāpiemēro atbilstības novērtēšanas procedūras, kas minētas 24. panta 2. punkta a) apakšpunktā, 24. panta 2. punkta b) apakšpunktā, 24. panta 3. punkta a) apakšpunktā un 24. panta 3. punkta b) apakšpunktā saskaņā ar šo regulu, un kuri ir arī klasificēti kā augsta riska MI sistēmas saskaņā ar Regulas [MI regula] pantu [6. pants], un uz kuriem attiecas Regulas [MI regula] pielikumā [VI pielikums] minētā uz iekšējo kontroli pamatotā atbilstības novērtēšanas procedūra, piemēro šajā regulā noteiktās atbilstības novērtēšanas procedūras, ciktāl tās attiecas uz šīs regulas pamatprasībām.

9. pants

Mašīnbūves produkti

Mašīnbūves produktus, kuri ietilpst Regulas [Mašīnu regulas priekšlikums] darbības jomā un kuri ir produkti ar digitāliem elementiem šīs regulas nozīmē, un par kuriem uz šīs regulas pamata ir izdota ES atbilstības deklarācija, uzskata par atbilstīgiem veselības aizsardzības un drošības pamatprasībām, kas izklāstītas Regulas [Mašīnu regulas priekšlikums] pielikumā [III pielikuma 1.1.9. un 1.2.1. iedaļa] attiecībā uz aizsardzību pret korupciju un vadības sistēmu drošumu un uzticamību, un ciktāl ar minētajām prasībām noteiktā aizsardzības līmeņa panākšana ir pierādīta saskaņā ar šo regulu izdotā ES atbilstības deklarācijā.

II NODAĻA

UZŅĒMĒJU PIENĀKUMI

10. pants

Ražotāju pienākumi

1. Laižot tirgū produktu ar digitāliem elementiem, ražotāji nodrošina, ka tas ir projektēts, izstrādāts un ražots saskaņā ar I pielikuma 1. sadaļā izklāstītajām 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 drošības incidentus un samazinātu šādu incidentu ietekmi, arī attiecībā uz lietotāju veselību un drošību.

3. Laižot tirgū produktu ar digitāliem elementiem, ražotājs iekļauj kiberdrošības riska novērtējumu tehniskajā dokumentācijā, kā noteikts 23. pantā un V pielikumā. Attiecībā uz 8. pantā un 24. panta 4. punktā minētajiem produktiem ar digitāliem elementiem, uz kuriem attiecas arī citi Savienības tiesību akti, kiberdrošības riska novērtējums var būt daļa no attiecīgajos Savienības aktos prasītā riska novērtējuma. Ja konkrētas pamatprasības nav piemērojamas tirgotajam produktam ar digitāliem elementiem, ražotājs minētajā dokumentācijā iekļauj skaidru pamatojumu.

4. Lai izpildītu 1. punktā noteikto pienākumu, ražotāji veic uzticamības pārbaudi, ja produktos ar digitāliem elementiem tiek integrēti no trešām personām iegūti komponenti. Tie nodrošina, ka šādi komponenti neapdraud produkta ar digitāliem elementiem drošību.

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

6. Ražotāji, laižot tirgū produktu ar digitāliem elementiem, un paredzamajā produkta kalpošanas laikā vai piecus gadus pēc produkta laišanas tirgū, atkarībā no tā, kurš termiņš ir īsāks, minētā produkta ievainojamības gadījumā nodrošina efektīvu un I pielikuma 2. iedaļā noteiktajām pamatprasībām atbilstīgu rīcību.

   Ražotājiem ir atbilstīga politika un procedūras, tajā skaitā I pielikuma 2. iedaļas 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.

7. Pirms produkta ar digitāliem elementiem laišanas tirgū ražotāji sagatavo 23. pantā norādīto tehnisko dokumentāciju.

   Tie veic izvēlētās 24. pantā minētās atbilstības novērtēšanas procedūras vai nodrošina to veikšanu.

   Ja minētajā atbilstības novērtēšanas procedūrā ir pierādīts, ka produkts ar digitāliem elementiem atbilst I pielikuma 1. iedaļā noteiktajām pamatprasībām un ražotāja ieviestie procesi atbilst I pielikuma 2. iedaļā noteiktajām pamatprasībām, ražotāji sagatavo ES atbilstības deklarāciju saskaņā ar 20. pantu un uzliek *CE* zīmi saskaņā ar 22. pantu.

8. Ražotāji tehnisko dokumentāciju un — attiecīgā gadījumā — ES atbilstības deklarāciju glabā pieejamu tirgus uzraudzības iestādēm desmit gadus pēc produkta ar digitāliem elementiem laišanas tirgū.

9. Ražotāji nodrošina, ka ir ieviestas procedūras, ar kurām attiecībā uz produktiem ar digitāliem elementiem, kas ietverti ražošanas sērijās, tiek panākta pastāvīga atbilstība šai regulai. Ražotājs 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 19. pantā minētajās kopīgajās specifikācijās, uz ko atsaucoties deklarēta produkta ar digitāliem elementiem atbilstība vai kuras piemērojot verificēta tā atbilstība.

10. Ražotāji nodrošina, ka produktiem ar digitāliem elementiem tiek pievienota II pielikumā noteiktā informācija un norādījumi elektroniskā vai fiziskā formā. Šāda informācija un norādījumi ir lietotājiem viegli saprotamā valodā. Tās ir skaidras, saprotamas, nepārprotamas un salasāmas. Tās ļauj droši uzstādīt, ekspluatēt un lietot produktus ar digitāliem elementiem.

11. Ražotāji vai nu pievieno produktam ar digitāliem elementiem ES atbilstības deklarāciju, vai II pielikumā noteiktajos norādījumos un informācijā norāda tīmekļvietnes adresi, kurā var piekļūt ES atbilstības deklarācijai.

12. Sākot no produkta ar digitāliem elementiem laišanas tirgū un paredzamajā tā kalpošanas laikā vai piecu gadu laikposmā pēc tā laišanas tirgū, atkarībā no tā, kurš termiņš ir īsāks, ražotāji, kas zina vai kam ir iemesls uzskatīt, ka produkts ar digitāliem elementiem vai ražotāja ieviestie procesi neatbilst I pielikumā izklāstītajām pamatprasībām, nekavējoties veic korektīvus pasākumus, kas

nepieciešami, lai panāktu produkta ar digitāliem elementiem vai ražotāja procesu atbilstību, attiecīgā gadījumā šo produktu izņemtu vai atsauktu.

13. Pēc tirgus uzraudzības iestādes pamatota pieprasījuma ražotāji šai iestādei viegli saprotamā valodā papīra vai elektroniskā formātā sniedz tai visu informāciju un dokumentāciju, kas nepieciešama, lai pierādītu produkta ar digitāliem elementiem un ražotāja ieviesto procesu atbilstību I pielikumā izklāstītajām 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.

14. Ražotājs, kas pārtrauc darbību un līdz ar to nespēj izpildīt šajā regulā noteiktos pienākumus, pirms faktiskās darbības pārtraukšanas 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.

15. Komisija ar īstenošanas aktiem var precizēt I pielikuma 2. iedaļas 1. punktā noteikto programmatūras materiālu komplekta formātu un elementus. Minētos īstenošanas aktus pieņem saskaņā ar 51. panta 2. punktā minēto pārbaudes procedūru.

11. pants

Ražotāju ziņošanas pienākumi

1. Ražotājs bez nepamatotas kavēšanās un jebkurā gadījumā 24 stundu laikā pēc tam, kad tas ir uzzinājis par jebkuru aktīvi izmantotu ievainojamību, ko satur produkts ar digitāliem elementiem, paziņo par to *ENISA*. Paziņojumā iekļauj informāciju par minēto ievainojamību un attiecīgā gadījumā par veiktajiem korektīvajiem vai riska mazināšanas pasākumiem. *ENISA* pēc paziņojuma saņemšanas bez nepamatotas kavēšanās, izņemot gadījumus, ja pastāv ar kiberdrošības risku saistīti pamatoti iemesli, to pārsūta attiecīgo dalībvalstu *CSIRT*, kas izraudzītas koordinētas ievainojamības atklāšanas nolūkā saskaņā ar Direktīvas [Direktīva XXX/XXXX (TID2)] pantu [X. pants], un informē tirgus uzraudzības iestādi par paziņoto ievainojamību.

2. Ražotājs bez nepamatotas kavēšanās un jebkurā gadījumā 24 stundu laikā pēc tam, kad tam ir kļuvis zināms par jebkuru incidentu, kas ietekmē produkta ar digitāliem elementiem drošību, paziņo par to *ENISA*. *ENISA* bez nepamatotas kavēšanās, izņemot gadījumus, ja pastāv ar kiberdrošības risku saistīti pamatoti iemesli, paziņojumu pārsūta attiecīgo dalībvalstu vienotajiem kontaktpunktiem, kas izraudzīti saskaņā ar Direktīvas [Direktīva XXX/XXXX (TID2)] pantu [X. pants], un informē tirgus uzraudzības iestādi par paziņotajiem incidentiem. Paziņojumā par incidentu iekļauj informāciju par incidenta nopietnības pakāpi un ietekmi un attiecīgā gadījumā norāda, vai ražotājam ir aizdomas, ka incidentu izraisījušas nelikumīgas vai ļaunprātīgas darbības, vai tas uzskata, ka incidentam ir pārrobežu ietekme.

3. *ENISA* iesniedz ar Direktīvas [Direktīva XXX/XXXX (TID2)] pantu [X. pants] izveidotajam Eiropas Kiberkrīžu sadarbības organizāciju tīklam (*EU-CyCLONe*) saskaņā ar 1. un 2. punktu paziņoto informāciju, ja šāda informācija ir būtiska plaša mēroga kiberdrošības incidentu un krīžu koordinētai pārvaldībai operatīvā līmenī.

4. Ražotājs bez nepamatotas kavēšanās un pēc tam, kad tam ir kļuvis zināms par incidentu, informē produkta ar digitāliem elementiem lietotājus par to un vajadzības

gadījumā par korektīviem pasākumiem, ko lietotājs var veikt, lai mazinātu incidenta ietekmi.

5. Komisija ar īstenošanas aktiem var papildus precizēt atbilstīgi 1. un 2. punktam iesniegtajos paziņojumos iekļaujamās informācijas veidu, paziņojuma formātu un paziņošanas procedūru. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 51. panta 2. punktā.

6. *ENISA*, pamatojoties uz atbilstīgi 1. un 2. punktam saņemtajiem paziņojumiem, reizi divos gados sagatavo tehnisko ziņojumu par jaunākajām tendencēm attiecībā uz kiberdrošības riskiem produktos ar digitāliem elementiem un to iesniedz Direktīvas [Direktīva XXX/XXXX (TID2)] pantā [X. pants] minētajai sadarbības grupai. Pirmo šādu ziņojumu iesniedz 24 mēnešu laikā pēc tam, kad sāk piemērot 1. un 2. punktā noteiktos pienākumus.

7. Ražotāji pēc ievainojamības identificēšanas attiecībā uz kādu komponentu, ieskaitot atklātā pirmkoda komponentu, kas integrēts produktā ar digitāliem elementiem, ziņo par šo ievainojamību personai vai vienībai, kas veic attiecīgā komponenta uzturēšanu.

12. pants

Pilnvarotie pārstāvji

1. Ražotājs ar rakstisku pilnvarojumu var iecelt pilnvaroto pārstāvi.

2. Pilnvarotā pārstāvja pilnvarās neietilpst pienākumi, kas noteikti no 10. panta 1. punkta līdz 7. punkta pirmajam ievilkumam un minētā panta 9. punktā.

3. Pilnvarotais pārstāvis veic uzdevumus, kas noteikti no ražotāja saņemtajā pilnvarojumā. Pilnvarojums pilnvarotajam pārstāvim ļauj veikt vismaz šādas darbības:

   (a) desmit gadus pēc produkta ar digitāliem elementiem laišanas tirgū glabāt 20. pantā minēto ES atbilstības deklarāciju un 23. 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.

13. pants

Importētāju pienākumi

1. Importētāji laiž tirgū tikai tādus produktus ar digitāliem elementiem, kuri atbilst I pielikuma 1. iedaļā izklāstītajām pamatprasībām, un tikai tad, ja ražotāja ieviestie procesi atbilst I pielikuma 2. iedaļā izklāstītajām pamatprasībām.

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

   (a) ražotājs ir veicis pienācīgas atbilstības novērtēšanas procedūras, kas minētas 24. pantā;

(b) ražotājs ir sagatavojis tehnisko dokumentāciju;

(c) produktam ar digitāliem elementiem ir 22. pantā minētā *CE* zīme, un tam ir pievienota II pielikumā noteiktā informācija un norādījumi lietotājam.

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

4. Importētāji uz produkta ar digitāliem elementiem vai, ja tas nav iespējams, uz tā iepakojuma vai produktam ar digitāliem elementiem pievienotajā dokumentā norāda sava uzņēmuma nosaukumu, reģistrēto komercnosaukumu vai reģistrēto preču zīmi un saziņai pasta adresi un e-pasta adresi. Kontaktinformācija ir lietotājiem un tirgus uzraudzības iestādēm viegli saprotamā valodā.

5. Importētāji nodrošina, ka produktam ar digitāliem elementiem ir pievienotas II pielikumā sniegtie norādījumi un informācija lietotājiem viegli saprotamā valodā.

6. Importētāji, kuri zina vai kuriem ir iemesls uzskatīt, ka produkts ar digitāliem elementiem, ko tie ir laiduši tirgū, vai tā ražotāja ieviestie procesi neatbilst I pielikumā izklāstītajām pamatprasībām, nekavējoties veic korektīvus pasākumus, kas nepieciešami, lai panāktu produkta ar digitāliem elementiem vai tā ražotāja ieviesto procesu atbilstību I pielikumā izklāstītajām pamatprasībām vai attiecīgā gadījumā šo produktu izņemtu vai atsauktu.

Identificējot 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.

7. Importētāji desmit gadus pēc produkta ar digitāliem elementiem laišanas tirgū glabā ES atbilstības deklarācijas kopiju, lai tā būtu pieejama tirgus uzraudzības iestādēm, un nodrošina, ka minētajām iestādēm pēc pieprasījuma ir pieejama tehniskā dokumentācija.

8. 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 1. iedaļā izklāstītajām pamatprasībām un ka ražotāja ieviestie procesi atbilst I pielikuma 2. iedaļā izklāstītajām 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.

9. 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.

14. pants

Izplatītāju pienākumi

1. Darot produktu ar digitāliem elementiem pieejamu tirgū, izplatītāji rūpīgi ievēro šīs regulas 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 attiecīgi 10. panta 10. un 11. punktā un 13. panta 4. punktā noteiktos pienākumus.

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

4. Izplatītāji, kuri zina vai kuriem ir iemesls uzskatīt, ka produkts ar digitāliem elementiem, ko tie darījuši pieejamu tirgū, vai tā ražotāja ieviestie procesi neatbilst I pielikumā izklāstītajām pamatprasībām, 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.

   Pēc produkta ar digitāliem elementiem ievainojamības identificēšanas, 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 tai 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 I pielikumā izklāstītajām pamatprasībām. Izplatītāji pēc minētās iestādes pieprasījuma sadarbojas ar to visos pasākumos, kas tiek veikti, lai novērstu kiberdrošības riskus, ko rada produkts ar digitāliem elementiem, ko tie darījuši pieejamu tirgū.

6. Ja produkta ar digitāliem elementiem izplatītājam ir kļuvis zināms, ka minētā produkta ražotājs ir pārtraucis darbību un līdz ar to nespēj izpildīt šajā regulā noteiktos pienākumus, izplatītājs 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.

15. 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 10. pantā un 11. panta 1., 2., 4. un 7. punktā noteiktie ražotāja pienākumi.

16. pants

Citi gadījumi, kad piemēro ražotāja pienākumus

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

Minētajai personai 10. pantā un 11. panta 1., 2., 4. un 7. punktā noteiktos ražotāja pienākumus piemēro attiecībā uz to produkta daļu, kuru ir skārusi būtiskā modifikācija, vai attiecībā uz visu produktu, ja būtiskā modifikācija ietekmē produkta ar digitāliem elementiem kiberdrošību kopumā.

17. pants

Uzņēmēju identifikācija

1. Uzņēmēji pēc pieprasījuma, un ja informācija ir pieejama, tirgus uzraudzības iestādēm sniedz šādu informāciju:

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

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

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

III NODAĻA

PRODUKTA AR DIGITĀLIEM ELEMENTIEM ATBILSTĪBA

18. 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 pamatprasībām, uz kurām attiecas minētie standarti vai to daļas.

2. Produktus ar digitāliem elementiem un ražotāja ieviestos procesus, kas atbilst 19. pantā minētajām kopīgajām specifikācijām, uzskata par atbilstīgiem I pielikumā izklāstītajām pamatprasībām, ciktāl minētās kopīgās specifikācijas attiecas uz minētajām prasībām.

3. Produktus ar digitāliem elementiem un ražotāja ieviestos procesus, par kuriem ir izdots ES atbilstības apliecinājums vai sertifikāts saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu, kas pieņemta, pamatojoties uz Regulu (ES) 2019/881, un precizēta saskaņā ar 4. punktu, uzskata par atbilstīgiem I pielikumā izklāstītajām pamatprasībām, ciktāl ES atbilstības apliecinājums vai kiberdrošības sertifikāts vai tā daļas attiecas uz minētajām prasībām.

4. Komisija tiek pilnvarota ar īstenošanas aktiem precizēt Eiropas kiberdrošības sertifikācijas shēmas, kuras pieņemtas saskaņā ar Regulu (ES) 2019/881 un kuras var izmantot, lai pierādītu atbilstību I pielikumā izklāstītajām pamatprasībām vai to daļām. Turklāt Komisija attiecīgā gadījumā norāda, vai saskaņā ar šādām shēmām izdots kiberdrošības sertifikāts atceļ ražotāja pienākumu īstenot trešās personas veiktu atbilstības novērtēšanu attiecīgajām prasībām, kā noteikts 24. panta 2. punkta a) un b) apakšpunktā, 3. punkta a) un b) apakšpunktā. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 51. panta 2. punktā.

19. pants

Kopīgās specifikācijas

Ja 18. pantā minēto saskaņoto standartu nav vai ja Komisija uzskata, ka attiecīgie saskaņotie standarti nav pietiekami, lai apmierinātu šīs regulas prasības vai izpildītu Komisijas standartizācijas pieprasījumu, vai ja standartizācijas procedūra ir nepamatoti aizkavējusies, vai ja Eiropas standartizācijas organizācijas nav pieņēmušas Komisijas pieprasījumu par saskaņotajiem standartiem, Komisija tiek pilnvarota ar īstenošanas aktiem pieņemt kopīgās specifikācijas attiecībā uz I pielikumā izklāstītajām pamatprasībām. Minētos īstenošanas aktus pieņem saskaņā ar 51. panta 2. punktā minēto pārbaudes procedūru.

20. pants

ES atbilstības deklarācija

1. ES atbilstības deklarāciju sagatavo ražotāji saskaņā ar 10. panta 7. punktu, un tā norāda, ka ir pierādīta atbilstība I pielikumā izklāstītajām pamatprasībām.

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

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

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

5. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 50. pantu nolūkā papildināt šo regulu, pievienojot elementus IV pielikumā sniegtās ES atbilstības deklarācijas minimālajam saturam, lai ņemtu vērā tehnoloģiju attīstību.

21. pants

CE zīmes vispārējie principi

Uz *CE* zīmi, kas definēta 3. panta 32. punktā, attiecas Regulas (EK) Nr. 765/2008 30. pantā izklāstītie vispārējie principi.

22. 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 20. pantā minētajā ES atbilstības deklarācijā, kas pievienota produktam ar digitāliem elementiem. Tādiem produktiem ar digitāliem elementiem, kas veidoti kā programmatūra, *CE* zīmi norāda vai nu 20. pantā minētajā ES atbilstības deklarācijā, vai attiecīgo programmatūras produktu papildinošajā tīmekļvietnē.

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 risku vai lietojumu, kas noteikts 6. punktā minētajos īstenošanas aktos.

4. Aiz *CE* zīmes norāda paziņotās struktūras identifikācijas numuru, ja minētā struktūra ir iesaistīta 24. 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 vēl ar citiem Savienības tiesību aktiem, kas arī paredz *CE* zīmes uzlikšanu, *CE* zīme norāda uz to, ka šis produkts atbilst arī šo citu tiesību aktu prasībām.

6. Komisija ar īstenošanas aktiem var noteikt tehniskās specifikācijas piktogrammām vai citām zīmēm, kas saistītas ar produktu ar digitāliem elementiem drošību, un mehānismus to lietošanas veicināšanai. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 51. panta 2. punktā.

23. 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 pamatprasībām. Tajā ir ietverti vismaz tie elementi, kas izklāstīti V pielikumā.

2. Tehnisko dokumentāciju sagatavo pirms produkta ar digitāliem elementiem laišanas tirgū un vajadzības gadījumā pastāvīgi atjaunina paredzamajā produkta kalpošanas laikā vai piecus gadus pēc produkta ar digitāliem elementiem laišanas tirgū, atkarībā no tā, kurš termiņš ir īsāks.

3. Attiecībā uz 8. pantā un 24. panta 4. punktā minētajiem produktiem ar digitāliem elementiem, kam piemēro arī citus Savienības aktus, sagatavo vienu vienotu tehnisko dokumentāciju, kurā tiek ietverta šīs regulas V pielikumā minētā informācija un attiecīgajos Savienības aktos prasītā informācija.

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

5. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 50. pantu nolūkā papildināt šo regulu ar elementiem, kas iekļaujami V pielikumā izklāstītajā tehniskajā dokumentācijā, lai ņemtu vērā tehnoloģiju attīstību, kā arī šīs regulas īstenošanas procesā konstatētās attīstības norises.

24. 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 pamatprasības. Ražotājs vai ražotāja pilnvarotais pārstāvis pierāda atbilstību pamatprasībām, izmantojot vienu no šādām procedūrām:

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

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

   (c) uz visaptverošu kvalitātes nodrošināšanu pamatota atbilstības novērtēšanas procedūra (pamatojoties uz H moduli), kas norādīta VI pielikumā.

2. Ja, izvērtējot I klases kritiski svarīga produkta ar digitāliem elementiem, kas noteikts III pielikumā, un tā ražotāja ieviesto procesu atbilstību I pielikumā izklāstītajām pamatprasībām, ražotājs vai ražotāja pilnvarotais pārstāvis nav piemērojis vai ir tikai daļēji piemērojis 18. pantā minētos saskaņotos standartus, kopīgās specifikācijas vai Eiropas kiberdrošības sertifikācijas shēmas, 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 pamatprasībām paredz vienu no šādām procedūrām:

   (a) ES tipa pārbaudes procedūra (pamatojoties uz B moduli), kura paredzēta VI pielikumā un kurai seko VI 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 VI pielikumā.

3. Ja produkts ir II klases kritiski svarīgs produkts ar digitāliem elementiem, kas noteikts III pielikumā, ražotājs vai ražotāja pilnvarotais pārstāvis pierāda atbilstību I pielikumā izklāstītajām pamatprasībām, izmantojot vienu no šādām procedūrām:

   (a) ES tipa pārbaudes procedūra (pamatojoties uz B moduli), kura paredzēta VI pielikumā un kurai seko VI 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 VI pielikumā.

4. Tādu produktu ar digitāliem elementiem ražotāji, kas atbilstoši Regulas [Eiropas veselības datu telpas regula] darbības jomai klasificēti kā EVPK sistēmas, atbilstību šīs regulas I pielikumā noteiktajām pamatprasībām pierāda, izmantojot attiecīgo

atbilstības novērtēšanas procedūru, kā tas noteikts Regulā [Eiropas veselības datu telpas regulas III nodaļa].

5. Nosakot maksas par atbilstības novērtēšanas procedūrām, paziņotās struktūras ņem vērā mazo un vidējo uzņēmumu (MVU) īpašās intereses un vajadzības un samazina šīs maksas proporcionāli MVU īpašajām interesēm un vajadzībām.

IV NODAĻA

ATBILSTĪBAS NOVĒRTĒŠANAS STRUKTŪRU PAZIŅOŠANA

25. pants

Paziņošana

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

26. pants

Paziņojošās iestādes

1. Dalībvalstis izraugās paziņojošo iestādi, kas ir atbildīga par tādu procedūru izveidi un veikšanu, kuras nepieciešamas, lai novērtētu un paziņotu atbilstības novērtēšanas struktūras un pārraudzītu paziņotās struktūras, ieskaitot to atbilstību 31. pantam.

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

27. 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, vai 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.

28. 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 dara šo informāciju publiski pieejamu.

29. 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, 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, var tikt uzskatīta par šādu struktūru, ja ir pierādīta tās neatkarība un interešu konflikta neesamība.

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, uzstādītāji, 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 šo produktu projektēšanu, izstrādi, ražošanu, tirdzniecību, uzstādīšanu, 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 VI 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) darbinieki ar tehniskām zināšanām un atbilstības novērtēšanas uzdevumu veikšanai pietiekamu un piemērotu pieredzi;

(b) atbilstības novērtējuma veikšanas procedūru apraksti, kuri nodrošina šo procedūru pārredzamību un atkārtojamību. 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.

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

7. Darbiniekiem, kas atbildīgi 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 pamatprasībām, piemērojamajiem saskaņotajiem standartiem un attiecīgajiem noteikumiem Savienības saskaņošanas tiesību aktos un to 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 darbinieku, kas veic novērtēšanu, objektivitāte.

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

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

10. Atbilstības novērtēšanas struktūras darbinieki glabā dienesta noslēpumus attiecībā uz visu informāciju, kas iegūta, veicot pienākumus, uz kuriem attiecas VI 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 darbinieki, kas ir atbildīgi par atbilstības novērtēšanas uzdevumu veikšanu, ir informēti par attiecīgajām standartizācijas darbībām un saskaņā ar 40. 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 un saprātīgiem noteikumiem, jo īpaši attiecībā uz maksām ņemot vērā MVU intereses.

30. 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 29. panta prasībām, ciktāl piemērojamie saskaņotie standarti attiecas uz minētajām prasībām.

31. 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 29. panta prasībām, un attiecīgi informē paziņojošo iestādi.

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

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.

32. 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, attiecībā uz kuriem struktūra sevi piesaka par kompetentu, kā arī akreditācijas sertifikātu, ja tāds ir, ko izsniegusi valsts akreditācijas struktūra, apliecinot, ka atbilstības izvērtēšanas struktūra atbilst 29. 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 29. panta prasībām.

33. pants

Paziņošanas procedūra

1. Paziņojošās iestādes var paziņot tikai tās atbilstības novērtēšanas struktūras, kas atbilst 29. pantā noteiktajām prasībām.

2. Paziņojošā iestāde Komisiju un pārējās dalībvalstis informē, izmantojot atbilstīgi jaunajai pieejai paziņoto un izraudzīto organizāciju (*NANDO*) 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 un attiecīgo kompetences apliecinājumu.

4. Ja paziņošana ir veikta, neizmantojot 32. 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 29. panta prasībām.

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

   Šajā regulā tikai šādu struktūru uzskata par paziņoto struktūru.

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

34. 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.

35. pants

Izmaiņas paziņojumos

1. Ja paziņojošā iestāde ir noskaidrojusi vai ir tikusi informēta, ka paziņotā struktūra vairs neatbilst 29. pantā noteiktajām prasībām vai nepilda savus pienākumus, paziņojošā iestāde attiecīgi ierobežo, aptur vai anulē paziņojumu, ņemot vērā to, kādā mērā attiecīgā struktūra nav spējusi nodrošināt atbilstību 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.

36. pants

Paziņoto struktūru kompetences apšaubīšana

1. Komisija izmeklē visus gadījumus, kad tai ir radušās šaubas vai 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.

37. pants

Paziņoto struktūru darba pienākumi

1. Paziņotās struktūras veic atbilstības novērtēšanu saskaņā ar 24. pantā un VI 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, nozari, kurā tas darbojas, struktūru, attiecīgās tehnoloģijas sarežģītības pakāpi un to, vai ražošanas process ir masveidīgs vai sērijveida.

3. Paziņotās struktūras tomēr ievēro tādu stingrību un aizsardzības līmeni, kāds vajadzīgs, lai produkts atbilstu regulas noteikumiem.

4. Ja paziņotā struktūra konstatē, ka ražotājs nav izpildījis II pielikumā vai atbilstīgajos saskaņotajos standartos, vai 19. 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 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.

38. 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 veic līdzīgas atbilstības novērtēšanas darbības, kuras attiecas uz tiem pašiem produktiem, sniedz attiecīgu informāciju par jautājumiem saistībā ar negatīviem un, pēc pieprasījuma, arī pozitīviem atbilstības novērtēšanas rezultātiem.

39. pants

Pieredzes apmaiņa

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

40. 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

41. 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. Attiecīgā gadījumā tirgus uzraudzības iestādes sadarbojas ar valsts kiberdrošības sertifikācijas iestādēm, kas izraudzītas saskaņā ar Regulas (ES) 2019/881 58. pantu, kā arī regulāri apmainās ar informāciju. Izraudzītās tirgus uzraudzības iestādes attiecībā uz šīs regulas 11. pantā noteikto ziņošanas pienākumu īstenošanas uzraudzību sadarbojas ar *ENISA*.

4. Vajadzības gadījumā tirgus uzraudzības iestādes sadarbojas ar citām tirgus uzraudzības iestādēm, kas izraudzītas, pamatojoties uz citiem Savienības saskaņošanas tiesību aktiem, kuri attiecas uz citiem produktiem, kā arī regulāri apmainās ar informāciju.

5. Tirgus uzraudzības iestādes attiecīgā gadījumā sadarbojas ar iestādēm, kas uzrauga Savienības datu aizsardzības tiesību aktus. Šāda sadarbība ietver šo iestāžu informēšanu par visiem konstatējumiem, kas ir būtiski to kompetences īstenošanai,

tostarp, kad tiek sniegti norādījumi un padomi saskaņā ar šā panta 8. punktu, ja šādi norādījumi un padomi attiecas uz persondatu apstrādi.

Iestādes, kas uzrauga Savienības datu aizsardzības tiesību aktus, ir pilnvarotas pieprasīt dokumentāciju, kas izveidota vai 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.

6. Dalībvalstis nodrošina, ka izraudzītajām tirgus uzraudzības iestādēm tiek sniegti atbilstoši finanšu resursi un cilvēkresursi, lai tās varētu izpildīt uzdevumus, kas tām noteikti šajā regulā .

7. Komisija veicina pieredzes apmaiņu starp izraudzītajām tirgus uzraudzības iestādēm.

8. Tirgus uzraudzības iestādes ar Komisijas atbalstu var sniegt uzņēmējiem norādījumus un padomus par šīs regulas īstenošanu.

9. 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 tās varētu interesēt Savienības konkurences tiesību normu piemērošanā.

10. Produktiem ar digitāliem elementiem, kas ietilpst šīs regulas darbības jomā un ir klasificēti kā augsta riska MI sistēmas saskaņā ar Regulas [MI regula] pantu [6. pants], tirgus uzraudzības iestādes, kas izraudzītas Regulas [MI regula] vajadzībām, ir iestādes, kas atbild par šajā regulā noteiktajām tirgus uzraudzības darbībām. Atbilstīgi Regulai [MI regula] izraudzītās tirgus uzraudzības iestādes attiecīgā gadījumā sadarbojas ar atbilstīgi šai regulai izraudzītajām tirgus uzraudzības iestādēm un — attiecībā uz 11. pantā noteikto ziņošanas pienākumu īstenošanas uzraudzību — ar *ENISA*. Tirgus uzraudzības iestādes, kas izraudzītas saskaņā ar Regulu [MI regula], 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.

11. Šīs regulas vienotai piemērošanai izveido īpašu administratīvās sadarbības grupu (*ADCO*), ievērojot Regulas (ES) 2019/1020 30. panta 2. punktu. Šīs *ADCO* sastāvā ir izraudzīto tirgus uzraudzības iestāžu pārstāvji un attiecīgā gadījumā arī vienoto sadarbības biroju pārstāvji.

42. pants

Piekļuve datiem un dokumentācijai

Ja tas nepieciešams, lai novērtētu produktu ar digitāliem elementiem un to ražotāju ieviesto procesu atbilstību I pielikumā izklāstītajām pamatprasībām, un ja ir sniegts pamatots pieprasījums, tirgus uzraudzības iestādēm piešķir piekļuvi šādu produktu projektēšanas, izstrādes, ražošanas un ievainojamību novēršanas izvērtēšanai vajadzīgajiem datiem, ieskaitot attiecīgā uzņēmēja saistīto iekšējo dokumentāciju.

43. pants

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

1. Ja dalībvalsts tirgus uzraudzības iestādei ir pietiekami iemesli uzskatīt, ka produkts ar digitāliem elementiem, ieskaitot ievainojamību novēršanu, rada būtisku kiberdrošības risku, tā 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 atbilstību vai lai samērīgi riskam to izņemtu no tirgus vai atsauktu šīs iestādes noteiktā pienācīgā termiņā.

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

2. 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.

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

4. Ja produkta ar digitāliem elementiem ražotājs 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 tiek darīts pieejams tās valsts tirgū, izņemtu to no minētā tirgus vai atsauktu to.

   Par minētajiem pasākumiem šī iestāde nekavējoties informē Komisiju un pārējās dalībvalstis.

5. Šā panta 4. punktā minētajā informācijā ietver visas pieejamās ziņas, jo īpaši datus neatbilstīgo produktu ar digitāliem elementiem identificēšanai, datus par 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 vai ražotāja ieviesto procesu neatbilstība I pielikumā izklāstītajām pamatprasībām;

   (b) trūkumi 18. pantā minētajos saskaņotajos standartos, kiberdrošības sertifikācijas shēmās vai kopīgajās specifikācijās.

6. 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 neatbilstību un — ja tās nepiekrīt paziņotajam valsts pasākumam — par saviem iebildumiem.

7. Ja triju mēnešu laikā pēc 4. punktā minētās informācijas 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.

8. Visu dalībvalstu tirgus uzraudzības iestādes nodrošina, ka attiecībā uz attiecīgo produktu nekavējoties tiek veikti atbilstoši ierobežojoši pasākumi, piemēram, produkta izņemšana no to tirgus.

44. pants

Savienības drošības procedūra

1. Ja trīs mēnešu laikā pēc 43. panta 4. 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 43. panta 4. punktā minētā paziņojuma saņemšanas izlemj, vai valsts pasākums ir vai nav pamatots, un šo 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 šo pasākumu atsauc.

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 10. pantā paredzēto procedūru.

4. Ja valsts pasākums tiek uzskatīts par pamatotu un produkta ar digitāliem elementiem neatbilstība tiek saistīta ar trūkumiem 18. pantā minētajā Eiropas kiberdrošības sertifikācijas shēmā, Komisija apsver, vai grozīt vai atcelt 18. panta 4. punktā minēto īstenošanas aktu, kurā precizēts pieņēmums par atbilstību attiecībā uz šo sertifikācijas shēmu.

5. Ja valsts pasākums tiek uzskatīts par pamatotu un produkta ar digitāliem elementiem neatbilstība tiek saistīta ar trūkumiem 19. pantā minētajās kopīgajās specifikācijās, Komisija apsver, vai grozīt vai atcelt 19. pantā minēto īstenošanas aktu, kurā izklāstītas šīs kopīgās specifikācijas.

45. pants

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

1. Ja Komisijai, arī pamatojoties uz *ENISA* sniegto informāciju, ir pietiekams pamats uzskatīt, ka produkts ar digitāliem elementiem, kas rada būtisku kiberdrošības risku, neatbilst šajā regulā noteiktajām prasībām, tā var pieprasīt attiecīgajām tirgus uzraudzības iestādēm veikt atbilstības izvērtēšanu un rīkoties atbilstoši 43. pantā minētajām procedūrām.

2. Izņēmuma apstākļos, kas pamato tūlītēju intervenci ar mērķi saglabāt iekšējā tirgus pareizu darbību, un ja Komisijai ir pietiekams pamats uzskatīt, ka 1. punktā minētais produkts joprojām neatbilst šajā regulā noteiktajām prasībām un attiecīgās tirgus uzraudzības iestādes nav veikušas efektīvus pasākumus, Komisija var pieprasīt *ENISA* veikt atbilstības izvērtēšanu. Komisija attiecīgi informē attiecīgās tirgus uzraudzības iestādes. Attiecīgie uzņēmēji pēc vajadzības sadarbojas ar *ENISA*.

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

4. Pamatojoties uz 3. punktā minēto apspriešanos, Komisija var pieņemt īstenošanas aktus, lai lemtu par korektīviem vai ierobežojošiem pasākumiem Savienības līmenī, tajā skaitā uzdodot izņemšanu no tirgus vai atsaukšanu pienācīgā termiņā, kas samērīgs ar risku. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 51. panta 2. punktā.

5. Komisija nekavējoties informē attiecīgo uzņēmēju vai uzņēmējus par 4. punktā minēto lēmumu. Dalībvalstis nekavējoties īsteno 4. punktā minētos aktus un attiecīgi informē Komisiju.

6. Šā panta 2.–5. punktu piemēro uz laiku, kamēr ir spēkā ārkārtas situācija, kas ir pamatojusi Komisijas intervenci, un tik ilgi, kamēr nav panākta attiecīgā produkta atbilstība šai regulai.

46. pants

Atbilstīgi produkti ar digitāliem elementiem, kas rada būtisku kiberdrošības risku

1. Ja dalībvalsts tirgus uzraudzības iestāde pēc 43. pantā noteiktās izvērtēšanas konstatē, ka, lai gan produkts ar digitāliem elementiem un ražotāja ieviestie procesi atbilst šai regulai, tie rada būtisku kiberdrošības risku un turklāt rada risku cilvēku veselībai vai drošībai, atbilstībai Savienības vai valstu tiesību aktos noteiktajiem pienākumiem, kuru mērķis ir aizsargāt pamattiesības, tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus, izmantojot elektronisko informācijas sistēmu, piedāvā [Direktīvas XXX/XXXX (TID2) I pielikumā] minēto veidu būtiskās vienības, vai citiem sabiedrības interešu aizsardzības aspektiem, tā pieprasa attiecīgajam uzņēmējam veikt visus atbilstīgos pasākumus, lai nodrošinātu, ka produkts ar digitāliem elementiem un ražotāja ieviestie procesi, laižot šo produktu tirgū, vairs nerada šādu risku, vai lai samērīgi riskam produktu ar digitāliem elementiem izņemtu no tirgus vai atsauktu pienācīgā termiņā.

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. Minēto lēmumu Komisija adresē dalībvalstīm.

6. Ja Komisijai, arī pamatojoties uz *ENISA* sniegto informāciju, ir pietiekams pamats uzskatīt, ka, lai gan produkts ar digitāliem elementiem atbilst šai regulai, tas rada 1. punktā minētos riskus, tā var pieprasīt attiecīgajai tirgus uzraudzības iestādei vai

iestādēm veikt atbilstības izvērtēšanu un rīkoties atbilstoši 43. pantā un šā panta 1., 2. un 3. punktā minētajām procedūrām.

7. Izņēmuma apstākļos, kas pamato tūlītēju intervenci ar mērķi saglabāt iekšējā tirgus pareizu darbību, un ja Komisijai ir pietiekams pamats uzskatīt, ka 6. punktā minētais produkts joprojām rada 1. punktā minētos riskus un attiecīgās valsts tirgus uzraudzības iestādes nav veikušas efektīvus pasākumus, Komisija var pieprasīt *ENISA* veikt minētā produkta radīto risku izvērtēšanu 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 8. punktā minēto apspriešanos, Komisija var pieņemt īstenošanas aktus, lai lemtu par korektīviem vai ierobežojošiem pasākumiem Savienības līmenī, tajā skaitā uzdodot izņemšanu no tirgus vai atsaukšanu pienācīgā termiņā, kas samērīgs ar risku. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 51. panta 2. punktā.

10. Komisija nekavējoties informē attiecīgo uzņēmēju vai uzņēmējus par 9. punktā minēto lēmumu. Dalībvalstis nekavējoties īsteno šādus aktus un attiecīgi informē Komisiju.

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

47. pants

Formāla neatbilstība

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

   (a) atbilstības zīme ir uzlikta, pārkāpjot 21. un 22. pantu;

   (b) atbilstības zīme nav uzlikta;

   (c) nav sagatavota ES 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.

48. 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 vai darīti pieejami tirgū, jo īpaši produktiem, par kuriem bieži konstatēts, ka tie rada kiberdrošības riskus.

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

3. Attiecīgā gadījumā tirgus uzraudzības iestādes un 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, veicot darbības kā daļu no izmeklēšanas, ko tā veic.

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

49. pants

Kontrolreidi

1. Tirgus uzraudzības iestādes var nolemt veikt vienlaicīgas koordinētas kontroles darbības ("kontrolreidi") attiecībā uz konkrētiem produktiem ar digitāliem elementiem vai to kategorijām, lai pārbaudītu atbilstību šai regulai vai konstatētu pārkāpumus.

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

3. *ENISA*, veicot savus uzdevumus, arī tos, kas pamatojas uz saskaņā ar 11. panta 1. un 2. punktu saņemtiem paziņojumiem, var noteikt produktu kategorijas, attiecībā uz kurām var organizēt kontrolreidus. Priekšlikumu par kontrolreidiem iesniedz 2. punktā minētajam iespējamajam koordinatoram izskatīšanai tirgus uzraudzības iestādēs.

4. Veicot kontrolreidus, iesaistītās tirgus uzraudzības iestādes var izmantot 41.–47. 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

50. pants

Deleģēšanas īstenošana

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

2. Pilnvaras pieņemt 2. panta 4. punktā, 6. panta 2. punktā, 6. panta 3. punktā, 6. panta 5. punktā, 20. panta 5. punktā un 23. panta 5. punktā minētos deleģētos aktus piešķir Komisijai.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 2. panta 4. punktā, 6. panta 2. punktā, 6. panta 3. punktā, 6. panta 5. punktā, 20. panta 5. punktā un 23. 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 4. punktu, 6. panta 2. punktu, 6. panta 3. punktu, 6. panta 5. punktu, 20. panta 5. punktu un 23. 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.

51. 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

52. 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 2016/943[24] 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.

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.

53. pants

Sankcijas

1. Dalībvalstis paredz noteikumus par sankcijām, kas piemērojamas uzņēmējiem par šīs regulas noteikumu pārkāpumiem, un veic visus pasākumus, kas nepieciešami, lai nodrošinātu to izpildi. Paredzētie sodi ir efektīvi, samērīgi un atturoši.

2. Dalībvalstis minētos noteikumus un pasākumus nekavējoties dara zināmus Komisijai un nekavējoties paziņo tai par jebkādiem turpmākiem grozījumiem, kas tos ietekmē.

3. Par neatbilstību I pielikumā noteiktajām kiberdrošības pamatprasībām un 10. un 11. 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.

4. Par jebkuru citu šajā regulā 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.

5. 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.

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

[24] 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.).

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

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

(c) uzņēmēja, kurš veicis pārkāpumu, lielumu un tirgus daļu.

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

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

9. 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.

10. 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.

VIII NODAĻA

PĀREJAS UN NOBEIGUMA NOTEIKUMI

54. pants

Grozījums Regulā (ES) 2019/1020

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

“71. [Regula XXX][Kibernoturības akts]”.

55. 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 citi Savienības saskaņošanas tiesību akti, paliek spēkā līdz [42 mēneši pēc šīs regulas spēkā stāšanās dienas], ja vien to derīguma termiņš nav beidzies pirms minētās dienas vai ja citos Savienības 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 [šīs regulas piemērošanas diena, kas minēta 57. pantā], šīs regulas prasības attiecas tikai tad, ja no minētās dienas šajos produktos notikušas būtiskas modifikācijas to uzbūvē vai tiem paredzētajā nolūkā.

3. Atkāpjoties no 2. punkta, pienākumus, kas noteikti 11. pantā, piemēro visiem šīs regulas darbības jomā ietilpstošajiem produktiem ar digitāliem elementiem, kuri laisti tirgū pirms [šīs regulas piemērošanas diena, kas minēta 57. pantā].

56. pants

Izvērtēšana un pārskatīšana

Līdz [36 mēneši pēc šīs regulas piemērošanas dienas] un pēc tam ik pēc četriem gadiem Komisija iesniedz Eiropas Parlamentam un Padomei ziņojumu par šīs regulas izvērtēšanu un pārskatīšanu. Šos ziņojumus publisko.

57. pants

Stāšanās spēkā un piemērošana

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

To piemēro no [24 mēneši pēc šīs regulas spēkā stāšanās dienas]. Tomēr 11. pantu piemēro no [12 mēneši pēc šīs regulas spēkā stāšanās dienas].

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

Briselē,

Eiropas Parlamenta vārdā — priekšsēdētāja	*Padomes vārdā — priekšsēdētājs*

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

1.2. Attiecīgās politikas jomas

1.3. Priekšlikums/iniciatīva attiecas uz:

1.4. Mērķis(-i)

1.4.1. Vispārīgais(-ie) mērķis(-i)

1.4.2. Konkrētais(-ie) mērķis(-i)

1.4.3. Paredzamais(-ie) rezultāts(-i) un ietekme

1.4.4. Snieguma rādītāji

1.5. Priekšlikuma/iniciatīvas pamatojums

1.5.1. Īstermiņā vai ilgtermiņā izpildāmās vajadzības, ieskaitot sīki izstrādātu iniciatīvas izvēršanas grafiku

1.5.2. Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka rezultativitāte vai komplementaritāte). Šā punkta izpratnē "Savienības iesaistīšanās pievienotā vērtība" ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.

1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas

1.5.4. Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem

1.5.5. Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtējums

1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme

1.7. Paredzētais(-ie) pārvaldības veids(-i)

2. PĀRVALDĪBAS PASĀKUMI

2.1. Pārraudzības un ziņošanas noteikumi

2.2. Pārvaldības un kontroles sistēma(-s)

2.2.1. Ierosināto pārvaldības veidu, finansējuma apgūšanas mehānismu, maksāšanas kārtības un kontroles stratēģijas pamatojums

2.2.2. Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto iekšējās kontroles sistēmu

2.2.3. Kontroles izmaksefektivitātes (kontroles izmaksu attiecība pret attiecīgo pārvaldīto līdzekļu vērtību) aplēse un pamatojums un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas brīdī un slēgšanas brīdī)

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

3. PRIEKŠLIKUMA/INICIATĪVAS APLĒSTĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorija(-s) un budžeta izdevumu pozīcija(-s)

3.2. Priekšlikuma aplēstā finansiālā ietekme uz apropriācijām

3.2.1. Kopsavilkums par aplēsto ietekmi uz darbības apropriācijām

3.2.2. Aplēstais iznākums, ko dos finansējums no darbības apropriācijām

3.2.3. Kopsavilkums par aplēsto ietekmi uz administratīvajām apropriācijām

3.2.4. Saderība ar pašreizējo daudzgadu finanšu shēmu

3.2.5. Trešo personu iemaksas

3.3. Aplēstā ietekme uz ieņēmumiem

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

Priekšlikums regulai par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem (Kibernoturības akts)

1.2. Attiecīgās politikas jomas

Komunikācijas tīkli, saturs un tehnoloģijas

1.3. Priekšlikums/iniciatīva attiecas uz:

× **jaunu darbību**

☐ **jaunu darbību, pamatojoties uz izmēģinājuma projektu / sagatavošanas darbību**[37]

☐ **esošas darbības pagarināšanu**

☐ **vienas vai vairāku darbību apvienošanu vai pārorientēšanu uz citu/jaunu darbību**

1.4. Mērķis(-i)

1.4.1. Vispārīgais(-ie) mērķis(-i)

Priekšlikumam ir šādi divi galvenie mērķi, kas vērsti uz iekšējā tirgus pareizas darbības nodrošināšanu: 1) **radīt apstākļus, lai tiktu izstrādāti droši produkti ar digitāliem elementiem**, nodrošinot, ka aparatūras un programmatūras produkti tirgū tiek laisti ar mazāku ievainojamību un ka ražotājiem ir nopietna attieksme pret drošību visā produkta aprites ciklā; un 2) **radīt apstākļus, kas lietotājiem, izvēloties un lietojot produktus ar digitāliem elementiem, dod iespēju ņemt vērā kiberdrošību**.

1.4.2. Konkrētais(-ie) mērķis(-i)

Priekšlikumam tika noteikti četri **konkrētie mērķi**: i) nodrošināt, ka ražotāji, sākot no projektēšanas un izstrādes posma, kā arī visā aprites ciklā uzlabo produktu ar digitāliem elementiem drošību; ii) nodrošināt saskaņotu kiberdrošības satvaru, sekmējot aparatūras un programmatūras ražotāju atbilstību; iii) uzlabot produktu ar digitāliem elementiem drošības īpašību pārredzamību un iv) sniegt iespēju uzņēmumiem un patērētājiem droši lietot produktus ar digitāliem elementiem.

Paredzamais(-ie) rezultāts(-i) un ietekme

Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz labuma guvējiem / mērķgrupām.

Priekšlikums sniegtu ievērojamu labumu dažādām ieinteresētajām personām. Uzņēmumiem tas novērstu atšķirīgus drošības noteikumus attiecībā uz produktiem ar digitāliem elementiem un samazinātu atbilstības nodrošināšanas izmaksas attiecībā uz saistītajiem kiberdrošības tiesību aktiem. Tas samazinātu kiberincidentu skaitu, incidentu risināšanas izmaksas un kaitējumu reputācijai. Tiek lēsts, ka visā ES šī

[37] Kā paredzēts Finanšu regulas 58. panta 2. punkta a) vai b) apakšpunktā.

iniciatīva uzņēmumus ietekmējošu incidentu radītās izmaksas varētu samazināt par aptuveni 180 līdz 290 miljardiem EUR gadā[38]. Tas radītu apgrozījuma palielināšanos, jo pieaugtu pieprasījums pēc produktiem ar digitāliem elementiem. Tas uzlabotu uzņēmumu globālo reputāciju, kā rezultātā pieprasījums pieaugtu arī ārpus ES. Lietotājiem vēlamais risinājums uzlabotu drošības īpašību pārredzamību un sekmētu produktu ar digitāliem elementiem lietošanu. Patērētāji un iedzīvotāji iegūtu arī no tā, ka tiktu labāk aizsargātas viņu pamattiesības, piemēram, privātums un datu aizsardzība.

Tajā pašā laikā šis priekšlikums palielinātu atbilstības un izpildes panākšanas izmaksas uzņēmumiem, paziņotajām struktūrām un publiskā sektora iestādēm, to vidū akreditācijas un tirgus uzraudzības iestādēm. Programmatūras izstrādātājiem un aparatūras ražotājiem tas palielinās atbilstības nodrošināšanas tiešās izmaksas saistībā ar jaunām drošības prasībām, atbilstības novērtēšanu, dokumentāciju un ziņošanas pienākumiem, kā rezultātā atbilstības nodrošināšanas kopējās izmaksas sasniegs aptuveni 29 miljardus EUR attiecībā uz apgrozījuma aplēsto tirgus vērtību 1485 miljardi EUR[39]. Lietotājiem, ietverot uzņēmumus, patērētājiem un iedzīvotājiem varētu tikt noteiktas augstākas cenas par produktiem ar digitāliem elementiem. Tomēr tās būtu jāvērtē, ņemot vērā iepriekš aprakstītos būtiskos ieguvumus.

1.4.3. Snieguma rādītāji

Norādīt rādītājus attiecībā uz progresa un sasniegumu uzraudzību.

Lai pārbaudītu, vai ražotāji uzlabo drošību saviem produktiem ar digitāliem elementiem, sākot no minēto produktu projektēšanas un izstrādes posma, un visā to aprites ciklā, varētu ņemt vērā vairākus rādītājus. Tie varētu būt ievainojamības izraisītu nozīmīgu incidentu skaits Savienībā, tādu aparatūras un programmatūras ražotāju īpatsvars, kuri ievēro sistemātiskas un drošas izstrādes aprites ciklu, kvalitatīva drošības analīze attiecībā uz produktiem ar digitāliem elementiem, ievainojamību datubāzu kvantitatīvs un kvalitatīvs novērtējums, ražotāju nodrošināto programmatūras drošības ielāpu biežums vai vidējais dienu skaits starp ievainojamības atklāšanu un programmatūras drošības ielāpu nodrošināšanu.

Rādītājs attiecībā uz saskaņotu kiberdrošības satvaru varētu būt mērķtiecīgu valsts kiberdrošības tiesību aktu trūkums.

Rādītājs labākai pārredzamībai attiecībā uz produktu ar digitāliem elementiem drošības īpašībām varētu būt to produktu ar digitāliem elementiem īpatsvars, kuri tiek piegādāti kopā ar informāciju par drošības īpašībām. Turklāt to produktu ar digitāliem elementiem īpatsvaru, kuri tiek piegādāti kopā ar norādījumiem lietotājam par drošu lietošanu, varētu izmantot kā rādītāju attiecībā uz to, vai organizācijām un patērētājiem tiek sniegta iespēja droši lietot produktus ar digitāliem elementiem.

Attiecībā uz regulas ietekmes uzraudzību šajā ziņā būtu jāapsver noteikti rādītāji, kas — vajadzības gadījumā ar *ENISA* atbalstu — jāizvērtē Komisijai. Atkarībā no sasniedzamā darbības mērķa daži uzraudzības rādītāji, uz kuru pamata tiktu izvērtēta horizontālo kiberdrošības prasību ietekme, ir šādi:

[38] Skatīt [Komisijas dienestu darba dokumentu par ietekmes novērtējuma ziņojumu, kas pievienots Regulai par horizontālajām kiberdrošības prasībām attiecībā uz produktiem, ar digitāliem elementiem].

[39] Skatīt [Komisijas dienestu darba dokumentu par ietekmes novērtējuma ziņojumu, kas pievienots Regulai par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem].

Lai izvērtētu produktu ar digitāliem elementiem kiberdrošības līmeni:

- statistika un kvalitatīva analīze par incidentiem, kas skar produktus ar digitāliem elementiem, un par to, kā tie tikuši risināti. To varētu apkopot un izvērtēt Komisija ar *ENISA* atbalstu;

- zināmo ievainojamību uzskaite un analīze par to, kā tās ir tikušas risinātas. Šādu analīzi varētu veikt *ENISA*, pamatojoties uz Eiropas ievainojamību datubāzi, kas izveidota, pamatojoties uz [Direktīva XXX/XXXX (TID2)];

- aparatūras un programmatūras ražotāju apsekojumi ar mērķi uzraudzīt progresu.

Lai izvērtētu informācijas līmeni attiecībā uz drošības elementiem, drošības atbalstu, ekspluatācijas laika beigām un rūpības pienākumu: to apsekojumu rezultāti, kas Komisijai ar *ENISA* atbalstu jāveic gan par lietotājiem, gan uzņēmumiem.

Lai izvērtētu īstenošanu, Komisija centīsies nodrošināt, ka atbilstības novērtējumi tiek veikti efektīvi. Šajā nolūkā tiks izdots standartizācijas pieprasījums un tiks sekots tā īstenošanai. Komisija arī pārbaudīs paziņoto struktūru un attiecīgā gadījumā sertifikācijas struktūru spējas.

Attiecībā uz piemērošanu Komisija, izmantojot dalībvalstu ziņojumus, pārbaudīs, vai valstu iniciatīvas neattiecas uz aspektiem, kuriem piemēro šo regulu.

1.5. Priekšlikuma/iniciatīvas pamatojums

1.5.1. Īstermiņā vai ilgtermiņā izpildāmās vajadzības, ieskaitot sīki izstrādātu iniciatīvas izvēršanas grafiku

Regulai vajadzētu būt pilnīgi piemērojamai 24 mēnešus pēc tās stāšanās spēkā. Taču pārvaldes struktūras elementi būtu jāievieš agrāk. Konkrēti – dalībvalstīm ir jānorīko pastāvošas iestādes un/vai jāizveido jaunas iestādes tiesību aktos noteikto uzdevumu izpildei.

1.5.2. Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka rezultativitāte vai komplementaritāte). Šā punkta izpratnē "Savienības iesaistīšanās pievienotā vērtība" ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.

Kiberdrošības izteiktais pārrobežu raksturs un pieaugošais to incidentu skaits, kuru ietekme izvēršas pāri robežām, starp dažādām nozarēm un produktiem, nozīmē, ka dalībvalstis vienas pašas nevar efektīvi sasniegt mērķus. Ņemot vērā produktu ar digitāliem elementiem tirgu globālo raksturu, dalībvalstis savā teritorijā attiecībā uz vienu un to pašu produktu ar digitāliem elementiem saskaras ar vieniem un tiem pašiem riskiem. Jauns sadrumstalots regulējums, ko veido potenciāli atšķirīgi valstu noteikumi, arī rada risku, ka varētu tikt kavēts atvērts un konkurētspējīgs vienotais tirgus attiecībā uz produktiem ar digitāliem elementiem. Tāpēc, lai palielinātu lietotāju uzticēšanos un ES produktu ar digitāliem elementiem pievilcību, ir vajadzīga vienota rīcība ES līmenī. Tā nāktu par labu arī iekšējam tirgum, nodrošinot juridisko noteiktību un panākot vienlīdzīgus konkurences apstākļus produktu ar digitāliem elementiem tirgotājiem.

1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas

Kibernoturības akts ir pirmais šāda veida regulējums, ar ko ievieš kiberdrošības prasības attiecībā uz produktu ar digitāliem elementiem laišanu tirgū. Tomēr tas pamatojas uz jaunā tiesiskā regulējuma izveidi un pieredzi, kas gūta dažādiem produktiem paredzētu spēkā esošu Savienības saskaņošanas tiesību aktu īstenošanas procesā, jo īpaši attiecībā uz sagatavošanos īstenošanai, ieskaitot tādus aspektus kā saskaņoto standartu sagatavošana.

1.5.4. Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem

Regulā par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem ir noteiktas jaunas kiberdrošības prasības visiem produktiem ar digitāliem elementiem, kas laisti ES tirgū, pārsniedzot spēkā esošajos tiesību aktos paredzētās prasības. Tajā pašā laikā šis priekšlikums pamatojas uz pašreizējo JTR tiesību aktu izveidi. Tāpēc tas pamatotos uz esošajām JTR struktūrām un procedūrām, piemēram, paziņoto struktūru sadarbību un tirgus uzraudzību, atbilstības novērtēšanas moduļiem, saskaņoto standartu izstrādi. Jaunais priekšlikums balstītos arī uz dažām struktūrām, kas izstrādātas saskaņā ar citiem kiberdrošības tiesību aktiem, piemēram, Direktīvu 2016/1148 (TID direktīva) — attiecīgi [Direktīva XXX/XXXX (TID2)] vai Regulu 2019/881 (Kiberdrošības akts).

1.5.5. Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtējums

ENISA uzticēto darbības jomu pārvaldība atbilst tās pašreizējam pilnvarojumam un vispārējiem uzdevumiem. Šīm darbības jomām varētu būt nepieciešami konkrēti darbības virzieni vai jauni uzdevumi, bet tie nebūtu īpaši nozīmīgi, un tos varētu apgūt ar *ENISA* esošajiem resursiem un atrisināt, pārdalot vai sasaistot dažādus uzdevumus. Piemēram, viena no galvenajām *ENISA* uzticētajām darbības jomām attiecas uz ražotāju paziņojumu par izmantotajām produktu ievainojamībām vākšanu un apstrādi. [Direktīvā XXX/XXXX (TID2)] jau ir uzdots *ENISA* izveidot Eiropas ievainojamību datubāzi, kurā var brīvprātīgi atklāt un reģistrēt publiski zināmas ievainojamības, lai lietotāji varētu veikt atbilstīgus riska mazināšanas pasākumus. Šim nolūkam piešķirtos resursus varētu izmantot arī attiecībā uz iepriekš minētajiem jaunajiem uzdevumiem, kas saistīti ar paziņojumiem par produktu ievainojamībām. Tas varētu nodrošināt esošo resursu efektīvu izmantošanu un arī radītu nepieciešamo šādu uzdevumu sinerģiju, kas varētu uzlabot *ENISA* kiberdrošības risku un apdraudējumu analīzes informēšanu.

1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme

☐ **ierobežots ilgums**

– ☐ Priekšlikuma/iniciatīvas darbības laiks: [DD.MM.]GGGG.–[DD.MM.]GGGG.

– ☐ Finansiālā ietekme uz saistību apropriācijām – no GGGG. līdz GGGG. gadam, uz maksājumu apropriācijām – no GGGG. līdz GGGG. gadam.

× **beztermiņa**

– Īstenošana ar sākumposmu no 2025. gada.

– pēc kura turpinās normāla darbība.

1.7. Paredzētais(-tie) pārvaldības veids(-i)[40]

☐ Komisijas īstenota **tieša pārvaldība**:

– × ko veic tās struktūrvienības, tostarp personāls Savienības delegācijās;

– ☐ ko veic izpildaģentūras.

☐ **Dalīta pārvaldība** kopā ar dalībvalstīm

☐ **Netieša pārvaldība**, kurā budžeta izpildes uzdevumi uzticēti:

– ☐ trešām valstīm vai to izraudzītām struktūrām;

– ☐ starptautiskām organizācijām un to aģentūrām (precizēt);

– ☐ EIB un Eiropas Investīciju fondam;

– ☐ Finanšu regulas 70. un 71. pantā minētajām struktūrām;

– ☐ publisko tiesību subjektiem;

– ☐ privāttiesību subjektiem, kas veic sabiedrisko pakalpojumu sniedzēju uzdevumus, tādā mērā, kādā tiem ir pienācīgas finansiālās garantijas;

– ☐ dalībvalstu privāttiesību subjektiem, kuriem ir uzticēta publiskā un privātā sektora partnerības īstenošana un kuriem ir pienācīgas finansiālas garantijas;

– ☐ personām, kurām, ievērojot Līguma par Eiropas Savienību V sadaļu, uzticēts īstenot konkrētas KĀDP darbības un kuras ir noteiktas attiecīgajā pamataktā.

– *Ja norādīti vairāki pārvaldības veidi, sniedziet papildu informāciju iedaļā "Piezīmes".*

Piezīmes

Ar šo regulu *ENISA* tiek uzticētas konkrētas darbības saskaņā ar tās esošajām pilnvarām un jo īpaši ar Regulas 2019/881 3. panta 2. punktu, kurā noteikts, ka *ENISA* būtu jāpilda uzdevumi, kas tai noteikti Savienības tiesību aktos, kuros paredzēti pasākumi dalībvalstu kiberdrošības jomā izstrādāto normatīvo un administratīvo aktu tuvināšanai. Konkrēti *ENISA* ir uzdots saņemt ražotāju paziņojumus par aktīvi izmantotām ievainojamībām produktos ar digitāliem elementiem, kā arī par incidentiem, kuri ietekmē minēto produktu drošību. *ENISA* būtu arī jāpārsūta šie paziņojumi attiecīgajām *CSIRT* vai attiecīgi noteiktajam dalībvalstu vienotajam kontaktpunktam, kas izraudzīts saskaņā ar Direktīvas [Direktīva XXX/XXXX (TID2)] pantu [X. pants], kā arī jāinformē tirgus uzraudzības iestādes. *ENISA*, pamatojoties uz savākto informāciju, reizi divos gados būtu jāsagatavo tehniskais ziņojums par jaunākajām tendencēm

[40] Sīkāku informāciju par pārvaldības veidiem un atsauces uz Finanšu regulu skatīt *BudgWeb* tīmekļvietnē: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

attiecībā uz kiberdrošības riskiem produktos ar digitāliem elementiem, un tas jāiesniedz TID sadarbības grupai. Turklāt, ņemot vērā *ENISA* īpašās zināšanas, savākto informāciju un apdraudējumu analīzi, *ENISA* var atbalstīt šīs regulas īstenošanas procesu, ierosinot kopīgas darbības, kas valstu 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 varētu organizēt vienlaicīgas koordinētas kontroles darbības. Izņēmuma apstākļos Komisija var pieprasīt *ENISA* veikt konkrētu produktu izvērtēšanu attiecībā uz produktiem ar digitāliem elementiem, kas rada būtisku kiberdrošības risku, un ja ir nepieciešama tūlītēja intervence ar mērķi saglabāt pareizu iekšējā tirgus darbību.

Tiek lēsts, ka visi šie uzdevumi veidos aptuveni 4,5 pilnslodzes ekvivalentus (FTE) no esošajiem *ENISA* resursiem, pamatojoties uz jau esošajām *ENISA* īpašajām zināšanām un sagatavošanas darbu, ko tā pašlaik veic, cita starpā atbalstot [Direktīvas XXX/XXXX (TID2)] gaidāmo īstenošanu, kuras vajadzībām *ENISA* resursi tika papildināti.

2. PĀRVALDĪBAS PASĀKUMI

2.1. Pārraudzības un ziņošanas noteikumi

Norādīt biežumu un nosacījumus.

36 mēnešus pēc šīs regulas piemērošanas dienas un pēc tam reizi četros gados Komisija iesniegs Eiropas Parlamentam un Padomei ziņojumu par tās izvērtēšanu un pārskatīšanu. Šos ziņojumus publisko.

2.2. Pārvaldības un kontroles sistēma(-s)

2.2.1. Ierosināto pārvaldības veidu, finansējuma apgūšanas mehānismu, maksāšanas kārtības un kontroles stratēģijas pamatojums

Ar šo regulu izveido jaunu politiku attiecībā uz saskaņotām kiberdrošības prasībām, ko piemēro produktiem ar digitāliem elementiem, ko laiž iekšējā tirgū, visā to aprites ciklā. Pēc tiesību akta pieņemšanas Komisija lūgs Eiropas standartizācijas iestādēm izstrādāt standartus.

Lai veiktu šos jaunos uzdevumus, Komisijas dienestiem ir nepieciešami atbilstīgi resursi. Tiek lēsts, ka jaunās regulas izpildes panākšanai būs vajadzīgi 7 FTE (no tiem viens END), lai nodrošinātu šādu uzdevumu veikšanu:

- standartizācijas pieprasījuma un/vai kopīgo specifikāciju sagatavošana, izmantojot īstenošanas aktus, ja standartizācijas process nav sekmīgs;
- [12 mēnešu laikā pēc regulas stāšanās spēkā] tāda deleģētā akta sagatavošana, kurā precizētas kritiski svarīgo produktu ar digitāliem elementiem definīcijas;
- iespējamā deleģēto aktu sagatavošana attiecībā uz I un II klases kritiski svarīgo produktu saraksta atjaunināšanu; precizēšana, vai ir nepieciešams ierobežojums vai izslēgšana attiecībā uz produktiem ar digitāliem elementiem, uz kuriem attiecas citi Savienības noteikumi, ar ko nosaka prasības, kas nodrošina tādu pašu aizsardzības līmeni kā šī regula; pilnvaru piešķiršana attiecībā uz noteiktu ļoti kritiski svarīgu produktu ar digitāliem elementiem sertificēšanu, pamatojoties uz šajā regulā noteiktajiem kritērijiem; ES atbilstības deklarācijas minimālā satura precizēšana un tehniskajā dokumentācijā iekļaujamo elementu papildināšana;
- iespējamā īstenošanas aktu sagatavošana attiecībā uz ziņošanas pienākumu, programmatūras materiālu komplekta, kopīgo specifikāciju vai *CE* zīmes uzlikšanas formātu vai elementiem;
- iespējamā tūlītējas intervences sagatavošana, lai izņēmuma apstākļos piemērotu korektīvus vai ierobežojošus pasākumus nolūkā saglabāt iekšējā tirgus pareizu darbību, arī īstenošanas akta sagatavošana;
- dalībvalstu paziņoto struktūru paziņojumu organizēšana un koordinēšana un paziņoto struktūru koordinēšana;
- dalībvalstu tirgus uzraudzības iestāžu koordinācijas atbalstīšana.

2.2.2. Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto iekšējās kontroles sistēmu

Lai nodrošinātu, ka paziņotās struktūras un tirgus uzraudzības iestādes apmainās ar informāciju un sekmīgi sadarbojas, Komisija ir atbildīga par to koordināciju. Īpašo tehnisko un tirgus zināšanu nodrošināšanai tiktu izveidota ekspertu grupa.

2.2.3. Kontroles izmaksefektivitātes (kontroles izmaksu attiecība pret attiecīgo pārvaldīto līdzekļu vērtību) aplēse un pamatojums un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas brīdī un slēgšanas brīdī)

2.3. Sanāksmju izdevumiem pietiekamas šķiet standarta kontroles procedūras, jo viena darījuma (piemēram, ceļa izdevumu atmaksāšana delegātam pēc dalības sanāksmē) vērtība ir zema. Krāpšanas un pārkāpumu novēršanas pasākumi

Norādīt esošos vai plānotos novēršanas pasākumus un citus pretpasākumus, piemēram, krāpšanas apkarošanas stratēģijā iekļautos pasākumus.

Pašreizējie krāpšanas novēršanas pasākumi, kas piemērojami Komisijai, attieksies arī uz papildu apropriācijām, kas nepieciešamas saskaņā ar šo regulu.

3. PRIEKŠLIKUMA/INICIATĪVAS APLĒSTĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorija(-s) un budžeta izdevumu pozīcija(-s)

- Esošās budžeta pozīcijas

Shēma

- No jauna veidojamās budžeta pozīcijas

Neattiecas

3.2. Priekšlikuma aplēstā finansiālā ietekme uz apropriācijām

3.2.1. Kopsavilkums par aplēsto ietekmi uz darbības apropriācijām

– ☑ Priekšlikumam/iniciatīvai nav vajadzīgas darbības apropriācijas

– ☐ Priekšlikumam/iniciatīvai ir vajadzīgas šādas darbības apropriācijas:

miljonos EUR (trīs zīmes aiz komata)

Daudzgadu finanšu shēmas izdevumu kategorija	Numurs	

ĢD: <…….>			Gads **N**[41]	Gads **N+1**	Gads **N+2**	Gads **N+3**	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			**KOPĀ**
• Darbības apropriācijas										
Budžeta pozīcija[42]	Saistības	(1a)								
	Maksājumi	(2a)								
Budžeta pozīcija	Saistības	(1b)								
	Maksājumi	(2b)								
Administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem[43]										
Budžeta pozīcija		(3)								
KOPĀ apropriācijas attiecībā uz ĢD <…….>	Saistības	=1a+1b +3								
	Maksājumi	=2a+2b								

41 N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet "N" ar paredzēto pirmo īstenošanas gadu (piemēram, 2021). Tas pats attiecas uz turpmākajiem gadiem.

42 Saskaņā ar oficiālo budžeta nomenklatūru.

43 Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās BA pozīcijas), netiešā pētniecība, tiešā pētniecība.

		+3								

• KOPĀ darbības apropriācijas	Saistības	(4)								
	Maksājumi	(5)								
• KOPĀ administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem		(6)								
KOPĀ daudzgadu finanšu shēmas <….> **IZDEVUMU KATEGORIJAS apropriācijas**	Saistības	=4+6								
	Maksājumi	=5+6								

<u>Ja priekšlikums/iniciatīva ietekmē vairāk nekā vienu darbības izdevumu kategoriju, atkārtot iepriekš minēto iedaļu:</u>

• KOPĀ darbības apropriācijas (visas darbības izdevumu kategorijas)	Saistības	(4)								
	Maksājumi	(5)								
KOPĀ administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem (visas darbības izdevumu kategorijas)		(6)								
KOPĀ daudzgadu finanšu shēmas **1.–6. IZDEVUMU KATEGORIJAS apropriācijas** (Atsauces summa)	Saistības	=4+6								
	Maksājumi	=5+6								

Daudzgadu finanšu shēmas izdevumu kategorija	**7**	"Administratīvie izdevumi"

Šī iedaļa būtu jāaizpilda, izmantojot administratīva rakstura budžeta datu izklājlapu, kas vispirms jānoformē tiesību akta finanšu pārskata pielikumā (iekšējo noteikumu V pielikums), kurš starpdienestu konsultāciju vajadzībām tiek augšupielādēts sistēmā *DECIDE*.

miljonos EUR (trīs zīmes aiz komata)

		Gads **2024**	Gads **2025**	Gads **2026**	Gads **2027**	**KOPĀ**
ĢD: CNECT						
• Cilvēkresursi		1,030	1,030	1,030	1,030	**4,120**
• Pārējie administratīvie izdevumi		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
KOPĀ CNECT **ĢD**	Apropriācijas	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

KOPĀ daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS apropriācijas	(Saistību summa = maksājumu summa)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

miljonos EUR (trīs zīmes aiz komata)

		Gads **2024**	Gads **2025**	Gads **2026**	Gads **2027**	**KOPĀ**
KOPĀ daudzgadu finanšu shēmas **1.–7. IZDEVUMU KATEGORIJAS apropriācijas**	Saistības	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Maksājumi	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Aplēstais iznākums, ko dos finansējums no darbības apropriācijām

Saistību apropriācijas miljonos EUR (trīs zīmes aiz komata)

Norādīt mērķus un iznākumus ⇩			Gads **N**		Gads **N+1**		Gads **N+2**		Gads **N+3**		Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)						**KOPĀ**	
	IZNĀKUMI																	
	Veids [44]	Vidējais izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Kopējais daudzums	Kopējās izmaksas
KONKRĒTAIS MĒRĶIS Nr. 1 [45]…																		
- Iznākums																		
- Iznākums																		
- Iznākums																		
Starpsumma – konkrētais mērķis Nr. 1																		
KONKRĒTAIS MĒRĶIS Nr. 2 ...																		
- Iznākums																		
Starpsumma – konkrētais mērķis Nr. 2																		
KOPSUMMAS																		

[44] Iznākumi ir attiecīgie produkti vai pakalpojumi, kas jānodrošina (piemēram, finansēto studentu apmaiņu skaits, uzbūvēto ceļu garums kilometros utt.).

[45] Kā norādīts 1.4.2. punktā "Konkrētais(-ie) mērķis(mērķi)...".

3.2.3. Kopsavilkums par aplēsto ietekmi uz administratīvajām apropriācijām

– ☐ Priekšlikumam/iniciatīvai nav vajadzīgas administratīvās apropriācijas

– ☑ Priekšlikumam/iniciatīvai ir vajadzīgas šādas administratīvās apropriācijas:

miljonos EUR (trīs zīmes aiz komata)

	Gads **2024**	Gads **2025**	Gads **2026**	Gads **2027**	
Daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJA					
Cilvēkresursi	1,030	1,030	1,030	1,030	**4,120**
Citi administratīvie izdevumi	0,222	0,222	0,222	0,222	**0,888**
Starpsumma — daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJA	1,252	1,252	1,252	1,252	**5,008**
Ārpus daudzgadu finanšu shēmas[46] 7. IZDEVUMU KATEGORIJAS					
Cilvēkresursi					
Pārējie administratīvie izdevumi					
Starpsumma — ārpus daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS					
KOPĀ	1,252	1,252	1,252	1,252	**5,008**

Vajadzīgās cilvēkresursu un citu administratīvu izdevumu apropriācijas tiks nodrošinātas no ĢD apropriācijām, kas jau ir piešķirtas darbības pārvaldībai un/vai ir pārdalītas attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtus papildu resursus un ņemot vērā budžeta ierobežojumus.

46 Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās BA pozīcijas), netiešā pētniecība, tiešā pētniecība.

3.2.3.1. Aplēstās cilvēkresursu vajadzības

– ☐ Priekšlikumam/iniciatīvai nav vajadzīgi cilvēkresursi

– ☑ Priekšlikumam/iniciatīvai ir vajadzīgi šādi cilvēkresursi:

Aplēse izsakāma ar pilnslodzes ekvivalentu

		Gads **2024**	Gads **2025**	Gads **2026**	Gads **2027**
20 01 02 01 (Galvenā mītne un Komisijas pārstāvniecības)		6	6	6	6
20 01 02 03 (Delegācijas)					
01 01 01 01 (Netiešā pētniecība)					
01 01 01 11 (Tiešā pētniecība)					
Citas budžeta pozīcijas (norādīt)					
• Ārštata darbinieki (izsakot ar pilnslodzes ekvivalentu FTE)[47]					
20 02 01 (AC, END, INT, ko finansē no vispārīgajām apropriācijām)		1	1	1	1
20 02 03 (AC, AL, END, INT un JPD delegācijās)					
XX 01 xx **yy zz** [48]	- galvenajā mītnē				
	- delegācijās				
01 01 01 02 (AC, END, INT – netiešā pētniecība)					
01 01 01 12 (AC, END, INT – tiešā pētniecība)					
Citas budžeta pozīcijas (norādīt)					
KOPĀ		**7**	**7**	**7**	**7**

XX ir attiecīgā politikas joma vai budžeta sadaļa.

Nepieciešamie cilvēkresursi tiks nodrošināti, izmantojot attiecīgā ĢD darbiniekus, kuri jau ir iesaistīti konkrētās darbības pārvaldībā un/vai ir pārgrupēti attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtos papildu resursus un ņemot vērā budžeta ierobežojumus.

Veicamo uzdevumu apraksts:

Ierēdņi un pagaidu darbinieki 6 FTE x 157 000 EUR/gadā = 942 000 EUR	Kā aprakstīts 2.2.1. punktā: – standartizācijas pieprasījuma un/vai kopīgo specifikāciju sagatavošana, izmantojot īstenošanas aktus, ja standartizācijas process nav sekmīgs; – [12 mēnešu laikā pēc regulas stāšanās spēkā] tāda deleģētā akta sagatavošana, kurā precizētas kritiski svarīgo produktu ar digitāliem elementiem definīcijas; – iespējamā deleģēto aktu sagatavošana attiecībā uz I un II klases kritiski svarīgo produktu saraksta atjaunināšanu; precizēšana, vai ir nepieciešams ierobežojums vai izslēgšana attiecībā uz produktiem ar digitāliem elementiem, uz kuriem attiecas citi Savienības noteikumi, ar ko nosaka prasības, kas nodrošina tādu pašu aizsardzības līmeni kā šī regula; pilnvaru piešķiršana attiecībā uz noteiktu ļoti kritiski svarīgu produktu ar digitāliem elementiem sertificēšanu, pamatojoties uz šajā regulā noteiktajiem kritērijiem; ES atbilstības deklarācijas minimālā satura

47 AC – līgumdarbinieki; AL – vietējie darbinieki, END – valstu norīkotie eksperti, INT – aģentūru darbinieki, JPD – jaunākie eksperti delegācijās.

48 Ārštata darbiniekiem paredzēto maksimālo summu finansē no darbības apropriācijām (kādreizējām BA pozīcijām).

	precizēšana un tehniskajā dokumentācijā iekļaujamo elementu papildināšana; – iespējamā īstenošanas aktu sagatavošana attiecībā uz ziņošanas pienākumu, programmatūras materiālu komplekta, kopīgo specifikāciju vai *CE* zīmes uzlikšanas formātu vai elementiem; – iespējamā tūlītējas intervences sagatavošana, lai izņēmuma apstākļos piemērotu korektīvus vai ierobežojošus pasākumus nolūkā saglabāt iekšējā tirgus pareizu darbību, arī īstenošanas akta sagatavošana; – dalībvalstu paziņoto struktūru paziņojumu organizēšana un koordinēšana un paziņoto struktūru koordinēšana; – dalībvalstu tirgus uzraudzības iestāžu koordinācijas atbalstīšana.
Ārštata darbinieki 1 END x 88 000 EUR/gadā	Kā aprakstīts 2.2.1. punktā: – standartizācijas pieprasījuma un/vai kopīgo specifikāciju sagatavošana, izmantojot īstenošanas aktus, ja standartizācijas process nav sekmīgs; – [12 mēnešu laikā pēc regulas stāšanās spēkā] tāda deleģētā akta sagatavošana, kurā precizētas kritiski svarīgo produktu ar digitāliem elementiem definīcijas; – iespējamā deleģēto aktu sagatavošana attiecībā uz I un II klases kritiski svarīgo produktu saraksta atjaunināšanu; precizēšana, vai ir nepieciešams ierobežojums vai izslēgšana attiecībā uz produktiem ar digitāliem elementiem, uz kuriem attiecas citi Savienības noteikumi, ar ko nosaka prasības, kas nodrošina tādu pašu aizsardzības līmeni kā šī regula; pilnvaru piešķiršana attiecībā uz noteiktu ļoti kritiski svarīgu produktu ar digitāliem elementiem sertificēšanu, pamatojoties uz šajā regulā noteiktajiem kritērijiem; ES atbilstības deklarācijas minimālā satura precizēšana un tehniskajā dokumentācijā iekļaujamo elementu papildināšana; – iespējamā īstenošanas aktu sagatavošana attiecībā uz ziņošanas pienākumu, programmatūras materiālu komplekta, kopīgo specifikāciju vai *CE* zīmes uzlikšanas formātu vai elementiem; – iespējamā tūlītējas intervences sagatavošana, lai izņēmuma apstākļos piemērotu korektīvus vai ierobežojošus pasākumus nolūkā saglabāt iekšējā tirgus pareizu darbību, arī īstenošanas akta sagatavošana; – dalībvalstu paziņoto struktūru paziņojumu organizēšana un koordinēšana un paziņoto struktūru koordinēšana; – dalībvalstu tirgus uzraudzības iestāžu koordinācijas atbalstīšana.

3.2.4. Saderība ar pašreizējo daudzgadu finanšu shēmu

Priekšlikuma/iniciatīvas finansēšanai:

– x pilnībā pietiek ar līdzekļu pārvietošanu daudzgadu finanšu shēmas (DFS) attiecīgajā izdevumu kategorijā.

Pārplānošana nav nepieciešama.

– ☐ jāizmanto no DFS attiecīgās izdevumu kategorijas nepiešķirtās rezerves un/vai īpašie instrumenti, kas noteikti DFS regulā.

-

– ☐ jāpārskata DFS.

-

3.2.5. Trešo personu iemaksas

Priekšlikums/iniciatīva:

– x neparedz trešo personu līdzfinansējumu

– ☐ paredz trešo personu sniegtu līdzfinansējumu atbilstoši šādai aplēsei:

Apropriācijas miljonos EUR (trīs zīmes aiz komata)

	Gads **N**[49]	Gads **N+1**	Gads **N+2**	Gads **N+3**	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			Kopā
Norādīt līdzfinansētāju struktūru								
KOPĀ līdzfinansētās apropriācijas								

[49] N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet "N" ar paredzēto pirmo īstenošanas gadu (piemēram, 2021). Tas pats attiecas uz turpmākajiem gadiem.

3.3. Aplēstā ietekme uz ieņēmumiem

– ☐ Priekšlikums/iniciatīva finansiāli neietekmē ieņēmumus.

– ☐ Priekšlikums/iniciatīva finansiāli ietekmē:

– ☐ pašu resursus

– ☐ citus ieņēmumus

– Atzīmējiet, ja ieņēmumi ir piešķirti izdevumu pozīcijām ☐

miljonos EUR (trīs zīmes aiz komata)

Budžeta ieņēmumu pozīcija:	Kārtējā finanšu gadā pieejamās apropriācijas	Priekšlikuma/iniciatīvas ietekme[50]						
		Gads **N**	Gads **N+1**	Gads **N+2**	Gads **N+3**	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		
... pants								

Attiecībā uz piešķirtajiem ieņēmumiem norādīt attiecīgo(-ās) izdevumu pozīciju(-as).

Citas piezīmes (piemēram, metode/formula, ko izmanto, lai aprēķinātu ietekmi uz ieņēmumiem, vai jebkura cita informācija).

[50] Norādītajām tradicionālo pašu resursu (muitas nodokļi, cukura nodevas) summām jābūt neto summām, t. i., bruto summām, no kurām atskaitītas iekasēšanas izmaksas 20 % apmērā.