EUROPOS
KOMISIJA

Briuselis, 2022 09 15
COM(2022) 454 final

2022/0272 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams, kuriuo iš dalies keičiamas Reglamentas (ES) 2019/1020

(Tekstas svarbus EEE)

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

AIŠKINAMASIS MEMORANDUMAS

1. PASIŪLYMO APLINKYBĖS

• Pasiūlymo pagrindimas ir tikslai

Aparatinės ir programinės įrangos produktai vis dažniau nukenčia nuo sėkmingų kibernetinių atakų – apskaičiuota, kad 2021 m. metinė kibernetinių nusikaltimų žala pasaulyje siekė 5,5 trln. EUR. Šiems produktams būdingos dvi pagrindinės problemos, dėl kurių naudotojai ir visuomenė patiria papildomų sąnaudų: 1) mažas kibernetinio saugumo lygis, kurį atspindi plačiai paplitę pažeidžiamumai ir nepakankamas bei nenuoseklus saugumo naujinių teikimas jiems spręsti, ir 2) nepakankamas naudotojų supratimas ir prieiga prie informacijos – todėl jie negali pasirinkti tinkamomis kibernetinio saugumo savybėmis pasižyminčių produktų ar saugiai juos naudoti. Susietoje aplinkoje kibernetinio saugumo incidentas viename produkte gali paveikti visą organizaciją ar visą tiekimo grandinę, dažnai išplisdamas per vidaus rinkos sienas vos per kelias minutes. Dėl to gali būti labai sutrikdyta ekonominė ir socialinė veikla ar netgi gali kilti grėsmė gyvybei.

Produktų su skaitmeniniais elementais kibernetiniam saugumui būdingas stiprus tarpvalstybinis aspektas, nes vienoje šalyje pagaminti produktai dažnai naudojami visoje vidaus rinkoje. Be to, incidentai, kurie iš pradžių paveikė vieną subjektą arba vieną valstybę narę, dažnai per kelias minutes išplinta visoje vidaus rinkoje.

Nors esami vidaus rinkos teisės aktai taikomi tam tikriems produktams su skaitmeniniais elementais, daugumai aparatinės ir programinės įrangos produktų šiuo metu netaikomi jokie ES teisės aktai, kuriais būtų sprendžiamas jų kibernetinis saugumas. Visų pirma, dabartinėje ES teisinėje sistemoje nesprendžiamas neįtaisytosios programinės įrangos kibernetinis saugumas, nors kibernetinėse atakose vis dažniau siekiama pasinaudoti šių produktų pažeidžiamumais ir dėl to patiriama didelė socialinė ir ekonominė žala. Yra daug pavyzdžių, kai dėmesio verta kibernetinė ataka kilo dėl nepakankamo produktų saugumo, pvz., išpirkos reikalaujanti programa „WannaCry“ išnaudojo „Windows“ pažeidžiamumą, dėl to 2017 m. buvo paveikta 200 000 kompiuterių 150 šalių ir padaryta daugelio milijardų JAV dolerių žala; „Kaseya VSA“ tiekimo grandinės ataka, per kurią pasinaudojus „Kaseya“ tinklo administravimo programine įranga buvo atakuota daugiau kaip 1 000 įmonių, o prekybos centrų tinklas buvo priverstas uždaryti visas savo 500 parduotuvių Švedijoje; arba daugybė incidentų, per kuriuos įsilaužta į bankų programas siekiant pavogti pinigus iš nieko neįtariančių vartotojų.

Nustatyti du pagrindiniai tikslai, kuriais siekiama užtikrinti tinkamą vidaus rinkos veikimą: 1) sudaryti sąlygas kurti saugius produktus su skaitmeniniais elementais užtikrinant, kad aparatinės ir programinės įrangos produktai būtų pateikiami rinkai su mažiau pažeidžiamumų ir kad gamintojai rimtai atsižvelgtų į saugumą viso produkto gyvavimo ciklo metu; ir 2) sudaryti sąlygas, kad rinkdamiesi ir naudodami produktus su skaitmeniniais elementais naudotojai galėtų atsižvelgti į kibernetinį saugumą. Nustatyti keturi konkretūs tikslai: i) užtikrinti, kad gamintojai padidintų produktų su skaitmeniniais elementais saugumą nuo projektavimo ir kūrimo etapo ir per visą gyvavimo ciklą; ii) užtikrinti nuoseklią kibernetinio saugumo sistemą, palengvinančią aparatinės ir programinės įrangos gamintojų reikalavimų laikymąsi; iii) padidinti produktų su skaitmeniniais elementais saugumo savybių skaidrumą ir iv) sudaryti sąlygas įmonėms ir vartotojams saugiai naudoti produktus su skaitmeniniais elementais.

Dėl kibernetinio saugumo stipraus tarpvalstybinio pobūdžio ir daugėjančių incidentų, persiduodančių tarp skirtingų valstybių narių, sektorių bei produktų, pavienės valstybės narės negali veiksmingai pasiekti šių tikslų. Atsižvelgiant į pasaulinį produktų su skaitmeniniais elementais rinkų pobūdį, valstybės narės savo teritorijoje susiduria su ta pačia rizika dėl to paties produkto su skaitmeniniais elementais. Besiformuojanti fragmentuota galimai skirtingų nacionalinių taisyklių sistema gali trukdyti atvirai ir konkurencingai bendrai produktų su skaitmeniniais elementais rinkai. Todėl reikia imtis bendrų veiksmų ES lygmeniu siekiant padidinti naudotojų pasitikėjimą ES produktais su skaitmeniniais elementais bei šių produktų patrauklumą. Tai taip pat būtų naudinga vidaus rinkai, nes suteiktų teisinio tikrumo ir sudarytų vienodas sąlygas produktų su skaitmeniniais elementais pardavėjams, kaip pabrėžta ir galutinėje Konferencijos dėl Europos ateities ataskaitoje, kurioje piliečiai ragina ES aktyviau kovoti su kibernetinio saugumo grėsmėmis.

- **Sąveika su toje pačioje politikos srityje galiojančiomis nuostatomis**

ES sistemą sudaro keletas horizontaliųjų teisės aktų, kurie apima skirtingus aspektus, susijusius su kibernetiniu saugumu (produktus, paslaugas, krizių valdymą ir nusikaltimus). 2013 m. įsigaliojo direktyva dėl atakų prieš informacines sistemas[1], kuria buvo suderintas kriminalizavimas ir sankcijos už įvairius nusikaltimus, nukreiptus prieš informacines sistemas. 2016 m. rugpjūčio mėn. įsigaliojo Direktyva (ES) 2016/1148 dėl tinklų ir informacinių sistemų saugumo (TIS direktyva)[2] kaip pirmasis visos ES teisės aktas dėl kibernetinio saugumo. Ją peržiūrėjus, parengta Direktyva [Direktyva XXX/XXXX (TIS2)], kuria padidinamas bendras ES užmojis. 2019 m. įsigaliojo ES Kibernetinio saugumo aktas[3], kuriuo siekiama padidinti IRT produktų, IRT paslaugų ir IRT procesų saugumą įvedant savanorišką Europos kibernetinio saugumo sertifikavimo sistemą[4].

Visos tiekimo grandinės kibernetinis saugumas užtikrinamas tik tuo atveju, jei visi jos komponentai yra kibernetiniu požiūriu saugūs. Tačiau minėtuose ES teisės aktuose šiuo atžvilgiu yra didelių spragų, nes jie neapima privalomų produktų su skaitmeniniais elementais saugumo reikalavimų.

Nors siūlomas Kibernetinio atsparumo aktas apima rinkai pateikiamus produktus su skaitmeniniais elementais, Direktyva [Direktyva XXX/XXX (TIS2)] siekiama užtikrinti aukštą esminių ir svarbių subjektų teikiamų paslaugų kibernetinio saugumo lygį. Direktyvoje [Direktyva XXX/XXXX (TIS2)] reikalaujama, kad valstybės narės užtikrintų, kad į taikymo sritį įtraukti esminiai ir svarbūs subjektai, pvz., sveikatos priežiūros arba debesijos kompiuterijos paslaugų teikėjai ir viešojo administravimo subjektai, imtųsi tinkamų ir proporcingų techninių, operacinių ir organizacinių kibernetinio saugumo priemonių. Tai, be kita ko, apima reikalavimą užtikrinti tinklų ir informacinių sistemų įsigijimo, kūrimo ir

---

1 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR OL L 218, 2013 8 14, p. 8–14.

2 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194/1, 2016 7 19, p. 1).

3 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15).

4 Kibernetinio saugumo aktu leidžiama kurti specialias sertifikavimo schemas. Kiekvienoje schemoje pateikiamos nuorodos į atitinkamus standartus, technines specifikacijas ar kitus schemoje nustatytus kibernetinio saugumo reikalavimus. Sprendimas plėtoti kibernetinio saugumo sertifikavimą pagrįstas rizika.

priežiūros saugumą, apimantį pažeidžiamumų valdymą ir atskleidimą. Direktyvoje [Direktyva XXX/XXXX (TIS2)] reikalaujama, kad Komisija per 21 mėnesį nuo tos direktyvos įsigaliojimo dienos priimtų įgyvendinimo aktus, kuriuose būtų nustatyti šių priemonių techniniai ir metodiniai reikalavimai tam tikrų tipų subjektams, pavyzdžiui, debesijos kompiuterijos paslaugų teikėjams. Visiems kitiems subjektams Komisija gali priimti įgyvendinimo aktą, kuriame būtų nustatyti techniniai ir metodiniai reikalavimai, taip pat sektorių reikalavimai. Ši sistema užtikrins, kad techninės specifikacijos ir priemonės, panašios į esminius Kibernetinio atsparumo akto kibernetinio saugumo reikalavimus, taip pat būtų įgyvendintos programinės įrangos, kuri teikiama kaip paslauga (paslauginės programinės įrangos), projektavimui, kūrimui ir pažeidžiamumų valdymui. Pavyzdžiui, tai galėtų būti būdas užtikrinti aukštą kibernetinio saugumo lygį elektroninių sveikatos įrašų sistemų atveju, taip pat tuomet, kai jie teikiami kaip paslauginė programinė įranga (SaaS) arba kuriami pačiose sveikatos priežiūros įstaigose (vietoje) pagal siūlomą [Europos sveikatos duomenų erdvės reglamentą].

- **Sąveika su kitomis Sąjungos politikos sritimis**

Komunikate „Europos skaitmeninės ateities formavimas“[5] pažymima, kad ES labai svarbu pasinaudoti visais skaitmeninio amžiaus privalumais ir sustiprinti savo pramonės bei inovacijų pajėgumą neperžengiant saugumo ir etikos ribų. Europos duomenų strategijoje nustatyti keturi ramsčiai – duomenų apsauga, pagrindinės teisės, sauga ir kibernetinis saugumas – yra būtinos sąlygos duomenų teikiamomis galimybėmis besinaudojančiai visuomenei.

Dabartinę produktams, kurie gali turėti ir skaitmeninių elementų, taikomą ES sistemą[6] sudaro keletas teisės aktų, įskaitant ES teisės aktus dėl konkrečių produktų, kuriais reglamentuojami su sauga susiję aspektai, ir bendruosius teisės aktus dėl atsakomybės už produktus. Pasiūlymas yra suderinamas su dabartine su produktais susijusia ES reglamentavimo sistema, taip pat su naujausiais teisės aktų pasiūlymais, tokiais kaip Komisijos pasiūlymas dėl Reglamento [Dirbtinio intelekto (DI) reglamentas][7].

Siūlomas reglamentas būtų taikomas visiems radijo įrenginiams, kuriems taikomas Komisijos deleguotasis reglamentas (ES) 2022/30. Be to, šiame reglamente nustatyti reikalavimai apima visus Direktyvos 2014/53/ES 3 straipsnio 3 dalies d, e ir f punktuose nurodytus esminius reikalavimus, įskaitant pagrindinius elementus, išdėstytus [Komisijos įgyvendinimo sprendime XXX/2022 dėl standartizacijos prašymo Europos standartizacijos organizacijoms], paskelbtame remiantis tuo deleguotuoju reglamentu. Siekiant išvengti reguliavimo dubliavimosi, numatoma, kad Komisija panaikins arba iš dalies pakeis deleguotąjį reglamentą dėl radijo įrenginių, kuriuos apima siūlomas reglamentas, kad jiems būtų taikomas pastarasis, kai jis bus taikytinas.

Be to, siekiant išvengti darbo dubliavimosi, numatoma, kad rengdamos ir plėtodamos darniuosius standartus, padėsiančius įgyvendinti reglamentą, Komisija ir Europos standartizacijos organizacijos atsižvelgs į standartizavimo darbą, atliekamą pagal Komisijos

---

5 2020 m. vasario 19 d. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos skaitmeninės ateities formavimas“, COM(2020) 67 *final*.

6 Daugiausia naujosios teisės aktų sistemos (NTAS) teisės aktai.

7 2021 m. balandžio 21 d. pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) ir iš dalies keičiami tam tikri Sąjungos teisėkūros procedūra priimti aktai, COM(2021) 206 *final*.

įgyvendinimo sprendimą C(2022)5637 dėl RED deleguotojo reglamento 2022/30 standartizacijos prašymo.

2. TEISINIS PAGRINDAS, SUBSIDIARUMO IR PROPORCINGUMO PRINCIPAI

• Teisinis pagrindas

Šio pasiūlymo teisinis pagrindas yra Sutarties dėl Europos Sąjungos veikimo (toliau – SESV) 114 straipsnis, kuriame numatyta galimybė priimti priemones, siekiant užtikrinti vidaus rinkos sukūrimą ir veikimą. Pasiūlymo tikslas – suderinti produktų su skaitmeniniais elementais kibernetinio saugumo reikalavimus visose valstybėse narėse ir pašalinti kliūtis laisvam prekių judėjimui.

SESV 114 straipsnis gali būti naudojamas kaip teisinis pagrindas siekiant išvengti tokių kliūčių atsiradimo dėl skirtingų nacionalinių teisės aktų ir teisinio netikrumo bei spragų esamose teisinėse sistemose sprendimo metodų[8]. Be to, Teisingumo Teismas pripažino, kad skirtingų techninių reikalavimų taikymas galėtų būti svarus pagrindas pradėti taikyti SESV 114 straipsnį[9].

Dabartinė produktams su skaitmeniniais elementais taikoma ES teisės aktų sistema pagrįsta SESV 114 straipsniu ir ją sudaro keletas teisės aktų, įskaitant teisės aktus dėl konkrečių produktų ir su sauga susijusių aspektų arba bendruosius teisės aktus dėl atsakomybės už produktus. Tačiau ji apima tik tam tikrus aspektus, susijusius su materialių skaitmeninių produktų ir, jei taikytina, į šiuos produktus įtaisytos programinės įrangos kibernetiniu saugumu. Nacionaliniu lygmeniu valstybės narės pradeda imtis nacionalinių priemonių, kuriomis reikalaujama, kad skaitmeninių produktų pardavėjai padidintų kibernetinį saugumą[10]. Be to, skaitmeninių produktų kibernetiniam saugumui būdingas itin stiprus tarpvalstybinis aspektas, nes vienoje šalyje pagamintus produktus dažnai naudoja organizacijos ir vartotojai visoje vidaus rinkoje. Incidentai, kurie iš pradžių apima vieną subjektą arba valstybę narę, dažnai per kelias minutes išplinta į kitas organizacijas, sektorius ir valstybes nares.

Įvairiais aktais ir iniciatyvomis, kurių iki šiol imtasi ES ir nacionaliniu lygmenimis, tik iš dalies sprendžiamos nustatytos problemos, tačiau kyla pavojus, kad vidaus rinkoje atsiras padrikas teisės aktų darinys, dėl kurio padidės teisinis netikrumas tiek šių produktų tiekėjams, tiek jų vartotojams, o įmonėms bus užkrauta nereikalinga našta, nes jos turės laikytis skirtingų tos pačios rūšies produktams taikomų reikalavimų.

Siūlomu reglamentu būtų suderinta ir supaprastinta ES reguliavimo aplinka įvedant produktų su skaitmeniniais elementais kibernetinio saugumo reikalavimus ir išvengiant iš skirtingų teisės aktų kylančių reikalavimų dubliavimosi. Tai užtikrintų didesnį teisinį tikrumą veiklos vykdytojams ir naudotojams visoje Sąjungoje, geriau suderintų Europos bendrąją rinką ir sudarytų palankesnes sąlygas veiklos vykdytojams, siekiantiems patekti į ES rinką.

---

8 2019 m. gruodžio 3 d. Europos Sąjungos Teisingumo Teismo (didžiosios kolegijos) sprendimas *Čekijos Respublika prieš Europos Parlamentą ir Europos Sąjungos Tarybą*, C-482/17, 35 punktas.

9 2006 m. gegužės 2 d. Europos Sąjungos Teisingumo Teismo (didžiosios kolegijos) sprendimas *Jungtinė Didžiosios Britanijos ir Šiaurės Airijos Karalystė prieš Europos Parlamentą ir Europos Sąjungos Tarybą*, C-217/04, 62–63 punktai.

10 Pavyzdžiui, 2019 m. Suomija sukūrė tokių daiktų interneto įrenginių, kaip išmanieji televizoriai, išmanieji telefonai ir žaislai ženklinimo sistemą, pagrįstą ETSI standartais. Vokietija neseniai pradėjo taikyti plačiajuosčio ryšio maršruto parinktuvų, išmaniųjų televizorių, kamerų, garsiakalbių, žaislų ir valymo ir sodo robotų vartotojų saugumo ženklinimą.

- **Subsidiarumo principas (neišimtinės kompetencijos atveju)**

Dėl kibernetinio saugumo stipraus tarpvalstybinio pobūdžio bendrąja prasme bei augančio skaičiaus pavojų ir incidentų, persiduodančių tarp skirtingų valstybių narių, sektorių ir produktų, pavienės valstybės narės negali veiksmingai pasiekti šios intervencijos tikslų. Nacionaliniai problemų sprendimo metodai, visų pirma metodai, kuriais nustatomi privalomi reikalavimai, sukurs papildomą teisinį netikrumą ir teisines kliūtis. Tai galėtų neleisti įmonėms sklandžiai plėstis į kitas valstybes nares, o naudotojai negautų šių įmonių produktų naudos.

Todėl reikia imtis bendrų veiksmų ES lygmeniu siekiant aukšto naudotojų pasitikėjimo ir didinant ES produktų su skaitmeniniais elementais patrauklumą. Tai taip pat būtų naudinga bendrai skaitmeninių produktų rinkai ir vidaus rinkai bendrąja prasme, nes suteiktų teisinio tikrumo ir sudarytų vienodas sąlygas produktų su skaitmeniniais elementais gamintojams.

Galiausiai 2022 m. gegužės 23 d. Tarybos išvadose dėl Europos Sąjungos kibernetinės pozicijos kūrimo Komisija raginama iki 2022 m. pabaigos pasiūlyti bendrus kibernetinio saugumo reikalavimus prijungtiesiems įrenginiams.

- **Proporcingumo principas**

Siūlomo reglamento proporcingumo požiūriu, svarstomų politikos galimybių priemonės neviršytų to, kas būtina bendriems ir konkretiems tikslams pasiekti, ir nesukeltų neproporcingų sąnaudų. Kalbant konkrečiau, nagrinėjama intervencija užtikrintų, kad produktai su skaitmeniniais elementais būtų apsaugoti per visą jų gyvavimo ciklą, proporcingai rizikai, su kuria susiduriama taikant į objektyvumą orientuotus ir technologiškai neutralius reikalavimus, kurie išliktų pagrįsti ir apskritai atitiktų susijusių subjektų interesus.

Esminiai pasiūlyme pateikti kibernetinio saugumo reikalavimai grindžiami plačiai taikomais standartais, o vėliau vyksiančiame standartizacijos procese būtų atsižvelgiama į techninius produktų ypatumus. Tai reiškia, kad prireikus saugumo kontrolės priemonės būtų pritaikomos konkrečiam rizikos lygiui. Be to, pagal numatytas horizontaliąsias taisykles trečiųjų šalių vertinimas numatomas tik ypatingos svarbos produktams. Tai apimtų tik nedidelę produktų su skaitmeniniais elementais rinkos dalį. Poveikis MVĮ priklausytų nuo jų dalyvavimo šių konkrečių kategorijų produktų rinkoje.

Kalbant apie atitikties vertinimo sąnaudų proporcingumą, trečiųjų šalių vertinimus atliekančios notifikuotosios įstaigos, nustatydamos mokesčius, atsižvelgtų į įmonės dydį. Taip pat būtų numatytas pagrįstas pereinamasis 24 mėnesių laikotarpis įgyvendinimui parengti – tai suteiktų laiko atitinkamoms rinkoms pasiruošti ir kartu nustatytų aiškią kryptį MTTP investicijoms. Įmonėms tenkančias reikalavimų laikymosi išlaidas atsvertų nauda, kurią atneštų didesnis produktų su skaitmeniniais elementais saugumo lygis, o galiausiai ir didesnis naudotojų pasitikėjimas šiais produktais.

- **Priemonės pasirinkimas**

Reglamentavimo intervencija reikštų, kad reikia priimti reglamentą, o ne direktyvą. Taip yra todėl, kad šios rūšies produktų teisės akto atveju reglamentu būtų veiksmingiau sprendžiamos nustatytos problemos ir siekiama suformuluotų tikslų, nes tai yra intervencija, kuria nustatomos sąlygos labai plačios kategorijos produktų pateikimui vidaus rinkai. Direktyvos atveju tokios intervencijos perkėlimo į nacionalinę teisę procesas galėtų palikti pernelyg daug veiksmų laisvės nacionaliniu lygmeniu, o tai galėtų lemti tam tikrų esminių kibernetinio saugumo reikalavimų nevienodumą, teisinį netikrumą, dar didesnę fragmentaciją ar net diskriminacines situacijas tarp skirtingų valstybių, ypač atsižvelgiant į tai, kad apimami

produktai galėtų turėti ne vieną funkciją ar paskirtį, o gamintojai gali gaminti įvairių kategorijų tokius produktus.

3. *EX POST* VERTINIMO, KONSULTACIJŲ SU SUINTERESUOTOSIOMIS ŠALIMIS IR POVEIKIO VERTINIMO REZULTATAI

- **Konsultacijos su suinteresuotosiomis šalimis**

Komisija konsultavosi su įvairiomis suinteresuotosiomis šalimis. Valstybės narės ir suinteresuotosios šalys buvo pakviestos dalyvauti atvirose viešose konsultacijose ir apklausose bei praktiniuose seminaruose, surengtuose atsižvelgiant į tyrimą, kurį atliko Komisijos parengiamąjį darbą atliekant poveikio vertinimą remiantis konsorciumas: „Wavestone“, Europos politikos studijų centras (CEPS) ir ICF. Suinteresuotieji subjektai, su kuriais konsultuotasi, buvo nacionalinės rinkos priežiūros institucijos, kibernetinio saugumo klausimus sprendžiančios Sąjungos įstaigos, aparatinės ir programinės įrangos gamintojai, aparatinės ir programinės įrangos importuotojai ir platintojai, prekybos asociacijos, vartotojų organizacijos, produktų su skaitmeniniais elementais naudotojai, piliečiai, tyrėjai ir akademinė bendruomenė, notifikuotosios įstaigos ir akreditacijos įstaigos bei kibernetinio saugumo sektoriaus specialistai.

Konsultuojantis vykdyta ši veikla:

- Pirmasis tyrimas, kurį atliko konsorciumas, sudarytas iš ICF, „Wavestone“, „Carsa“ ir CEPS, paskelbtas 2021 m. gruodžio mėn.[11] Tyrime nustatyti keli rinkos trūkumai ir įvertintos galimos reglamentavimo intervencijos.
- Atviros viešos konsultacijos, skirtos piliečiams, suinteresuotiesiems subjektams ir kibernetinio saugumo ekspertams. Buvo pateikti 176 atsakymai. Tai padėjo surinkti įvairias nuomones ir patirtį iš visų suinteresuotųjų subjektų grupių.
- Praktiniuose seminaruose, surengtuose atliekant tyrimą, kuriuo buvo pagrįstas Komisijos parengiamasis darbas rengiant Kibernetinio atsparumo aktą, dalyvavo apie 100 atstovų iš visų 27 valstybių narių, atstovaujančių įvairiems suinteresuotiesiems subjektams.
- Surengtos ekspertų apklausos siekiant geriau suprasti kibernetinio saugumo problemas, susijusias su produktais su skaitmeniniais elementais, ir aptarti galimos reglamentavimo intervencijos politikos galimybes.
- Vyko dvišalės diskusijos su nacionalinėmis kibernetinio saugumo institucijomis, privačiuoju sektoriumi ir vartotojų organizacijomis.
- Buvo tikslingai susisiekta su pagrindiniais MVĮ suinteresuotaisiais subjektais.

- **Tiriamųjų duomenų rinkimas ir naudojimas**

Konsultacijų metu buvo siekiama gauti informacijos pagal penkis pagrindinius vertinimo kriterijus, pagrįstus ES Geresnio reglamentavimo gairėmis (veiksmingumas, efektyvumas, aktualumas, darna, ES pridėtinė vertė), taip pat apie potencialų galimų galimybių poveikį ateityje. Rangovas ne tik susisiekė su suinteresuotaisiais subjektais, kuriems pasiūlytas

[11] Tyrimas dėl kibernetinio saugumo reikalavimų IRT produktams poreikio – Nr. 2020-0715, galutinė tyrimo ataskaita, kurią galima rasti https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

reglamentas turėtų tiesioginį poveikį, bet ir konsultavosi su įvairiais kibernetinio saugumo srities ekspertais.

- **Poveikio vertinimas**

Komisija atliko šio pasiūlymo poveikio vertinimą, kurį išnagrinėjo Komisijos reglamentavimo patikros valdyba. 2022 m. liepos 6 d. įvyko susitikimas su reglamentavimo patikros valdyba, po jo buvo pateikta teigiama nuomonė. Poveikio vertinimas pakoreguotas atsižvelgiant į reglamentavimo patikros valdybos rekomendacijas ir pastabas.

Komisija išnagrinėjo skirtingas politikos galimybes, kad būtų pasiektas bendras pasiūlymo tikslas:

- Neprivalomų teisės aktų metodas ir savanoriškos priemonės (1 galimybė). Pasirinkus šią galimybę, nebūtų jokios privalomos reglamentavimo intervencijos. Vietoje to Komisija skelbtų pranešimus, gaires, rekomendacijas ir galimai elgesio kodeksus, kuriais būtų skatinamos savanoriškos priemonės. Siekiant kompensuoti ES horizontaliųjų taisyklių trūkumą ir toliau būtų kuriamos savanoriškos arba privalomos nacionalinės schemos.
- *Ad hoc* reglamentavimo intervencija, skirta materialių produktų su skaitmeniniais elementais ir atitinkama įtaisytąja programine įranga kibernetiniam saugumui užtikrinti (2 galimybė). Pagal šią galimybę reikėtų *ad hoc* konkrečiam produktui skirtos reglamentavimo intervencijos, kuri apsiribotų kibernetinio saugumo reikalavimų pridėjimu ir (arba) pakeitimais jau galiojančiuose teisės aktuose arba naujų teisės aktų priėmimu atsiradus naujoms rizikoms, tai galimai apimtų ir neįtaisytąją programinę įrangą.

Pagal 3 ir 4 galimybes reikėtų horizontaliojo reglamentavimo intervencijos, kuri skirtųsi savo taikymo sritimi ir daugiausia būtų pagrįsta naująja teisės aktų sistema (NTAS). Šia sistema būtų nustatomi esminiai reikalavimai kaip tam tikrų produktų pateikimo vidaus rinkai sąlyga. NTAS taip pat paprastai numatomas atitikties vertinimas, gamintojo atliekamas procesas, kuriuo siekiama įrodyti, kad įvykdyti konkretūs su produktu susiję reikalavimai.

- Mišrus metodas, apimantis horizontaliąsias privalomas materialių produktų su skaitmeniniais elementais ir atitinkama įtaisytąja programine įranga kibernetinio saugumo taisykles ir paskirstytąjį metodą neįtaisytajai programinei įrangai (3 galimybė). Pasirinkus šią galimybę reikėtų reglamento, kuriuo būtų priimti horizontalieji kibernetinio saugumo reikalavimai visiems materialiems produktams su skaitmeniniais elementais ir juose įtaisyta programine įranga kaip pateikimo rinkai sąlyga, ir ji apimtų dvi antrines galimybes su privalomu trečiųjų šalių vertinimu ir be jo (3i ir 3ii). Neįtaisytoji programinė įranga nebūtų reglamentuojama.
- Horizontalioji reguliavimo intervencija nustatant kibernetinio saugumo reikalavimus, taikomus įvairiems materialiems ir nematerialiesiems produktams su skaitmeniniais elementais, įskaitant neįtaisytąją programinę įrangą (4 galimybė). Ši galimybė panaši į 3 galimybę, išskyrus taikymo sritį. Galimo reglamento pagal 4 galimybę taikymo sritis apimtų neįtaisytąją programinę įrangą (su dviem antrinėmis galimybėmis, įskaitant tik ypatingos svarbos (4a) arba visą programinę įrangą (4b)). Kiekvienos antrinės galimybės atveju būtų svarstomos tos pačios antrinės galimybės, susijusios su atitikties vertinimu, kaip ir 3 galimybės atveju.

Remiantis veiksmingumo vertinimu pagal konkrečius tikslus ir sąnaudų bei naudos efektyvumu, 4 galimybė (su antrinėmis galimybėmis, apimančiomis visą programinę įrangą ir privalomą trečiųjų šalių atliekamą ypatingos svarbos produktų vertinimą) pasirodė tinkamiausia. Pasirinkus šią galimybę būtų užtikrintas konkrečių horizontaliųjų kibernetinio saugumo reikalavimų taikymas visiems produktams su skaitmeniniais elementais, pateikiamiems vidaus rinkai ar joje tiekiamiems, ir tai būtų vienintelė galimybė, apimanti visą skaitmeninę tiekimo grandinę. Tokia reglamentavimo intervencija būtų taikoma ir neįtaisytajai programinei įrangai, dažnai turinčiai pažeidžiamumų, taip užtikrinant nuoseklų visų produktų su skaitmeniniais elementais traktavimą ir aiškią įvairių ekonominės veiklos vykdytojų atsakomybės dalį.

Ši politikos galimybė kuria pridėtinę vertę ir dėl to, kad apima pareigą rūpintis ir viso gyvavimo ciklo aspektais po produktų su skaitmeniniais elementais pateikimo rinkai – be kita ko, tuo siekiama užtikrinti tinkamą informaciją apie saugumo palaikymą ir saugumo naujinių teikimą. Ši politikos galimybė taip pat veiksmingiausiai papildytų neseniai atliktą TIS sistemos peržiūrą užtikrindama sustiprinto tiekimo grandinės saugumo sąlygų įgyvendinimą.

Tinkamiausia galimybė suteiktų daug naudos įvairiems suinteresuotiesiems subjektams. Įmonės išvengtų skirtingų produktams su skaitmeniniais elementais taikomų saugumo taisyklių ir tai sumažintų susijusių kibernetinio saugumo teisės aktų reikalavimų laikymosi išlaidas. Tai sumažintų kibernetinių incidentų skaičių, incidentų valdymo išlaidas ir žalą reputacijai. Apskaičiuota, kad visoje ES dėl šios iniciatyvos gali sumažėti įmonių išlaidos dėl patiriamų incidentų maždaug 180–290 mlrd. EUR per metus. Dėl išaugusios produktų su skaitmeniniais elementais paklausos padidėtų apyvarta. Tai gerintų įmonių reputaciją pasaulyje, dėl to išaugtų paklausa ir ES nepriklausančiose šalyse. Naudotojams tinkamiausia galimybė padidintų saugumo savybių skaidrumą ir palengvintų produktų su skaitmeniniais elementais naudojimą. Be to, vartotojams ir piliečiams būtų naudinga geresnė jų pagrindinių teisių apsauga, pavyzdžiui, teisės į privatumą ir duomenų apsaugą.

Paprašyti įvertinti politinių intervencijų veiksmingumą, viešų konsultacijų respondentai sutiko, kad 4 galimybė būtų veiksmingiausia priemonė (4,08 balo skalėje nuo 1 iki 5). Tai apima vartotojų organizacijas (5,00), vartotojais prisistatančius respondentus (4,22), notifikuotąsias įstaigas (4,17), rinkos priežiūros institucijas (5,00) ir produktų su skaitmeniniais elementais gamintojams (3,85), įskaitant mažąsias ir vidutinio dydžio įmones (4,05).

- **Reglamentavimo tinkamumas ir supaprastinimas**

Šiame pasiūlyme nustatyti reikalavimai, kurie bus taikomi programinės ir aparatinės įrangos gamintojams. Kyla poreikis užtikrinti teisinį tikrumą ir išvengti tolesnės su kibernetiniu saugumu susijusių produktų vidaus rinkos fragmentacijos – tą rodo plati įvairių suinteresuotųjų subjektų parama horizontaliajai intervencijai. Pasiūlymu bus sumažinta reglamentavimo našta, kurią gamintojams užkrauna keli produktų saugos aktai. Suderinimas su NTAS reiškia geresnį intervencijos veikimą ir jos vykdymo užtikrinimą. Pasiūlymu supaprastinamas apsaugos procedūrų procesas įtraukiant gamintojus ir valstybes nares prieš pranešant Komisijai. Didelė dalis gamintojų, kuriuos apima pasiūlymo taikymo sritis, jau yra susipažinę su NTAS veikla – tai prisidės prie jos supratimo ir įgyvendinimo. Pasiūlymu bus skatinamas vartotojų ir įmonių pasitikėjimas produktais su skaitmeniniais elementais.

- **Pagrindinės teisės**

Tikimasi, kad visos politikos galimybės tam tikru mastu geriau apsaugos pagrindines teises ir laisves, tokias kaip privatumas, asmens duomenų apsauga, laisvė užsiimti verslu, nuosavybės ar asmens orumo ir neliečiamumo apsauga. Tinkamiausia 4 politikos galimybė, kurią sudaro

horizontaliosios reglamentavimo intervencijos ir plati politikos taikymo sritis, šiuo atžvilgiu būtų veiksmingiausia, nes tikėtina, kad ji labiau padės sumažinti incidentų, įskaitant asmens duomenų saugumo pažeidimus, skaičių ir rimtumą. Be to, ji padidintų teisinį tikrumą ir sudarytų vienodas sąlygas ekonominės veiklos vykdytojams, padidintų bendrą naudotojų pasitikėjimą ES produktais su skaitmeniniais elementais bei šių produktų patrauklumą – taip būtų saugoma nuosavybė ir pagerintos sąlygos ekonominės veiklos vykdytojams užsiimti verslu.

Horizontalieji kibernetinio saugumo reikalavimai prisidėtų prie asmens duomenų saugumo, nes būtų apsaugotas produktuose su skaitmeniniais elementais esančios informacijos konfidencialumas, vientisumas ir prieinamumas. Šių reikalavimų laikymasis palengvins reikalavimo dėl asmens duomenų tvarkymo saugumo laikymąsi pagal Reglamentą (ES) 2016/679 dėl Bendrojo duomenų apsaugos reglamento (BDAR)[12]. Pasiūlymu būtų padidintas skaidrumas ir naudotojams teikiama informacija, įskaitant naudotojus, kurie neturi labai gerų kibernetinio saugumo įgūdžių. Naudotojai taip pat būtų geriau informuoti apie produktų su skaitmeniniais elementais riziką, galimybes ir apribojimus, todėl galėtų tinkamiau imtis būtinų prevencinių ir švelninančių priemonių likutinei rizikai sumažinti.

4. POVEIKIS BIUDŽETUI

Siekdama įvykdyti pagal šį reglamentą Europos Sąjungos kibernetinio saugumo agentūrai (ENISA) skirtas užduotis, ENISA turės perskirstyti maždaug 4,5 etato ekvivalento išteklius. Komisija turėtų skirti 7 etato ekvivalentus, kad įvykdytų savo įsipareigojimus, susijusius su vykdymo užtikrinimu pagal šį reglamentą.

Išsami susijusių išlaidų apžvalga pateikta su šiuo pasiūlymu susijusioje finansinėje pažymoje.

5. KITI ELEMENTAI

• Įgyvendinimo planai ir stebėsena, vertinimas ir ataskaitų teikimo tvarka

Komisija stebės naujų nuostatų įgyvendinimą, taikymą ir atitiktį joms, kad galėtų įvertinti jų efektyvumą. Pagal reglamentą Komisijos bus prašoma atlikti vertinimą ir peržiūrą, taip pat Europos Parlamentui ir Tarybai šiuo klausimu pateikti viešą ataskaitą per 36 mėnesius nuo taikymo pradžios dienos, o po to – kas ketverius metus.

• Išsamus konkrečių pasiūlymo nuostatų paaiškinimas

Bendrosios nuostatos (I skyrius)

Šiame siūlomame reglamente a) nustatytos produktų su skaitmeniniais elementais pateikimo rinkai taisyklės siekiant užtikrinti tokių produktų kibernetinį saugumą; b) nustatyti esminiai produktų su skaitmeniniais elementais projektavimo, kūrimo ir gamybos reikalavimai ir ekonominės veiklos vykdytojų pareigos, susijusios su šių produktų kibernetiniu saugumu; c) nustatyti esminiai pažeidžiamumų valdymo procesų, kuriuos turi taikyti gamintojai, kad užtikrintų produktų su skaitmeniniais elementais kibernetinį saugumą per visą gyvavimo ciklą, reikalavimai ir ekonominės veiklos vykdytojų pareigos, susijusios su šiais procesais; d) nustatytos taisyklės dėl rinkos priežiūros ir minėtų taisyklių bei reikalavimų vykdymo užtikrinimo.

[12] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

Siūlomas reglamentas bus taikomas visiems produktams su skaitmeniniais elementais, kurių paskirtis ir pagrįstai numatomas naudojimas apima tiesioginę arba netiesioginę loginę arba fizinę duomenų jungtį su įrenginiu arba tinklu.

Siūlomas reglamentas nebus taikomas produktams su skaitmeniniais elementais, kuriems taikomas Reglamentas (ES) 2017/745 [žmonėms skirtos medicinos priemonės ir tokių priemonių priedai] ir Reglamentas (ES) 2017/746 [žmonėms skirtos *in vitro* diagnostikos medicinos priemonės ir tokių priemonių priedai], nes abiejuose reglamentuose priemonėms nustatyti reikalavimai, įskaitant programinę įrangą ir bendrąsias gamintojų pareigas, apimantys visą produktų gyvavimo ciklą bei atitikties vertinimo procedūras. Šis reglamentas netaikomas produktams su skaitmeniniais elementais, kurie buvo sertifikuoti pagal Reglamentą 2018/1139 [vienodas aukštas civilinės aviacijos saugos lygis], ir produktams, kuriems taikomas Reglamentas (ES) 2019/2144 [dėl variklinių transporto priemonių, jų priekabų ir joms skirtų sistemų, sudėtinių dalių bei atskirų techninių mazgų tipo patvirtinimo reikalavimų].

Ypatingos svarbos produktams su skaitmeniniais elementais taikomos specialios atitikties vertinimo procedūros ir jie skirstomi į III priede nustatytas I ir II klases, atspindinčias jų kibernetinio saugumo rizikos lygį (II klasė reiškia didesnę riziką). Produktas su skaitmeniniais elementais laikomas ypatingos svarbos, todėl įtraukiamas į III priedą, atsižvelgiant į galimų produkto su skaitmeniniais elementais kibernetinio saugumo pažeidžiamumų poveikį. Nustatant kibernetinio saugumo riziką atsižvelgiama į produkto su skaitmeniniais elementais funkcijas ir numatomą paskirtį jautrioje aplinkoje, pvz., pramoninėje aplinkoje.

Komisija taip pat įgaliojama priimti deleguotuosius aktus, papildančius šį reglamentą nurodant didžiausios svarbos produktų su skaitmeniniais elementais kategorijas, kurioms gamintojai privalo gauti Europos kibernetinio saugumo sertifikatą pagal Europos kibernetinio saugumo sertifikavimo schemą, kad įrodytų atitiktį I priede ar jo dalyse nurodytiems esminiams reikalavimams. Nustatydama tokias didžiausios svarbos produktų su skaitmeniniais elementais kategorijas Komisija atsižvelgia į su produktų su skaitmeniniais elementais kategorija susijusios kibernetinio saugumo rizikos lygį pagal vieną ar kelis kriterijus, į kuriuos atsižvelgiama įtraukiant ypatingos svarbos produktus su skaitmeniniais elementais į III priedą, taip pat įvertindama, ar tos kategorijos produktus naudoja arba jais remiasi Direktyvos [Direktyva XXX/XXXX (TIS2) [I] priede nurodytos rūšies pagrindiniai subjektai; ar šie produktai gali būti reikšmingi šių subjektų veiklai ateityje; ir ar šie produktai aktualūs visos produktų su skaitmeniniais elementais tiekimo grandinės atsparumui destruktyviems įvykiams.

Ekonominės veiklos vykdytojų pareigos (II skyrius)

Į pasiūlymą įtrauktos gamintojų, importuotojų ir platintojų pareigos pagal Sprendime 768/2008/EB numatytas pamatines nuostatas. Pagal esminius kibernetinio saugumo reikalavimus ir pareigas numatoma, kad visi produktai su skaitmeniniais elementais pateikiami rinkai tik jei jie tinkamai tiekiami, tinkamai įrengiami, prižiūrimi ir naudojami pagal numatytąją paskirtį arba tokiomis sąlygomis, kurias galima pagrįstai numatyti, ir atitinka šiame reglamente nustatytus esminius kibernetinio saugumo reikalavimus.

Esminiai reikalavimai ir pareigos įpareigotų gamintojus atsižvelgti į kibernetinio saugumo aspektą projektuojant, kuriant ir gaminant produktus su skaitmeniniais elementais, vykdyti deramą saugumo aspektų patikrinimą projektuojant ir kuriant produktus, skaidriai nurodyti kibernetinio saugumo aspektus, apie kuriuos turi būti pranešta klientams, proporcingai užtikrinti saugumo palaikymą (naujinius) ir laikytis pažeidžiamumų valdymo reikalavimų.

Ekonominės veiklos vykdytojams, pradedant gamintojais, baigiant platintojais ir importuotojais, pagal jų vaidmenį ir atsakomybę tiekimo grandinėje būtų nustatytos pareigos, susijusios su produktų su skaitmeniniais elementais pateikimu rinkai.

Produktų su skaitmeniniais elementais atitiktis (III skyrius)

Jeigu produktas su skaitmeniniais elementais atitinka darniuosius standartus arba tam tikras jų dalis, kurių nuorodos buvo paskelbtos *Europos Sąjungos oficialiajame leidinyje,* laikoma, kad jis atitinka šio siūlomo reglamento esminius reikalavimus. Tais atvejais, kai darniųjų standartų nėra arba jų nepakanka, arba kai standartizacijos procedūra pernelyg vėluoja, arba kai Europos standartizacijos organizacijos nepriima Komisijos prašymo, Komisija gali įgyvendinimo aktais priimti bendrąsias specifikacijas.

Be to, jeigu produktai su skaitmeniniais elementais yra sertifikuoti arba yra išduotas jų ES atitikties pareiškimas arba sertifikatas pagal Europos kibernetinio saugumo sertifikavimo schemą, kaip numatyta Reglamente (ES) 2019/881, ir Komisija įgyvendinimo aktu nurodė, kad šiems produktams gali suteikti šio reglamento atitikties prielaidą, daroma prielaida, kad šie produktai atitinka esminius šio reglamento ar jo dalių reikalavimus tiek, kiek tuos reikalavimus apima ES atitikties pareiškimas arba kibernetinio saugumo sertifikatas, arba jų dalys.

Be to, siekdama išvengti pernelyg didelės administracinės naštos gamintojams, jei taikytina, Komisija turėtų nurodyti, ar pagal tokią Europos kibernetinio saugumo sertifikavimo schemą išduotas kibernetinio saugumo sertifikatas panaikina gamintojų pareigą atlikti trečiųjų šalių atitikties atitinkamiems reikalavimams vertinimą, kaip numatyta šiame reglamente.

Gamintojas atlieka produkto su skaitmeniniais elementais ir jo įdiegtų pažeidžiamumų valdymo procesų atitikties vertinimą, kad įrodytų atitiktį I priede nurodytiems esminiams reikalavimams, vadovaudamasis viena iš VI priede nurodytų procedūrų. I ir II klasių ypatingos svarbos produktų gamintojai naudoja atitinkamus modulius, būtinus reikalavimų laikymuisi užtikrinti. II klasės ypatingos svarbos produkto gamintojai į atitikties vertinimą turi įtraukti trečiąją šalį.

Atitikties vertinimo įstaigų notifikavimas (IV skyrius)

Tinkamas notifikuotųjų įstaigų veikimas yra labai svarbus siekiant užtikrinti aukštą kibernetinio saugumo lygį bei visų suinteresuotųjų subjektų pasitikėjimą naujojo metodo sistema. Todėl, vadovaujantis Sprendimu Nr. 768/2008/EB, pasiūlyme nustatyti reikalavimai, taikomi už atitikties vertinimo įstaigas (notifikuotąsias įstaigas) atsakingoms nacionalinėms institucijoms. Galutinė atsakomybė už notifikuotųjų įstaigų skyrimą ir priežiūrą paliekama valstybėms narėms. Valstybės narės paskiria notifikuojančiąją instituciją, atsakingą už procedūrų, reikalingų atitikties vertinimo įstaigoms įvertinti ir notifikuoti bei notifikuotųjų įstaigų stebėsenai atlikti, nustatymą ir taikymą.

Rinkos priežiūra ir vykdymo užtikrinimas (V skyrius)

Pagal Reglamentą (ES) 2019/1020 nacionalinės rinkos priežiūros institucijos vykdo rinkos priežiūrą tos valstybės narės teritorijoje. Valstybės narės gali nuspręsti paskirti bet kurią esamą arba naują instituciją, kuri veiktų kaip rinkos priežiūros institucija, įskaitant nacionalines kompetentingas institucijas, nustatytas Direktyvos [Direktyva XXX/XXXX (TIS2)] [X] straipsnyje, arba paskirtas nacionalines kibernetinio saugumo sertifikavimo institucijas, nurodytas Reglamento (ES) 2019/881 58 straipsnyje. Ekonominės veiklos vykdytojų prašoma visapusiškai bendradarbiauti su rinkos priežiūros institucijomis ir kitomis kompetentingomis institucijomis.

Deleguotieji įgaliojimai ir komiteto procedūra (VI skyrius)

Siekiant užtikrinti, kad prireikus būtų galima pritaikyti reglamentavimo sistemą, Komisijai deleguojama teisė pagal SESV 290 straipsnį priimti aktus, kuriais būtų galima atnaujinti I ir II klasių ypatingos svarbos produktų sąrašą ir nurodyti šių produktų apibrėžtis; nurodyti, ar produktams su skaitmeniniais elementais, kuriems taikomos kitos Sąjungos taisyklės, nustatančios reikalavimus, kuriais užtikrinamas toks pat apsaugos lygis kaip ir šiuo reglamentu, reikalingas apribojimas arba išimtis; įpareigoti sertifikuoti tam tikrus didžiausios svarbos produktus su skaitmeniniais elementais remiantis šiame reglamente nustatytais kriterijais; nurodyti minimalų ES atitikties deklaracijos turinį ir papildyti elementus, kurie turi būti įtraukti į techninius dokumentus.

Komisija taip pat įgaliojama priimti įgyvendinimo aktus, kuriais būtų galima: nurodyti pareigos pranešti ir programinės įrangos medžiagų žiniaraščio formatą arba elementus; nurodyti Europos kibernetinio saugumo sertifikavimo schemas, kurios gali būti naudojamos siekiant įrodyti atitiktį šiame reglamente nurodytiems esminiams reikalavimams ar jų dalims; priimti bendrąsias specifikacijas; nustatyti technines ženklinimo CE ženklu specifikacijas; Sąjungos lygmeniu priimti taisomąsias arba ribojamąsias priemones išskirtinėmis aplinkybėmis, dėl kurių būtų pagrįsta nedelsiant atlikti intervenciją, kad būtų išsaugotas tinkamas vidaus rinkos veikimas.

Konfidencialumas ir sankcijos (VII skyrius)

Visos šį reglamentą taikančios šalys laikosi informacijos ir duomenų, gautų vykdant jų užduotis ir veiklą, konfidencialumo.

Siekiant užtikrinti veiksmingą šiame reglamente nustatytų pareigų vykdymą, kiekvienai rinkos priežiūros institucijai turėtų būti suteikti įgaliojimai skirti administracines baudas arba prašyti jas skirti. Be to, šiuo reglamentu nustatomi didžiausi administracinių baudų dydžiai, kurie turėtų būti numatyti nacionalinės teisės aktuose už šiame reglamente nustatytų pareigų nevykdymą.

Pereinamojo laikotarpio ir baigiamosios nuostatos (VIII skyrius)

Siekiant gamintojams, notifikuotosioms įstaigoms ir valstybėms narėms skirti laiko prisitaikyti prie naujų reikalavimų, siūlomas reglamentas įsigalios praėjus [24 mėnesiams] nuo jo įsigaliojimo dienos, išskyrus gamintojams taikomą pareigą pranešti, kuri bus taikoma praėjus [12 mėnesių] nuo įsigaliojimo dienos.

2022/0272 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams, kuriuo iš dalies keičiamas Reglamentas (ES) 2019/1020

(Tekstas svarbus EEE)

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 114 straipsnį,

atsižvelgdami į Europos Komisijos pasiūlymą,

perdavus įstatymo galią turinčio teisės akto projektą nacionaliniams parlamentams,

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę[1],

atsižvelgdami į Regionų komiteto nuomonę[2],

laikydamiesi įprastos teisėkūros procedūros,

kadangi:

(1) būtina gerinti vidaus rinkos veikimą nustatant vienodą teisinę esminių kibernetinio saugumo reikalavimų, susijusių su produktų su skaitmeniniais elementais pateikimu Sąjungos rinkai, sistemą. Reikėtų spręsti dvi pagrindines problemas, dėl kurių naudotojai ir visuomenė patiria papildomų sąnaudų: mažas kibernetinio produktų su skaitmeniniais elementais saugumo lygis, kurį atspindi plačiai paplitę pažeidžiamumai ir nepakankamas bei nenuoseklus saugumo naujinių teikimas jiems spręsti, ir nepakankamas naudotojų supratimas ir prieiga prie informacijos – todėl jie negali pasirinkti tinkamomis kibernetinio saugumo savybėmis pasižyminčių produktų ar saugiai juos naudoti;

(2) šiuo reglamentu siekiama nustatyti ribines sąlygas kurti saugius produktus su skaitmeniniais elementais užtikrinant, kad aparatinės ir programinės įrangos produktai būtų pateikiami rinkai su mažiau pažeidžiamumų ir kad gamintojai rimtai atsižvelgtų į saugumą per visą produkto gyvavimo ciklą. Juo taip pat siekiama sudaryti tokias sąlygas, kad rinkdamiesi ir naudodami produktus su skaitmeniniais elementais naudotojai galėtų atsižvelgti į kibernetinį saugumą;

(3) šiuo metu galiojančius aktualius Sąjungos teisės aktus sudaro keli horizontaliųjų taisyklių rinkiniai, kuriais įvairiai sprendžiami tam tikri su kibernetiniu saugumu susiję aspektai, įskaitant priemones, skirtas skaitmeninės tiekimo grandinės saugumui gerinti. Tačiau galiojantys su kibernetiniu saugumu susiję Sąjungos teisės aktai, įskaitant Europos Parlamento ir Tarybos [Direktyvą XXX/XXXX (TIS2)] ir

[1] OL C, , p. .
[2] OL C, , p. .

Reglamentą (ES) 2019/881[3], tiesiogiai neapima privalomų reikalavimų dėl produktų su skaitmeniniais elementais saugumo;

(4) nors galiojantys Sąjungos teisės aktai taikomi tam tikriems produktams su skaitmeniniais elementais, nėra horizontaliojo Sąjungos reglamentavimo sistemos, kuria būtų nustatyti išsamūs kibernetinio saugumo reikalavimai visiems produktams su skaitmeniniais elementais. Įvairiais aktais ir iniciatyvomis, kurių iki šiol imtasi Sąjungos ir nacionaliniu lygmenimis, tik iš dalies sprendžiamos nustatytos su kibernetiniu saugumu susijusios problemos ir rizikos, todėl vidaus rinkoje kuriama nevientisa teisės aktų sistema, didėja teisinis netikrumas tiek šių produktų gamintojams, tiek jų naudotojams, o įmonėms užkraunama nereikalinga našta, nes jos turi laikytis skirtingų tos pačios rūšies produktams taikomų reikalavimų. Šių produktų kibernetiniam saugumui būdingas itin stiprus tarpvalstybinis aspektas, nes vienoje šalyje pagamintus produktus dažnai naudoja organizacijos ir vartotojai visoje vidaus rinkoje. Todėl šią sritį būtina reglamentuoti Sąjungos lygmeniu. Sąjungos reglamentavimo aplinka turėtų būti suderinta nustatant produktų su skaitmeniniais elementais kibernetinio saugumo reikalavimus. Be to, turėtų būti užtikrintas teisinis tikrumas veiklos vykdytojams ir naudotojams visoje Sąjungoje, geriau suderinta bendroji rinka ir sudarytos palankesnės sąlygos veiklos vykdytojams, siekiantiems patekti į Sąjungos rinką;

(5) Sąjungos lygmeniu įvairiuose programiniuose ir politiniuose dokumentuose, pavyzdžiui, ES skaitmeninio dešimtmečio kibernetinio saugumo strategijoje[4], 2020 m. gruodžio 2 d. ir 2022 m. gegužės 23 d. Tarybos išvadose arba 2021 m. birželio 10 d. Europos Parlamento rezoliucijoje[5], raginama nustatyti konkrečius Sąjungos kibernetinio saugumo reikalavimus skaitmeniniams arba prijungtiesiems produktams, o kelios pasaulio šalys ėmėsi priemonių šiam klausimui spręsti savo iniciatyva. Galutinėje Konferencijos dėl Europos ateities ataskaitoje[6] piliečiai ragino „stiprinti ES vaidmenį kovoje su kibernetinėmis grėsmėmis“;

(6) siekiant padidinti bendrą visų produktų su skaitmeniniais elementais, pateikiamų vidaus rinkai, kibernetinio saugumo lygį, būtina nustatyti objektyvius ir technologiškai neutralius esminius šių produktų kibernetinio saugumo reikalavimus, kurie būtų taikomi horizontaliai;

(7) tam tikromis sąlygomis visus produktus su skaitmeniniais elementais, integruotus į didesnę elektroninę informacinę sistemą arba prie jos prijungtus, piktavaliai subjektai gali panaudoti atakai. Todėl net aparatinė ir programinė įranga, kuri laikoma mažiau svarbia, gali palengvinti pradinį įrenginio ar tinklo pažeidimą ir sudaryti sąlygas piktavaliams subjektams įgyti privilegijuotąją prieigą prie sistemos arba pereiti nuo vienos sistemos prie kitos. Todėl gamintojai turėtų užtikrinti, kad visi prijungiamieji produktai su skaitmeniniais elementais būtų suprojektuoti ir sukurti laikantis šiame

---

[3] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15).

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

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

[6] *Konferencija dėl Europos ateities. Galutinių rezultatų ataskaita*, 2022 m. gegužės mėn., pasiūlymas 28(2). Konferencija vyko 2021 m. balandžio mėn. ir 2022 m. gegužės mėn. Tai buvo unikalus europinis konsultacinės demokratijos aktas, kuriame dalyvavo tūkstančiai Europos piliečių, taip pat politiniai veikėjai, socialiniai partneriai, pilietinės visuomenės atstovai ir pagrindiniai suinteresuotieji subjektai.

reglamente nustatytų esminių reikalavimų. Tai apima ir produktus, kuriuos galima prijungti fiziškai per aparatinės įrangos sąsajas, ir produktus, kurie prijungiami loginiu būdu, pvz., per tinklo lizdus, kanalus, failus, programų sąsajas arba bet kokio kito tipo programinės įrangos sąsają. Kadangi kibernetinio saugumo grėsmės gali plisti per įvairius produktus su skaitmeniniais elementais prieš pasiekdamos tam tikrą tikslą, pavyzdžiui, pasinaudodamos kelių pažeidžiamumų grandine, gamintojai turėtų užtikrinti ir tų produktų, kurie su kitais įrenginiais ar tinklais yra sujungti tik netiesiogiai, kibernetinį saugumą;

(8) nustačius kibernetinio saugumo reikalavimus dėl produktų su skaitmeniniais elementais pateikimo rinkai, padidės šių produktų kibernetinis saugumas tiek vartotojams, tiek įmonėms. Tai taip pat apima reikalavimus dėl produktų su skaitmeniniais elementais, skirtų pažeidžiamiems vartotojams, pvz., žaislų ir kūdikio monitorių, pateikimo rinkai;

(9) šiuo reglamentu užtikrinamas aukštas produktų su skaitmeniniais elementais kibernetinis saugumas. Juo nereglamentuojamos paslaugos, tokios kaip paslauginė programinė įranga (SaaS), išskyrus nuotolinius su produktu su skaitmeniniais elementais susijusius duomenų tvarkymo sprendimus, kurie suprantami kaip bet koks duomenų tvarkymas per atstumą ir kuriems programinę įrangą projektuoja ir kuria atitinkamo produkto gamintojas arba tas gamintojas yra už tai atsakingas, ir be kurių toks produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų. [Direktyva XXX/XXXX (TIS2)] nustatomi kibernetinio saugumo ir ataskaitų apie incidentus teikimo reikalavimai pagrindiniams ir svarbiems subjektams, pvz., ypatingos svarbos infrastruktūrai, siekiant padidinti jų teikiamų paslaugų atsparumą. [Direktyva XXX/XXXX (TIS2)] taikoma debesijos kompiuterijos paslaugoms ir debesijos paslaugų modeliams, pvz., SaaS. Ši direktyva taikoma visiems Sąjungoje debesijos kompiuterijos paslaugas teikiantiems subjektams, kurie atitinka arba viršija nustatytą vidutinio dydžio įmonės ribą;

(10) siekiant netrukdyti inovacijoms ar moksliniams tyrimams, šis reglamentas neturėtų apimti nemokamos ir atvirojo kodo programinės įrangos, kuriamos ar tiekiamos nekomerciniais sumetimais. Tai visų pirma taikytina programinei įrangai, įskaitant jos šaltinio kodą ir modifikuotas versijas, kuri yra atvirai bendrinama ir laisvai prieinama, naudojama, modifikuojama ir perskirstoma. Kalbant apie programinę įrangą, komercinė veikla gali būti apibūdinama ne tik kaip užmokesčio už produktą taikymas, bet ir kaip užmokesčio už techninės pagalbos paslaugas taikymas, programinės įrangos platformos, per kurią gamintojas gauna pajamų iš kitų paslaugų, teikimas arba asmens duomenų naudojimas kitais nei vien programinės įrangos saugumo, suderinamumo ar sąveikos gerinimo tikslais;

(11) saugus internetas yra būtinas ypatingos svarbos infrastruktūros objektų veikimui ir visai visuomenei. [Direktyva XXX/XXXX (TIS2)] siekiama užtikrinti aukštą paslaugų, kurias teikia pagrindiniai ir svarbūs subjektai, įskaitant skaitmeninės infrastruktūros teikėjus, kurie palaiko pagrindines atvirojo interneto funkcijas, užtikrina interneto prieigą ir interneto paslaugas, kibernetinio saugumo lygį. Todėl svarbu, kad produktai su skaitmeniniais elementais, būtini skaitmeninės infrastruktūros teikėjams, kad užtikrintų interneto veikimą, būtų kuriami saugiai ir atitiktų nusistovėjusius interneto saugumo standartus. Šiuo reglamentu, taikomu visiems prijungiamiesiems aparatinės ir programinės įrangos produktams, taip pat siekiama palengvinti skaitmeninės infrastruktūros teikėjų atitiktį tiekimo grandinės reikalavimams pagal [Direktyvą XXX/XXXX (TIS2)] užtikrinant, kad produktai su

skaitmeniniais elementais, kuriuos jie naudoja savo paslaugoms teikti, būtų kuriami saugiai ir kad jie turėtų prieigą prie savalaikių tokių produktų saugumo naujinių;

(12) Europos Parlamento ir Tarybos reglamente (ES) 2017/745[7] nustatomos medicinos priemonių taisyklės, o Europos Parlamento ir Tarybos reglamente (ES) 2017/746[8] nustatomos *in vitro* diagnostikos medicinos priemonių taisyklės. Abiem reglamentais sprendžiama kibernetinio saugumo rizika ir laikomasi tam tikrų metodų, kurie taip pat aptariami šiame reglamente. Konkrečiau, reglamentuose (ES) 2017/745 ir (ES) 2017/746 nustatyti esminiai reikalavimai medicinos priemonėms, kurios veikia per elektroninę sistemą arba pačios yra programinė įranga. Šie reglamentai taip pat apima tam tikrą neįtaisytąją programinę įrangą ir viso gyvavimo ciklo metodą. Šie reikalavimai įpareigoja gamintojus kurti ir gaminti savo produktus taikant rizikos valdymo principus ir nustatant reikalavimus, susijusius su IT saugumo priemonėmis, taip pat atitinkamas atitikties vertinimo procedūras. Be to, nuo 2019 m. gruodžio mėn. medicinos priemonėms taikomos specialios kibernetinio saugumo gairės, kuriose medicinos priemonių, įskaitant *in vitro* diagnostikos priemones, gamintojams patariama, kaip įvykdyti visus esminius tų reglamentų I priedo reikalavimus, susijusius su kibernetiniu saugumu[9]. Todėl produktams su skaitmeniniais elementais, kuriems taikomas vienas iš tų reglamentų, šis reglamentas neturėtų būti taikomas;

(13) Europos Parlamento ir Tarybos Reglamentu (ES) 2019/2144[10] nustatomi transporto priemonių, jų sistemų ir komponentų tipo patvirtinimo reikalavimai, pradedami taikyti tam tikri kibernetinio saugumo reikalavimai, įskaitant reikalavimus dėl sertifikuotos kibernetinio saugumo valdymo sistemos veikimo, programinės įrangos naujinių, jis apima organizacijų politiką ir kibernetinės rizikos procesus, susijusius su visu transporto priemonių, įrangos ir paslaugų gyvavimo ciklu, laikantis galiojančių Jungtinių Tautų techninių specifikacijų ir kibernetinio saugumo taisyklių[11], ir jame nustatomos konkrečios atitikties vertinimo procedūros. Aviacijos srityje pagrindinis Europos Parlamento ir Tarybos Reglamento (ES) 2018/1139[12] tikslas – nustatyti ir

---

7 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/745 dėl medicinos priemonių, kuriuo iš dalies keičiama Direktyva 2001/83/EB, Reglamentas (EB) Nr. 178/2002 ir Reglamentas (EB) Nr. 1223/2009, ir kuriuo panaikinamos Tarybos direktyvos 90/385/EEB ir 93/42/EEB (OL L 117, 2017 5 5, p. 1).

8 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/746 dėl *in vitro* diagnostikos medicinos priemonių, kuriuo panaikinama Direktyva 98/79/EB ir Komisijos sprendimas 2010/227/ES (OL L 117, 2017 5 5, p. 176).

9 MPKG 2019-16, patvirtino Medicinos priemonių koordinavimo grupė (MPKG), įsteigta Reglamento (ES) 2017/745 103 straipsniu.

10 2019 m. lapkričio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2019/2144 dėl variklinių transporto priemonių, jų priekabų ir joms skirtų sistemų, sudėtinių dalių bei atskirų techninių mazgų tipo patvirtinimo reikalavimų, susijusių su jų bendrąja sauga ir transporto priemonėse esančių asmenų bei pažeidžiamų eismo dalyvių apsauga, kuriuo iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (ES) 2018/858 ir panaikinami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 78/2009, (EB) Nr. 79/2009 ir (EB) Nr. 661/2009 ir Komisijos reglamentai (EB) 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 ir (ES) 2015/166 (OL L 325, 2019 12 16, p. 1).

11 JT taisyklė Nr. 155. Vienodos nuostatos dėl transporto priemonių patvirtinimo kibernetinio saugumo ir kibernetinio saugumo valdymo sistemos atžvilgiu [2021/387].

12 2018 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1139 dėl bendrųjų civilinės aviacijos taisyklių, ir kuriuo įsteigiama Europos Sąjungos aviacijos saugos agentūra, iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 2111/2005, (EB) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 ir direktyvos 2014/30/ES ir 2014/53/ES bei panaikinami Europos

palaikyti aukštą vienodą civilinės aviacijos saugos lygį Sąjungoje. Juo sukuriama esminių tinkamumo skraidyti reikalavimų, taikomų aeronautikos produktams, dalims ir įrangai, įskaitant programinę įrangą, sistema, kurioje atsižvelgiama į pareigą apsisaugoti nuo informacijos saugumo grėsmių. Todėl produktams su skaitmeniniais elementais, kuriems taikomas Reglamentas (ES) 2019/2144, ir produktams, sertifikuotiems pagal Reglamentą (ES) 2018/1139, šiame reglamente nustatyti esminiai reikalavimai ir atitikties vertinimo procedūros netaikomi. Sertifikavimo procesas pagal Reglamentą (ES) 2018/1139 užtikrina šiuo reglamentu siekiamą užtikrinimo lygį;

(14) šiuo reglamentu nustatomos horizontaliosios kibernetinio saugumo taisyklės, kurios nėra skirtos konkretiems sektoriams ar tam tikriems produktams su skaitmeniniais elementais. Nepaisant to, galėtų būti priimtos sektorinės arba konkretiems produktams skirtos Sąjungos taisyklės, kuriose būtų nustatyti reikalavimai visai arba daliai rizikos, kuriai taikomi šiame reglamente nustatyti esminiai reikalavimai. Tokiais atvejais šio reglamento taikymas produktams su skaitmeniniais elementais, kuriems taikomos kitos Sąjungos taisyklės, kuriose nustatomi reikalavimai visai arba daliai rizikos, kuriai taikomi šio reglamento I priede nustatyti esminiai reikalavimai, gali būti apribotas arba daroma taikymo išimtis, jei toks apribojimas arba išimtis atitinka bendrą šiems produktams taikomą reguliavimo sistemą ir kai sektorių taisyklėmis užtikrinamas toks pat apsaugos lygis kaip ir šiuo reglamentu. Komisija įgaliojama priimti deleguotuosius aktus, kad galėtų iš dalies keisti šį reglamentą nustatydama tokius produktus ir taisykles. Šiame reglamente yra konkrečių nuostatų dėl galiojančių Sąjungos teisės aktų, kada turėtų būti taikomi tokie apribojimai arba išimtys, ir paaiškinamas jo ryšys su tais Sąjungos teisės aktais;

(15) Deleguotajame reglamente (ES) 2022/30 nurodyta, kad Direktyvos 2014/53/ES 3 straipsnio 3 dalies d punkte (žala tinklui ir netinkamas tinklo išteklių naudojimas), e punkte (asmens duomenys ir privatumas) ir f punkte (sukčiavimas) nustatyti esminiai reikalavimai taikomi tam tikriems radijo įrenginiams. [Komisijos įgyvendinimo sprendime XXX/2022 dėl standartizacijos prašymo Europos standartizacijos organizacijoms] nustatyti reikalavimai konkretiems standartams parengti ir papildomai nurodoma, kaip šie trys esminiai reikalavimai turėtų būti sprendžiami. Šiuo reglamentu nustatyti esminiai reikalavimai apima visus Direktyvos 2014/53/ES 3 straipsnio 3 dalies d, e ir f punktuose nurodytus esminius reikalavimus. Be to, šiame reglamente nustatyti esminiai reikalavimai yra suderinti su konkretiems standartams, įtrauktiems į tą standartizacijos prašymą, skirtų reikalavimų tikslais. Todėl, Komisijai atmetus ar iš dalies pakeitus Deleguotąjį reglamentą (ES) 2022/30 taip, kad jis nebebūtų taikomas tam tikriems produktams, kuriems taikomas šis reglamentas, rengdamos ir plėtodamos darniuosius standartus, padėsiančius įgyvendinti šį reglamentą, Komisija ir Europos standartizacijos organizacijos atsižvelgs į standartizavimo darbą, atliekamą pagal Komisijos įgyvendinimo sprendimą C(2022)5637 dėl RED deleguotojo reglamento 2022/30 standartizacijos prašymo;

(16) Direktyva 85/374/EEB[13] papildo šį reglamentą. Toje direktyvoje nustatytos taisyklės dėl atsakomybės už produktus su trūkumais, kad nukentėję asmenys galėtų reikalauti kompensacijos, kai žala padaryta dėl produktų su trūkumais. Joje nustatytas principas,

---

Parlamento ir Tarybos reglamentai (EB) Nr. 552/2004 ir (EB) Nr. 216/2008 bei Tarybos reglamentas (EEB) Nr. 3922/91 (OL L 212, 2018 8 22, p. 1).

[13] 1985 m. liepos 25 d. Tarybos direktyva 85/374/EEB dėl valstybių narių įstatymų ir kitų teisės aktų, reglamentuojančių atsakomybę už gaminius su trūkumais, suderinimo (OL L 210, 1985 8 7).

pagal kurį produkto gamintojas atsako už žalą, padarytą dėl saugumo stokos jo produkte, nepriklausomai nuo kaltės („griežta atsakomybė“). Jei toks saugumo trūkumas kyla dėl saugumo naujinių neteikimo po produkto pateikimo rinkai ir dėl to padaroma žala, gamintojas gali būti priverstas prisiimti atsakomybę. Šiame reglamente turėtų būti nustatytos gamintojų pareigos, susijusios su tokių saugumo naujinių teikimu;

(17) šis reglamentas neturėtų pažeisti Europos Parlamento ir Tarybos reglamento (ES) 2016/679[14], įskaitant nuostatas dėl duomenų apsaugos sertifikavimo mechanizmų ir duomenų apsaugos ženklų bei žymenų sukūrimo, kad būtų galima įrodyti, jog duomenų valdytojų ir tvarkytojų atliekamos tvarkymo operacijos atitinka šio reglamento reikalavimus. Tokios operacijos galėtų būti integruotos į produktą su skaitmeniniais elementais. Pagrindiniai Reglamento (ES) 2016/679 elementai yra integruotoji ir standartizuotoji duomenų apsauga bei bendras kibernetinis saugumas. Apsaugant vartotojus ir organizacijas nuo kibernetinio saugumo rizikos, esminiai šiame reglamente nustatyti kibernetinio saugumo reikalavimai taip pat yra padėti stiprinti asmens duomenų apsaugą ir asmenų privatumą. Kibernetinio saugumo aspektų standartizavimo ir sertifikavimo sinergija turėtų būti vertinama bendradarbiaujant Komisijai, Europos standartizacijos organizacijoms, Europos Sąjungos kibernetinio saugumo agentūrai (ENISA), Reglamentu (ES) 2016/679 įsteigtai Europos duomenų apsaugos valdybai ir nacionalinėms duomenų apsaugos priežiūros institucijoms. Sinergija tarp šio reglamento ir Sąjungos duomenų apsaugos teisės turėtų būti sukurta ir rinkos priežiūros bei vykdymo užtikrinimo srityje. Šiuo tikslu pagal šį reglamentą paskirtos nacionalinės rinkos priežiūros institucijos turėtų bendradarbiauti su institucijomis, prižiūrinčiomis Sąjungos duomenų apsaugos teisę. Pastarosios taip pat turėtų turėti prieigą prie informacijos, susijusios su jų užduočių vykdymu;

(18) tiek, kiek jų produktams taikomas šis reglamentas, [Reglamento (ES) Nr. 910/2014 6a straipsnio 2 dalis, iš dalies pakeista pasiūlymu dėl reglamento, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 dėl Europos skaitmeninės tapatybės sistemos nustatymo] straipsnyje nurodytos Europos skaitmeninės tapatybės piniginės leidėjai turėtų laikytis ir šiame reglamente nustatytų horizontaliųjų esminių reikalavimų, ir konkrečių saugumo reikalavimų, nustatytų [Reglamento (ES) Nr. 910/2014 6a straipsnis, iš dalies pakeistas pasiūlymu dėl reglamento, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 dėl Europos skaitmeninės tapatybės sistemos nustatymo] straipsnyje. Kad būtų lengviau laikytis reikalavimų, piniginės leidėjai turėtų galėti įrodyti, kad Europos skaitmeninės tapatybės piniginės atitinka abiejuose teisės aktuose nustatytus reikalavimus, sertifikuodami savo produktus pagal Europos kibernetinio saugumo sertifikavimo schemą, nustatytą pagal Reglamentą (ES) 2019/881, ir Komisija įgyvendinimo aktu turi nurodyti prielaidą, kad šie produktai atitinka šį reglamentą tiek, kiek sertifikatas arba jo dalys apima šiuos reikalavimus;

(19) tam tikras šiame reglamente numatytas užduotis turėtų vykdyti ENISA pagal Reglamento (ES) 2019/881 3 straipsnio 2 dalį. Visų pirma ENISA turėtų gauti gamintojų pranešimus apie aktyviai išnaudojamus pažeidžiamumus, esančius produktuose su skaitmeniniais elementais, taip pat apie incidentus, darančius poveikį tų produktų saugumui. ENISA taip pat turėtų perduoti šiuos pranešimus atitinkamoms

[14] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

reagavimo į kompiuterių saugumo incidentus tarnyboms (CSIRT) arba atitinkamiems valstybių narių bendriems kontaktiniams punktams, paskirtiems pagal Direktyvos [Direktyva XXX/XXXX (TIS2)] [X straipsnis] straipsnį, ir informuoti atitinkamas rinkos priežiūros institucijas apie praneštą pažeidžiamumą. Remdamasi surinkta informacija ENISA turėtų kas dvejus metus parengti techninę ataskaitą apie besiformuojančias produktų su skaitmeniniais elementais kibernetinio saugumo rizikos tendencijas ir pateikti ją Direktyvoje [Direktyva XXX/XXXX (TIS2)] nurodytai bendradarbiavimo grupei. Be to, atsižvelgiant į jos patirtį ir įgaliojimus, ENISA turėtų galėti remti šio reglamento įgyvendinimo procesą. Visų pirma ji turėtų galėti pasiūlyti bendrą veiklą, kurią vykdys rinkos priežiūros institucijos remdamosi įrodymais arba informacija apie galimą produktų su skaitmeniniais elementais neatitikimą reglamento reikalavimams keliose valstybėse narėse, arba nustatyti produktų kategorijas, kurioms turėtų būti vienu metu organizuojami koordinuoti kontrolės veiksmai. Išskirtinėmis aplinkybėmis, Komisijos prašymu ENISA turėtų galėti atlikti konkrečių produktų su skaitmeniniais elementais vertinimus, kai šiems produktams būdinga reikšminga kibernetinio saugumo rizika ir kai reikia nedelsiant įsikišti, kad būtų išsaugotas tinkamas vidaus rinkos veikimas;

(20) kad produktai su skaitmeniniais elementais galėtų laisvai judėti vidaus rinkoje, jie turėtų būti ženklinami CE ženklu, iš kurio būtų matyti, kad jie atitinka šį reglamentą. Valstybės narės neturėtų sudaryti nepagrįstų kliūčių pateikti rinkai produktus su skaitmeniniais elementais, kurie atitinka šiame reglamente nustatytus reikalavimus ir yra paženklinti CE ženklu;

(21) siekdamos užtikrinti, kad prieš atlikdami savo produktų atitikties vertinimą gamintojai galėtų išleisti programinę įrangą bandymo tikslais, valstybės narės neturėtų neleisti pateikti nebaigtos programinės įrangos, pvz., alfa versijos, beta versijos ar kandidatinės versijos, jeigu tokia versija pateikiama ne ilgesniam laikui nei būtina jai patikrinti ir grįžtamajai informacijai gauti. Gamintojai turėtų užtikrinti, kad tokiomis sąlygomis pateikta programinė įranga būtų išleista tik atlikus rizikos vertinimą ir kad ji kiek įmanoma atitiktų saugumo reikalavimus, susijusius su šiame reglamente nustatytomis produktų su skaitmeniniais elementais savybėmis. Gamintojai taip pat turėtų kiek įmanoma įgyvendinti pažeidžiamumų valdymo reikalavimus. Gamintojai neturėtų versti naudotojų atnaujinti versijų, išleistų tik bandymo tikslais;

(22) siekiant užtikrinti, kad rinkai pateikti produktai su skaitmeniniais elementais nekeltų kibernetinio saugumo rizikos asmenims ir organizacijoms, tokiems produktams turėtų būti nustatyti esminiai reikalavimai. Jei vėliau daromi produktų pakeitimai fizinėmis ar skaitmeninėmis priemonėmis gamintojo nenumatytu būdu ir tai galėtų reikšti, kad produktai nebeatitinka susijusių esminių reikalavimų, pakeitimas turėtų būti laikomas esminiu. Pavyzdžiui, programinės įrangos naujiniai arba taisymai galėtų būti prilyginti priežiūros operacijoms, jei jais nekeičiamas rinkai jau pateiktas produktas taip, kad galėtų būti paveiktas taikytinų reikalavimų laikymasis arba kad galėtų būti pakeista numatytoji paskirtis, dėl kurios produktas buvo įvertintas. Kaip ir fizinio taisymo ar pakeitimų atveju, produktas su skaitmeniniais elementais turėtų būti laikomas iš esmės pakeistu pakeitus programinę įrangą, kai programinės įrangos naujinys pakeičia pradines numatytas produkto funkcijas, tipą ar našumą, ir šie pakeitimai nebuvo numatyti pradiniame rizikos vertinime arba dėl programinės įrangos naujinio pasikeitė pavojaus pobūdis arba padidėjo rizikos lygis;

(23) atsižvelgiant į visuotinai nusistovėjusį esminio Sąjungos derinamaisiais teisės aktais reglamentuojamų produktų pakeitimo supratimą, kiekvieną kartą, kai įvyksta esminis pakeitimas, galintis turėti įtakos produkto atitikčiai šio reglamento reikalavimams arba

kai pasikeičia produkto numatytoji paskirtis, tikslinga patikrinti produkto su skaitmeniniais elementais atitiktį reikalavimams ir, jei taikytina, atlikti naują atitikties vertinimą. Kai taikytina, jei gamintojas atlieka atitikties vertinimą, kuriame dalyvauja trečioji šalis, šiai trečiajai šaliai turėtų būti pranešta apie pakeitimus, kurie gali būti esminiai;

(24) produkto su skaitmeniniais elementais atnaujinimas, priežiūra ir taisymas, kaip apibrėžta reglamente [Ekologinio projektavimo reglamentas], nebūtinai reiškia esminį produkto pakeitimą, pavyzdžiui, jei numatytoji paskirtis nepasikeičia ir funkcijos bei rizikos lygis lieka nepakitę. Tačiau gamintojo atliekamas produkto atnaujinimas gali reikšti produkto projektavimo ir kūrimo pokyčius, todėl gali turėti įtakos produkto numatytajai paskirčiai ir atitikčiai šiame reglamente nustatytiems reikalavimams;

(25) produktai su skaitmeniniais elementais turėtų būti laikomi ypatingos svarbos, jei neigiamas potencialių produkto kibernetinio saugumo pažeidžiamumų išnaudojimo poveikis gali būti sunkus taip pat dėl su kibernetiniu saugumu susijusių funkcijų arba numatytosios paskirties. Visų pirma produktų su skaitmeniniais elementais, kurie turi su kibernetiniu saugumu susijusių funkcijų, pvz., saugių elementų, pažeidžiamumai gali sukelti saugumo problemų išplitimą visoje tiekimo grandinėje. Kibernetinio saugumo incidento poveikio sunkumas taip pat gali padidėti atsižvelgiant į numatytąją produkto paskirtį, pvz., pramoninėje aplinkoje arba Direktyvos [Direktyva XXX/XXXX (TIS2)] [I] priede nurodyto tipo pagrindinio subjekto kontekste arba atliekant ypatingos svarbos arba jautrias funkcijas, pvz., tvarkant asmens duomenis;

(26) ypatingos svarbos produktams su skaitmeniniais elementais turėtų būti taikomos griežtesnės atitikties vertinimo procedūros, tačiau išlaikomas proporcingumo principas. Šiuo tikslu ypatingos svarbos produktai su skaitmeniniais elementais turėtų būti suskirstyti į dvi klases, atspindinčias kibernetinio saugumo rizikos lygį, susijusį su šių kategorijų produktais. Galimas kibernetinis incidentas su II klasės produktais gali sukelti didesnį neigiamą poveikį nei incidentas su I klasės produktais, pavyzdžiui, dėl jų su kibernetiniu saugumu susijusios funkcijos pobūdžio arba numatytosios paskirties naudoti jautrioje aplinkoje, todėl jam turėtų būti taikoma griežtesnė atitikties vertinimo procedūra;

(27) šio reglamento III priede nurodytos ypatingos svarbos produktų su skaitmeniniais elementais kategorijos turėtų būti suprantamos kaip produktai, turintys pagrindines šio reglamento III priede nurodytų tipų funkcijas. Pavyzdžiui, šio reglamento III priede išvardyti produktai, kurie pagal savo pagrindines funkcijas apibrėžiami kaip II klasės bendrosios paskirties mikroprocesoriai. Todėl turi būti privalomai atliekamas bendrosios paskirties mikroprocesorių atitikties trečiosios šalies vertinimas. Tai netaikoma kitiems produktams, kurie nėra aiškiai nurodyti šio reglamento III priede ir kuriuose gali būti integruotas bendrosios paskirties mikroprocesorius. Komisija turėtų priimti deleguotuosius aktus [per 12 mėnesių nuo šio reglamento įsigaliojimo], kad patikslintų III priede pateiktas I ir II klasei priskiriamų produktų kategorijų apibrėžtis;

(28) šiuo reglamentu tikslingai siekiama spręsti kibernetinio saugumo riziką. Tačiau produktai su skaitmeniniais elementais gali kelti ir kitą saugumo riziką, nesusijusią su kibernetiniu saugumu. Ši rizika turėtų ir toliau būti reglamentuojama kitais atitinkamais Sąjungos produktų teisės aktais. Jei jokie kiti Sąjungos derinamieji teisės aktai netaikomi, turėtų būti taikomas Reglamentas [reglamentas dėl bendros gaminių saugos]. Todėl, atsižvelgiant į tikslinį šio reglamento pobūdį, kaip nukrypti nuo Reglamento [reglamentas dėl bendros gaminių saugos] 2 straipsnio 1 dalies trečios pastraipos b punkto leidžianti nuostata turėtų būti taikomi Reglamento [reglamentas

dėl bendros gaminių saugos] III skyrius, 1 skirsnis, V ir VII skyriai ir IX–XI skyriai produktams su skaitmeniniais elementais, susijusiems su saugumo rizikomis, kurių šis reglamentas neapima, jei šiems produktams netaikomi konkretūs reikalavimai, nustatyti kituose Sąjungos derinamuosiuose teisės aktuose, kaip apibrėžta [reglamento dėl bendros gaminių saugos 3 straipsnio 25 punkte];

(29) produktai su skaitmeniniais elementais, pagal Reglamento[15] [DI reglamentas] 6 straipsnį priskirti didelės rizikos DI sistemoms, kurios patenka į šio reglamento taikymo sritį, turėtų atitikti šiame reglamente nustatytus esminius reikalavimus. Kai tos didelės rizikos DI sistemos atitinka esminius šio reglamento reikalavimus, jos turėtų būti laikomos atitinkančiomis Reglamento [DI reglamentas] [15] straipsnyje nustatytus kibernetinio saugumo reikalavimus tiek, kiek šiuos reikalavimus apima pagal šį reglamentą parengiama ES atitikties deklaracija arba jos dalys. Kalbant apie atitikties vertinimo procedūras, susijusias su esminiais kibernetinio saugumo reikalavimais produktui su skaitmeniniais elementais, kuriam taikomas šis reglamentas ir kuris priskiriamas prie didelės rizikos DI sistemų, kaip taisyklė turėtų būti taikomos atitinkamos Reglamento [DI reglamentas] 43 straipsnio nuostatos vietoje atitinkamų šio reglamento nuostatų. Tačiau ši taisyklė neturėtų sumažinti būtino ypatingos svarbos produktų su skaitmeniniais elementais, kuriems taikomas šis reglamentas, užtikrinimo lygio. Todėl, nukrypstant nuo šios taisyklės, didelės rizikos DI sistemoms, kurios patenka į Reglamento [DI reglamentas] taikymo sritį ir kurios pagal šį reglamentą laikomos ypatingos svarbos produktais su skaitmeniniais elementais, ir kurioms taikoma Reglamento [DI reglamentas] VI priede nurodyta vidaus kontrole pagrįsto atitikties vertinimo procedūra, turėtų būti taikomos šio reglamento atitikties vertinimo nuostatos tiek, kiek tai susiję su esminiais šio reglamento reikalavimais. Šiuo atveju visais kitais aspektais, kuriuos apima Reglamentas [DI reglamentas], turėtų būti taikomos atitinkamos Reglamento [DI reglamentas] VI priede nustatytos vidaus kontrole pagrįsto atitikties vertinimo nuostatos;

(30) mašinų gaminiai, kuriems taikomas Reglamentas [pasiūlymas dėl mašinų reglamento] ir kurie yra produktai su skaitmeniniais elementais, apibrėžti šiame reglamente, ir kuriems pagal šį reglamentą yra parengta atitikties deklaracija, turėtų būti laikomi atitinkančiais esminius sveikatos ir saugos reikalavimus, nustatytus Reglamento [pasiūlymas dėl mašinų reglamento] [III priedo 1.1.9 ir 1.2.1 skirsniuose], kiek tai susiję su apsauga nuo duomenų vientisumo pažeidimo ir valdymo sistemų saugumu bei patikimumu ir tiek, kiek šių reikalavimų laikymąsi įrodo pagal šį reglamentą parengta ES atitikties deklaracija;

(31) Reglamentu [pasiūlymas dėl Europos sveikatos duomenų erdvės reglamento] papildomi šiame reglamente nustatyti esminiai reikalavimai. Todėl elektroninių sveikatos įrašų sistemos (toliau – ESĮ sistemos), kurios patenka į Reglamento [pasiūlymas dėl Europos sveikatos duomenų erdvės reglamento] taikymo sritį ir kurios yra produktai su skaitmeniniais elementais, apibrėžti šiame reglamente, taip pat turėtų atitikti šiame reglamente nustatytus esminius reikalavimus. Jų gamintojai turėtų įrodyti atitiktį, kaip reikalaujama Reglamente [pasiūlymas dėl Europos sveikatos duomenų erdvės reglamento]. Kad būtų lengviau laikytis reikalavimų, gamintojai gali parengti vieną techninį dokumentą, kuriame būtų nurodyti elementai, privalomi pagal abu teisės aktus. Kadangi šis reglamentas netaikomas SaaS, pagal SaaS licencijavimo ir pristatymo modelį siūlomos ESĮ sistemos nepatenka į šio reglamento taikymo sritį.

[15] Reglamentas [DI reglamentas].

Panašiai į šio reglamento taikymo sritį nepatenka ir ESĮ sistemos, sukurtos ir naudojamos organizacijos viduje, nes jos nėra pateikiamos rinkai;

(32) siekiant užtikrinti, kad produktai su skaitmeniniais elementais būtų saugūs tiek jų pateikimo rinkai metu, tiek per visą jų gyvavimo ciklą, būtina nustatyti esminius pažeidžiamumų valdymo reikalavimus ir esminius kibernetinio saugumo reikalavimus, susijusius su produktų su skaitmeniniais elementais savybėmis. Nors gamintojai turėtų laikytis visų esminių reikalavimų, susijusių su pažeidžiamumų valdymu, ir užtikrinti, kad visi jų produktai būtų pristatomi be jokių žinomų pažeidžiamumų, kuriuos būtų galima išnaudoti, jie turėtų nustatyti, kurie kiti su produkto savybėmis susiję esminiai reikalavimai yra aktualūs atitinkamam produkto tipui. Šiuo tikslu gamintojai turėtų atlikti kibernetinio saugumo rizikos, susijusios su produktu su skaitmeniniais elementais, vertinimą, kad nustatytų atitinkamą riziką ir atitinkamus esminius reikalavimus ir kad būtų deramai taikomi tinkami darnieji standartai arba bendrosios specifikacijos;

(33) siekiant pagerinti vidaus rinkai pateikiamų produktų su skaitmeniniais elementais saugumą, būtina nustatyti esminius reikalavimus. Šie esminiai reikalavimai turėtų nedaryti poveikio ES koordinuotiems ypatingos svarbos tiekimo grandinių rizikos vertinimams, nustatytiems Direktyvos [Direktyva XXX/XXXX (TIS2)][16] [X straipsnyje], per kuriuos atsižvelgiama į techninius ir, jei taikytina, į netechninius rizikos veiksnius, tokius kaip nederama trečiosios šalies įtaka tiekėjams. Be to, neturėtų būti pažeidžiamos valstybių narių prerogatyvos nustatyti papildomus reikalavimus, kuriais būtų atsižvelgiama į netechninius veiksnius, įskaitant apibrėžtus Rekomendacijoje (ES) 2019/534, siekiant užtikrinti aukštą atsparumo lygį Sąjungos mastu koordinuojamame 5G tinklų saugumo rizikos vertinime ir ES priemonių rinkinyje dėl 5G kibernetinio saugumo, dėl kurio susitarė TIS bendradarbiavimo grupė, kaip nurodyta [Direktyvoje XXX/XXXX (TIS2)];

(34) siekdami užtikrinti, kad nacionalinėms CSIRT ir bendram kontaktiniam punktui, paskirtam pagal Direktyvos [Direktyva XX/XXXX (TIS2) [X] straipsnį, būtų suteikta informacija, būtina jų užduotims atlikti, bendram pagrindinių ir svarbių subjektų kibernetinio saugumo lygiui padidinti ir veiksmingam rinkos priežiūros institucijų veikimui užtikrinti, produktų su skaitmeniniais elementais gamintojai turėtų pranešti ENISA apie pažeidžiamumus, kurie yra aktyviai išnaudojami. Kadangi dauguma produktų su skaitmeniniais elementais parduodami visoje vidaus rinkoje, bet koks išnaudojamas produkto su skaitmeniniais elementais pažeidžiamumas turėtų būti laikomas grėsme vidaus rinkos veikimui. Gamintojai taip pat turėtų apsvarstyti galimybę nurodyti ištaisytus pažeidžiamumus Europos pažeidžiamumų duomenų bazėje, kuri sukurta pagal Direktyvą [Direktyva XX/XXXX (TIS2)] ir kurią valdo ENISA, arba bet kurioje kitoje viešai prieinamoje pažeidžiamumų duomenų bazėje;

(35) gamintojai taip pat turėtų pranešti ENISA apie bet kokį incidentą, darantį poveikį produkto su skaitmeniniais elementais saugumui. Nepaisant direktyvoje [Direktyva XXX/XXXX (TIS2)] pagrindiniams ir svarbiems subjektams nustatytos pareigos pranešti apie incidentus, labai svarbu, kad ENISA, pagal Direktyvos [Direktyva XXX/XXXX (TIS2)] [X] straipsnį valstybių narių paskirti bendri kontaktiniai punktai ir rinkos priežiūros institucijos iš produktų su skaitmeniniais elementais gamintojų

[16] [data] Europos Parlamento ir Tarybos direktyva XXX [dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148 (OL L xx, data, p.x)].

gautų informaciją, kuri leistų jiems įvertinti šių produktų saugumą. Siekdami užtikrinti, kad naudotojai galėtų greitai reaguoti į incidentus, darančius poveikį jų produktų su skaitmeniniais elementais saugumui, gamintojai taip pat turėtų informuoti savo naudotojus apie tokius incidentus ir, jei taikytina, apie visas taisomąsias priemones, kurių naudotojai gali imtis incidento poveikiui sumažinti, pavyzdžiui, skelbdami atitinkamą informaciją savo interneto svetainėje arba, jei gamintojas gali susisiekti su naudotojais ir jei tai pateisinama dėl kylančios rizikos, susisiekdami su naudotojais tiesiogiai;

(36) produktų su skaitmeniniais elementais gamintojai turėtų įdiegti suderinto pažeidžiamumų atskleidimo politiką, kad asmenys arba subjektai galėtų lengviau pranešti apie pažeidžiamumus. Suderinto pažeidžiamumų atskleidimo politikoje turėtų būti nurodytas susistemintas procesas, kuriuo gamintojui pranešama apie pažeidžiamumus taip, kad gamintojas galėtų nustatyti ir ištaisyti tokius pažeidžiamumus prieš atskleidžiant išsamią informaciją apie pažeidžiamumus trečiosioms šalims arba visuomenei. Atsižvelgiant į tai, kad informacija apie plačiai naudojamų produktų su skaitmeniniais elementais pažeidžiamumus, kuriuos galima išnaudoti, gali būti didelėmis kainomis parduodama juodojoje rinkoje, tokių produktų gamintojai, vykdydami suderinto pažeidžiamumų atskleidimo politiką, turėtų galėti naudoti programas, kuriomis skatinama pranešti apie pažeidžiamumus užtikrinant, kad asmenys arba subjektai už savo pastangas sulauktų pripažinimo ir kompensacijos (vadinamoji atlygio už surastus riktus programa);

(37) kad būtų lengviau atlikti pažeidžiamumų analizę, gamintojai turėtų nustatyti ir dokumentuoti produktuose su skaitmeniniais elementais esančius komponentus, taip pat parengdami programinės įrangos medžiagų žiniaraštį. Programinės įrangos medžiagų žiniaraštis tiems, kurie gamina, perka ir valdo programinę įrangą, gali suteikti informacijos, kuri didina supratimą apie tiekimo grandinę, o tai turi daug privalumų – visų pirma tai padeda gamintojams ir naudotojams sekti žinomus naujus atskleistus pažeidžiamumus ir riziką. Gamintojams ypač svarbu užtikrinti, kad jų produktuose nebūtų pažeidžiamų komponentų, kuriuos sukuria trečiosios šalys;

(38) siekiant palengvinti atitikties šiame reglamente nustatytiems reikalavimams vertinimą, turėtų būti daroma prielaida, kad produktai su skaitmeniniais elementais atitinka šiuos reikalavimus, kai jie atitinka darniuosius standartus, kurie esminius šio reglamento reikalavimus paverčia išsamiomis techninėmis specifikacijomis ir kurie priimami pagal Europos Parlamento ir Tarybos reglamentą (ES) Nr. 1025/2012[17]. Reglamente (ES) Nr. 1025/2012 numatyta prieštaravimo darniesiems standartams procedūra, taikoma, kai tie standartai nevisiškai atitinka šio reglamento reikalavimus;

(39) Reglamentu (ES) 2019/881 sukuriama savanoriška IRT produktų, procesų ir paslaugų Europos kibernetinio saugumo sertifikavimo sistema. Europos kibernetinio saugumo sertifikavimo schemos gali apimti produktus su skaitmeniniais elementais, kuriems taikomas šis reglamentas. Šiuo reglamentu turėtų būti sukuriama sinergija su Reglamentu (ES) 2019/881. Siekiant palengvinti atitikties šiame reglamente nustatytiems reikalavimams vertinimą, daroma prielaida, kad produktai su skaitmeniniais elementais, kurie yra sertifikuoti arba kuriems išduotas atitikties

[17] 2012 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1025/2012 dėl Europos standartizacijos, kuriuo iš dalies keičiamos Tarybos direktyvos 89/686/EEB ir 93/15/EEB ir Europos Parlamento ir Tarybos direktyvos 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB ir 2009/105/EB ir panaikinamas Tarybos sprendimas 87/95/EEB ir Europos Parlamento ir Tarybos sprendimas Nr. 1673/2006/EB (OL L 316, 2012 11 14, p. 12).

pareiškimas pagal kibernetinio saugumo schemą pagal Reglamentą (ES) 2019/881 ir kuriuos Komisija nustatė įgyvendinimo akte, atitinka esminius šio reglamento reikalavimus tiek, kiek kibernetinio saugumo sertifikatas arba atitikties pareiškimas, arba jų dalys apima tuos reikalavimus. Atsižvelgiant į šį reglamentą, turėtų būti įvertintas naujų Europos kibernetinio saugumo sertifikavimo schemų, skirtų produktams su skaitmeniniais elementais, poreikis. Tokiose būsimose Europos kibernetinio saugumo sertifikavimo schemose, apimančiose produktus su skaitmeniniais elementais, turėtų būti atsižvelgiama į šiame reglamente nustatytus esminius reikalavimus ir palengvinamas šio reglamento reikalavimų laikymasis. Komisijai turėtų būti suteikti įgaliojimai įgyvendinimo aktais nurodyti Europos kibernetinio saugumo sertifikavimo schemas, kurios gali būti naudojamos siekiant įrodyti atitiktį šiame reglamente nurodytiems esminiams reikalavimams. Be to, siekdama išvengti pernelyg didelės administracinės naštos gamintojams, jei taikytina, Komisija turėtų nurodyti, ar pagal tokias Europos kibernetinio saugumo sertifikavimo schemas išduotas kibernetinio saugumo sertifikatas panaikina gamintojų pareigą atlikti trečiųjų šalių atitikties atitinkamiems reikalavimams vertinimą, kaip numatyta šiame reglamente;

(40) įsigaliojus įgyvendinimo aktui, kuriuo nustatomas [XXX Komisijos įgyvendinimo reglamentas (ES) Nr. …/... dėl Europos bendraisiais kriterijais grindžiamos kibernetinio saugumo sertifikavimo schemos] (EUCC), susijęs su šiuo reglamentu reglamentuojamais aparatinės įrangos produktais, pvz., aparatinės įrangos saugumo moduliais ir mikroprocesoriais, Komisija įgyvendinimo aktu gali nurodyti, kaip EUCC suteikia prielaidą dėl atitikties šio reglamento I priede ar jo dalyse nurodytiems esminiams reikalavimams. Be to, tokiame įgyvendinimo akte gali būti nurodyta, kaip pagal EUCC išduotas sertifikatas panaikina gamintojų pareigą atlikti trečiųjų šalių vykdomą atitinkamų reikalavimų atitikties vertinimą, reikalaujamą šiame reglamente;

(41) tais atvejais, kai nėra priimtų darniųjų standartų arba kai darnieji standartai nepakankamai atitinka esminius šio reglamento reikalavimus, Komisija turi galėti įgyvendinimo aktais priimti bendrąsias specifikacijas. Tokios bendrosios specifikacijos gali būti kuriamos vietoje rėmimosi darniaisiais standartais, pavyzdžiui, dėl to, kad kuri nors Europos standartizacijos organizacija atmetė standartizacijos prašymą, atitinkamų darniųjų standartų nustatymas pernelyg vėluoja, arba sukurti standartai neatitinka šio reglamento reikalavimų arba Komisijos prašymo. Siekiant palengvinti atitikties esminiams šiame reglamente nustatytiems reikalavimams vertinimą, turėtų būti daroma prielaida, kad produktai su skaitmeniniais elementais atitinka tuos reikalavimus, jeigu jie atitinka bendrąsias specifikacijas, kurias priėmė Komisija pagal šį reglamentą, kad išreikštų išsamias tų reikalavimų technines specifikacijas;

(42) gamintojai turėtų parengti ES atitikties deklaraciją, kad pateiktų pagal šį reglamentą reikalaujamą informaciją apie produktų su skaitmeniniais elementais atitiktį esminiams šio reglamento reikalavimams ir, jei taikytina, kitiems aktualiems Sąjungos derinamiesiems teisės aktams, reglamentuojantiems produktą. Iš gamintojų taip pat gali būti reikalaujama parengti ES atitikties deklaraciją pagal kitus Sąjungos teisės aktus. Siekiant užtikrinti efektyvią prieigą prie informacijos rinkos priežiūros tikslais, turėtų būti parengta viena ES atitikties deklaracija dėl atitikties visų aktualių Sąjungos aktų reikalavimams. Siekiant sumažinti administracinę naštą ekonominės veiklos vykdytojams, turėtų būti įmanoma, kad ta viena ES atitikties deklaracija būtų byla, sudaryta iš atitinkamų atskirų atitikties deklaracijų;

(43) CE ženklas, kuriuo rodoma produkto atitiktis, yra matomas viso proceso, apimančio atitikties vertinimą plačiąja prasme, rezultatas. Bendrieji ženklinimo CE ženklu principai nustatyti Europos Parlamento ir Tarybos reglamente (EB) Nr. 765/2008[18]. Šiame reglamente turėtų būti nustatytos produktų su skaitmeniniais elementais ženklinimo CE ženklu taisyklės. CE ženklas turėtų būti vienintelis ženklinimas kuriuo užtikrinama produktų su skaitmeniniais elementais atitiktis šio reglamento reikalavimams;

(44) siekiant sudaryti sąlygas ekonominės veiklos vykdytojams įrodyti atitiktį šiame reglamente nustatytiems esminiams reikalavimams, o rinkos priežiūros institucijoms – užtikrinti, kad rinkoje tiekiami produktai su skaitmeniniais elementais atitiktų šiuos reikalavimus, būtina nustatyti atitikties vertinimo procedūras. Europos Parlamento ir Tarybos sprendime Nr. 768/2008/EB[19] nustatomi atitikties vertinimo procedūrų moduliai, atitinkantys susijusios rizikos lygį ir reikalaujamą saugumo lygį. Siekiant užtikrinti nuoseklumą tarp skirtingų sektorių ir išvengti *ad hoc* variantų, tais moduliais buvo grindžiamos atitikties vertinimo procedūros, tinkamos tikrinti produktų su skaitmeniniais elementais atitiktį esminiams šiame reglamente nustatytiems reikalavimams. Atitikties vertinimo procedūrose turėtų būti nagrinėjami ir tikrinami tiek su produktu, tiek su procesu susiję reikalavimai, apimantys visą produktų su skaitmeniniais elementais gyvavimo ciklą, įskaitant produkto planavimą, projektavimą, kūrimą ar gamybą, bandymus ir priežiūrą;

(45) paprastai produktų su skaitmeniniais elementais atitikties vertinimą turėtų savo atsakomybe atlikti gamintojas pagal procedūrą, pagrįstą Sprendimo 768/2008/EB A moduliu. Gamintojas turėtų galėti lanksčiai pasirinkti griežtesnę atitikties vertinimo procedūrą, kurioje dalyvautų trečioji šalis. Jei produktas priskiriamas prie I klasės ypatingos svarbos produktų, reikia papildomo užtikrinimo, kad būtų įrodyta atitiktis šiame reglamente nurodytiems esminiams reikalavimams. Pagal Reglamentą (ES) 2019/881 gamintojas turėtų taikyti darniuosius standartus, bendrąsias specifikacijas ar kibernetinio saugumo sertifikavimo schemas, kuriuos Komisija nustatė įgyvendinimo akte, jei jis nori atlikti atitikties vertinimą savo atsakomybe (A modulis). Jei gamintojas netaiko tokių darniųjų standartų, bendrųjų specifikacijų ar kibernetinio saugumo sertifikavimo schemų, jis turėtų atlikti atitikties vertinimą, kuriame dalyvautų trečioji šalis. Atsižvelgiant į gamintojams tenkančią administracinę naštą ir į tai, kad materialių ir nematerialių produktų su skaitmeniniais elementais projektavimo ir kūrimo etape svarbus vaidmuo tenka kibernetiniam saugumui, pasirinktos atitikties vertinimo procedūros, pagrįstos Sprendimo 768/2008/EB atitinkamai B+C arba H moduliais, kaip tinkamiausios siekiant proporcingai ir veiksmingai įvertinti ypatingos svarbos produktų su skaitmeniniais elementais atitiktį. Trečiųjų šalių atitikties vertinimą atliekantis gamintojas gali pasirinkti geriausiai jo projektavimo ir gamybos procesui tinkančią procedūrą. Atsižvelgiant į dar didesnę kibernetinio saugumo riziką, susijusią su produktų, priskiriamų prie II klasės ypatingos svarbos produktų, naudojimu, atitikties vertinime visada turėtų dalyvauti trečioji šalis;

(46) kurdami materialius produktus su skaitmeniniais elementais gamintojai paprastai turi dėti dideles pastangas projektavimo, kūrimo ir gamybos etapuose, tačiau kuriant programinės įrangos tipo produktus su skaitmeniniais elementais orientuojamasi

---

[18] 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 765/2008, nustatantis akreditavimo reikalavimus ir panaikinantis Reglamentą (EEB) Nr. 339/93 (OL L 218, 2008 8 13, p. 30).

[19] 2008 m. liepos 9 d. Europos Parlamento ir Tarybos sprendimas Nr. 768/2008/EB dėl bendrosios gaminių pardavimo sistemos ir panaikinantis Sprendimą 93/465/EEB (OL L 218, 2008 8 13, p. 82).

beveik vien į projektavimą ir kūrimą, o gamybos etapo vaidmuo yra nedidelis. Nepaisant to, daugeliu atvejų programinės įrangos produktai vis tiek turi būti sukompiliuojami, sukuriami, supakuojami, pateikiami atsisiųsti arba nukopijuojami į fizinę laikmeną prieš pateikiant juos rinkai. Ši veikla turėtų būti laikoma apimančia gamybą, kai taikomi atitinkami atitikties vertinimo moduliai siekiant patikrinti, ar produktas atitinka esminius šio reglamento reikalavimus projektavimo, kūrimo ir gamybos etapuose;

(47) siekiant atlikti produktų su skaitmeniniais elementais atitikties trečiųjų šalių vertinimą, nacionalinės notifikuojančiosios institucijos turėtų pranešti Komisijai ir kitoms valstybėms narėms apie atitikties vertinimo įstaigas, jeigu jos atitinka tam tikrus reikalavimus, visų pirma dėl nepriklausomumo, kompetencijos ir interesų konfliktų nebuvimo;

(48) siekiant užtikrinti vienodą kokybės lygį atliekant produktų su skaitmeniniais elementais atitikties vertinimą, taip pat reikia nustatyti reikalavimus notifikuojančiosioms institucijoms ir kitoms įstaigoms, dalyvaujančioms atliekant notifikuotųjų įstaigų vertinimą, notifikavimą ir stebėseną. Šiame reglamente nustatytą sistemą turėtų papildyti akreditavimo sistema, numatyta Reglamente (EB) Nr. 765/2008. Kadangi akreditacija yra labai svarbi atitikties vertinimo įstaigų kompetencijos vertinimo priemonė, reikėtų ją taikyti ir notifikavimo tikslais;

(49) Reglamente (EB) Nr. 765/2008 numatytą skaidrią akreditaciją, kuria užtikrinamas būtinas pasitikėjimo atitikties sertifikatais lygis, nacionalinės viešosios institucijos visoje Sąjungoje turėtų laikyti pageidautinu atitikties vertinimo įstaigų techninės kompetencijos įrodymo būdu. Vis dėlto nacionalinės institucijos gali manyti turinčios tam vertinimui atlikti tinkamų priemonių. Tokiais atvejais, siekiant užtikrinti tinkamą kitų nacionalinių institucijų atliktų vertinimų patikimumo lygį, šios institucijos turėtų pateikti Komisijai ir kitoms valstybėms narėms reikiamus dokumentinius įrodymus, kad įvertintos atitikties vertinimo įstaigos atitinka aktualius norminius reikalavimus;

(50) dažnai atitikties vertinimo įstaigos dalį savo veiklos, susijusios su atitikties vertinimu, paveda atlikti subrangovams arba jiems pavaldžioms įstaigoms. Siekiant išsaugoti reikiamą rinkai pateiktinų produktų su skaitmeniniais elementais apsaugos lygį, labai svarbu, kad atitikties vertinimą atliekantys subrangovai ir pavaldžiosios įstaigos atitiktų notifikuotosioms įstaigoms keliamus atitikties vertinimo užduočių atlikimo reikalavimus;

(51) notifikuojančioji institucija turėtų pranešti Komisijai ir kitoms valstybėms narėms apie atitikties vertinimo įstaigą per informacinę sistemą „Naujojo požiūrio paskelbtos ir paskirtos organizacijos“ (NANDO). NANDO yra Komisijos sukurta ir valdoma elektroninių pranešimų priemonė, kurioje galima rasti visų notifikuotųjų įstaigų sąrašą;

(52) notifikuotosios įstaigos gali teikti paslaugas visoje Sąjungoje, todėl tikslinga suteikti kitoms valstybėms narėms ir Komisijai galimybę pareikšti prieštaravimus dėl notifikuotosios įstaigos. Todėl svarbu nustatyti laikotarpį, per kurį būtų galima išsiaiškinti visas abejones ar klausimus dėl atitikties vertinimo įstaigų kompetencijos prieš šioms įstaigoms pradedant veikti kaip notifikuotosioms įstaigoms;

(53) dėl konkurencingumo labai svarbu, kad notifikuotosios įstaigos atitikties vertinimo procedūras taikytų taip, kad ekonominės veiklos vykdytojams nebūtų užkrauta nereikalinga našta. Dėl tos pačios priežasties ir siekiant užtikrinti vienodas sąlygas ekonominės veiklos vykdytojams, reikia užtikrinti atitikties vertinimo procedūrų

techninio taikymo nuoseklumą. Geriausias būdas tai pasiekti – notifikuotosioms įstaigoms tinkamai koordinuoti tarpusavio veiksmus ir bendradarbiauti;

(54) rinkos priežiūra yra svarbi priemonė, užtikrinanti tinkamą ir vienodą Sąjungos teisės aktų taikymą. Todėl reikėtų įgyvendinti teisinę sistemą, pagal kurią rinkos priežiūra galėtų būti vykdoma tinkamu būdu. Produktams su skaitmeniniais elementais, kuriems taikomas šis reglamentas, taikomos Sąjungos rinkos priežiūros ir Sąjungos rinkai tiekiamų produktų kontrolės taisyklės, nustatytos Europos Parlamento ir Tarybos reglamente (ES) 2019/1020[20];

(55) pagal Reglamentą (ES) 2019/1020 rinkos priežiūros institucijos vykdo rinkos priežiūrą tos valstybės narės teritorijoje. Šis reglamentas neturėtų neleisti valstybėms narėms pasirinkti kompetentingų institucijų šioms užduotims vykdyti. Kiekviena valstybė narė savo teritorijoje turėtų paskirti vieną ar daugiau rinkos priežiūros institucijų. Valstybės narės gali nuspręsti paskirti bet kurią esamą arba naują instituciją, kuri veiktų kaip rinkos priežiūros institucija, įskaitant nacionalines kompetentingas institucijas, nurodytas Direktyvos [Direktyva XXX/XXXX (TIS2)] [X] straipsnyje, arba paskirtas nacionalines kibernetinio saugumo sertifikavimo institucijas, nurodytas Reglamento (ES) 2019/881 58 straipsnyje. Ekonominės veiklos vykdytojai turėtų visapusiškai bendradarbiauti su rinkos priežiūros institucijomis ir kitomis kompetentingomis institucijomis. Kiekviena valstybė narė turėtų pranešti Komisijai ir kitoms valstybėms narėms apie savo rinkos priežiūros institucijas ir kiekvienos iš tų institucijų kompetencijos sritis ir užtikrinti būtinus išteklius ir įgūdžius, kad būtų galima vykdyti su šiuo reglamentu susijusias priežiūros užduotis. Pagal Reglamento (ES) 2019/1020 10 straipsnio 2 ir 3 dalis kiekviena valstybė narė turėtų paskirti bendrą ryšių palaikymo tarnybą, kuri, be kita ko, turėtų būti atsakinga už rinkos priežiūros institucijų koordinuotos pozicijos atstovavimą ir pagalbą rinkos priežiūros institucijų bendradarbiavimui įvairiose valstybėse narėse;

(56) siekiant vienodai taikyti šį reglamentą, turėtų būti sudaryta speciali administracinio bendradarbiavimo grupė pagal Reglamento (ES) 2019/1020 30 straipsnio 2 dalį. Administracinio bendradarbiavimo grupę sudaro paskirtos rinkos priežiūros institucijos ir, jei taikytina, bendrų ryšių palaikymo tarnybų atstovai. Komisija turėtų remti ir skatinti rinkos priežiūros institucijų bendradarbiavimą per Sąjungos gaminių atitikties tinklą, įsteigtą pagal Reglamento (ES) 2019/1020 29 straipsnį ir apimantį kiekvienos valstybės narės atstovus, įskaitant kiekvienos bendros ryšių palaikymo tarnybos, nurodytos Reglamento (ES) 2019/1020 10 straipsnyje, atstovą ir neprivalomą nacionalinį ekspertą, administracinio bendradarbiavimo grupių pirmininkus ir Komisijos atstovus. Komisija turėtų dalyvauti tinklo, jo pogrupių ir šios atitinkamos administracinio bendradarbiavimo grupės posėdžiuose. Be to, ji turėtų padėti administracinio bendradarbiavimo grupei pasitelkdama vykdomąjį sekretoriatą, teikiantį techninę ir logistinę paramą;

(57) siekiant laiku, proporcingai ir veiksmingai taikyti priemones produktams su skaitmeniniais elementais, keliančiais reikšmingą kibernetinio saugumo riziką, reikėtų numatyti Sąjungos apsaugos procedūrą, pagal kurią suinteresuotosios šalys būtų informuojamos apie priemones, kurių ketinama imtis tokių produktų atžvilgiu. Tai taip pat suteiktų galimybę rinkos priežiūros institucijoms bendradarbiaujant su atitinkamais

[20] 2019 m. birželio 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/1020 dėl rinkos priežiūros ir gaminių atitikties, kuriuo iš dalies keičiama Direktyva 2004/42/EB ir reglamentai (EB) Nr. 765/2008 ir (ES) Nr. 305/2011 (OL L 169, 2019 6 25, p. 1).

ekonominės veiklos vykdytojais imtis veiksmų ankstesniame etape, kai to reikia. Jei valstybės narės ir Komisija sutaria dėl valstybės narės taikomų priemonių pagrįstumo, Komisija neturėtų imtis papildomų veiksmų, išskyrus atvejus, kai neatitiktis gali būti susijusi su darniojo standarto trūkumais;

(58) tam tikrais atvejais produktas su skaitmeniniais elementais, kuris atitinka šį reglamentą, vis tiek gali kelti reikšmingą kibernetinio saugumo riziką arba pavojų asmenų sveikatai ar saugai, pareigų pagal Sąjungos ar nacionalinę teisę, kuria siekiama saugoti pagrindines teises, vykdymui, paslaugų, kurias per elektroninę informacinę sistemą siūlo [Direktyvos XXX/XXXX (TIS2) I priede] nurodyti pagrindiniai subjektai, prieinamumui, autentiškumui, vientisumui ar konfidencialumui, arba kitiems viešojo intereso apsaugos aspektams. Todėl būtina nustatyti taisykles, kurios užtikrintų šios rizikos mažinimą. Rinkos priežiūros institucijos turėtų imtis priemonių ir nustatyti ekonominės veiklos vykdytojui reikalavimą užtikrinti, kad, priklausomai nuo rizikos, produktas tokios rizikos nebekeltų, būtų atšauktas arba būtų pašalintas iš rinkos. Kai tik rinkos priežiūros institucija apriboja arba uždraudžia laisvą gaminio judėjimą tokia tvarka, atitinkama valstybė narė turėtų nedelsdama pranešti Komisijai ir kitoms valstybėms narėms apie laikinąsias priemones nurodydama tokio sprendimo priėmimo priežastis ir pagrindimą. Jeigu rinkos priežiūros institucija imasi tokių priemonių dėl pavojų keliančių gaminių, Komisija turėtų nedelsdama pradėti konsultacijas su valstybėmis narėmis ir atitinkamu ekonominės veiklos vykdytoju ar vykdytojais ir įvertinti nacionalinę priemonę. Remdamasi šio vertinimo rezultatais Komisija turėtų nuspręsti, ar ta nacionalinė priemonė pagrįsta, ar ne. Komisija sprendimą turėtų skirti visoms valstybėms narėms ir nedelsdama apie jį pranešti joms ir atitinkamam ekonominės veiklos vykdytojui ar vykdytojams. Jei priemonė laikoma pagrįsta, Komisija taip pat gali svarstyti galimybę priimti pasiūlymus peržiūrėti atitinkamus Sąjungos teisės aktus;

(59) jei produktai su skaitmeniniais elementais kelia reikšmingą kibernetinio saugumo riziką ir jei yra pagrindo manyti, kad jie neatitinka šio reglamento, arba jei produktai atitinka šį reglamentą, bet kelia kitą svarbią riziką, pvz., pavojų asmenų sveikatai ar saugai, pagrindinėms teisėms ar [Direktyvos XXX/XXXX (TIS2) I priede] nurodytų pagrindinių subjektų vykdomam paslaugų teikimui, Komisija gali prašyti ENISA atlikti vertinimą. Remdamasi šiuo vertinimu Komisija Sąjungos lygmeniu įgyvendinimo aktais gali priimti taisomąsias arba ribojamąsias priemones, įskaitant nurodymą išimti iš rinkos arba atšaukti atitinkamus produktus per pagrįstą laikotarpį, atitinkantį rizikos pobūdį. Komisija gali pasinaudoti tokia intervencija tik išskirtinėmis aplinkybėmis, dėl kurių būtų pateisinama nedelsiant vykdyti intervenciją, kad būtų išsaugotas tinkamas vidaus rinkos veikimas, ir tik tais atvejais, kai priežiūros institucijos nesiėmė veiksmingų priemonių padėčiai ištaisyti. Tokios išskirtinės aplinkybės gali būti ekstremaliosios situacijos, kai, pavyzdžiui, gamintojas ne vienoje valstybėje narėje platina reikalavimų neatitinkantį produktą, kurį pagrindiniuose sektoriuose naudoja ir subjektai, kuriems taikoma [Direktyva XXX/XXXX (TIS2)], nors jame yra žinomų pažeidžiamumų, kuriais naudojasi piktavaliai subjektai ir kuriems ištaisyti gamintojas nepateikia pataisų. Tokiais ekstremaliais atvejais Komisija gali įsikišti tik tol, kol trunka išskirtinės aplinkybės, ir jei neatitiktis šio reglamento reikalavimams arba svarbi rizika išlieka;

(60) jei yra požymių, kad daugiau nei vienoje valstybėje narėje nesilaikoma šio reglamento, rinkos priežiūros institucijos turėtų galėti veikti bendrai su kitomis institucijomis, kad patikrintų produktų su skaitmeniniais elementais atitiktį reikalavimams ir nustatytų šių produktų kibernetinio saugumo riziką;

(61) tuo pačiu metu atliekami koordinuoti kontrolės veiksmai (tikslinės patikros) yra konkretūs rinkos priežiūros institucijų vykdymo užtikrinimo veiksmai, kuriais galima dar labiau padidinti produktų saugumą. Visų pirma tikslinės patikros turėtų būti vykdomos tais atvejais, kai rinkos tendencijos, vartotojų skundai ar kiti požymiai rodo, kad tam tikrų kategorijų produktams dažnai būdinga kibernetinio saugumo rizika. ENISA turėtų rinkos priežiūros institucijoms teikti pasiūlymus dėl produktų kategorijų, kurioms galėtų būti organizuojamos tikslinės patikros, remdamasi, be kita ko, ir savo gaunamais pranešimais apie produktų pažeidžiamumus ir incidentus;

(62) siekiant užtikrinti, kad prireikus būtų galima pritaikyti reglamentavimo sistemą, Komisijai turėtų būti deleguota teisė pagal SESV 290 straipsnį priimti aktus, kuriais būtų galima atnaujinti III priede pateiktą ypatingos svarbos produktų sąrašą ir nurodyti šių produktų kategorijų apibrėžtis. Komisijai turėtų būti deleguotas įgaliojimas priimti aktus pagal tą straipsnį, kad būtų nustatyti produktai su skaitmeniniais elementais, kuriems taikomos kitos Sąjungos taisyklės, kuriomis užtikrinamas toks pat apsaugos lygis kaip ir šiuo reglamentu, nurodant, ar reikėtų apriboti šio reglamento taikymo sritį arba jo netaikyti ir, kai taikytina, tokio apribojimo taikymo sritį. Komisijai taip pat turėtų būti deleguotas įgaliojimas priimti aktus pagal tą straipsnį dėl galimo įpareigojimo sertifikuoti tam tikrus didžiausios svarbos produktus su skaitmeniniais elementais remiantis šiame reglamente nurodytais ypatingo svarbumo kriterijais, taip pat minimalaus ES atitikties deklaracijos turinio nurodymo ir elementų, kurie turi būti įtraukti į techninius dokumentus, papildymo. Ypač svarbu, kad atlikdama parengiamąjį darbą Komisija tinkamai konsultuotųsi, taip pat ir su ekspertais, ir kad tos konsultacijos būtų vykdomos vadovaujantis 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros[21] nustatytais principais. Visų pirma siekiant užtikrinti vienodas galimybes dalyvauti atliekant su deleguotaisiais aktais susijusį parengiamąjį darbą, Europos Parlamentas ir Taryba visus dokumentus gauna tuo pačiu metu kaip ir valstybių narių ekspertai, o jų ekspertams sistemingai suteikiama galimybė dalyvauti Komisijos ekspertų grupių, kurios atlieka su deleguotaisiais aktais susijusį parengiamąjį darbą, posėdžiuose;

(63) siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai, kuriais būtų galima: nurodyti programinės įrangos medžiagų žiniaraščio formatą ir elementus, papildomai nurodyti pranešimų apie aktyviai išnaudojamus pažeidžiamumus ir incidentus, kuriuos ENISA pateikia gamintojai, formatą ir procedūrą, nurodyti pagal Reglamentą (ES) 2019/881 priimtas Europos kibernetinio saugumo sertifikavimo schemas, kurias galima naudoti siekiant įrodyti atitiktį esminiams reikalavimams ar jų dalims, kaip nurodyta šio reglamento I priede, priimti bendrąsias specifikacijas dėl I priede nustatytų esminių reikalavimų, nustatyti technines specifikacijas piktogramoms arba bet kokiems kitiems su produktų su skaitmeniniais elementais saugumu susijusiems ženklams ir jų naudojimo skatinimo mechanizmus, Sąjungos lygmeniu priimti sprendimus dėl taisomųjų arba ribojamųjų priemonių išskirtinėmis aplinkybėmis, dėl kurių būtų pagrįsta nedelsiant atlikti intervenciją, kad būtų išsaugotas tinkamas vidaus rinkos veikimas. Tais įgaliojimais turėtų būti naudojamasi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011[22];

---

21 OL L 123, 2016 5 12, p. 1.

22 2011 m. vasario 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 182/2011, kuriuo nustatomos valstybių narių vykdomos Komisijos naudojimosi įgyvendinimo įgaliojimais kontrolės mechanizmų taisyklės ir bendrieji principai (OL L 55, 2011 2 28, p. 13).

(64) siekiant užtikrinti patikimą ir konstruktyvų rinkos priežiūros institucijų bendradarbiavimą Sąjungos ir nacionaliniu lygmenimis, visos šalys, taikančios šį reglamentą, turėtų gerbti informacijos ir duomenų, gautų vykdant savo užduotis, konfidencialumą;

(65) siekiant užtikrinti veiksmingą šiame reglamente nustatytų pareigų vykdymą, kiekvienai rinkos priežiūros institucijai turėtų būti suteikti įgaliojimai skirti administracines baudas arba prašyti jas skirti. Todėl turėtų būti nustatyti maksimalūs nacionaliniuose teisės aktuose numatomi administracinių baudų dydžiai už šiame reglamente nustatytų pareigų nevykdymą. Priimant sprendimą dėl administracinės baudos dydžio kiekvienu konkrečiu atveju reikėtų atsižvelgti į visas atitinkamas konkrečios situacijos aplinkybes ir bent jau į šiame reglamente aiškiai nustatytas aplinkybes, taip pat į tai, ar kitos rinkos priežiūros institucijos jau yra skyrusios administracines baudas tam pačiam vykdytojui už panašius pažeidimus. Tokios aplinkybės gali būti sunkinančios tais atvejais, kai tas pats veiklos vykdytojas toliau nevykdo pareigų kitų valstybių narių nei tos, kurioje administracinė bauda jau paskirta, teritorijose, arba lengvinančios, siekiant užtikrinti, kad skiriant bet kokią kitą administracinę baudą, kurią svarsto pritaikyti kita rinkos priežiūros institucija tam pačiam ekonominės veiklos vykdytojui arba už tos pačios rūšies pažeidimą, jau būtų atsižvelgta į kitose valstybėse narėse skirtą baudą ir jos dydį kartu su kitomis aktualiomis konkrečiomis aplinkybėmis. Visais tokiais atvejais bendra administracinė bauda, kurią skirtingų valstybių narių rinkos priežiūros institucijos galėtų pritaikyti tam pačiam ekonominės veiklos vykdytojui už tos pačios rūšies pažeidimą, turėtų atitikti proporcingumo principą;

(66) jei administracinės baudos skiriamos asmenims, kurie nėra įmonė, svarstydama, koks būtų tinkamas baudos dydis, kompetentinga institucija turėtų atsižvelgti į bendrą pajamų lygį valstybėje narėje ir į to asmens ekonominę padėtį. Valstybės narės turėtų nustatyti, ar ir kokiu mastu valdžios institucijoms turėtų būti skiriamos administracinės baudos;

(67) palaikydama santykius su trečiosiomis valstybėmis, ES siekia skatinti tarptautinę prekybą reglamentuojamais produktais. Siekiant palengvinti prekybą, gali būti taikomos įvairios priemonės, įskaitant skirtingas teisines priemones, pvz., dvišalius (tarpvyriausybinius) abipusio pripažinimo susitarimus, skirtus reglamentuojamų produktų atitikties vertinimui ir ženklinimui. Abipusio pripažinimo susitarimai sudaromi tarp Sąjungos ir trečiųjų valstybių, kurios yra panašaus techninio išsivystymo lygio ir turi suderinamą atitikties vertinimo metodą. Šie susitarimai grindžiami abipusiu sertifikatų, atitikties ženklų ir bandymų ataskaitų, kurias išduoda bet kurios iš šalių atitikties vertinimo įstaigos, pripažinimu pagal kitos šalies teisės aktus. Šiuo metu abipusio pripažinimo susitarimai sudaryti keliose valstybėse. Susitarimai sudaromi dėl tam tikrų konkrečių sektorių, kurie skirtingose valstybėse gali skirtis. Siekiant papildomai palengvinti prekybą ir pripažįstant, kad produktų su skaitmeniniais elementais tiekimo grandinės yra pasaulinės, vadovaujantis SESV 218 straipsniu gali būti sudaromi abipusio pripažinimo susitarimai dėl produktų, kurie Sąjungoje reglamentuojami pagal šį reglamentą, atitikties vertinimo. Taip pat svarbu bendradarbiauti su šalimis partnerėmis, kad kibernetinis atsparumas būtų sustiprintas visame pasaulyje, nes ilgainiui tai prisidės prie stipresnės kibernetinio saugumo sistemos tiek ES viduje, tiek už jos ribų;

(68) Komisija, konsultuodamasi su suinteresuotosiomis šalimis, turėtų periodiškai peržiūrėti šį reglamentą, visų pirma siekdama nustatyti, ar reikia jį keisti atsižvelgiant į kintančias visuomenines, politines, technologines ar rinkos sąlygas;

(69) ekonominės veiklos vykdytojams turėtų būti skirta pakankamai laiko prisitaikyti prie šio reglamento reikalavimų. Šis reglamentas turėtų būti taikomas praėjus [24 mėnesiams] nuo jo įsigaliojimo, išskyrus pareigą pranešti apie aktyviai išnaudojamus pažeidžiamumus ir incidentus, kuri turėtų būti taikoma praėjus [12 mėnesių] nuo šio reglamento įsigaliojimo;

(70) kadangi šio reglamento tikslo valstybės narės negali deramai pasiekti, o dėl veiksmo poveikio to tikslo būtų geriau siekti Sąjungos lygmeniu, laikydamasi Europos Sąjungos sutarties 5 straipsnyje nustatyto subsidiarumo principo Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šiuo reglamentu neviršijama to, kas būtina nurodytam tikslui pasiekti;

(71) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725[23] 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis pateikė nuomonę […],

PRIĖMĖ ŠĮ REGLAMENTĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas

Šiuo reglamentu nustatoma:

(a) produktų su skaitmeniniais elementais pateikimo rinkai taisyklės, kuriomis siekiama užtikrinti tokių produktų kibernetinį saugumą;

(b) esminiai produktų su skaitmeniniais elementais projektavimo, kūrimo ir gamybos reikalavimai ir ekonominės veiklos vykdytojų pareigos, susijusios su šių produktų kibernetiniu saugumu;

(c) esminiai pažeidžiamumų valdymo procesų, kuriuos taiko gamintojai, kad užtikrintų produktų su skaitmeniniais elementais kibernetinį saugumą per visą gyvavimo ciklą, reikalavimai ir ekonominės veiklos vykdytojų pareigos, susijusios su šiais procesais;

(d) taisyklės dėl rinkos priežiūros ir minėtų taisyklių bei reikalavimų vykdymo užtikrinimo.

2 straipsnis

Taikymo sritis

1. Šis reglamentas taikomas produktams su skaitmeniniais elementais, kurių paskirtis arba pagrįstai numatomas naudojimas apima tiesioginę arba netiesioginę loginę arba fizinę duomenų jungtį su įrenginiu arba tinklu.

[23] 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

2. Šis reglamentas netaikomas produktams su skaitmeniniais elementais, kuriems taikomi šie Sąjungos teisės aktai:

(a) Reglamentas (ES) 2017/745;

(b) Reglamentas (ES) 2017/746;

(c) Reglamentas (ES) 2019/2144.

3. Šis reglamentas netaikomas produktams su skaitmeniniais elementais, kurie buvo sertifikuoti pagal Reglamentą (ES) 2018/1139.

4. Šio reglamento taikymas produktams su skaitmeniniais elementais, kuriems taikomos kitos Sąjungos taisyklės, kuriomis nustatomi reikalavimai, skirti visai arba daliai rizikos, kurią apima I priede nustatyti esminiai reikalavimai, gali būti apribotas arba daroma taikymo išimtis, jeigu:

(a) toks apribojimas arba išimtis atitinka bendrą šiems produktams taikomą reglamentavimo sistemą; ir

(b) sektorių taisyklėmis užtikrinamas toks pat apsaugos lygis kaip ir šiuo reglamentu.

Komisija įgaliojama priimti deleguotuosius aktus pagal 50 straipsnį, kad galėtų iš dalies keisti šį reglamentą nurodydama, ar toks apribojimas arba išimtis yra būtinas (-a), susijusius produktus ir taisykles, taip pat, jei taikytina, apribojimo taikymo sritį.

5. Šis reglamentas netaikomas produktams su skaitmeniniais elementais, sukurtiems išimtinai nacionalinio saugumo ar kariniams tikslams, taip pat produktams, specialiai sukurtiems įslaptintai informacijai tvarkyti.

3 straipsnis

Apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

(1) produktas su skaitmeniniais elementais – programinės ar aparatinės įrangos produktas ir jo nuotolinio duomenų tvarkymo sprendiniai, įskaitant atskirai rinkai pateikiamus programinės ar aparatinės įrangos komponentus;

(2) nuotolinis duomenų tvarkymas – per atstumą vykdomas duomenų tvarkymas, kuriam programinę įrangą projektuoja ir kuria arba atsakomybę už tai prisiima gamintojas ir be kurio produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų;

(3) ypatingos svarbos produktas su skaitmeniniais elementais – produktas su skaitmeniniais elementais, kuriam būdinga kibernetinio saugumo rizika pagal 6 straipsnio 2 dalyje nustatytus kriterijus ir kurio pagrindinės funkcijos nustatytos III priede;

(4) didžiausios svarbos produktas su skaitmeniniais elementais – produktas su skaitmeniniais elementais, kuriam būdinga kibernetinio saugumo rizika pagal 6 straipsnio 5 dalyje nustatytus kriterijus;

(5) operacinė technologija – programuojama skaitmeninė sistema ar įrenginys, kurie sąveikauja su fizine aplinka arba valdo su fizine aplinka sąveikaujančius įrenginius;

(6) programinė įranga – elektroninės informacinės sistemos dalis, sudaryta iš kompiuterinio kodo;

(7) aparatinė įranga – fizinė elektroninė informacinė sistema ar jos dalys, galinčios tvarkyti, saugoti ar perduoti skaitmeninius duomenis;

(8) komponentas – programinė ar aparatinė įranga, skirta integruoti į elektroninę informacinę sistemą;

(9) elektroninė informacinė sistema – sistema, įskaitant elektrinę ar elektroninę įrangą, galinti tvarkyti, saugoti ar perduoti skaitmeninius duomenis;

(10) loginė jungtis – virtuali duomenų jungtis per programinės įrangos sąsają;

(11) fizinė jungtis – jungtis tarp elektroninių informacinių sistemų ar komponentų, įdiegta fizinėmis priemonėmis, įskaitant elektrines ar mechanines sąsajas, laidus ar radijo bangas;

(12) netiesioginė jungtis – jungtis su įrenginiu ar tinklu, kuri pati nėra tiesioginė, bet yra didesnės su tokiu įrenginiu ar tinklu tiesiogiai sujungtos sistemos dalis;

(13) privilegijuotosios prieigos teisė – prieigos teisė, suteikta konkretiems naudotojams ar programoms su saugumu susijusioms operacijoms elektroninėje informacinėje sistemoje atlikti;

(14) itin privilegijuotos prieigos teisė – prieigos teisė, kuri suteikta konkretiems naudotojams ar programoms sudėtingesnėms su saugumu susijusioms operacijoms elektroninėje informacinėje sistemoje atlikti ir kuri piktavaliui subjektui, jei ja būtų piktnaudžiaujama ar jei ji būtų perimta, galėtų suteikti platesnę prieigą prie sistemos ar organizacijos išteklių;

(15) galinis įrenginys – įrenginys, prijungtas prie tinklo ir naudojamas kaip prieigos prie to tinklo priemonė;

(16) tinklo ar kompiuterijos ištekliai – duomenų, aparatinės ar programinės įrangos funkcijos, prieinamos vietoje arba per tinklą ar kitą prijungtą įrenginį;

(17) ekonominės veiklos vykdytojas – gamintojas, įgaliotasis atstovas, importuotojas, platintojas arba bet kuris kitas fizinis ar juridinis asmuo, kuriam taikomos šiame reglamente nustatytos pareigos;

(18) gamintojas – fizinis arba juridinis asmuo, kuris kuria arba gamina produktus su skaitmeniniais elementais arba organizuoja produktų su skaitmeniniais elementais projektavimą, kūrimą ar gamybą ir parduoda juos savo vardu arba su savo prekių ženklu už atlygį arba nemokamai;

(19) įgaliotasis atstovas – Sąjungoje įsisteigęs fizinis arba juridinis asmuo, gavęs gamintojo rašytinį įgaliojimą veikti jo vardu siekiant atlikti nurodytas užduotis;

(20) importuotojas – Sąjungoje įsisteigęs fizinis arba juridinis asmuo, rinkai pateikiantis produktą su skaitmeniniais elementais, kurio pavadinimas arba prekių ženklas priklauso ne Sąjungoje įsisteigusiam fiziniam arba juridiniam asmeniui;

(21) platintojas – tiekimo grandinėje veikiantis fizinis arba juridinis asmuo (išskyrus gamintoją ir importuotoją), kuris pateikia produktą su skaitmeniniais elementais Sąjungos rinkai nepakeisdamas jo savybių;

(22) pateikimas rinkai – produkto su skaitmeniniais elementais pateikimas Sąjungos rinkai pirmą kartą;

(23) tiekimas rinkai – produkto su skaitmeniniais elementais tiekimas platinti ar naudoti Sąjungos rinkoje vykdant komercinę veiklą už atlygį arba nemokamai;

(24) numatytoji paskirtis – gamintojo numatyta produkto su skaitmeniniais elementais paskirtis, įskaitant konkrečias naudojimo aplinkybes ir sąlygas, nurodyta informacijoje, kurią gamintojas pateikė naudojimo instrukcijose, reklaminėje ar pardavimo medžiagoje bei teiginiuose ir techniniuose dokumentuose;

(25) pagrįstai numatomas naudojimas – naudojimas nebūtinai pagal gamintojo numatytą paskirtį, kurią jis nurodė naudojimo instrukcijose, reklaminėje ar pardavimo medžiagoje bei teiginiuose ir techniniuose dokumentuose, kuris galimas dėl pagrįstai numatomo žmogaus elgesio, techninių operacijų ar sąveikos;

(26) pagrįstai numatomas netinkamas naudojimas – produkto su skaitmeniniais elementais naudojimas ne pagal numatytąją paskirtį, kurį gali nulemti pagrįstai numatomas žmogaus elgesys ar sąveika su kitomis sistemomis;

(27) notifikuojančioji institucija – nacionalinė institucija, atsakinga už atitikties vertinimo įstaigoms vertinti, skirti ir notifikuoti būtinų procedūrų nustatymą bei vykdymą ir už tų įstaigų stebėseną;

(28) atitikties vertinimas – tikrinimo, ar įvykdyti I priede nustatyti esminiai reikalavimai, procesas;

(29) atitikties vertinimo įstaiga – įstaiga, apibrėžta Reglamento (ES) Nr. 765/2008 2 straipsnio 13 dalyje;

(30) notifikuotoji įstaiga – atitikties vertinimo įstaiga, paskirta pagal šio reglamento 33 straipsnį ir kitus atitinkamus Sąjungos derinamuosius teisės aktus;

(31) esminis pakeitimas – produkto su skaitmeniniais elementais pakeitimas po jo pateikimo rinkai, kuris daro poveikį produkto su skaitmeniniais elementais atitikčiai I priedo 1 skirsnyje nustatytiems esminiams reikalavimams arba dėl kurio pasikeičia numatytoji paskirtis, pagal kurią buvo atliekamas produkto su skaitmeniniais elementais vertinimas;

(32) CE ženklas – ženklas, kuriuo gamintojas nurodo, kad produktas su skaitmeniniais elementais ir gamintojo įdiegti procesai atitinka I priede ir kituose taikomuose Sąjungos teisės aktuose, kuriais suderinamos gaminių pardavimo sąlygos (toliau – Sąjungos derinamieji teisės aktai), nustatytus esminius reikalavimus, kuriais nustatomas toks ženklinimas;

(33) rinkos priežiūros institucija – rinkos priežiūros institucija, apibrėžta Reglamento (ES) 2019/1020 3 straipsnio 4 punkte;

(34) darnusis standartas – darnusis standartas, apibrėžtas Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkto c papunktyje;

(35) kibernetinio saugumo rizika – rizika, apibrėžta Direktyvos [Direktyva XXX/XXXX (TIS2)] [X] straipsnyje;

(36) reikšminga kibernetinio saugumo rizika – kibernetinio saugumo rizika, dėl kurios, atsižvelgiant į jos technines charakteristikas, galima manyti, kad yra didelė incidento, galinčio sukelti didelį neigiamą poveikį, įskaitant didelius materialinius ar nematerialinius nuostolius arba sutrikimus, tikimybė;

(37) programinės įrangos medžiagų žiniaraštis – oficialus dokumentas, kuriame pateikiama produkto su skaitmeniniais elementais programinės įrangos elementuose naudojamų komponentų informacija ir tiekimo grandinės ryšiai;

(38) pažeidžiamumas – pažeidžiamumas, apibrėžtas Direktyvos [Direktyva XXX/XXXX (TIS2)] [X] straipsnyje;

(39) aktyviai išnaudojamas pažeidžiamumas – pažeidžiamumas, kuriuo, kaip matyti iš patikimų įrodymų, pasinaudodamas subjektas sistemoje paleido kenkimo kodą be sistemos savininko leidimo;

(40) asmens duomenys – duomenys, apibrėžti Reglamento (ES) 2016/679 4 straipsnio 1 dalyje.

4 straipsnis

Laisvas judėjimas

1. Valstybės narės netrukdo tiekti rinkai šį reglamentą atitinkančių gaminių su skaitmeniniais elementais dėl priežasčių, susijusių su šiuo reglamentu reguliuojamais aspektais.

2. Prekybos mugėse, parodose ir demonstracijose ar panašiuose renginiuose valstybės narės netrukdo pristatyti ir naudoti produkto su skaitmeniniais elementais, kuris neatitinka šio reglamento.

3. Valstybės narės netrukdo tiekti nebaigtos programinės įrangos, kuri neatitinka šio reglamento, su sąlyga, kad ši programinė įranga tiekiama tik ribotą bandymo tikslais reikalingą laikotarpį ir kad matomas ženklas aiškiai nurodo, jog ji neatitinka šio reglamento ir nebus tiekiama rinkai kitais nei bandymo tikslais.

5 straipsnis

Reikalavimai produktams su skaitmeniniais elementais

Produktai su skaitmeniniais elementais tiekiami rinkai tik jeigu:

(1) jie atitinka I priedo 1 skirsnyje nustatytus esminius reikalavimus su sąlyga, kad jie tinkamai įrengiami, prižiūrimi, naudojami pagal numatytąją paskirtį arba tokiomis sąlygomis, kurias galima pagrįstai numatyti, ir, jei taikytina, atnaujinami; ir

(2) gamintojo įdiegti procesai atitinka I priedo 2 skirsnyje nustatytus esminius reikalavimus.

6 straipsnis

Ypatingos svarbos produktai su skaitmeniniais elementais

1. Produktai su skaitmeniniais elementais, kurie priklauso III priede nurodytai kategorijai, laikomi ypatingos svarbos produktais su skaitmeniniais elementais. Produktai, kurių pagrindinės funkcijos priskiriamos šio reglamento III priede nurodytai kategorijai, laikomi priklausančiais tai kategorijai. Ypatingos svarbos produktų su skaitmeniniais elementais kategorijos skirstomos į III priede nustatytas I ir II klases, atspindinčias su šiais produktais susijusios kibernetinio saugumo rizikos lygį.

2. Komisija įgaliojama priimti deleguotuosius aktus pagal 50 straipsnį, kad galėtų iš dalies keisti III priedą, į ypatingos svarbos produktų su skaitmeniniais elementais kategorijų sąrašą įtraukdama naują kategoriją arba pašalindama iš jo esamą kategoriją. Vertindama poreikį iš dalies keisti III priede pateiktą sąrašą Komisija atsižvelgia į kibernetinio saugumo rizikos lygį, susijusį su produktų su skaitmeniniais

elementais kategorija. Vertinant kibernetinio saugumo rizikos lygį, atsižvelgiama į vieną ar daugiau iš šių kriterijų:

(a) produkto su skaitmeniniais elementais funkcijas, susijusias su kibernetiniu saugumu, ir tai, ar produktas su skaitmeniniais elementais pasižymi bent viena iš šių savybių:

(i) jis skirtas veikti naudodamasis itin privilegijuotos prieigos teisėmis arba valdyti privilegijuotosios prieigos teises;

(ii) jis turi tiesioginę arba privilegijuotąją prieigą prie tinklų ar kompiuterijos išteklių;

(iii) jis skirtas prieigai prie duomenų arba operacinei technologijai kontroliuoti;

(iv) jis atlieka funkciją, kuri yra itin svarbi pasitikėjimui – tai visų pirma apima saugumo funkcijas, pvz., tinklo valdymą, galinio įrenginio saugumą ir tinklo apsaugą;

(b) numatytąją paskirtį naudoti jautrioje aplinkoje, įskaitant pramoninę aplinką, arba kad jį naudoja Direktyvos [Direktyva XXX/XXXX (TIS2)] [I] priede nurodytos rūšies pagrindiniai subjektai;

(c) numatytąją paskirtį vykdyti ypatingos svarbos arba jautrias funkcijas, pvz., tvarkyti asmens duomenis;

(d) galimą neigiamo poveikio mastą, visų pirma atsižvelgiant į jo dydį ir galėjimą paveikti daugelį asmenų;

(e) kokiu mastu produktų su skaitmeniniais elementais naudojimas jau sukėlė materialinių ar nematerialinių nuostolių ar sutrikimų arba sukėlė didelį susirūpinimą dėl neigiamo poveikio pasireiškimo.

3. Komisija įgaliojama priimti deleguotąjį aktą pagal 50 straipsnį, kad papildytų šį reglamentą nurodydama III priede pateiktas I ir II klasei priskiriamų produktų kategorijų apibrėžtis. Deleguotasis aktas priimamas [per 12 mėnesių nuo šio reglamento įsigaliojimo].

4. Ypatingos svarbos produktams su skaitmeniniais elementais taikomos 24 straipsnio 2 ir 3 dalyse nurodytos atitikties vertinimo procedūros.

5. Komisija įgaliojama priimti deleguotuosius aktus pagal 50 straipsnį, kad papildytų šį reglamentą nurodydama didžiausios svarbos produktų su skaitmeniniais elementais kategorijas, kurioms priklausantiems produktams gamintojai privalo gauti Europos kibernetinio saugumo sertifikatą pagal Europos kibernetinio saugumo sertifikavimo schemą, kaip numatyta Reglamente (ES) 2019/881, kad įrodytų atitiktį I priede ar jo dalyse nurodytiems esminiams reikalavimams. Nustatydama tokias didžiausios svarbos produktų su skaitmeniniais elementais kategorijas Komisija atsižvelgia į kibernetinio saugumo rizikos, susijusios su produktų su skaitmeniniais elementais kategorija, lygį pagal vieną arba daugiau 2 dalyje nurodytų kriterijų, taip pat atsižvelgdama į vertinimą, ar tos kategorijos produktais:

(a) naudojasi arba remiasi Direktyvos [Direktyva XXX/XXXX (TIS2)] [I] priede nurodytos rūšies pagrindiniai subjektai ir ar jie ateityje gali būti svarbūs šių subjektų veiklai; arba

(b) jie aktualūs visos produktų su skaitmeniniais elementais tiekimo grandinės atsparumui ardomiesiems įvykiams.

7 straipsnis

Bendroji produktų sauga

Nukrypstant nuo Reglamento [reglamentas dėl bendros gaminių saugos] 2 straipsnio 1 dalies trečios pastraipos b punkto, kai produktams su skaitmeniniais elementais netaikomi specialūs reikalavimai, nustatyti kituose Sąjungos derinamuosiuose teisės aktuose, apibrėžtuose [Reglamento dėl bendros gaminių saugos 3 straipsnio 25 punkte], su tokiais produktais susijusiai saugumo rizikai, kurios neapima šis reglamentas, taikomi Reglamento [reglamentas dėl bendros gaminių saugos] III skyrius, 1 skirsnis, V ir VII skyriai bei IX–XI skyriai.

8 straipsnis

Didelės rizikos DI sistemos

1. Jei produktai su skaitmeniniais elementais pagal Reglamento [DI reglamentas] [6] straipsnį priskiriami prie didelės rizikos DI sistemų, kurios patenka į šio reglamento taikymo sritį ir atitinka esminius reikalavimus, nustatytus šio reglamento I priedo 1 skirsnyje, ir jei gamintojo įdiegti procesai atitinka esminius reikalavimus, nustatytus I priedo 2 skirsnyje, tokie produktai laikomi atitinkančiais su kibernetiniu saugumu susijusius reikalavimus, nustatytus Reglamento [DI reglamentas] [15] straipsnyje, nedarant poveikio kitų su tikslumu ir patikimumu susijusių reikalavimų, numatytų minėtame straipsnyje, taikymui ir tiek, kiek pagal šiuos reikalavimus privalomo apsaugos lygio pasiekimą įrodo pagal šį reglamentą parengta ES atitikties deklaracija.

2. 1 dalyje nurodytiems produktams ir kibernetinio saugumo reikalavimams taikoma atitinkama atitikties vertinimo procedūra, kurios reikalaujama Reglamento [DI reglamentas] [43] straipsnyje. To vertinimo tikslais teisę tikrinti didelės rizikos DI sistemų atitiktį pagal Reglamentą [DI reglamentas] turinčios notifikuotosios įstaigos taip pat turi teisę tikrinti didelės rizikos DI sistemų atitiktį pagal šio reglamento I priede nustatytus reikalavimus su sąlyga, kad atliekant notifikavimo pagal Reglamentą [DI reglamentas] procedūrą buvo įvertinta tų notifikuotųjų įstaigų atitiktis šio reglamento 29 straipsnyje nustatytiems reikalavimams.

3. Nukrypstant nuo 2 dalies, šio reglamento III priede išvardytiems ypatingos svarbos produktams su skaitmeniniais elementais, kuriems turi būti taikomos šio reglamento 24 straipsnio 2 dalies a punkte, 24 straipsnio 2 dalies b punkte, 24 straipsnio 3 dalies a punkte ir 24 straipsnio 3 dalies b punkte nurodytos atitikties vertinimo procedūros ir kurie pagal Reglamento [DI reglamentas] [6] straipsnį taip pat priskiriami didelės rizikos DI sistemoms ir kuriems taikoma Reglamento [DI reglamentas] [VI] priede nurodyta vidaus kontrole pagrįsta atitikties vertinimo procedūra, šiuo reglamentu reikalaujamos atitikties vertinimo procedūros taikomos tiek, kiek jos yra susijusios su esminiais šio reglamento reikalavimais.

9 straipsnis

Mašinų gaminiai

Mašinų gaminiai, kuriems taikomas Reglamentas [pasiūlymas dėl mašinų reglamento] ir kurie yra produktai su skaitmeniniais elementais, apibrėžti šiame reglamente, ir kuriems pagal šį

reglamentą yra parengta ES atitikties deklaracija, laikomi atitinkančiais esminius sveikatos ir saugos reikalavimus, nustatytus Reglamento [pasiūlymas dėl mašinų reglamento] priede [III priedo 1.1.9 ir 1.2.1 skirsniuose], kiek tai susiję su apsauga nuo duomenų vientisumo pažeidimo ir valdymo sistemų saugumu bei patikimumu ir tiek, kiek pagal šiuos reikalavimus privalomo apsaugos lygio pasiekimą įrodo pagal šį reglamentą parengta ES atitikties deklaracija.

II SKYRIUS

EKONOMINĖS VEIKLOS VYKDYTOJŲ PAREIGOS

10 straipsnis

Gamintojų pareigos

1. Pateikdami produktą su skaitmeniniais elementais rinkai gamintojai užtikrina, kad jis būtų suprojektuotas, sukurtas ir pagamintas pagal I priedo 1 skirsnyje nustatytus esminius reikalavimus.

2. Siekdami laikytis 1 dalyje nustatytos pareigos gamintojai atlieka kibernetinio saugumo rizikos, susijusios su produktu su skaitmeniniais elementais, vertinimą ir atsižvelgia į to vertinimo rezultatus produkto su skaitmeniniais elementais planavimo, projektavimo, kūrimo, gamybos, pristatymo ir priežiūros etapuose, kad būtų kuo labiau sumažinta kibernetinio saugumo rizika, išvengta saugumo incidentų ir kuo labiau sumažintas tokių incidentų poveikis, įskaitant atvejus, kai tai susiję su naudotojų sveikata ir sauga.

3. Pateikdamas produktą su skaitmeniniais elementais rinkai gamintojas į 23 straipsnyje ir V priede nurodytus techninius dokumentus įtraukia kibernetinio saugumo rizikos vertinimą. 8 straipsnyje ir 24 straipsnio 4 dalyje nurodytų produktų su skaitmeniniais elementais, kuriems taikomi ir kiti Sąjungos aktai, kibernetinio saugumo rizikos vertinimas gali būti tų atitinkamų Sąjungos aktų reikalaujamo rizikos vertinimo dalis. Jei parduodamam produktui su skaitmeniniais elementais netaikomi tam tikri esminiai reikalavimai, gamintojas tai aiškiai pagrindžia minėtuose dokumentuose.

4. Kai į produktus su skaitmeniniais elementais integruojami iš trečiųjų šalių gauti komponentai, siekdami laikytis 1 dalyje nustatytos pareigos gamintojai atlieka deramą patikrinimą. Jie užtikrina, kad tokie komponentai nekeltų pavojaus produkto su skaitmeniniais elementais saugumui.

5. Gamintojas sistemingai, proporcingai kibernetinio saugumo rizikai ir pobūdžiui, dokumentuoja atitinkamus kibernetinio saugumo aspektus, susijusius su produktu su skaitmeniniais elementais, įskaitant pažeidžiamumus, apie kuriuos sužino, ir visą aktualią trečiųjų šalių pateiktą informaciją ir prireikus atnaujina produkto rizikos vertinimą.

6. Pateikdami produktą su skaitmeniniais elementais rinkai ir per numatomą produkto gyvavimo laikotarpį arba penkerius metus nuo produkto pateikimo rinkai, atsižvelgiant į tai, kuris laikotarpis trumpesnis, gamintojai užtikrina veiksmingą to produkto pažeidžiamumų valdymą laikantis I priedo 2 skirsnyje nustatytų esminių reikalavimų.

   Gamintojai taiko tinkamą politiką ir procedūras, įskaitant suderinto pažeidžiamumų atskleidimo politiką, nurodytą I priedo 2 skirsnio 5 punkte, kad apdorotų ir ištaisytų

galimus produkto su skaitmeniniais elementais pažeidžiamumus, apie kuriuos pranešė vidiniai arba išoriniai šaltiniai.

7. Prieš pateikdami produktą su skaitmeniniais elementais rinkai gamintojai parengia 23 straipsnyje nurodytus techninius dokumentus.

   Jie atlieka 24 straipsnyje nurodytas pasirinktas atitikties vertinimo procedūras arba organizuoja jų vykdymą.

   Jeigu pagal tą atitikties vertinimo procedūrą įrodyta, kad produktas su skaitmeniniais elementais atitinka I priedo 1 skirsnyje nustatytus esminius reikalavimus ir kad gamintojo įdiegti procesai atitinka I priedo 2 skirsnyje nustatytus esminius reikalavimus, gamintojas parengia ES atitikties deklaraciją pagal 20 straipsnį ir paženklina produktą CE ženklu pagal 22 straipsnį.

8. Gamintojas saugo techninius dokumentus ir ES atitikties deklaraciją, kai aktualu, dešimt metų po produkto su skaitmeniniais elementais pateikimo rinkai, kad nacionalinės rinkos priežiūros institucijos galėtų juos patikrinti.

9. Gamintojas užtikrina, kad būtų nustatytos procedūros, kurias taikant būtų išlaikoma serijinės gamybos būdu gaminamų produktų su skaitmeniniais elementais atitiktis. Gamintojas tinkamai atsižvelgia į produkto su skaitmeniniais elementais kūrimo ir gamybos procesų, taip pat projektavimo ir charakteristikų pakeitimus bei į 19 straipsnyje nurodytų darniųjų standartų, Europos kibernetinio saugumo sertifikavimo schemų arba bendrųjų specifikacijų, pagal kurias deklaruojama produkto su skaitmeniniais elementais atitiktis arba kurias taikant tikrinama jo atitiktis, pakeitimus.

10. Gamintojai užtikrina, kad prie produktų su skaitmeniniais elementais būtų pridėta II priede nurodyta informacija ir instrukcijos elektronine arba fizine forma. Tokia informacija ir instrukcijos pateikiamos tokia kalba, kurią naudotojai gali lengvai suprasti. Jos turi būti aiškios, suprantamos ir įskaitomos. Jos turi užtikrinti galimybę saugiai įrengti, eksploatuoti ir naudoti produktus su skaitmeniniais elementais.

11. Gamintojai ES atitikties deklaraciją pateikia kartu su produktu su skaitmeniniais elementais arba į II priedo nurodytas instrukcijas ir informaciją įtraukia interneto svetainės, kurioje galima rasti ES atitikties deklaraciją, adresą.

12. Pateikę produktą su skaitmeniniais elementais rinkai ir per numatomą produkto gyvavimo laikotarpį arba penkerius metus nuo produkto su skaitmeniniais elementais pateikimo rinkai, atsižvelgiant į tai, kuris laikotarpis trumpesnis, gamintojai, žinantys arba turintys pagrindo manyti, kad produktas su skaitmeniniais elementais arba gamintojo įdiegti procesai neatitinka I priede nustatytų esminių reikalavimų, nedelsdami imasi taisomųjų priemonių, būtinų to produkto su skaitmeniniais elementais arba gamintojo procesų atitikčiai užtikrinti, o prireikus tokį produktą atšaukia arba išima iš rinkos.

13. Gamintojai, gavę pagrįstą rinkos priežiūros institucijos prašymą, pateikia tai institucijai tokia kalba, kurią ji gali lengvai suprasti, visą informaciją ir dokumentus popierine arba elektronine forma, būtinus įrodyti produkto su skaitmeniniais elementais ir gamintojo įdiegtų procesų atitiktį I priede nustatytiems esminiams reikalavimams. Šios institucijos prašymu jie bendradarbiauja su ja dėl visų priemonių, kurių imamasi siekiant pašalinti jų rinkai pateikto produkto su skaitmeniniais elementais keliamą kibernetinio saugumo riziką.

14. Gamintojas, kuris nutraukia savo veiklą ir dėl to negali vykdyti šiame reglamente nustatytų pareigų, prieš veiklos nutraukimą apie šią padėtį informuoja atitinkamas rinkos priežiūros institucijas, taip pat visomis turimomis priemonėmis ir kiek įmanoma informuoja atitinkamų rinkai pateiktų produktų su skaitmeniniais elementais naudotojus.

15. Komisija gali įgyvendinamaisiais aktais nurodyti I priedo 2 skirsnio 1 punkte nurodyto programinės įrangos medžiagų žiniaraščio formatą ir elementus. Šie įgyvendinimo aktai priimami laikantis 51 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

11 straipsnis

Gamintojų pareiga pranešti

1. Gamintojas nedelsdamas (ir bet kuriuo atveju per 24 valandas nuo to momento, kai apie tai sužino) praneša ENISA apie bet kokį produkto su skaitmeniniais elementais aktyviai išnaudojamą pažeidžiamumą. Pranešime pateikiama išsami informacija apie tą pažeidžiamumą ir, jei taikytina, apie visas taisomąsias arba švelninimo priemones, kurių buvo imtasi. Gavusi pranešimą, ENISA nedelsdama, nebent tai būtų daroma dėl pagrįstų kibernetinio saugumo rizikos priežasčių, jį perduoda atitinkamų valstybių narių CSIRT, paskirtai siekiant suderintai atskleisti pažeidžiamumą pagal Direktyvos [Direktyva XXX/XXXX (TIS2)] [X] straipsnį, ir informuoja rinkos priežiūros instituciją apie praneštą pažeidžiamumą.

2. Gamintojas nedelsdamas ir bet kuriuo atveju per 24 valandas nuo to momento, kai apie tai sužino, praneša ENISA apie kiekvieną incidentą, turintį įtakos produkto su skaitmeniniais elementais saugumui. ENISA nedelsdama, nebent tai būtų daroma dėl pagrįstų kibernetinio saugumo rizikos priežasčių, jį perduoda atitinkamų valstybių narių bendram kontaktiniam punktui, paskirtam pagal Direktyvos [Direktyva XXX/XXXX (TIS2)] [X] straipsnį, ir informuoja rinkos priežiūros instituciją apie praneštus incidentus. Pranešime apie incidentą pateikiama informacija apie incidento sunkumą ir poveikį ir, kai taikytina, nurodoma, ar gamintojas įtaria, kad incidentas kilo dėl neteisėtų ar piktavališkų veiksmų arba mano, kad jis turi tarpvalstybinį poveikį.

3. ENISA pateikia Europos ryšių palaikymo dėl kibernetinių krizių organizaciniam tinklui (EU-CyCLONe), įsteigtam Direktyvos [Direktyva XXX/XXXX (TIS2)] [X] straipsniu, informaciją, apie kurią pranešta pagal 1 ir 2 dalis, jei tokia informacija yra aktuali koordinuotam didelio masto kibernetinio saugumo incidentų ir krizių valdymui operaciniu lygmeniu.

4. Sužinojęs apie incidentą, gamintojas nedelsdamas informuoja produkto su skaitmeniniais elementais naudotojus apie šį incidentą ir, jei reikia, apie taisomąsias priemones, kurių naudotojas gali imtis incidento poveikiui sumažinti.

5. Komisija gali įgyvendinimo aktais išsamiau nustatyti pagal 1 ir 2 dalis pateikiamų pranešimų informacijos rūšį, formatą ir procedūrą. Tie įgyvendinimo aktai priimami laikantis 51 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

6. Remdamasi pagal 1 ir 2 dalis gautais pranešimais ENISA kas dvejus metus parengia techninę ataskaitą apie kylančias kibernetinio saugumo rizikos tendencijas produktuose su skaitmeniniais elementais ir pateikia ją Direktyvos [Direktyva XXX/XXXX (TIS2)] [X] straipsnyje nurodytai bendradarbiavimo grupei. Pirmoji

tokia ataskaita pateikiama per 24 mėnesius nuo 1 ir 2 dalyse nustatytų pareigų taikymo pradžios.

7. Nustatę pažeidžiamumą komponente, įskaitant atvirojo kodo komponentą, integruotą į produktą su skaitmeniniais elementais, gamintojai praneša apie pažeidžiamumą šį komponentą prižiūrinčiam asmeniui ar subjektui.

12 straipsnis

Įgaliotieji atstovai

1. Gamintojas gali rašytiniu įgaliojimu paskirti įgaliotąjį atstovą.

2. Įgaliotojo atstovo įgaliojimas neapima 10 straipsnio 1–7 dalies pirmoje įtraukoje ir 9 dalyje nustatytų pareigų.

3. Įgaliotasis atstovas atlieka gamintojo suteiktame įgaliojime nustatytas užduotis. Įgaliojimu įgaliotajam atstovui leidžiama atlikti bent šiuos veiksmus:

   (a) saugoti 20 straipsnyje nurodytą ES atitikties deklaraciją ir 23 straipsnyje nurodytus techninius dokumentus dešimt metų po produkto su skaitmeniniais elementais pateikimo rinkai, kad rinkos priežiūros institucijos galėtų juos patikrinti;

   (b) jei rinkos priežiūros institucija pateikia pagrįstą prašymą, pateikti visą informaciją ir dokumentus, būtinus produkto su skaitmeniniais elementais atitikčiai reikalavimams įrodyti;

   (c) rinkos priežiūros institucijų prašymu bendradarbiauti su jomis dėl visų veiksmų, kurių imamasi siekiant pašalinti produkto su skaitmeniniais elementais, dėl kurio įgaliotajam atstovui suteikti įgaliojimai, keliamą riziką.

13 straipsnis

Importuotojų pareigos

1. Importuotojai rinkai pateikia tik tuos produktus su skaitmeniniais elementais, kurie atitinka I priedo 1 skirsnyje nustatytus esminius reikalavimus ir kai gamintojo įdiegti procesai atitinka I priedo 2 skirsnyje nustatytus esminius reikalavimus.

2. Prieš pateikdami rinkai produktą su skaitmeniniais elementais importuotojai užtikrina, kad:

   (a) gamintojas būtų atlikęs atitinkamas atitikties vertinimo procedūras, nurodytas 24 straipsnyje;

   (b) gamintojas būtų parengęs techninius dokumentus;

   (c) produktas su skaitmeniniais elementais būtų paženklintas 22 straipsnyje nurodytu CE ženklu ir prie jo būtų pridedama II priede nurodyta informacija ir naudojimo instrukcijos.

3. Jei importuotojas mano arba turi pagrindo manyti, kad produktas su skaitmeniniais elementais arba gamintojo įdiegti procesai neatitinka I priede nustatytų esminių reikalavimų, jis neteikia produkto rinkai, kol neužtikrinama to produkto arba gamintojo įdiegtų procesų atitiktis I priede nustatytiems esminiams reikalavimams. Be to, jei produktas su skaitmeniniais elementais kelia reikšmingą kibernetinio

saugumo riziką, importuotojas apie tai informuoja gamintoją ir rinkos priežiūros institucijas.

4. Ant produkto su skaitmeniniais elementais arba, jei to neįmanoma padaryti, ant pakuotės arba produkto su skaitmeniniais elementais lydimajame dokumente importuotojas nurodo savo pavadinimą, registruotą prekės pavadinimą arba registruotą prekės ženklą, pašto adresą ir elektroninio pašto adresą, kuriuo su jais galima susisiekti. Kontaktiniai duomenys pateikiami naudotojams bei rinkos priežiūros institucijoms lengvai suprantama kalba.

5. Importuotojai užtikrina, kad prie produkto su skaitmeniniais elementais būtų pridėtos II priede nurodytos instrukcijos ir informacija, pateikta galutiniams naudotojams lengvai suprantama kalba.

6. Jei importuotojai žino arba turi pagrindo manyti, kad produktas su skaitmeniniais elementais, kurį jie pateikė rinkai, arba jo gamintojo įdiegti procesai neatitinka I priede nustatytų esminių reikalavimų, jie nedelsdami imasi taisomųjų priemonių, būtinų to produkto su skaitmeniniais elementais arba jo gamintojo įdiegtų procesų atitikčiai I priede nustatytiems esminiams reikalavimams užtikrinti, o prireikus tokį produktą atšaukia arba pašalina iš rinkos.

   Nustatę produkto su skaitmeniniais elementais pažeidžiamumą, importuotojai apie šį pažeidžiamumą nedelsdami praneša gamintojui. Be to, jei produktas su skaitmeniniais elementais kelia reikšmingą kibernetinio saugumo riziką, importuotojai nedelsdami apie tai praneša valstybių narių, kuriose jie tiekė rinkai tokį produktą su skaitmeniniais elementais, rinkos priežiūros institucijoms, pateikdami išsamią informaciją, visų pirma apie neatitiktį ir apie visas taisomąsias priemones, kurių buvo imtasi.

7. Importuotojas dešimt metų po produkto su skaitmeniniais elementais pateikimo rinkai dienos saugo ES atitikties deklaracijos kopiją, kad rinkos priežiūros institucijos galėtų ją patikrinti, ir užtikrina, kad tų institucijų prašymu joms galėtų būti pateikti techniniai dokumentai.

8. Jei rinkos priežiūros institucija pateikia pagrįstą prašymą, importuotojai tai institucijai lengvai suprantama kalba popierine ar elektronine forma pateikia visą informaciją ir dokumentus, būtinus siekiant įrodyti, kad produktas su skaitmeniniais elementais atitinka I priedo 1 skirsnyje nustatytus esminius reikalavimus ir kad gamintojo įdiegti procesai atitinka I priedo 2 skirsnyje nustatytus esminius reikalavimus. Tos institucijos prašymu importuotojai bendradarbiauja su ja dėl visų priemonių, kurių imamasi siekiant pašalinti produkto su skaitmeniniais elementais, kurį jie pateikė rinkai, keliamą kibernetinio saugumo pavojų.

9. Kai produkto su skaitmeniniais elementais importuotojas sužino, kad to produkto gamintojas nutraukė savo veiklą ir dėl to negali vykdyti šiame reglamente nustatytų pareigų, importuotojas informuoja apie šią padėtį atitinkamas rinkos priežiūros institucijas ir visomis turimomis priemonėmis ir kiek įmanoma informuoja rinkai pateiktų produktų su skaitmeniniais elementais naudotojus.

14 straipsnis

Platintojų pareigos

1. Tiekdami rinkai produktą su skaitmeniniais elementais, platintojai pakankamai rūpestingai laikosi šio reglamento reikalavimų.

2. Prieš tiekdami produktą su skaitmeniniais elementais rinkai platintojai patikrina, ar:

(a) produktas su skaitmeniniais elementais paženklintas CE ženklu;

(b) gamintojas ir importuotojas įvykdė atitinkamai 10 straipsnio 10 ir 11 dalyse bei 13 straipsnio 4 dalyje nustatytas pareigas.

3. Jei platintojas mano arba turi pagrindo manyti, kad produktas su skaitmeniniais elementais arba gamintojo įdiegti procesai neatitinka I priede nustatytų esminių reikalavimų, platintojas netiekia produkto su skaitmeniniais elementais rinkai, kol nebus užtikrinta to produkto arba gamintojo įdiegtų procesų atitiktis. Be to, jei produktas su skaitmeniniais elementais kelia reikšmingą kibernetinio saugumo riziką, platintojas apie tai praneša gamintojui ir rinkos priežiūros institucijoms.

4. Jei platintojai žino arba turi pagrindo manyti, kad produktas su skaitmeniniais elementais, kurį jie tiekė rinkai, arba jo gamintojo įdiegti procesai neatitinka I priede nustatytų esminių reikalavimų, jie pasirūpina, kad būtų imtasi taisomųjų priemonių, būtinų to produkto su skaitmeniniais elementais arba jo gamintojo įdiegtų procesų atitikčiai užtikrinti, o prireikus tokį produktą atšaukia arba pašalina iš rinkos.

Nustatę produkto su skaitmeniniais elementais pažeidžiamumą, platintojai apie pažeidžiamumą nedelsdami praneša gamintojui. Be to, jei produktas su skaitmeniniais elementais kelia reikšmingą kibernetinio saugumo riziką, platintojai nedelsdami apie tai praneša valstybių narių, kuriose jie tiekė rinkai tokį produktą su skaitmeniniais elementais, rinkos priežiūros institucijoms, pateikdami išsamią informaciją, visų pirma apie neatitiktį ir apie visas taisomąsias priemones, kurių buvo imtasi.

5. Jei rinkos priežiūros institucija pateikia pagrįstą prašymą, platintojai tai institucijai lengvai suprantama kalba popierine ar elektronine forma pateikia visą informaciją ir dokumentus, būtinus siekiant įrodyti, kad produktas su skaitmeniniais elementais ir jo gamintojo įdiegti procesai atitinka I priede nustatytus esminius reikalavimus. Tos institucijos prašymu platintojai bendradarbiauja su ja dėl visų priemonių, kurių imamasi siekiant pašalinti produkto su skaitmeniniais elementais, kurį jie tiekė rinkai, keliamą kibernetinio saugumo pavojų.

6. Kai produkto su skaitmeniniais elementais platintojas sužino, kad to produkto gamintojas nutraukė savo veiklą ir dėl to negali vykdyti šiame reglamente nustatytų pareigų, jis informuoja apie šią padėtį atitinkamas rinkos priežiūros institucijas ir visomis turimomis priemonėmis ir kiek įmanoma informuoja rinkai pateiktų produktų su skaitmeniniais elementais naudotojus.

15 straipsnis

Atvejai, kuriais importuotojams ir platintojams taikomos gamintojų pareigos

Importuotojas arba platintojas pagal šį reglamentą laikomas gamintoju ir jam taikomos 10 straipsnyje ir 11 straipsnio 1, 2, 4 ir 7 dalyse nustatytos gamintojo pareigos, jei tas importuotojas ar platintojas pateikia rinkai produktą su skaitmeniniais elementais savo vardu arba naudodamas savo prekės ženklą, arba atlieka jau pateikto rinkai produkto su skaitmeniniais elementais esminį pakeitimą.

16 straipsnis

Kiti atvejai, kuriais taikomos gamintojų pareigos

Fizinis ar juridinis asmuo, išskyrus gamintoją, importuotoją ar platintoją, kuris atlieka esminį produkto su skaitmeniniais elementais pakeitimą, pagal šį reglamentą laikomas gamintoju.

Tam asmeniui taikomos 10 straipsnyje ir 11 straipsnio 1, 2, 4 ir 7 dalyse nustatytos gamintojo pareigos – jos taikomos tai produkto daliai, kuri yra paveikta esminio pakeitimo, arba visam produktui, jei esminis pakeitimas daro poveikį viso produkto su skaitmeniniais elementais kibernetiniam saugumui.

17 straipsnis

Ekonominės veiklos vykdytojų identifikavimas

1. Ekonominės veiklos vykdytojai, gavę rinkos priežiūros institucijos prašymą ir jei turi tokią informaciją, rinkos priežiūros institucijai pateikia šią informaciją:

   (a) kiekvieno ekonominės veiklos vykdytojo, kuris jiems tiekė produktą su skaitmeniniais elementais, pavadinimą ir adresą;

   (b) kiekvieno ekonominės veiklos vykdytojo, kuriam jie tiekė produktą su skaitmeniniais elementais, pavadinimą ir adresą.

2. Ekonominės veiklos vykdytojai pirmoje pastraipoje nurodytą informaciją turi gebėti pateikti dešimt metų po to, kai jiems buvo tiektas produktas su skaitmeniniais elementais, ir dešimt metų po to, kai jie tiekė produktą su skaitmeniniais elementais.

III SKYRIUS

PRODUKTO SU SKAITMENINIAIS ELEMENTAIS ATITIKTIS

18 straipsnis

Atitikties prielaida

1. Jei produktai su skaitmeniniais elementais ir gamintojo įdiegti procesai atitinka darniuosius standartus arba tam tikras jų dalis, kurių nuorodos buvo paskelbtos *Europos Sąjungos oficialiajame leidinyje*, daroma prielaida, kad jie atitinka I priede nustatytus esminius reikalavimus, kuriuos apima tie standartai ar jų dalys.

2. 19 straipsnyje nurodytas bendrąsias specifikacijas atitinkantys produktai su skaitmeniniais elementais ir gamintojo įdiegti procesai laikomi atitinkančiais I priede nustatytus esminius reikalavimus tiek, kiek tos bendrosios specifikacijos apima tuos reikalavimus.

3. Produktai su skaitmeniniais elementais ir gamintojo įdiegti procesai, dėl kurių yra parengtas ES atitikties pareiškimas arba sertifikatas pagal Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Reglamentą (ES) 2019/881 ir nurodytą 4 dalyje, laikomi atitinkančiais I priede nustatytus esminius reikalavimus tiek, kiek ES atitikties pareiškimas arba kibernetinio saugumo sertifikatas, arba jų dalys, apima tuos reikalavimus.

4. Komisija įgaliojama įgyvendinimo aktais nurodyti Europos kibernetinio saugumo sertifikavimo schemas, priimtas pagal Reglamentą (ES) 2019/881, kurios gali būti naudojamos siekiant įrodyti atitiktį esminiams reikalavimams ar jų dalims, kaip nurodyta I priede. Be to, jei taikytina, Komisija nurodo, ar pagal tokias schemas išduotas kibernetinio saugumo sertifikatas panaikina gamintojo pareigą atlikti atitikties atitinkamiems reikalavimams trečiosios šalies vertinimą, nurodytą 24

straipsnio 2 dalies a ir b punktuose ir 3 dalies a ir b punktuose. Tie įgyvendinimo aktai priimami laikantis 51 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

19 straipsnis

Bendrosios specifikacijos

Tais atvejais, kai 18 straipsnyje nurodytų darniųjų standartų nėra, arba kai Komisija mano, kad atitinkamų darniųjų standartų nepakanka šio reglamento reikalavimams įvykdyti ar Komisijos standartizacijos prašymui patenkinti, arba kai standartizacijos procedūra pernelyg vėluoja, arba kai Europos standartizacijos organizacijos nepriima Komisijos prašymo dėl darniųjų standartų, Komisija įgaliojama įgyvendinimo aktais priimti bendrąsias specifikacijas, susijusias su I priede nurodytais esminiais reikalavimais. Tie įgyvendinimo aktai priimami pagal 51 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.

20 straipsnis

ES atitikties deklaracija

1. ES atitikties deklaraciją gamintojai parengia pagal 10 straipsnio 7 dalį ir joje nurodo, kad įrodytas I priede nustatytų taikytinų esminių reikalavimų įvykdymas.
2. ES atitikties deklaracija parengiama pagal IV priede nustatytą modulinę struktūrą, joje pateikiami atitinkamose VI priede nustatytose atitikties vertinimo procedūrose nurodyti elementai. Tokia deklaracija nuolat atnaujinama. Ji pateikiama valstybės narės, kurios rinkai pateikiamas arba tiekiamas produktas su skaitmeniniais elementais, reikalaujama kalba ar kalbomis.
3. Jei produktui su skaitmeniniais elementais taikomas daugiau kaip vienas Sąjungos aktas, pagal kurį reikalaujama parengti ES atitikties deklaraciją, dėl visų tokių Sąjungos aktų parengiama viena ES atitikties deklaracija. Toje deklaracijoje nurodomi susiję Sąjungos aktai ir jų paskelbimo nuorodos.
4. Parengdamas ES atitikties deklaraciją gamintojas prisiima atsakomybę dėl produkto atitikties.
5. Komisija įgaliojama priimti deleguotuosius aktus pagal 50 straipsnį, kad papildytų šį reglamentą prie IV priede nustatyto minimalaus ES atitikties deklaracijos turinio pridėdama naujus elementus, atsižvelgiant į technologijų raidą.

21 straipsnis

Bendrieji ženklinimo CE ženklu principai

Ženklinimui CE ženklu, apibrėžtu 3 straipsnio 32 dalyje, taikomi bendrieji Reglamento (EB) Nr. 765/2008 30 straipsnyje nustatyti principai.

22 straipsnis

Ženklinimo CE ženklu taisyklės ir sąlygos

1. Produktas su skaitmeniniais elementais ženklinamas CE ženklu taip, kad šis ženklas būtų matomas, įskaitomas ir neištrinamas. Jei taip ženklinti neįmanoma arba negalima dėl produkto su skaitmeniniais elementais tipo, CE ženklas pateikiamas ant pakuotės ir 20 straipsnyje nurodytoje ES atitikties deklaracijoje, pateikiamoje kartu su produktu su skaitmeniniais elementais. Produktų su skaitmeniniais elementais,

kurie yra programinė įranga, atveju CE ženklas pateikiamas 20 straipsnyje nurodytoje ES atitikties deklaracijoje arba programinės įrangos produkto interneto svetainėje.

2. Atsižvelgiant į produkto su skaitmeniniais elementais pobūdį, CE ženklo, kuriuo ženklinamas produktas su skaitmeniniais elementais, aukštis gali būti mažesnis nei 5 mm su sąlyga, kad jis išliks matomas ir įskaitomas.

3. Produktas su skaitmeniniais elementais CE ženklu paženklinamas prieš jį pateikiant rinkai. Po ženklo gali būti pateikta piktograma arba bet koks kitas ženklas, nurodantis ypatingą riziką arba paskirtį, nustatytą 6 dalyje nurodytuose įgyvendinimo aktuose.

4. Po CE ženklo nurodomas notifikuotosios įstaigos identifikavimo numeris, jei ta įstaiga dalyvauja atitikties vertinimo procedūroje, pagrįstoje 24 straipsnyje nurodytu visišku kokybės užtikrinimu (remiantis H moduliu).

   Notifikuotosios įstaigos identifikavimo numerį pažymi pati notifikuotoji įstaiga arba pagal jos nurodymus tai padaro gamintojas arba gamintojo įgaliotasis atstovas.

5. Valstybės narės, naudodamosi esamais mechanizmais, užtikrina, kad būtų teisingai taikoma ženklinimą CE ženklu reglamentuojanti tvarka, o netinkamo to ženklinimo naudojimo atveju imamasi tinkamų veiksmų. Jei produktui su skaitmeniniais elementais taikomi kiti Sąjungos teisės aktai, kuriuose taip pat numatytas ženklinimas CE ženklu, CE ženklu turi būti nurodoma, kad produktas atitinka ir tų kitų teisės aktų reikalavimus.

6. Komisija gali įgyvendinimo aktais nustatyti piktogramų ar bet kokių kitų su produktų su skaitmeniniais elementais saugumu susijusių ženklų technines specifikacijas ir jų naudojimo skatinimo mechanizmus. Tie įgyvendinimo aktai priimami laikantis 51 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

23 straipsnis

Techniniai dokumentai

1. Techniniuose dokumentuose pateikiami visi aktualūs duomenys arba išsami informacija apie priemones, kurias gamintojas naudoja siekdamas užtikrinti, kad produktas su skaitmeniniais elementais ir gamintojo įdiegti procesai atitiktų I priede nustatytus esminius reikalavimus. Šiuose dokumentuose turi būti bent jau V priede nurodyti elementai.

2. Techniniai dokumentai parengiami prieš pateikiant produktą su skaitmeniniais elementais rinkai ir prireikus nuolat atnaujinami per numatomą produkto gyvavimo laikotarpį arba penkerius metus nuo produkto su skaitmeniniais elementais pateikimo rinkai, atsižvelgiant į tai, kuris laikotarpis trumpesnis.

3. 8 straipsnyje ir 24 straipsnio 4 dalyje nurodytų produktų su skaitmeniniais elementais, kuriems taip pat taikomi kiti Sąjungos aktai, atveju parengiamas vienas bendras techninis dokumentas, kuriame pateikiama šio reglamento V priede nurodyta informacija ir tuose atitinkamuose Sąjungos aktuose reikalaujama informacija.

4. Su bet kokiomis atitikties vertinimo procedūromis susiję techniniai dokumentai ir korespondencija rengiami oficialia tos valstybės narės, kurioje yra įsisteigusi notifikuotoji įstaiga, kalba arba kita tai įstaigai priimtina kalba.

5. Komisija įgaliojama priimti deleguotuosius aktus pagal 50 straipsnį, kad papildytų šį reglamentą elementais, kurie turi būti įtraukti į V priede nustatytus techninius dokumentus, atsižvelgdama į technologijų raidą ir pokyčius, su kuriais susiduriama įgyvendinant šį reglamentą.

24 straipsnis

Produktų su skaitmeniniais elementais atitikties vertinimo procedūros

1. Gamintojas atlieka produkto su skaitmeniniais elementais ir gamintojo įdiegtų procesų atitikties vertinimą, kad nustatytų, ar laikomasi I priede nurodytų esminių reikalavimų. Gamintojas arba įgaliotasis gamintojo atstovas turi įrodyti atitiktį esminiams reikalavimams taikydamas vieną iš šių procedūrų:

   (a) VI priede nustatytą vidaus kontrolės procedūrą (remiantis A moduliu); arba

   (b) VI priede nustatytą ES tipo tyrimo procedūrą (remiantis B moduliu) ir po to VI priede nustatytą ES tipo atitikties, pagrįstos vidine gamybos kontrole, procedūrą (remiantis C moduliu); arba

   (c) VI priede nustatytą visišku kokybės užtikrinimu pagrįstą atitikties vertinimo procedūrą (remiantis H moduliu).

2. Jei vertindamas I klasės ypatingos svarbos produkto su skaitmeniniais elementais atitiktį III priede nustatytiems esminiams reikalavimams ir jo gamintojo įdiegtų procesų atitiktį I priede nustatytiems esminiams reikalavimams gamintojas arba gamintojo įgaliotasis atstovas netaikė darniųjų standartų, bendrųjų specifikacijų ar Europos kibernetinio saugumo sertifikavimo schemų, nurodytų 18 straipsnyje, arba taikė juos tik iš dalies, arba jei tokių darniųjų standartų, bendrųjų specifikacijų ar Europos kibernetinio saugumo sertifikavimo schemų nėra, atitinkamas produktas su skaitmeniniais elementais ir gamintojo įdiegti procesai dėl tų esminių reikalavimų pateikiami pagal kurią nors iš šių procedūrų:

   (a) VI priede nustatytą ES tipo tyrimo procedūrą (remiantis B moduliu) ir po to VI priede nustatytą ES tipo atitikties, pagrįstos vidine gamybos kontrole, procedūrą (remiantis C moduliu); arba

   (b) VI priede nustatytą visišku kokybės užtikrinimu pagrįstą atitikties vertinimo procedūrą (remiantis H moduliu).

3. Jei produktas yra III priede nustatytas II klasės ypatingos svarbos produktas su skaitmeniniais elementais, gamintojas arba gamintojo įgaliotasis atstovas turi įrodyti atitiktį I priede nustatytiems esminiams reikalavimams taikydamas vieną iš šių procedūrų:

   (a) VI priede nustatytą ES tipo tyrimo procedūrą (remiantis B moduliu) ir po to VI priede nustatytą ES tipo atitikties, pagrįstos vidine gamybos kontrole, procedūrą (remiantis C moduliu); arba

   (b) VI priede nustatytą visišku kokybės užtikrinimu pagrįstą atitikties vertinimo procedūrą (remiantis H moduliu).

4. Produktų su skaitmeniniais elementais, kurie pagal Reglamento [Europos sveikatos duomenų erdvės reglamentas] taikymo sritį priskiriami prie ESĮ sistemų, gamintojai turi įrodyti atitiktį šio reglamento I priede nustatytiems esminiams reikalavimams taikydami atitinkamą atitikties vertinimo procedūrą, kaip reikalaujama Reglamente [Europos sveikatos duomenų erdvės reglamento III skyrius].

5. Nustatydamos mokesčius už atitikties vertinimo procedūras notifikuotosios įstaigos atsižvelgia į konkrečius mažų ir vidutinių įmonių (MVĮ) interesus bei poreikius ir sumažina tuos mokesčius proporcingai jų konkretiems interesams ir poreikiams.

IV SKYRIUS

ATITIKTIES VERTINIMO ĮSTAIGŲ NOTIFIKAVIMAS

25 straipsnis

Notifikavimas

Valstybės narės praneša Komisijai ir kitoms valstybėms narėms apie atitikties vertinimo įstaigas, įgaliotas atlikti atitikties vertinimą pagal šį reglamentą.

26 straipsnis

Notifikuojančiosios institucijos

1. Valstybės narės paskiria notifikuojančiąją instituciją, atsakingą už tai, kad būtų nustatytos ir taikomos reikiamos procedūros, pagal kurias įvertinamos atitikties vertinimo įstaigos, atliekama jų notifikavimo procedūra ir vykdoma notifikuotųjų įstaigų stebėsena, apimanti 31 straipsnio nuostatų laikymąsi.
2. Valstybės narės gali nuspręsti, kad 1 dalyje nurodytą vertinimą ir stebėseną turi vykdyti nacionalinė akreditacijos įstaiga, apibrėžta Reglamente (EB) Nr. 765/2008, pagal to reglamento nuostatas.

27 straipsnis

Notifikuojančiosioms institucijoms taikomi reikalavimai

1. Notifikuojančioji institucija turi būti įsteigta taip, kad nekiltų jos ir atitikties vertinimo įstaigų interesų konflikto.
2. Notifikuojančioji institucija organizuojama ir veikia taip, kad būtų užtikrintas jos veiklos objektyvumas ir nešališkumas.
3. Notifikuojančioji institucija organizuojama taip, kad kiekvieną sprendimą dėl atitikties vertinimo įstaigos notifikavimo priimtų kiti nei vertinimą atlikę kompetentingi asmenys.
4. Notifikuojančioji institucija nesiūlo ir nevykdo jokios veiklos, kurią vykdo atitikties vertinimo įstaigos, ir neteikia konsultavimo paslaugų komerciniu ar konkurenciniu pagrindu.
5. Notifikuojančioji institucija užtikrina informacijos, kurią gauna, konfidencialumą.
6. Notifikuojančiojoje institucijoje turi būti pakankamai kompetentingų darbuotojų, kad jos užduotys būtų atliekamos tinkamai.

28 straipsnis

Notifikuojančiųjų institucijų pareiga informuoti

1. Valstybės narės informuoja Komisiją apie savo procedūras, taikomas vertinant bei notifikuojant atitikties vertinimo įstaigas ir atliekant notifikuotųjų įstaigų stebėseną, taip pat apie visus jų pakeitimus.

2. Komisija tą informaciją skelbia viešai.

29 straipsnis

Notifikuotosioms įstaigoms taikomi reikalavimai

1. Atitikties vertinimo įstaiga notifikavimo procedūros tikslais turi atitikti 2–12 dalyse nustatytus reikalavimus.

2. Atitikties vertinimo įstaiga turi būti įsteigta pagal nacionalinę teisę ir turi turėti juridinio asmens statusą.

3. Atitikties vertinimo įstaiga yra trečiosios šalies įstaiga, nepriklausoma nuo organizacijos ar produkto, kurį ji vertina.

   Įstaiga, priklausanti verslo asociacijai arba profesinei federacijai, atstovaujančiai įmones, susijusias su jos vertinamų produktų su skaitmeniniais elementais projektavimu, kūrimu, gamyba, tiekimu, surinkimu, naudojimu ar priežiūra, gali būti laikoma tokia įstaiga, jeigu įrodoma, kad ji yra nešališka ir nėra jokio interesų konflikto.

4. Atitikties vertinimo įstaiga, jos aukščiausio lygio vadovai ir už atitikties vertinimo užduotis atsakingi darbuotojai negali būti vertinamų produktų su skaitmeniniais elementais projektuotojai, kūrėjai, gamintojai, tiekėjai, montuotojai, pirkėjai, savininkai, naudotojai ar prižiūrėtojai, arba tų šalių įgaliotieji atstovai. Tai netrukdo naudoti vertinamų produktų, kurie būtini atitikties vertinimo įstaigos veiklai, arba tokių produktų naudoti asmeniniais tikslais.

   Atitikties vertinimo įstaiga, jos aukščiausio lygio vadovai ir už atitikties vertinimo užduotis atsakingi darbuotojai tiesiogiai nedalyvauja projektuojant, kuriant, gaminant, parduodant, montuojant, naudojant šiuos produktus ar atliekant techninę jų priežiūrą, taip pat negali atstovauti tokia veikla užsiimančioms šalims. Jos nesiima jokios veiklos, kuri gali kliudyti joms nepriklausomai priimti sprendimus ar sąžiningai atlikti atitikties vertinimo užduotis, dėl kurių joms suteiktas notifikuotosios įstaigos statusas. Tai visų pirma taikoma konsultavimo paslaugoms.

   Atitikties vertinimo įstaigos užtikrina, kad jų pavaldžiųjų įstaigų ar subrangovų veikla nedarytų poveikio jų atitikties vertinimo veiklos konfidencialumui, objektyvumui ar nešališkumui.

5. Atitikties vertinimo įstaigos ir jų darbuotojai atitikties vertinimo veiklą turi vykdyti laikydamiesi griežčiausių profesinio sąžiningumo reikalavimų, turi turėti reikiamą konkrečios srities techninę kompetenciją ir nepasiduoti jokiam spaudimui ir paskatoms, visų pirma finansiniams, kurie galėtų paveikti jų sprendimų priėmimą ar jų vykdomos atitikties vertinimo veiklos rezultatus, ypač jei spaudimą daro ir paskatas siūlo tos veiklos rezultatais suinteresuoti asmenys ar asmenų grupės.

6. Atitikties vertinimo įstaiga turi būti pajėgi atlikti visas atitikties vertinimo užduotis, kurios yra nurodytos VI priede ir kurioms atlikti ji buvo notifikuota, neatsižvelgiant į tai, ar tas užduotis atlieka pati atitikties vertinimo įstaiga, ar jos yra atliekamos tos įstaigos vardu ir atsakomybe.

Visais atvejais kiekvienai atitikties vertinimo procedūrai ir kiekvienai produktų su skaitmeniniais elementais rūšiai ar kategorijai, kuriai atitikties vertinimo įstaiga yra notifikuota, atitikties vertinimo įstaiga turi turėti reikiamus:

(a) darbuotojus, turinčius techninių žinių ir pakankamą bei tinkamą patirtį atitikties vertinimo užduotims atlikti;

(b) procedūrų, pagal kurias atliekamas atitikties vertinimas, aprašymus, taip užtikrinant skaidrumą ir galimybę tas procedūras pakartoti. Ji turi taikyti tinkamą politiką ir procedūras, kuriomis būtų užtikrinamas užduočių, kurias ji atlieka kaip notifikuotoji įstaiga, ir kitos veiklos atskyrimas;

(c) procedūras, pagal kurias ji galėtų vykdyti savo veiklą tinkamai atsižvelgdama į įmonės dydį, jos veiklos sektorių, jos struktūrą, atitinkamos produktų technologijos sudėtingumo laipsnį ir į tai, ar gamybos procesas yra masinis, ar serijinis.

Ji turi turėti priemones, būtinas su atitikties vertinimu susijusioms techninėms ir administracinėms užduotims tinkamai atlikti, ir galėti naudotis visa reikiama įranga ar įrenginiais.

7. Už atitikties vertinimo veiklą atsakingi darbuotojai privalo:

(a) turėti tinkamą techninį ir profesinį parengimą, apimantį visą atitikties vertinimo veiklą, kuriai atitikties vertinimo įstaiga įgijo notifikuotosios įstaigos statusą;

(b) pakankamai gerai išmanyti jų atliekamų vertinimų reikalavimus ir turėti tinkamus įgaliojimus tiems vertinimams atlikti;

(c) turėti reikiamų žinių ir išmanyti pagrindinius reikalavimus, taikomus darniuosius standartus, atitinkamas derinamųjų Sąjungos teisės aktų nuostatas ir jų įgyvendinimo aktus;

(d) turėti gebėjimų rengti sertifikatus, daryti įrašus ir rašyti ataskaitas, kuriais patvirtinamas vertinimo atlikimo faktas.

8. Turi būti užtikrintas atitikties vertinimo įstaigų, jų aukščiausio lygio vadovų ir vertinimą atliekančių darbuotojų nešališkumas.

Atitikties vertinimo įstaigos aukščiausio lygio vadovų ir vertinimo darbuotojų atlyginimas neturi priklausyti nuo atliktų įvertinimų skaičiaus ar tų vertinimų rezultatų.

9. Atitikties vertinimo įstaigos turi apsidrausti civilinės atsakomybės draudimu, išskyrus atvejus, kai atsakomybę pagal nacionalinę teisę prisiima valstybė arba kai už atitikties vertinimą tiesiogiai atsako pati valstybė narė.

10. Atitikties vertinimo įstaigos darbuotojai laikosi profesinio slaptumo reikalavimo, taikomo visai informacijai, kurią jie gauna atlikdami užduotis pagal VI priedą arba bet kurią nacionalinės teisės nuostatą, kuria jis įgyvendinamas, išskyrus atvejus, susijusius su valstybės narės, kurioje vykdoma veikla, rinkos priežiūros institucijomis. Nuosavybės teisės turi būti saugomos. Atitikties vertinimo įstaiga turi turėti dokumentais patvirtintas procedūras, užtikrinančias šios dalies reikalavimų laikymąsi.

11. Atitikties vertinimo įstaigos dalyvauja atitinkamoje standartizacijos veikloje ir notifikuotosios įstaigos koordinavimo grupės, sudarytos pagal 40 straipsnį, veikloje arba užtikrina, kad vertinimą atliekantys jų darbuotojai būtų apie šią veiklą

informuoti, ir šios grupės priimtus administracinius sprendimus ir parengtus dokumentus taiko kaip bendrąsias gaires.

12. Atitikties vertinimo įstaigos veikia vadovaudamosi nuosekliomis, sąžiningomis ir pagrįstomis nuostatomis, ypač atsižvelgdamos į MVĮ interesus dėl mokesčių.

30 straipsnis

Notifikuotųjų įstaigų atitikties prielaida

Jei atitikties vertinimo įstaiga įrodo, kad atitinka kriterijus, nustatytus atitinkamuose darniuosiuose standartuose arba jų dalyse, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*, daroma prielaida, kad ji atitinka 29 straipsnyje nustatytus reikalavimus tiek, kiek juos apima taikomi darnieji standartai.

31 straipsnis

Notifikuotųjų įstaigų pavaldžiosios įstaigos ir subrangovai

1. Jei notifikuotoji įstaiga konkrečias su atitikties vertinimu susijusias užduotis paveda atlikti subrangovui ar pavaldžiajai įstaigai, ji užtikrina, kad tas subrangovas arba pavaldžioji įstaiga atitiktų 29 straipsnyje nustatytus reikalavimus, ir apie tai informuoja notifikuojančiąją instituciją.

2. Notifikuotosios įstaigos prisiima visą atsakomybę už subrangovų ar pavaldžiųjų įstaigų atliekamas užduotis, neatsižvelgiant į tai, kur jie yra įsteigti.

3. Pavesti darbą subrangovui arba pavaldžiajai įstaigai galima tik gavus gamintojo sutikimą.

4. Notifikuotosios įstaigos saugo aktualius dokumentus, susijusius su subrangovo ar pavaldžiosios įstaigos kvalifikacijos įvertinimu ir jų pagal šį reglamentą atliktu darbu, kad notifikuojančioji institucija galėtų juos patikrinti.

32 straipsnis

Notifikavimo paraiška

1. Atitikties vertinimo įstaiga notifikavimo paraišką pateikia valstybės narės, kurioje yra įsisteigusi, notifikuojančiajai institucijai.

2. Prie tos paraiškos pridedamas atitikties vertinimo veiklos, atitikties vertinimo procedūros arba procedūrų ir produkto arba produktų, kuriuos vertinti ta įstaiga teigia turinti kompetencijos, aprašas, taip pat nacionalinės akreditacijos įstaigos išduotas akreditacijos pažymėjimas, jeigu jis yra, kuriuo patvirtinama, kad atitikties vertinimo įstaiga atitinka 29 straipsnyje nustatytus reikalavimus.

3. Jeigu tam tikra atitikties vertinimo įstaiga negali pateikti akreditacijos pažymėjimo, ji pateikia notifikuojančiajai institucijai visus patvirtinamuosius dokumentus, būtinus jos atitikčiai 29 straipsnyje nustatytiems reikalavimams patikrinti, patvirtinti ir reguliariai stebėti.

33 straipsnis

Notifikavimo procedūra

1. Notifikuojančiosios institucijos gali pranešti tik apie tas atitikties vertinimo įstaigas, kurios atitinka 29 straipsnyje nustatytus reikalavimus.

2. Notifikuojančioji institucija teikia pranešimus Komisijai ir kitoms valstybėms narėms naudodama Komisijos sukurtą ir valdomą informacinę sistemą „Naujojo požiūrio paskelbtos ir paskirtos organizacijos“ (NANDO).

3. Notifikavimo pranešime pateikiama išsami informacija apie atitikties vertinimo veiklą, atitikties vertinimo modulį ar modulius, atitinkamą produktą ar produktus ir atitinkamą kompetencijos patvirtinimą.

4. Kai notifikavimas nėra grindžiamas akreditacijos pažymėjimu, nurodytu 32 straipsnio 2 dalyje, notifikuojančioji institucija Komisijai ir kitoms valstybėms narėms pateikia patvirtinamuosius dokumentus, kuriais patvirtinama atitikties vertinimo įstaigos kompetencija ir tai, kad yra nustatyta reguliarų tos įstaigos stebėjimą ir jos tolesnę atitiktį 29 straipsnyje nustatytiems reikalavimams užtikrinsianti tvarka.

5. Atitinkama įstaiga notifikuotosios įstaigos veiklą gali vykdyti tik tuo atveju, jei Komisija arba kitos valstybės narės per dvi savaites po notifikavimo, jeigu naudojamasi akreditacijos pažymėjimu, ar per du mėnesius po notifikavimo, jeigu nesinaudojama akreditacijos pažymėjimu, nepateikia prieštaravimų.

   Tik tokia įstaiga laikoma notifikuotąja įstaiga pagal šį reglamentą.

6. Komisijai ir kitoms valstybėms narėms pranešama apie visus susijusius vėlesnius notifikuotųjų įstaigų įgaliojimų pakeitimus.

34 straipsnis

Notifikuotųjų įstaigų identifikavimo numeriai ir sąrašai

1. Komisija suteikia notifikuotajai įstaigai identifikavimo numerį.

   Komisija suteikia tik vieną identifikavimo numerį net ir tuo atveju, kai apie įstaigą yra pranešta pagal kelis Sąjungos aktus.

2. Komisija viešai paskelbia įstaigų, notifikuotų pagal šį reglamentą, sąrašą, taip pat nurodo joms suteiktus identifikavimo numerius ir veiklą, kuriai atlikti jos yra notifikuotos.

   Komisija užtikrina, kad tas sąrašas būtų nuolat atnaujinamas.

35 straipsnis

Notifikavimų pakeitimai

1. Kai notifikuojančioji institucija išsiaiškina arba jai pranešama, kad notifikuotoji įstaiga nebeatitinka 29 straipsnyje nustatytų reikalavimų arba kad ji nevykdo savo pareigų, notifikuojančioji institucija atitinkamai apriboja, sustabdo arba panaikina pranešimo galiojimą, atsižvelgdama į tų reikalavimų nesilaikymo arba pareigų nevykdymo rimtumą. Apie tai ji atitinkamai nedelsdama informuoja Komisiją ir kitas valstybes nares.

2. Jeigu notifikavimo galiojimas apribojamas, laikinai sustabdomas arba panaikinamas, arba kai notifikuotoji įstaiga nutraukia veiklą, notifikuojančioji valstybė narė imasi tinkamų priemonių siekdama užtikrinti, kad tos įstaigos bylos būtų perduotos tvarkyti kitai notifikuotajai įstaigai arba saugomos, kad su jomis galėtų susipažinti prašymą

pateikusios atsakingos notifikuojančiosios institucijos ir rinkos priežiūros institucijos.

36 straipsnis

Notifikuotųjų įstaigų kompetencijos užginčijimas

1. Komisija tiria visus atvejus, kai jai kyla abejonių arba kai jai pranešama apie abejones dėl notifikuotosios įstaigos kompetencijos arba dėl to, ar notifikuotoji įstaiga vis dar atitinka jai taikomus reikalavimus ir vykdo jai pavestas pareigas.
2. Komisijos prašymu notifikuojančioji valstybė narė pateikia jai visą informaciją, susijusią su atitinkamos įstaigos paskyrimo notifikuotąja įstaiga pagrindu arba atitinkamos įstaigos kompetencijos užtikrinimu.
3. Komisija užtikrina, kad visa neskelbtina informacija, gauta jai atliekant tyrimą, būtų nagrinėjama konfidencialiai.
4. Jeigu Komisija sužino, kad notifikuotoji įstaiga neatitinka arba nebeatitinka jos notifikavimo reikalavimų, Komisija atitinkamai praneša apie tai notifikuojančiajai valstybei narei ir paprašo imtis būtinų korekcinių priemonių, įskaitant notifikavimo panaikinimą, jei būtina.

37 straipsnis

Notifikuotųjų įstaigų su veikla susijusios pareigos

1. Notifikuotosios įstaigos atlieka atitikties vertinimus pagal VI priedo 24 straipsnyje numatytas atitikties vertinimo procedūras.
2. Atitikties vertinimai atliekami proporcingai, siekiant išvengti nereikalingos naštos ekonominės veiklos vykdytojams. Atitikties vertinimo įstaiga atlieka savo veiklą tinkamai atsižvelgdama į įmonės dydį, jos veiklos sektorių, jos struktūrą, atitinkamos produktų technologijos sudėtingumo laipsnį ir į tai, ar gamybos procesas yra masinis, ar serijinis.
3. Tačiau notifikuotosios įstaigos laikosi tokio griežtumo ir apsaugos lygio, kokio reikia, kad būtų užtikrinta produkto atitiktis reglamento nuostatoms.
4. Kai notifikuotoji įstaiga nustato, kad gamintojas neįvykdė I priede, atitinkamuose darniuosiuose standartuose arba bendrosiose specifikacijose nustatytų reikalavimų, kaip nurodyta 19 straipsnyje, ji reikalauja, kad tas gamintojas imtųsi reikiamų taisomųjų priemonių, ir neišduoda atitikties sertifikato.
5. Jeigu išdavusi sertifikatą notifikuotoji įstaiga, vykdydama atitikties stebėseną, nustato, kad produktas nebeatitinka šiame reglamente nustatytų reikalavimų, ji reikalauja, kad gamintojas imtųsi tinkamų taisomųjų priemonių, ir, jei būtina, laikinai sustabdo arba panaikina sertifikato galiojimą.
6. Jeigu taisomųjų veiksmų nesiimama arba jie neturi reikiamo poveikio, notifikuotoji įstaiga prireikus apriboja, sustabdo arba panaikina sertifikatų galiojimą.

38 straipsnis

Notifikuotųjų įstaigų pareiga informuoti

1. Notifikuotosios įstaigos informuoja notifikuojančiąją instituciją apie:

(a) kiekvieną atsisakymą išduoti sertifikatą, sertifikato galiojimo apribojimą, sustabdymą ar panaikinimą;

(b) bet kokias aplinkybes, turinčias įtakos notifikavimo apimčiai ir sąlygoms;

(c) kiekvieną prašymą suteikti informaciją, kurį jos gavo iš rinkos priežiūros institucijų dėl atitikties vertinimo veiklos;

(d) jei prašoma, atitikties vertinimo veiklą, vykdomą pagal jai, kaip notifikuotajai įstaigai, suteiktus įgaliojimus, ir bet kokią kitą vykdomą veiklą, įskaitant tarpvalstybinę veiklą ir subrangą.

2. Notifikuotosios įstaigos kitoms pagal šį reglamentą notifikuotoms įstaigoms, vykdančioms panašią tokių pačių produktų atitikties vertinimo veiklą, teikia atitinkamą informaciją apie klausimus, susijusius su neigiamais ir, jei prašoma, teigiamais atitikties vertinimo rezultatais.

39 straipsnis

Keitimasis patirtimi

Komisija pasirūpina, kad būtų organizuojamas už notifikavimo politiką atsakingų valstybių narių nacionalinių institucijų keitimasis patirtimi.

40 straipsnis

Notifikuotųjų įstaigų veiklos koordinavimas

1. Komisija užtikrina, kad notifikuotųjų įstaigų veikla būtų tinkamai koordinuojama ir kad tos įstaigos tinkamai bendradarbiautų įvairių sektorių notifikuotųjų įstaigų grupėje.

2. Valstybės narės užtikrina, kad jų notifikuotos įstaigos tiesiogiai arba per paskirtus atstovus dalyvautų tos grupės veikloje.

V SKYRIUS

RINKOS PRIEŽIŪRA IR VYKDYMO UŽTIKRINIMAS

41 straipsnis

Produktų su skaitmeniniais elementais priežiūra ir kontrolė Sąjungos rinkoje

1. Į šio reglamento taikymo sritį patenkantiems produktams su skaitmeniniais elementais taikomas Reglamentas (ES) 2019/1020.

2. Kiekviena valstybė narė paskiria vieną ar daugiau rinkos priežiūros institucijų, kad užtikrintų veiksmingą šio reglamento įgyvendinimą. Valstybės narės gali paskirti esamą arba naują instituciją, kuri pagal šį reglamentą veiktų kaip rinkos priežiūros institucija.

3. Prireikus rinkos priežiūros institucijos bendradarbiauja su nacionalinėmis kibernetinio saugumo sertifikavimo institucijomis, paskirtomis pagal Reglamento (ES) 2019/881 58 straipsnį, ir reguliariai keičiasi informacija. Prižiūrėdamos, kaip vykdoma pareiga pranešti pagal šio reglamento 11 straipsnį, paskirtosios rinkos priežiūros institucijos bendradarbiauja su ENISA.

4. Prireikus rinkos priežiūros institucijos bendradarbiauja su kitomis rinkos priežiūros institucijomis, paskirtomis pagal kitiems produktams skirtus Sąjungos derinamuosius teisės aktus, ir reguliariai keičiasi informacija.

5. Rinkos priežiūros institucijos prireikus bendradarbiauja su institucijomis, prižiūrinčiomis Sąjungos duomenų apsaugos teisę. Toks bendradarbiavimas apima šių institucijų informavimą apie bet kokius nustatytus faktus, susijusius su jų pareigų pagal jų kompetenciją vykdymu, taip pat teikiant rekomendacijas ir patarimus pagal šio straipsnio 8 dalį, jei tokios rekomendacijos ir patarimai susiję su asmens duomenų tvarkymu.

   Institucijos, prižiūrinčios Sąjungos duomenų apsaugos teisę, įgaliotos prašyti pateikti bet kuriuos dokumentus, sukurtus ar tvarkomus pagal šį reglamentą, ir gauti prieigą prie jų, kai prieiga prie tų dokumentų yra būtina jų užduotims atlikti. Apie tokį prašymą jos praneša atitinkamos valstybės narės paskirtosioms rinkos priežiūros institucijoms.

6. Valstybės narės užtikrina, kad paskirtosioms rinkos priežiūros institucijoms būtų suteikta pakankamai finansinių ir žmogiškųjų išteklių jų užduotims pagal šį reglamentą vykdyti.

7. Komisija padeda paskirtosioms rinkos priežiūros institucijoms keistis patirtimi.

8. Rinkos priežiūros institucijos, padedamos Komisijos, gali teikti rekomendacijas ir patarimus ekonominės veiklos vykdytojams dėl šio reglamento įgyvendinimo.

9. Rinkos priežiūros institucijos kartą per metus praneša Komisijai atitinkamos rinkos priežiūros veiklos rezultatus. Paskirtosios rinkos priežiūros institucijos nedelsdamos praneša Komisijai ir atitinkamoms nacionalinėms konkurencijos institucijoms visą vykdant rinkos priežiūros veiklą nustatytą informaciją, kuri gali būti svarbi taikant Sąjungos konkurencijos teisę.

10. Produktų su skaitmeniniais elementais, kurie yra įtraukti į šio reglamento taikymo sritį ir pagal Reglamento [DI reglamentas] [6] straipsnį priskiriami prie didelės rizikos DI sistemų, atveju Reglamento [DI reglamentas] tikslais paskirtos rinkos priežiūros institucijos yra institucijos, atsakingos už rinkos priežiūros veiklą, kurią reikalaujama vykdyti pagal šį reglamentą. Pagal Reglamentą [DI reglamentas] paskirtos rinkos priežiūros institucijos prireikus bendradarbiauja su pagal šį reglamentą paskirtomis rinkos priežiūros institucijomis, o dėl pareigos pranešti vykdymo pagal 11 straipsnį priežiūros – su ENISA. Pagal Reglamentą [DI reglamentas] paskirtos rinkos priežiūros institucijos pagal šį reglamentą paskirtas rinkos priežiūros institucijas visų pirma informuoja apie visus nustatytus faktus, kurie yra aktualūs jų užduočių, susijusių su šio reglamento įgyvendinimu, vykdymui.

11. Siekiant vienodai taikyti šį reglamentą, sudaroma speciali administracinio bendradarbiavimo grupė pagal Reglamento (ES) 2019/1020 30 straipsnio 2 dalį. Administracinio bendradarbiavimo grupę sudaro paskirtos rinkos priežiūros institucijos ir, jei taikytina, bendrų ryšių palaikymo tarnybų atstovai.

42 straipsnis

Prieiga prie duomenų ir dokumentų

Kai reikia įvertinti produktų su skaitmeniniais elementais ir jų gamintojų įdiegtų procesų atitiktį I priede nustatytiems esminiams reikalavimams ir gavus pagrįstą prašymą, rinkos priežiūros institucijoms suteikiama prieiga prie duomenų, kurių reikia tokių produktų

projektavimui, kūrimui, gamybai ir pažeidžiamumų valdymui įvertinti, įskaitant susijusius atitinkamo ekonominės veiklos vykdytojo vidaus dokumentus.

43 straipsnis

Nacionalinio lygmens procedūra dėl produktų su skaitmeniniais elementais, keliančių reikšmingą kibernetinio saugumo riziką

1. Jeigu valstybės narės rinkos priežiūros institucija turi pakankamų priežasčių manyti, kad produktas su skaitmeniniais elementais, įskaitant jo pažeidžiamumų valdymą, kelia reikšmingą kibernetinio saugumo riziką, ji atlieka atitinkamo produkto su skaitmeniniais elementais atitikties visiems šiame reglamente nustatytiems reikalavimams vertinimą. Atitinkami ekonominės veiklos vykdytojai prireikus bendradarbiauja su rinkos priežiūros institucija.

   Jeigu atliekant šį vertinimą rinkos priežiūros institucija nustato, kad produktas su skaitmeniniais elementais neatitinka šiame reglamente nustatytų reikalavimų, ji nedelsdama pareikalauja, kad atitinkamas veiklos vykdytojas imtųsi visų reikiamų taisomųjų veiksmų, kad produktas atitiktų tuos reikalavimus, pašalintų produktą iš rinkos ar per pagrįstą laikotarpį, kurį ji nustato atsižvelgdama į rizikos pobūdį, jį atšauktų.

   Rinkos priežiūros institucija apie tai informuoja atitinkamą notifikuotąją įstaigą. Atitinkamiems taisomiesiems veiksmams taikomas Reglamento (ES) 2019/1020 18 straipsnis.

2. Jei rinkos priežiūros institucija mano, kad neatitikties esama ne tik jos nacionalinėje teritorijoje, ji informuoja Komisiją ir kitas valstybes nares apie vertinimo rezultatus ir veiksmus, kurių jos nurodymu turi imtis veiklos vykdytojas.

3. Gamintojas užtikrina, kad visų tinkamų taisomųjų veiksmų būtų imtasi dėl visų susijusių produktų su skaitmeniniais elementais, kuriuos jis tiekė rinkai visoje Sąjungoje.

4. Jei per 1 dalies antroje pastraipoje nurodytą laikotarpį produkto su skaitmeniniais elementais gamintojas nesiima reikiamų taisomųjų veiksmų, rinkos priežiūros institucija imasi visų tinkamų laikinųjų priemonių, kad būtų uždraustas arba apribotas to produkto tiekimas jo nacionalinei rinkai, kad gaminys būtų pašalintas iš tos rinkos arba atšauktas.

   Apie tokias priemones ta institucija nedelsdama informuoja Komisiją ir kitas valstybes nares.

5. 4 dalyje nurodyta informacija apima visus duomenis, visų pirma duomenis, reikalingus reikalavimų neatitinkančiam produktui su skaitmeniniais elementais, produkto su skaitmeniniais elementais kilmei, pareikšto neatitikimo ir keliamos rizikos pobūdžiui, nacionaliniu lygmeniu taikomų priemonių pobūdžiui ir trukmei bei atitinkamo veiklos vykdytojo pateiktiems argumentams nustatyti. Visų pirma rinkos priežiūros institucija nurodo, ar neatitiktis sietina su viena ar daugiau iš šių priežasčių:

   (a) produkto arba gamintojo įdiegtų procesų neatitiktimi I priede nustatytiems esminiams reikalavimams;

   (b) 18 straipsnyje nurodytų darniųjų standartų, kibernetinio saugumo sertifikavimo schemų ar bendrųjų specifikacijų trūkumais.

6. Valstybių narių, išskyrus procedūrą inicijavusią valstybę narę, rinkos priežiūros institucijos nedelsdamos praneša Komisijai ir kitoms valstybėms narėms apie visas priemones, kurių ėmėsi, ir pateikia visą turimą papildomą informaciją, susijusią su atitinkamo produkto neatitiktimi, ir, jei nesutinka su nacionaline priemone, apie kurią pranešta, savo prieštaravimus.

7. Jeigu per tris mėnesius nuo 4 dalyje nurodytos informacijos gavimo nei kuri nors valstybė narė, nei Komisija nepareiškia prieštaravimo dėl laikinosios priemonės, kurios ėmėsi valstybė narė, ta priemonė laikoma pagrįsta. Tai nedaro poveikio atitinkamo veiklos vykdytojo procesinėms teisėms pagal Reglamento (ES) 2019/1020 18 straipsnį.

8. Visų valstybių narių rinkos priežiūros institucijos užtikrina, kad atitinkamam produktui nedelsiant būtų taikomos tinkamos ribojamosios priemonės, pvz., produktas būtų pašalintas iš rinkos.

44 straipsnis

Sąjungos apsaugos procedūra

1. Jeigu per tris mėnesius nuo 43 straipsnio 4 dalyje nurodyto pranešimo gavimo kuri nors valstybė narė pareiškia prieštaravimų dėl priemonės, kurios ėmėsi kita valstybė narė, arba jeigu Komisija mano, kad priemonė prieštarauja Sąjungos teisės aktams, Komisija nedelsdama pradeda konsultacijas su atitinkama valstybe nare ir ekonominės veiklos vykdytoju ar vykdytojais ir tą nacionalinę priemonę įvertina. Remdamasi to vertinimo rezultatais, Komisija per devynis mėnesius nuo 43 straipsnio 4 dalyje nurodyto pranešimo dienos nusprendžia, ar nacionalinė priemonė yra pagrįsta, ir apie tokį sprendimą praneša atitinkamai valstybei narei.

2. Jeigu nacionalinė priemonė laikoma pagrįsta, visos valstybės narės imasi priemonių, būtinų užtikrinti, kad reikalavimų neatitinkantis produktas su skaitmeniniais elementais būtų pašalintas iš jų rinkos, ir atitinkamai informuoja Komisiją. Jeigu nacionalinė priemonė laikoma nepagrįsta, atitinkama valstybė narė tą priemonę pašalina.

3. Jei nacionalinė priemonė laikoma pagrįsta, o produkto su skaitmeniniais elementais neatitiktis siejama su darniųjų standartų trūkumais, Komisija taiko Reglamento (ES) Nr. 1025/2012 10 straipsnyje numatytą procedūrą.

4. Jei nacionalinė priemonė laikoma pagrįsta, o produkto su skaitmeniniais elementais neatitiktis siejama su 18 straipsnyje nurodytos Europos kibernetinio saugumo sertifikavimo sistemos trūkumais, Komisija svarsto, ar iš dalies pakeisti arba panaikinti 18 straipsnio 4 dalyje nurodytą įgyvendinimo aktą, kuriame nurodoma tos sertifikavimo sistemos atitikties prielaida.

5. Jei nacionalinė priemonė laikoma pagrįsta, o produkto su skaitmeniniais elementais neatitiktis siejama su 19 straipsnyje nurodytų bendrųjų specifikacijų trūkumais, Komisija svarsto, ar iš dalies pakeisti arba panaikinti įgyvendinimo aktą, nurodytą 19 straipsnyje, kuriame nustatomos tos bendrosios specifikacijos.

45 straipsnis

ES lygmens procedūra dėl produktų su skaitmeniniais elementais, keliančiais reikšmingą kibernetinio saugumo riziką

1. Jei Komisija turi pakankamai priežasčių manyti, taip pat remdamasi ENISA pateikta informacija, kad produktas su skaitmeniniais elementais, kuris kelia reikšmingą kibernetinio saugumo riziką, neatitinka šiame reglamente nustatytų reikalavimų, ji gali prašyti atitinkamų rinkos priežiūros institucijų atlikti atitikties vertinimą ir laikytis 43 straipsnyje nurodytų procedūrų.

2. Išskirtinėmis aplinkybėmis, kurios pateisina neatidėliotiną intervenciją siekiant išsaugoti gerą vidaus rinkos veikimą, ir kai Komisija turi pakankamai priežasčių manyti, kad 1 dalyje nurodytas produktas vis dar neatitinka šiame reglamente nustatytų reikalavimų ir atitinkamos rinkos priežiūros institucijos nesiėmė jokių veiksmingų priemonių, Komisija gali prašyti ENISA atlikti atitikties vertinimą. Komisija apie tai informuoja atitinkamas rinkos priežiūros institucijas. Atitinkami ekonominės veiklos vykdytojai prireikus bendradarbiauja su ENISA.

3. Remdamasi ENISA vertinimu Komisija gali nuspręsti, kad būtina taikyti taisomąją arba ribojamąją priemonę Sąjungos lygmeniu. Šiuo tikslu ji nedelsdama konsultuojasi su atitinkamomis valstybėmis narėmis ir atitinkamu ekonominės veiklos vykdytoju ar vykdytojais.

4. Remdamasi 3 dalyje nurodytomis konsultacijomis Komisija gali priimti įgyvendinimo aktus, kad priimtų sprendimą dėl taisomųjų arba ribojamųjų priemonių Sąjungos lygmeniu, įskaitant nurodymą pašalinti iš rinkos arba atšaukti per pagrįstą laikotarpį, nustatytą atsižvelgiant į rizikos pobūdį. Tie įgyvendinimo aktai priimami laikantis 51 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

5. Komisija apie 4 dalyje nurodytą sprendimą nedelsdama praneša atitinkamam ekonominės veiklos vykdytojui (-ams). Valstybės narės nedelsdamos įgyvendina 4 dalyje nurodytus aktus ir apie tai atitinkamai informuoja Komisiją.

6. 2–5 dalys taikomos tiek laiko, kiek trunka išskirtinė situacija, pateisinanti Komisijos įsikišimą, ir kol neužtikrinama atitinkamo produkto atitiktis šio reglamento reikalavimams.

46 straipsnis

Reikalavimus atitinkantys produktai su skaitmeniniais elementais, keliantys reikšmingą kibernetinio saugumo riziką

1. Jei valstybės narės rinkos priežiūros institucija, atlikusi vertinimą pagal 43 straipsnį, nustato, kad produktas su skaitmeniniais elementais ir gamintojo įdiegti procesai atitinka šį reglamentą, tačiau kelia reikšmingą kibernetinio saugumo riziką ir riziką asmenų sveikatai ar saugai, pareigų vykdymui pagal Sąjungos ar nacionalinę teisę, kuria siekiama apsaugoti pagrindines teises, paslaugų, kurias per elektroninę informacinę sistemą siūlo [Direktyvos XXX/XXXX (TIS2) I priede] nurodyti pagrindiniai subjektai, prieinamumui, autentiškumui, vientisumui ar konfidencialumui arba kitiems viešojo intereso apsaugos aspektams, ji reikalauja, kad atitinkamas veiklos vykdytojas imtųsi visų tinkamų priemonių užtikrinti, kad rinkai pateiktas produktas su skaitmeniniais elementais ir atitinkamo gamintojo įdiegti procesai nebekeltų tokios rizikos, pašalintų tą produktą su skaitmeniniais elementais iš rinkos arba atšauktų per pagrįstą laikotarpį, nustatytą atsižvelgiant į rizikos pobūdį.

2. Gamintojas arba kiti atitinkami veiklos vykdytojai užtikrina, kad taisomųjų veiksmų dėl produktų su skaitmeniniais elementais, kuriuos jie tiekė rinkai visoje Sąjungoje,

būtų imtasi per 1 dalyje nurodytos valstybės narės rinkos priežiūros institucijos nustatytą terminą.

3. Valstybė narė nedelsdama Komisijai ir kitoms valstybėms narėms praneša apie priemones, kurių imtasi pagal 1 dalį. Ta informacija apima visus turimus duomenis, visų pirma atitinkamam produktui su skaitmeniniais elementais identifikuoti būtinus duomenys, tų produktų su skaitmeniniais elementais kilmę ir tiekimo grandinę, susijusios rizikos pobūdį ir taikomų nacionalinių priemonių pobūdį bei trukmę.

4. Komisija nedelsdama pradeda konsultacijas su valstybėmis narėmis ir atitinkamu ekonominės veiklos vykdytoju bei įvertina taikomas nacionalines priemones. Remdamasi to vertinimo rezultatais Komisija nusprendžia, ar priemonė pagrįsta, ar ne, ir prireikus pasiūlo tinkamas priemones.

5. Komisija savo sprendimą skiria valstybėms narėms.

6. Jei Komisija turi pakankamai priežasčių manyti, taip pat remdamasi ENISA pateikta informacija, kad produktas su skaitmeniniais elementais atitinka šio reglamento reikalavimus, tačiau kelia 1 dalyje nurodytą riziką, ji gali prašyti atitinkamų rinkos priežiūros institucijų atlikti atitikties vertinimą ir laikytis 43 straipsnyje ir šio straipsnio 1, 2 ir 3 dalyse nurodytų procedūrų.

7. Išskirtinėmis aplinkybėmis, kuriomis pateisinama neatidėliotina intervencija siekiant išsaugoti gerą vidaus rinkos veikimą, ir kai Komisija turi pakankamai priežasčių manyti, kad 6 dalyje nurodytas produktas vis dar kelia 1 dalyje nurodytą riziką ir atitinkamos rinkos priežiūros institucijos nesiėmė jokių veiksmingų priemonių, Komisija gali prašyti ENISA atlikti to produkto keliamos rizikos vertinimą ir apie tai informuoja atitinkamas rinkos priežiūros institucijas. Atitinkami ekonominės veiklos vykdytojai prireikus bendradarbiauja su ENISA.

8. Remdamasi 7 dalyje nurodytu ENISA vertinimu Komisija gali priimti sprendimą, kad būtina taikyti taisomąją arba ribojamąją priemonę Sąjungos lygmeniu. Šiuo tikslu ji nedelsdama konsultuojasi su atitinkamomis valstybėmis narėmis ir atitinkamu veiklos vykdytoju ar vykdytojais.

9. Remdamasi 8 dalyje nurodytomis konsultacijomis Komisija gali priimti įgyvendinimo aktus, kad priimtų sprendimą dėl taisomųjų arba ribojamųjų priemonių Sąjungos lygmeniu, įskaitant nurodymą pašalinti iš rinkos arba atšaukti per pagrįstą laikotarpį, nustatytą atsižvelgiant į rizikos pobūdį. Tie įgyvendinimo aktai priimami laikantis 51 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

10. Komisija apie 9 dalyje nurodytą sprendimą nedelsdama praneša atitinkamam veiklos vykdytojui (-ams). Valstybės narės nedelsdamos įgyvendina tokius aktus ir apie tai atitinkamai informuoja Komisiją.

11. 6–10 dalys taikomos tiek laiko, kiek trunka išskirtinė situacija, pateisinanti Komisijos įsikišimą, ir kol atitinkamas produktas kelia 1 dalyje nurodytą riziką.

47 straipsnis

Oficiali neatitiktis

1. Jeigu valstybės narės rinkos priežiūros institucija nustato vieną iš toliau nurodytų faktų, ji reikalauja, kad atitinkamas gamintojas pašalintų nustatytą neatitiktį:

   (a) atitikties ženklu paženklinta pažeidžiant 21 ir 22 straipsnius;

   (b) nepaženklinta atitikties ženklu;

(c) neparengta ES atitikties deklaracija;

(d) ES atitikties deklaracija parengta netinkamai;

(e) nepažymėta atitikties vertinimo procedūroje dalyvaujančios notifikuotosios įstaigos identifikaciniu numeriu (jei taikoma).

(f) nėra techninių dokumentų arba jie yra neišsamūs.

2. Jeigu 1 dalyje nurodyta neatitiktis nepašalinama, atitinkama valstybė narė imasi visų tinkamų priemonių, kad būtų apribotas arba uždraustas produkto su skaitmeniniais elementais tiekimas rinkai arba užtikrinta, kad produktas būtų atšauktas arba pašalintas iš rinkos.

48 straipsnis

Bendra rinkos priežiūros institucijų veikla

1. Rinkos priežiūros institucijos gali susitarti su kitomis atitinkamomis institucijomis vykdyti bendrą veiklą, kuria siekiama užtikrinti vartotojų kibernetinį saugumą ir apsaugą, dėl konkrečių rinkai pateikiamų arba tiekiamų produktų su skaitmeniniais elementais, visų pirma produktų, kurie dažnai kelia kibernetinio saugumo riziką.

2. Komisija arba ENISA gali pasiūlyti bendrą veiklą, skirtą patikrinti atitiktį reglamento reikalavimams, kurią vykdo rinkos priežiūros institucijos remdamosi įrodymais arba informacija apie galimą produktų, kurie patenka į šio reglamento taikymo sritį, neatitiktį šio reglamento reikalavimams keliose valstybėse narėse.

3. Rinkos priežiūros institucijos ir Komisija, kai taikytina, užtikrina, kad susitarimu vykdyti bendrą veiklą nebūtų sudaroma nesąžininga ekonominės veiklos vykdytojų konkurencija ir nebūtų daromas neigiamas poveikis susitarimo šalių objektyvumui, nepriklausomumui ir nešališkumui.

4. Rinkos priežiūros institucija gali naudoti bet kokią informaciją, gautą vykdant bet kokią veiklą, kuri yra jos vykdomo tyrimo dalis.

5. Atitinkama rinkos priežiūros institucija ir, kai taikytina, Komisija sudaro sąlygas visuomenei susipažinti su susitarimu dėl bendros veiklos, įskaitant susijusių šalių pavadinimus.

49 straipsnis

Tikslinės patikros

1. Rinkos priežiūros institucijos gali nuspręsti tuo pačiu metu atlikti koordinuojamus kontrolės veiksmus (toliau – tikslinės patikros), kad patikrintų produktų su skaitmeniniais elementais ar jų kategorijų atitiktį šiam reglamentui arba nustatytų jo pažeidimus.

2. Jei atitinkamos rinkos priežiūros institucijos nesusitaria kitaip, tikslines patikras koordinuoja Komisija. Tikslinės patikros koordinatorius prireikus gali viešai paskelbti apibendrintus rezultatus.

3. Vykdydama savo užduotis ENISA gali, taip pat remdamasi pagal 11 straipsnio 1 ir 2 dalis gaunamais pranešimais, nustatyti produktų kategorijas, kurioms gali būti organizuojamos tikslinės patikros. Pasiūlymas dėl tikslinių patikrų pateikiamas 2 dalyje nurodytam potencialiam koordinatoriui, kad jį apsvarstytų rinkos priežiūros institucijos.

4. Vykdydamos tikslines patikras jose dalyvaujančios rinkos priežiūros institucijos gali naudotis 41–47 straipsniuose nustatytais įgaliojimais atlikti tyrimą ir visais kitais joms pagal nacionalinę teisę suteiktais įgaliojimais.

5. Rinkos priežiūros institucijos gali pakviesti Komisijos pareigūnus ir kitus juos lydinčius asmenis, įgaliotus Komisijos, dalyvauti tikslinėse patikrose.

VI SKYRIUS

DELEGUOTIEJI ĮGALIOJIMAI IR KOMITETO PROCEDŪRA

50 straipsnis

Naudojimasis įgaliojimais

1. Įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami šiame straipsnyje nustatytomis sąlygomis.

2. Komisijai suteikiami 2 straipsnio 4 dalyje, 6 straipsnio 2 dalyje, 6 straipsnio 3 dalyje, 6 straipsnio 5 dalyje, 20 straipsnio 5 dalyje ir 23 straipsnio 5 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus.

3. Europos Parlamentas arba Taryba gali bet kada atšaukti 2 straipsnio 4 dalyje, 6 straipsnio 2 dalyje, 6 straipsnio 3 dalyje, 6 straipsnio 5 dalyje, 20 straipsnio 5 dalyje ir 23 straipsnio 5 dalyje nurodytus deleguotuosius įgaliojimus. Sprendimu dėl įgaliojimų atšaukimo nutraukiami tame sprendime nurodyti įgaliojimai priimti deleguotuosius aktus. Sprendimas įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* arba vėlesnę jame nurodytą dieną. Jis nedaro poveikio jau galiojančių deleguotųjų aktų galiojimui.

4. Prieš priimdama deleguotąjį aktą Komisija konsultuojasi su kiekvienos valstybės narės paskirtais ekspertais vadovaudamasi 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros nustatytais principais.

5. Kai tik Komisija priima deleguotąjį aktą, apie tai ji tuo pačiu metu praneša Europos Parlamentui ir Tarybai.

6. Pagal 2 straipsnio 4 dalį, 6 straipsnio 2 dalį, 6 straipsnio 3 dalį, 6 straipsnio 5 dalį, 20 straipsnio 5 dalį ir 23 straipsnio 5 dalį priimtas deleguotasis aktas įsigalioja tik tuo atveju, jeigu per du mėnesius nuo pranešimo Europos Parlamentui ir Tarybai apie šį aktą dienos nei Europos Parlamentas, nei Taryba nepareiškia prieštaravimų arba jeigu dar nepasibaigus šiam laikotarpiui ir Europos Parlamentas, ir Taryba praneša Komisijai, kad prieštaravimų nereikš. Europos Parlamento arba Tarybos iniciatyva šis laikotarpis pratęsiamas dar dviem mėnesiams.

51 straipsnis

Komiteto procedūra

1. Komisijai padeda komitetas. Tas komitetas – tai komitetas, kaip nustatyta Reglamente (ES) Nr. 182/2011.

2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis.

3. Kai komiteto nuomonei gauti būtina rašytinė procedūra, tokia procedūra laikoma baigta be rezultato, jei per nuomonei pateikti nustatytą laikotarpį taip nusprendžia komiteto pirmininkas arba to prašo komiteto narys.

VII SKYRIUS

KONFIDENCIALUMAS IR SANKCIJOS

52 straipsnis

Konfidencialumas

1. Visos šį reglamentą taikančios šalys užtikrina informacijos ir duomenų, kuriuos jos gavo vykdydamos savo užduotis ir veiklą, konfidencialumą, kad būtų apsaugota:

   (a) intelektinės nuosavybės teisės ir fizinio ar juridinio asmens konfidenciali verslo informacija ar komercinės paslaptys, įskaitant pirminį kodą, išskyrus Europos Parlamento ir Tarybos direktyvos 2016/943[24] 5 straipsnyje nurodytus atvejus;

   (b) veiksmingas šio reglamento įgyvendinimas, ypač susijęs su patikrinimais, tyrimais arba auditu;

   (c) viešojo ir nacionalinio saugumo interesai;

   (d) baudžiamojo ar administracinio proceso vientisumas.

2. Nedarant poveikio 1 daliai, informacija, kuria konfidencialiai keičiamasi tarp rinkos priežiūros institucijų bei tarp rinkos priežiūros institucijų ir Komisijos, neatskleidžiama be išankstinio informaciją pateikusios rinkos priežiūros institucijos sutikimo.

3. 1 ir 2 dalimis nedaroma poveikio Komisijos, valstybių narių ir notifikuotųjų įstaigų teisėms ir pareigoms keistis informacija bei platinti įspėjimus, taip pat atitinkamų asmenų pareigoms teikti informaciją pagal valstybių narių baudžiamąją teisę.

4. Komisija ir valstybės narės prireikus gali keistis neskelbtina informacija su trečiųjų valstybių, su kuriomis jos yra sudariusios dvišalius arba daugiašalius konfidencialumo susitarimus, kuriais užtikrinamas reikiamas apsaugos lygis, atitinkamomis institucijomis.

53 straipsnis

Sankcijos

1. Valstybės narės nustato taisykles dėl sankcijų, taikytinų ekonominės veiklos vykdytojams pažeidus šį reglamentą, ir imasi visų būtinų priemonių jų įgyvendinimui užtikrinti. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasančios.

2. Valstybės narės nedelsdamos praneša apie tas taisykles ir tas priemones Komisijai ir nedelsdamos jai praneša apie visus vėlesnius joms įtakos turinčius pakeitimus.

[24] 2016 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/943 dėl neatskleistos praktinės patirties ir verslo informacijos (komercinių paslapčių) apsaugos nuo neteisėto jų gavimo, naudojimo ir atskleidimo (OL L 157, 2016 6 15, p. 1).

3. Už I priede nustatytų esminių kibernetinio saugumo reikalavimų ir 10 ir 11 straipsniuose nustatytų pareigų nesilaikymą skiriamos administracinės baudos iki 15 000 000 EUR arba, jei pažeidėjas yra įmonė, iki 2,5 proc. jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos (pasirenkama didesnioji iš šių sumų).

4. Už bet kurių kitų pareigų pagal šį reglamentą nesilaikymą skiriamos administracinės baudos iki 10 000 000 EUR arba, jei pažeidėjas yra įmonė, iki 2 proc. jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos (pasirenkama didesnioji iš šių sumų).

5. Už neteisingos, neišsamios ar klaidinančios informacijos pateikimą notifikuotosioms įstaigoms ir rinkos priežiūros institucijoms atsakant į jų prašymą taikomos administracinės baudos iki 5 000 000 EUR arba, jei pažeidėjas yra įmonė, iki 1 proc. jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos (pasirenkama didesnioji iš šių sumų).

6. Sprendžiant dėl administracinės baudos dydžio kiekvienu konkrečiu atveju deramai atsižvelgiama į visas reikšmingas konkrečios situacijos aplinkybes ir į šiuos dalykus:

   (a) pažeidimo pobūdį, sunkumą, trukmę ir jo pasekmes;

   (b) ar kitos rinkos priežiūros institucijos jau skyrė administracines baudas tam pačiam veiklos vykdytojui už panašų pažeidimą;

   (c) pažeidimą padariusio veiklos vykdytojo dydį ir rinkos dalį.

7. Administracines baudas taikančios rinkos priežiūros institucijos šia informacija dalijasi su kitų valstybių narių rinkos priežiūros institucijomis per Reglamento (ES) 2019/1020 34 straipsnyje nurodytą informacinę ir komunikacijos sistemą.

8. Kiekviena valstybė narė nustato taisykles, reglamentuojančias, ar toje valstybėje narėje įsisteigusioms valdžios institucijomis ir įstaigoms gali būti skiriamos administracinės baudos ir kokiu mastu.

9. Priklausomai nuo valstybių narių teisinės sistemos, administracines baudas reglamentuojančios taisyklės gali būti taikomos taip, kad tose valstybėse narėse baudas skirtų kompetentingi nacionaliniai teismai arba kitos įstaigos pagal nacionaliniu lygmeniu nustatytas kompetencijas. Tokių taisyklių taikymo poveikis tose valstybėse narėse turi būti lygiavertis.

10. Atsižvelgiant į kiekvieno atskiro atvejo aplinkybes, be kitų taisomųjų ar ribojamųjų priemonių, kurias taiko rinkos priežiūros institucijos, už tą patį pažeidimą gali būti skiriamos ir administracinės baudos.

VIII SKYRIUS

PEREINAMOJO LAIKOTARPIO IR BAIGIAMOSIOS NUOSTATOS

54 straipsnis

Reglamento (ES) 2019/1020 pakeitimas

Reglamento (ES) 2019/1020 I priedas papildomas šiuo punktu:

„71. [Reglamentas XXX] [Kibernetinio atsparumo aktas]“.

55 straipsnis

Pereinamojo laikotarpio nuostatos

1. ES tipo tyrimo sertifikatai ir patvirtinimo sprendimai dėl produktų su skaitmeniniais elementais, kuriems taikomi kiti Sąjungos derinamieji teisės aktai, kibernetinio saugumo reikalavimų galioja [42 mėnesius nuo šio reglamento įsigaliojimo dienos], išskyrus atvejus, kai jie nustoja galioti anksčiau tos dienos arba kai kituose Sąjungos teisės aktuose nurodyta kitaip – tokiu atveju jie galioja tiek, kiek nurodyta tuose Sąjungos teisės aktuose.
2. Produktams su skaitmeniniais elementais, pateiktiems rinkai iki [šio reglamento taikymo pradžios dienos, nurodytos 57 straipsnyje], šio reglamento reikalavimai taikomi tik tuo atveju, jei nuo tos dienos padaryta esminių tų produktų konstrukcijos arba paskirties pakeitimų.
3. Nukrypstant nuo 2 dalies, 11 straipsnyje nustatytos pareigos taikomos visiems produktams su skaitmeniniais elementais, patenkantiems į šio reglamento taikymo sritį, kurie rinkai buvo pateikti iki [šio reglamento taikymo pradžios dienos, nurodytos 57 straipsnyje].

56 straipsnis

Vertinimas ir peržiūra

Ne vėliau kaip [praėjus 36 mėnesiams nuo šio reglamento taikymo pradžios dienos], o vėliau kas ketverius metus Komisija teikia Europos Parlamentui ir Tarybai šio reglamento vertinimo ir peržiūros ataskaitas. Ataskaitos skelbiamos viešai.

57 straipsnis

Įsigaliojimas ir taikymas

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Jis taikomas nuo [24 mėnesiai po šio reglamento įsigaliojimo dienos]. Tačiau 11 straipsnis taikomas nuo [12 mėnesių po šio reglamento įsigaliojimo dienos].

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas / Pirmininkė	*Pirmininkas / Pirmininkė*

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

1.2. Atitinkama (-os) politikos sritis (-ys)

1.3. Pasiūlymas (iniciatyva) susijęs (-usi) su:

1.4. Tikslas (-ai)

1.4.1. Bendrasis (-ieji) tikslas (-ai)

1.4.2. Konkretus (-ūs) tikslas (-ai)

1.4.3. Numatomas (-i) rezultatas (-ai) ir poveikis

1.4.4. Veiklos rezultatų rodikliai

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.5.1. Trumpalaikiai arba ilgalaikiai poreikiai, įskaitant išsamų iniciatyvos įgyvendinimo pradinio etapo tvarkaraštį

1.5.2. Sąjungos dalyvavimo pridėtinė vertė (gali būti susijusi su įvairiais veiksniais, pvz., koordinavimo nauda, teisiniu tikrumu, didesniu veiksmingumu ar papildomumu). Šiame punkte „Sąjungos dalyvavimo pridėtinė vertė“ – dalyvaujant Sąjungai užtikrinama vertė, papildanti vertę, kuri būtų užtikrinta vien valstybių narių veiksmais.

1.5.3. Panašios patirties išvados

1.5.4. Suderinamumas su daugiamete finansine programa ir galima sinergija su kitomis atitinkamomis priemonėmis

1.5.5. Įvairių turimų finansavimo galimybių vertinimas, įskaitant perskirstymo mastą

1.6. Pasiūlymo (iniciatyvos) trukmė ir finansinis poveikis

1.7. Numatytas (-i) valdymo būdas (-ai)

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir ataskaitų teikimo taisyklės

2.2. Valdymo ir kontrolės sistema (-os)

2.2.1. Valdymo būdo (-ų), finansavimo įgyvendinimo mechanizmo (-ų), mokėjimo tvarkos ir siūlomos kontrolės strategijos pagrindimas

2.2.2. Informacija apie nustatytą riziką ir jai sumažinti įdiegtą (-as) vidaus kontrolės sistemą (-as)

2.2.3. Kontrolės išlaidų efektyvumo apskaičiavimas ir pagrindimas (kontrolės sąnaudų ir susijusių valdomų lėšų vertės santykis) ir numatomo klaidų rizikos lygio vertinimas (atliekant mokėjimą ir užbaigiant programą)

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Atitinkama (-os) daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės)

3.2. Numatomas pasiūlymo finansinis poveikis asignavimams

3.2.1. Numatomo poveikio veiklos asignavimams santrauka

3.2.2. Numatomas veiklos asignavimais finansuojamas atliktas darbas

3.2.3. Numatomo poveikio administraciniams asignavimams santrauka

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

3.2.5. Trečiųjų šalių įnašai

3.3. Numatomas poveikis pajamoms

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

Pasiūlymas dėl reglamento dėl produktams su skaitmeniniais elementais taikomų horizontaliųjų kibernetinio saugumo reikalavimų (Kibernetinio atsparumo aktas)

1.2. Atitinkama (-os) politikos sritis (-ys)

Ryšių tinklai, turinys ir technologijos

1.3. Pasiūlymas (iniciatyva) susijęs (-usi) su:

× **nauju veiksmu**

☐ **nauju veiksmu, kai bus įgyvendintas bandomasis projektas ir (arba) atlikti parengiamieji veiksmai**[37]

☐ **esamo veiksmo galiojimo pratęsimu**

☐ **vieno ar daugiau veiksmų sujungimu arba nukreipimu į kitą / naują veiksmą**

1.4. Tikslas (-ai)

1.4.1. Bendrasis (-ieji) tikslas (-ai)

Pasiūlymas turi du pagrindinius tikslus, kuriais siekiama užtikrinti tinkamą vidaus rinkos veikimą: 1) **sudaryti sąlygas kurti saugius produktus su skaitmeniniais elementais** užtikrinant, kad aparatinės ir programinės įrangos produktai būtų pateikti rinkai su mažiau pažeidžiamumų ir kad gamintojai rimtai atsižvelgtų į saugumą viso produkto gyvavimo ciklo metu; ir 2) **sudaryti sąlygas, kad rinkdamiesi ir naudodami produktus su skaitmeniniais elementais naudotojai galėtų atsižvelgti į kibernetinį saugumą**.

1.4.2. Konkretus (-ūs) tikslas (-ai)

Pasiūlymui nustatyti **keturi konkretūs tikslai**: i) Į užtikrinti, kad gamintojai padidintų produktų su skaitmeniniais elementais saugumą nuo projektavimo ir kūrimo etapo ir per visą gyvavimo ciklą; ii) užtikrinti nuoseklią kibernetinio saugumo sistemą, palengvinančią aparatinės ir programinės įrangos gamintojų reikalavimų laikymąsi; iii) padidinti produktų su skaitmeniniais elementais saugumo savybių skaidrumą ir iv) sudaryti sąlygas įmonėms ir vartotojams saugiai naudoti produktus su skaitmeniniais elementais.

Numatomas (-i) rezultatas (-ai) ir poveikis

Nurodyti poveikį, kurį pasiūlymas (iniciatyva) turėtų padaryti tiksliniams gavėjams (tikslinėms grupėms).

Pasiūlymu būtų suteikta didelės naudos įvairiems suinteresuotiesiems subjektams. Įmonėms nereikėtų tvarkytis su skirtingoms produktų su skaitmeniniais elementais saugumo taisyklėmis ir tai sumažintų susijusių kibernetinio saugumo teisės aktų reikalavimų laikymosi išlaidas. Tai sumažintų kibernetinių incidentų skaičių,

[37] Kaip nurodyta Finansinio reglamento 58 straipsnio 2 dalies a arba b punkte.

incidentų valdymo išlaidas ir žalą reputacijai. Apskaičiuota, kad visoje ES dėl šios iniciatyvos gali sumažėti įmonių išlaidos dėl patiriamų incidentų maždaug 180–290 mlrd. EUR per metus[38]. Dėl išaugusios produktų su skaitmeniniais elementais paklausos padidėtų apyvarta. Tai gerintų įmonių reputaciją pasaulyje, dėl to išaugtų paklausa ir ES nepriklausančiose šalyse. Naudotojams tinkamiausia galimybė padidintų saugumo savybių skaidrumą ir palengvintų produktų su skaitmeniniais elementais naudojimą. Be to, vartotojams ir piliečiams būtų naudinga geresnė jų pagrindinių teisių apsauga, pavyzdžiui, teisės į privatumą ir duomenų apsaugą.

Be to, dėl pasiūlymo atsirastų papildomų reikalavimų laikymosi ir vykdymo užtikrinimo išlaidų įmonėms, notifikuotosioms įstaigoms ir valdžios institucijoms, įskaitant notifikuojančiąsias, akreditavimo ir rinkos priežiūros institucijas. Programinės įrangos kūrėjams ir aparatinės įrangos gamintojams tai padidins tiesiogines išlaidas, susijusias su naujų saugumo reikalavimų laikymųsi, atitikties vertinimu, dokumentacijos ir ataskaitų teikimo pareigomis, dėl to bendros reikalavimų laikymosi išlaidos sieks maždaug 29 mlrd. EUR, o numatoma rinkos vertė (vertinant apyvartą) bus iki 1 485 mlrd. EUR[39]. Naudotojams, įskaitant verslo naudotojus, vartotojus ir piliečius, gali kilti produktų su skaitmeniniais elementais kainos. Tačiau tai turėtų būti vertinama atsižvelgiant į pirmiau aprašytą didelę naudą.

1.4.3. Veiklos rezultatų rodikliai

Nurodyti pažangos ir laimėjimų stebėsenos rodiklius.

Siekiant patikrinti, ar gamintojai didina savo produktų su skaitmeniniais elementais saugumą nuo projektavimo ir kūrimo etapo ir per visą tų produktų gyvavimo ciklą, galima būtų atsižvelgti į kelis rodiklius. Tai galėtų būti dėl pažeidžiamumų Sąjungoje kilusių reikšmingų incidentų skaičius, aparatinės ir programinės įrangos gamintojų, besilaikančių sistemingo saugaus kūrimo gyvavimo ciklo, dalis, kokybinė produktų su skaitmeniniais elementais saugumo analizė, kiekybinis ir kokybinis pažeidžiamumų duomenų bazių vertinimas, gamintojų pateikiamų saugumo pataisų dažnumas ar vidutinis dienų skaičius nuo pažeidžiamumo nustatymo iki saugumo pataisų pateikimo.

Nuoseklios kibernetinio saugumo sistemos rodiklis galėtų būti tikslinių konkretiems produktams skirtų nacionalinių kibernetinio saugumo teisės aktų nebuvimas.

Didesnio produktų su skaitmeniniais elementais saugumo savybių skaidrumo rodiklis galėtų būti produktų su skaitmeniniais elementais, kurie pristatomi su informacija apie saugumo ypatybes, dalis. Be to, produktų su skaitmeniniais elementais, kurie pristatomi su saugaus naudojimo instrukcijomis, dalis galėtų būti naudojama kaip rodiklis, parodantis, ar organizacijoms ir vartotojams sudaromos sąlygos saugiai naudoti produktus su skaitmeniniais elementais.

Kalbant apie reglamento poveikio stebėseną, šiuo tikslu būtų svarstomi tam tikri rodikliai, kuriuos vertina Komisija, prireikus, su ENISA pagalba. Atsižvelgiant į

[38] Žr. [Komisijos tarnybų darbinį dokumentą dėl poveikio vertinimo ataskaitos, pridedamą prie Reglamento dėl produktams su skaitmeniniais elementais taikomų horizontaliųjų kibernetinio saugumo reikalavimų]

[39] Žr. [Komisijos tarnybų darbinį dokumentą dėl poveikio vertinimo ataskaitos, pridedamą prie Reglamento dėl produktams su skaitmeniniais elementais taikomų horizontaliųjų kibernetinio saugumo reikalavimų]

siekiamą veiklos tikslą, kai kurie stebėsenos rodikliai, kuriais remiantis būtų vertinama horizontaliųjų kibernetinio saugumo reikalavimų sėkmė, yra šie:

Produktų su skaitmeniniais elementais kibernetinio saugumo lygiui įvertinti:

– Dėl produktų su skaitmeniniais elementais kylančių incidentų ir jų valdymo būdų statistika ir kokybinė analizė. Šiuos duomenis galėtų rinkti ir vertinti Komisija su ENISA pagalba.

– Žinomų pažeidžiamumų įrašai ir jų valdymo būdų analizė. Tokią analizę galėtų atlikti ENISA remdamasi Europos pažeidžiamumų duomenų baze, kuri sukurta remiantis [Direktyva XXX/XXXX (TIS2)].

– Aparatinės ir programinės įrangos gamintojų apklausos pažangai stebėti.

Informacijos apie saugumo savybes, saugumo palaikymą, gyvavimo ciklo pabaigą ir priežiūros įsipareigojimą lygiui įvertinti: naudotojų ir įmonių apklausų, kurias turi atlikti Komisija su ENISA pagalba, rezultatai.

Vertindama įgyvendinimą Komisija siektų užtikrinti, kad būtų veiksmingai atliekami atitikties vertinimai. Šiuo tikslu bus pateiktas standartizacijos prašymas ir bus stebimas jo įgyvendinimas. Komisija taip pat patikrins notifikuotųjų įstaigų ir, jei taikytina, sertifikavimo įstaigų pajėgumus.

Kalbant apie taikymą, remdamasi valstybių narių ataskaitomis Komisija tikrins, ar nacionalinės iniciatyvos neapima aspektų, kuriems taikomas reglamentas.

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.5.1. Trumpalaikiai arba ilgalaikiai poreikiai, įskaitant išsamų iniciatyvos įgyvendinimo pradinio etapo tvarkaraštį

Visas reglamentas turėtų būti pradėtas taikyti praėjus 24 mėnesiams nuo jo įsigaliojimo. Tačiau valdymo struktūros elementai iki to laiko jau turi būti nustatyti. Visų pirma valstybės narės turi paskirtas esamas institucijas ir (arba) sukūrė naujas institucijas, atliekančias teisės akte nustatytas užduotis.

1.5.2. Sąjungos dalyvavimo pridėtinė vertė (gali būti susijusi su įvairiais veiksniais, pvz., koordinavimo nauda, teisiniu tikrumu, didesniu veiksmingumu ar papildomumu). Šiame punkte „Sąjungos dalyvavimo pridėtinė vertė“ – dalyvaujant Sąjungai užtikrinama vertė, papildanti vertę, kuri būtų užtikrinta vien valstybių narių veiksmais.

Dėl kibernetinio saugumo stipraus tarpvalstybinio pobūdžio ir didėjančių incidentų, persiduodančių tarp skirtingų valstybių narių, sektorių bei produktų, pavienės valstybės narės negali veiksmingai pasiekti šių tikslų. Atsižvelgiant į pasaulinį produktų su skaitmeniniais elementais rinkų pobūdį, valstybės narės savo teritorijoje susiduria su ta pačia rizika dėl to paties produkto su skaitmeniniais elementais. Besiformuojanti netvarkinga galimai skirtingų nacionalinių taisyklių sistema taip pat gali trukdyti atvirai ir konkurencingai bendrai produktų su skaitmeniniais elementais rinkai. Todėl reikia imtis bendrų veiksmų ES lygmeniu siekiant padidinti naudotojų pasitikėjimą ES produktais su skaitmeniniais elementais bei šių produktų patrauklumą. Tai taip pat būtų naudinga vidaus rinkai, nes suteiktų teisinio tikrumo ir sudarytų vienodas sąlygas produktų su skaitmeniniais elementais pardavėjams.

1.5.3. Panašios patirties išvados

Kibernetinio atsparumo aktas yra pirmasis tokio pobūdžio reglamentas, kuriuo nustatomi kibernetinio saugumo reikalavimai produktų su skaitmeniniais elementais pateikimui rinkai. Tačiau jis pagrįstas naująja teisės aktų sistema ir patirtimi, įgyta įgyvendinant esamus įvairiems produktams skirtus Sąjungos teisės aktus, visų pirma susijusius su pasirengimu įgyvendinimui, įskaitant tokius aspektus kaip darniųjų standartų rengimas.

1.5.4. Suderinamumas su daugiamete finansine programa ir galima sinergija su kitomis atitinkamomis priemonėmis

Reglamentu dėl produktams su skaitmeniniais elementais taikomų horizontaliųjų kibernetinio saugumo reikalavimų apibrėžiami nauji kibernetinio saugumo reikalavimai visiems produktams su skaitmeniniais elementais, pateikiamiems ES rinkai. Šie reikalavimai yra išsamesni už visus esamuose teisės aktuose nustatytus reikalavimus. Tačiau pasiūlymas grindžiamas esama NTAS teisės aktų sistema. Todėl jis būtų paremtas esamomis NTAS struktūromis ir procedūromis, tokiomis kaip notifikuotųjų įstaigų bendradarbiavimas ir rinkos priežiūra, atitikties vertinimo moduliai, darniųjų standartų kūrimas. Naujasis pasiūlymas taip pat būtų pagrįstas kai kuriomis struktūromis, sukurtomis pagal kitus kibernetinio saugumo teisės aktus, pavyzdžiui, Direktyvą 2016/1148 (TIS direktyva), atitinkamai [Direktyvą XXX/XXXX (TIS2)] arba Reglamentą 2019/881 (Kibernetinio saugumo aktą).

1.5.5. Įvairių turimų finansavimo galimybių vertinimas, įskaitant perskirstymo mastą

ENISA priskirtų veiklos sričių valdymas atitinka jos turimus įgaliojimus ir bendrąsias užduotis. Šioms veiklos sritims gali prireikti specialių profilių arba naujų užduočių, tačiau jos nebūtų reikšmingos ir jas galėtų įsisavinti esami ENISA ištekliai bei perskirstant arba susiejant įvairias užduotis. Pavyzdžiui, viena iš pagrindinių ENISA priskirtų veiklos sričių yra gamintojų pranešimų apie išnaudojamus produkto pažeidžiamumus rinkimas ir tvarkymas. [Direktyva XXX/XXXX (TIS2)] ENISA jau pavesta sukurti Europos pažeidžiamumų duomenų bazę, kurioje galėtų būti atskleidžiami ir savanoriškai registruojami viešai žinomi pažeidžiamumai, kad naudotojai galėtų imtis tinkamų poveikį mažinančių priemonių. Tam skirti ištekliai galėtų būti naudojami ir naujoms minėtoms užduotims, susijusioms su pranešimais apie produktų pažeidžiamumus. Tai galėtų užtikrinti veiksmingą esamų išteklių naudojimą ir taip pat sukurtų būtiną tokių užduočių sinergiją, dėl kurios ENISA galėtų gauti geresnę informaciją savo kibernetinio saugumo rizikos ir grėsmių analizei.

1.6. Pasiūlymo (iniciatyvos) trukmė ir finansinis poveikis

☐ **Trukmė ribota**

– ☐ galioja nuo MMMM [MM DD] iki MMMM [MM DD],

– ☐ įsipareigojimų asignavimų finansinis poveikis nuo MMMM iki MMMM, o mokėjimų asignavimų – nuo MMMM iki MMMM;

× **trukmė neribota**

– įgyvendinimo pradinis laikotarpis – nuo 2025 m.,

– vėliau – visuotinis taikymas.

1.7. Numatytas (-i) valdymo būdas (-ai)[40]

☐ **Tiesioginis valdymas**, vykdomas Komisijos:

– × padalinių, įskaitant Sąjungos delegacijų darbuotojus;

– ☐ vykdomųjų įstaigų.

☐ **Pasidalijamasis valdymas** su valstybėmis narėmis

☐ **Netiesioginis valdymas**, biudžeto vykdymo užduotis pavedant:

– ☐ trečiosioms valstybėms arba jų paskirtoms įstaigoms;

– ☐ tarptautinėms organizacijoms ir jų agentūroms (nurodyti);

– ☐ EIB ir Europos investicijų fondui;

– ☐ įstaigoms, nurodytoms Finansinio reglamento 70 ir 71 straipsniuose;

– ☐ viešosios teisės reglamentuojamoms įstaigoms;

– ☐ įstaigoms, kurių veiklą reglamentuoja privatinė teisė ir kurioms pavesta teikti viešąsias paslaugas, tiek, kiek joms užtikrinamos pakankamos finansinės garantijos;

– ☐ įstaigoms, kurių veiklą reglamentuoja valstybės narės privatinė teisė, kurioms pavesta įgyvendinti viešojo ir privačiojo sektorių partnerystę ir kurioms užtikrinamos pakankamos finansinės garantijos;

– ☐ atitinkamame pagrindiniame akte nurodytiems asmenims, kuriems pavesta vykdyti konkrečius veiksmus BUSP srityje pagal ES sutarties V antraštinę dalį.

– *Jei nurodomas daugiau kaip vienas valdymo būdas, išsamią informaciją pateikti šio punkto pastabų skiltyje.*

Pastabos

Šiuo reglamentu ENISA priskiriami tam tikri veiksmai, atitinkantys jos turimus įgaliojimus, visų pirma pagal Reglamento 2019/881 3 straipsnio 2 dalį, kuria nustatoma, kad ENISA turėtų vykdyti užduotis, kurios jai pavedamos Sąjungos teisės aktais, kuriuose nustatomos su kibernetiniu saugumu susijusios valstybių narių įstatymų, reglamentų ir administracinių nuostatų derinimo priemonės. Visų pirma ENISA pavedama užduotis priimti gamintojų pranešimus apie aktyviai išnaudojamus pažeidžiamumus, esančius produktuose su skaitmeniniais elementais, taip pat apie incidentus, darančius poveikį tų produktų saugumui. ENISA taip pat turėtų perduoti šiuos pranešimus atitinkamai CSIRT arba atitinkamam

[40] Informacija apie valdymo būdus ir nuorodos į Finansinį reglamentą pateikiamos svetainėje „BudgWeb“: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

bendram valstybių narių kontaktiniam punktui, paskirtam pagal Direktyvos [Direktyva XXX/XXXX (TIS2)] straipsnį [X straipsnis], ir informuoti rinkos priežiūros institucijas. Remdamasi surinkta informacija ENISA turėtų kas dvejus metus parengti techninę ataskaitą apie kylančias kibernetinio saugumo rizikos tendencijas produktuose su skaitmeniniais elementais ir pateikti ją TIS bendradarbiavimo grupei. Be to, atsižvelgdama į savo kompetenciją, surinktą informaciją ir grėsmių analizę, ENISA gali palaikyti šio reglamento įgyvendinimo procesą pasiūlydama bendrą veiklą, kurią vykdys nacionalinės rinkos priežiūros institucijos remdamosi įrodymais arba informacija apie galimą produktų su skaitmeniniais elementais neatitikimą reglamento reikalavimams keliose valstybėse narėse, arba nustatyti produktų kategorijas, kurioms gali būti vienu metu organizuojami koordinuoti kontrolės veiksmai. Komisija gali prašyti ENISA išskirtinėmis aplinkybėmis įvertinti konkrečius produktus su skaitmeniniais elementais, kurie kelia reikšmingą kibernetinio saugumo riziką, ir kai reikia nedelsiant atlikti intervenciją, kad būtų išsaugotas tinkamas vidaus rinkos veikimas.

Apskaičiuota, kad visos šios užduotys esamiems ENISA ištekliams sudarys maždaug 4,5 etato ekvivalento ir bus pagrįstos ENISA šiuo metu jau turima patirtimi ir atliktais parengiamaisiais darbais, taip pat teikiant paramą būsimos [Direktyvos XXX/XXXX (TIS2)] įgyvendinimui, dėl kurio buvo papildyti ENISA ištekliai.

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir ataskaitų teikimo taisyklės

Nurodyti dažnumą ir sąlygas.

Ne vėliau kaip praėjus 36 mėnesiams nuo šio reglamento taikymo pradžios dienos, o vėliau kas ketverius metus Komisija teiks Europos Parlamentui ir Tarybai vertinimo ir peržiūros ataskaitas. Ataskaitos skelbiamos viešai.

2.2. Valdymo ir kontrolės sistema (-os)

2.2.1. Valdymo būdo (-ų), finansavimo įgyvendinimo mechanizmo (-ų), mokėjimo tvarkos ir siūlomos kontrolės strategijos pagrindimas

Šiuo reglamentu nustatoma nauja politika darniesiems kibernetinio saugumo reikalavimams, kurie taikomi vidaus rinkai pateikiamiems produktams su skaitmeniniais elementais per visą jų gyvavimo ciklą. Po teisės akto Komisija pateiks prašymus Europos standartizacijos institucijoms parengti standartus.

Siekiant vykdyti šias naujas užduotis, būtina užtikrinti, kad Komisijos tarnybos turėtų pakankamai išteklių. Apskaičiuota, kad siekiant įgyvendinti naująjį reglamentą, reikės 7 etato ekvivalentų (iš kurių vienas END), kurie apims šias užduotis:

- parengti standartizacijos prašymą ir (arba) bendrąsias specifikacijas įgyvendinimo aktais, kai nėra sėkmingo standartizacijos proceso;
- parengti deleguotąjį aktą [per 12 mėnesių nuo reglamento įsigaliojimo], kuriame būtų nurodytos ypatingos svarbos produktų su skaitmeniniais elementais apibrėžtys;
- galimai parengti deleguotuosius aktus I ir II klasių ypatingos svarbos produktų sąrašui atnaujinti; nurodyti, ar produktams su skaitmeniniais elementais, kuriems taikomos kitos Sąjungos taisyklės, nustatančios reikalavimus, kuriais užtikrinamas toks pat apsaugos lygis kaip ir šiuo reglamentu, reikalingas apribojimas arba išimtis; įpareigoti sertifikuoti tam tikrus didžiausios svarbos produktus su skaitmeniniais elementais remiantis šiame reglamente nustatytais kriterijais; nurodyti minimalų ES atitikties deklaracijos turinį ir papildyti elementus, kurie turi būti įtraukti į techninius dokumentus;
- galimai parengti įgyvendinimo aktus, susijusius su pareigos pranešti formatu arba elementais, programinės įrangos medžiagų žiniaraščiu, bendrosiomis specifikacijomis arba ženklinimu CE ženklu;
- galimai parengti nedelsiant atliekamą intervenciją taisomosioms arba ribojamosioms priemonėms pritaikyti išskirtinėmis aplinkybėmis, kad būtų išsaugotas tinkamas vidaus rinkos veikimas, įskaitant įgyvendinimo akto rengimą;
- organizuoti ir koordinuoti valstybių narių notifikuotųjų įstaigų pranešimus bei koordinuoti notifikuotąsias įstaigas;
- teikti paramą valstybių narių rinkos priežiūros institucijų koordinavimui.

2.2.2. Informacija apie nustatytą riziką ir jai sumažinti įdiegtą (-as) vidaus kontrolės sistemą (-as)

Siekiant užtikrinti, kad notifikuotosios įstaigos ir rinkos priežiūros institucijos keistųsi informacija ir gerai bendradarbiautų, už jų koordinavimą atsako Komisija. Siekiant pasitelkti techninę ir rinkos kompetenciją, būtų sukurta ekspertų grupė.

2.2.3. Kontrolės išlaidų efektyvumo apskaičiavimas ir pagrindimas (kontrolės sąnaudų ir susijusių valdomų lėšų vertės santykis) ir numatomo klaidų rizikos lygio vertinimas (atliekant mokėjimą ir užbaigiant programą)

2.3. Dėl susitikimų išlaidų, atsižvelgiant į mažą kiekvieno sandorio vertę (pvz., į susitikimą siunčiamo delegato kelionės išlaidų grąžinimas), atrodo, kad standartinės kontrolės procedūros yra pakankamos. Sukčiavimo ir pažeidimų prevencijos priemonės

Nurodyti dabartines arba numatytas prevencijos ir apsaugos priemones, pvz., išdėstytas Kovos su sukčiavimu strategijoje.

Papildomi asignavimai, reikalingi šiam reglamentui, bus padengiami esamomis Komisijai taikomomis sukčiavimo prevencijos priemonėmis.

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Atitinkama (-os) daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės)

- Dabartinės biudžeto eilutės

Schema

- Prašomos sukurti naujos biudžeto eilutės

Netaikoma

3.2. Numatomas pasiūlymo finansinis poveikis asignavimams

3.2.1. Numatomo poveikio veiklos asignavimams santrauka

– ☑ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai nenaudojami

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

Daugiametės finansinės programos išlaidų kategorija	Numeris	

GD: <…….>			Metai **N**[41]	Metai **N+1**	Metai **N+2**	Metai **N+3**	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)			**IŠ VISO**
• Veiklos asignavimai										
Biudžeto eilutė[42]	Įsipareigojimai	(1a)								
	Mokėjimai	(2a)								
Biudžeto eilutė	Įsipareigojimai	(1b)								
	Mokėjimai	(2b)								
Administracinio pobūdžio asignavimai, finansuojami iš konkrečių programų paketo lėšų[43]										
Biudžeto eilutė		(3)								
IŠ VISO asignavimų	Įsipareigojimai	= 1a + 1b + 3								

41 N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai. Pakeiskite „N“ numatomais pirmaisiais įgyvendinimo metais (pavyzdžiui, 2021). Atitinkamai pakeiskite vėlesnius metus.

42 Pagal oficialią biudžeto nomenklatūrą.

43 Techninė ir (arba) administracinė parama bei išlaidos ES programų ir (arba) veiksmų įgyvendinimui remti (buvusios BA eilutės), netiesioginiai moksliniai tyrimai, tiesioginiai moksliniai tyrimai.

<…….> **GD**	Mokėjimai	= 2a + 2b +3								

• IŠ VISO veiklos asignavimų	Įsipareigojimai	(4)								
	Mokėjimai	(5)								
• IŠ VISO administracinio pobūdžio asignavimų, finansuojamų iš konkrečių programų paketo lėšų		(6)								
IŠ VISO asignavimų pagal daugiametės finansinės programos **<….> IŠLAIDŲ KATEGORIJĄ**	Įsipareigojimai	= 4 + 6								
	Mokėjimai	= 5 + 6								

Jei pasiūlymas (iniciatyva) daro poveikį kelioms veiklos išlaidų kategorijoms, pakartokite pirmiau pateiktą dalį:

• IŠ VISO veiklos asignavimų (visose veiklos išlaidų kategorijose)	Įsipareigojimai	(4)								
	Mokėjimai	(5)								
IŠ VISO administracinio pobūdžio asignavimų, finansuojamų iš konkrečių programų paketo lėšų (visose veiklos išlaidų kategorijose)		(6)								
IŠ VISO asignavimų daugiametės finansinės programos **pagal 1–6 IŠLAIDŲ KATEGORIJAS** (Orientacinė suma)	Įsipareigojimai	= 4 + 6								
	Mokėjimai	= 5 + 6								

Daugiametės finansinės programos išlaidų kategorija	**7**	„Administracinės išlaidos“

Šią dalį pildyti naudojant administracinio pobūdžio biudžeto duomenų lentelę, kuri pirmiausia bus pateikta finansinės teisės akto pasiūlymo pažymos priede (Vidaus taisyklių V priedas) ir įkelta į DECIDE tarnybų tarpusavio konsultacijoms.

mln. EUR (tūkstantųjų tikslumu)

		2024 metai	**2025** metai	**2026** metai	**2027** metai	**IŠ VISO**
GD: Ryšių tinklų, turinio ir technologijų (CNECT)						
•Žmogiškieji ištekliai		1,030	1,030	1,030	1,030	**4,120**
•Kitos administracinės išlaidos		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
IŠ VISO CNECT GD	Asignavimai	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

IŠ VISO asignavimų pagal daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJĄ**	(Iš viso įsipareigojimų = Iš viso mokėjimų)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

mln. EUR (tūkstantųjų tikslumu)

		Metai **2024**	Metai **2025**	Metai **2026**	Metai **2027**	**IŠ VISO**
IŠ VISO asignavimų daugiametės finansinės programos **1–7 IŠLAIDŲ KATEGORIJAS**	Įsipareigojimai	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Mokėjimai	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Numatomas veiklos asignavimais finansuojamas atliktas darbas

Įsipareigojimų asignavimai mln. EUR (tūkstantųjų tikslumu)

Nurodyti tikslus ir išvedinius ⇩			N metai		N+1 metai		N+2 metai		N+3 metai		Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)						**IŠ VISO**	
	IŠVEDINIAI																	
	Rūšis 44	Vidutinės sąnaudos	Nr.	Sąnaudos	Nr.	Sąnaudos	Nr.	Sąnaudos	Nr.	Sąnaudos	Nr.	Sąnaudos	Nr.	Sąnaudos	Nr.	Sąnaudos	Iš viso Nr.	Iš viso sąnaudų
KONKRETUS TIKSLAS Nr. 1[45]…																		
– Išvedinys																		
– Išvedinys																		
– Išvedinys																		
1 konkretaus tikslo tarpinė suma																		
2 KONKRETUS TIKSLAS ...																		
– Išvedinys																		
2 konkretaus tikslo tarpinė suma																		
IŠ VISO																		

44 Atlikti darbai – tai būsimi produktai ir paslaugos (pvz., finansuota studentų mainų, nutiesta kelių kilometrų ir kt.).

45 Kaip apibūdinta 1.4.2 skirsnyje. „Konkretus (-ūs) tikslas (-ai)...“.

3.2.3. Numatomo poveikio administraciniams asignavimams santrauka

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimų nenaudojama

– ☑ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

	2024 metai	**2025** metai	**2026** metai	**2027** metai	
Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJA					
Žmogiškieji ištekliai	1,030	1,030	1,030	1,030	**4,120**
Kitos administracinės išlaidos	0,222	0,222	0,222	0,222	**0,888**
Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJOS tarpinė suma	1,252	1,252	1,252	1,252	**5,008**

Neįtraukta į daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ[46]					
Žmogiškieji ištekliai					
Kitos administracinio pobūdžio išlaidos					
Tarpinė suma, neįtraukta į daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ					

IŠ VISO	1,252	1,252	1,252	1,252	**5,008**

Žmogiškųjų išteklių ir kitų administracinio pobūdžio išlaidų asignavimų poreikiai bus tenkinami iš GD asignavimų, jau paskirtų veiksmui valdyti ir (arba) perskirstytų generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

[46] Techninė ir (arba) administracinė parama bei išlaidos ES programų ir (arba) veiksmų įgyvendinimui remti (buvusios BA eilutės), netiesioginiai moksliniai tyrimai, tiesioginiai moksliniai tyrimai.

3.2.3.1. Numatomi žmogiškųjų išteklių poreikiai

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškųjų išteklių nenaudojama.

– ☑ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai naudojami taip:

Sąmatą surašyti etatų vienetais

		2024 metai	**2025** metai	**2026** metai	**2027** metai
20 01 02 01 (Komisijos būstinė ir atstovybės)		6	6	6	6
20 01 02 03 (Delegacijos)					
01 01 01 01 (Netiesioginiai moksliniai tyrimai)					
01 01 01 11 (Tiesioginiai moksliniai tyrimai)					
Kitos biudžeto eilutės (nurodyti)					
• Išorės darbuotojai (etatų vienetais)[47]					
20 02 01 (AC, END, INT finansuojami iš bendrojo biudžeto)		1	1	1	1
20 02 03 (AC, AL, END, INT ir JPD delegacijose)					
XX 01 xx **yy zz** [48]	– būstinėje				
	– delegacijose				
01 01 01 02 (AC, END, INT – netiesioginiai moksliniai tyrimai)					
01 01 01 12 (AC, END, INT – tiesioginiai moksliniai tyrimai)					
Kitos biudžeto eilutės (nurodyti)					
IŠ VISO		**7**	**7**	**7**	**7**

XX yra atitinkama politikos sritis arba biudžeto antraštinė dalis.

Žmogiškųjų išteklių poreikiai bus tenkinami panaudojant GD darbuotojus, jau paskirtus veiksmui valdyti ir (arba) perskirstytus generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

Vykdytinų užduočių aprašymas:

Pareigūnai ir laikinieji darbuotojai 6 etato ekvivalentai x 157 000 EUR per metus = 942 000 EUR	Kaip apibūdinta 2.2.1 skirsnyje: – parengti standartizacijos prašymą ir (arba) bendrąsias specifikacijas įgyvendinimo aktais, kai nėra sėkmingo standartizacijos proceso; – parengti deleguotąjį aktą [per 12 mėnesių nuo reglamento įsigaliojimo], kuriame būtų nurodytos ypatingos svarbos produktų su skaitmeniniais elementais apibrėžtys; – galimai parengti deleguotuosius aktus I ir II klasių ypatingos svarbos produktų sąrašui atnaujinti; nurodyti, ar produktams su skaitmeniniais elementais, kuriems taikomos kitos Sąjungos taisyklės, nustatančios reikalavimus, kuriais užtikrinamas toks pat apsaugos lygis kaip ir šiuo reglamentu, reikalingas apribojimas arba išimtis; įpareigoti sertifikuoti tam tikrus didžiausios svarbos produktus su skaitmeniniais elementais remiantis šiame reglamente nustatytais kriterijais; nurodyti minimalų ES atitikties deklaracijos turinį ir papildyti elementus, kurie turi būti įtraukti į techninius dokumentus; – galimai parengti įgyvendinimo aktus, susijusius su pareigos pranešti

[47] AC – sutartininkas („Contract Staff“), AL – vietinis darbuotojas, END – deleguotasis nacionalinis ekspertas, INT – per agentūrą įdarbintas darbuotojas, JPD – jaunesnysis delegacijos specialistas.

[48] Neviršijant viršutinės ribos, nustatytos išorės darbuotojams, finansuojamiems iš veiklos asignavimų (buvusių BA eilučių).

	formatu arba elementais, programinės įrangos medžiagų žiniaraščiu, bendrosiomis specifikacijomis arba ženklinimu CE ženklu; – galimai parengti nedelsiant atliekamą intervenciją taisomosioms arba ribojamosioms priemonėms pritaikyti išskirtinėmis aplinkybėmis, kad būtų išsaugotas tinkamas vidaus rinkos veikimas, įskaitant įgyvendinimo akto rengimą; – organizuoti ir koordinuoti valstybių narių notifikuotųjų įstaigų pranešimus bei koordinuoti notifikuotąsias įstaigas; – teikti paramą valstybių narių rinkos priežiūros institucijų koordinavimui.
Išorės darbuotojai 1 END x 88 000 EUR per metus	Kaip apibūdinta 2.2.1 skirsnyje: – parengti standartizacijos prašymą ir (arba) bendrąsias specifikacijas įgyvendinimo aktais, kai nėra sėkmingo standartizacijos proceso; – parengti deleguotąjį aktą [per 12 mėnesių nuo reglamento įsigaliojimo], kuriame būtų nurodytos ypatingos svarbos produktų su skaitmeniniais elementais apibrėžtys; – galimai parengti deleguotuosius aktus I ir II klasių ypatingos svarbos produktų sąrašui atnaujinti; nurodyti, ar produktams su skaitmeniniais elementais, kuriems taikomos kitos Sąjungos taisyklės, nustatančios reikalavimus, kuriais užtikrinamas toks pat apsaugos lygis kaip ir šiuo reglamentu, reikalingas apribojimas arba išimtis; įpareigoti sertifikuoti tam tikrus didžiausios svarbos produktus su skaitmeniniais elementais remiantis šiame reglamente nustatytais kriterijais; nurodyti minimalų ES atitikties deklaracijos turinį ir papildyti elementus, kurie turi būti įtraukti į techninius dokumentus; – galimai parengti įgyvendinimo aktus, susijusius su pareigos pranešti formatu arba elementais, programinės įrangos medžiagų žiniaraščiu, bendrosiomis specifikacijomis arba ženklinimu CE ženklu; – galimai parengti nedelsiant atliekamą intervenciją taisomosioms arba ribojamosioms priemonėms pritaikyti išskirtinėmis aplinkybėmis, kad būtų išsaugotas tinkamas vidaus rinkos veikimas, įskaitant įgyvendinimo akto rengimą; – organizuoti ir koordinuoti valstybių narių notifikuotųjų įstaigų pranešimus bei koordinuoti notifikuotąsias įstaigas; – teikti paramą valstybių narių rinkos priežiūros institucijų koordinavimui.

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

Pasiūlyme (iniciatyvoje):

– x Galima visiškai finansuoti perskirstant asignavimą atitinkamoje daugiametės finansinės programos (DFP) išlaidų kategorijoje.

Perprogramavimas nereikalingas.

– ☐ Reikia panaudoti nepaskirstytą maržą pagal atitinkamą DFP išlaidų kategoriją ir (arba) specialias priemones, kaip apibrėžta DFP reglamente.

–

– ☐ Reikia persvarstyti DFP.

–

3.2.5. Trečiųjų šalių įnašai

Pasiūlyme (iniciatyvoje):

– x nenumatyta bendro su trečiosiomis šalimis finansavimo

– ☐ numatytas trečiųjų šalių bendras finansavimas apskaičiuojamas taip:

Asignavimai mln. EUR (tūkstantųjų tikslumu)

	Metai **N**[49]	Metai **N+1**	Metai **N+2**	Metai **N+3**	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)			Iš viso
Nurodyti bendrą finansavimą teikiančią įstaigą								
IŠ VISO bendrai finansuojamų asignavimų								

[49] N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai. Pakeiskite „N“ numatomais pirmaisiais įgyvendinimo metais (pavyzdžiui, 2021). Atitinkamai pakeiskite vėlesnius metus.

3.3. Numatomas poveikis pajamoms

– ☐ Pasiūlymas (iniciatyva) neturi finansinio poveikio pajamoms.

– ☐ Pasiūlymas (iniciatyva) turi finansinį poveikį:

  – ☐ nuosaviems ištekliams

  – ☐ kitoms pajamoms

  – nurodyti, jei pajamos priskirtos išlaidų eilutėms ☐

mln. EUR (tūkstantųjų tikslumu)

Biudžeto pajamų eilutė:	Einamųjų finansinių metų asignavimai	Pasiūlymo (iniciatyvos) poveikis[50]						
		N metai	**N+1** metai	**N+2** metai	**N+3** metai	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)		
……. straipsnis								

Asignuotųjų pajamų atveju nurodyti biudžeto išlaidų eilutę (-es), kuriai (-ioms) daromas poveikis.

Kitos pastabos (pvz., poveikio pajamoms apskaičiavimo metodas (formulė) arba kita informacija).

[50] Tradiciniai nuosavi ištekliai (muitai, cukraus mokesčiai) turi būti nurodomi grynosiomis sumomis, t. y. iš bendros sumos atskaičius 20 % surinkimo sąnaudų.