EUROPOS SĄJUNGA

EUROPOS PARLAMENTAS **TARYBA**

Briuselis, 2024 m. rugsėjo 25 d.
(OR. en)

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

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

TEISĖS AKTAI IR KITI DOKUMENTAI

Dalykas:	EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas)

EUROPOS PARLAMENTO IR TARYBOS
REGLAMENTAS (ES) 2024/…

… m. … … d.

dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas)

(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,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

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

pasikonsultavę su Regionų komitetu,

laikydamiesi įprastos teisėkūros procedūros[2],

---

1 OL C 100, 2023 3 16, p. 101.

2 2024 m. kovo 12 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir … m. … … d. Tarybos sprendimas.

kadangi:

(1) kibernetinis saugumas yra vienas iš pagrindinių Sąjungos iššūkių. Prijungtųjų įrenginių skaičius ir įvairovė ateinančiais metais sparčiai didės. Kibernetiniai išpuoliai yra viešojo intereso klausimas, nes jie daro itin didelį poveikį ne tik Sąjungos ekonomikai, bet ir demokratijai, taip pat vartotojų saugai ir sveikatai. Todėl būtina stiprinti Sąjungos požiūrį į kibernetinį saugumą, spręsti kibernetinio atsparumo problemą Sąjungos lygmeniu ir gerinti vidaus rinkos veikimą nustatant vienodą teisinę sistemą, susijusią su esminiais kibernetinio saugumo reikalavimais, taikomais produktų su skaitmeniniais elementais pateikimui Sąjungos rinkai. Reikėtų išspręsti dvi pagrindines problemas, dėl kurių naudotojai ir visuomenė patiria papildomų sąnaudų: žemas produktų su skaitmeniniais elementais kibernetinio saugumo lygis, kurį atspindi plačiai paplitę pažeidžiamumai ir nepakankamas bei nenuoseklus saugumo naujinių teikimas jiems spręsti, ir nepakankamas naudotojų supratimas ir prieiga prie informacijos, dėl ko 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 produktus su skaitmeniniais elementais ir juos naudodami, naudotojai galėtų atsižvelgti į kibernetinį saugumą, pavyzdžiui, didinant skaidrumą, susijusį su rinkai pateiktų produktų su skaitmeniniais elementais palaikymo laikotarpiu;

(3) galiojančius susijusius 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 reglamentą (ES) 2019/881[3] ir Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555[4], tiesiogiai neapima privalomų reikalavimų produktų su skaitmeniniais elementais saugumo srityje;

---

[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] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva) (OL L 333, 2022 12 27, p. 80).

(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 rizika, todėl vidaus rinkoje kuriama nevientisa teisės aktų sistema, didėja teisinis netikrumas tiek tų produktų gamintojams, tiek jų naudotojams, o įmonėms ir organizacijoms užkraunama nereikalinga našta, nes jos turi laikytis tam tikrų tos pačios rūšies produktams taikomų reikalavimų ir pareigų. Tų produktų kibernetiniam saugumui būdingas itin stiprus tarpvalstybinis aspektas, nes vienoje valstybėje narėje ar trečiojoje valstybėje pagamintus produktus su skaitmeniniais elementais dažnai naudoja organizacijos ir vartotojai visoje vidaus rinkoje. Todėl šią sritį būtina reglamentuoti Sąjungos lygmeniu, kad naudotojams, organizacijoms ir įmonėms, įskaitant labai mažas įmones ir mažąsias bei vidutines įmones, kaip apibrėžta Komisijos rekomendacijos 2003/361/EB[5] priede, būtų užtikrinta suderinta reglamentavimo sistema ir teisinis tikrumas. Sąjungos reglamentavimo aplinka turėtų būti suderinta nustatant produktų su skaitmeniniais elementais horizontaliuosius kibernetinio saugumo reikalavimus. Be to, visoje Sąjungoje turėtų būti užtikrintas teisinis tikrumas ekonominės veiklos vykdytojams ir naudotojams, ir geriau suderinta vidaus rinka bei užtikrintas proporcingumas labai mažoms įmonėms ir mažosioms bei vidutinėms įmonėms ir taip sudarytos palankesnės sąlygos ekonominės veiklos vykdytojams, siekiantiems patekti į tą rinką;

---

[5] 2003 m. gegužės 6 d. Komisijos rekomendacija 2003/361/EB dėl labai mažų, mažųjų ir vidutinių įmonių apibrėžimo (OL L 124, 2003 5 20, p. 36).

(5) kalbant apie labai mažas įmones ir mažąsias bei vidutines įmones, nustatant, kokiai kategorijai priskiriama įmonė, turėtų būti taikomos visos Rekomendacijos 2003/361/EB priedo nuostatos. Todėl apskaičiuojant darbuotojų skaičių ir finansines viršutines ribas, pagal kuriuos nustatomos įmonių kategorijos, taip pat turėtų būti taikomos Rekomendacijos 2003/361/EB priedo 6 straipsnio nuostatos dėl įmonės duomenų nustatymo atsižvelgiant į konkrečias įmonių rūšis, pavyzdžiui, įmones partneres arba susijusias įmones;

(6) Komisija turėtų pateikti gaires, skirtas padėti ekonominės veiklos vykdytojams, visų pirma labai mažoms įmonėms ir mažosioms bei vidutinėms įmonėms, taikyti šį reglamentą. Tokiose gairėse turėtų būti aptariama, *inter alia*, šio reglamento taikymo sritis, visų pirma nuotolinis duomenų tvarkymas ir jo poveikis laisvosios ir atvirosios programinės įrangos kūrėjams, kriterijų, taikomų nustatant produktų su skaitmeniniais elementais palaikymo laikotarpius, taikymas, šio reglamento ir kitų Sąjungos teisės aktų sąveika ir esminio pakeitimo koncepcija;

(7) Sąjungos lygmeniu įvairiuose programiniuose ir politiniuose dokumentuose, pavyzdžiui, 2020 m. gruodžio 16 d. Komisijos ir Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai bendrame komunikate „ES skaitmeninio dešimtmečio kibernetinio saugumo strategija“, 2020 m. gruodžio 2 d. Tarybos išvadose dėl prijungtųjų įrenginių kibernetinio saugumo, 2022 m. gegužės 23 d. Tarybos išvadose dėl Europos Sąjungos kibernetinio saugumo būklės raidos ir 2021 m. birželio 10 d. Europos Parlamento rezoliucijoje dėl ES skaitmeninio dešimtmečio kibernetinio saugumo strategijos[6] raginama nustatyti konkrečius Sąjungos kibernetinio saugumo reikalavimus, keliamus skaitmeniniams arba prijungtiesiems produktams, o kelios trečiosios valstybės ėmėsi priemonių šiam klausimui spręsti savo iniciatyva. Galutinėje Konferencijos dėl Europos ateities ataskaitoje piliečiai „ragino stiprinti ES vaidmenį kovoje su kibernetinėmis grėsmėmis“. Kad Sąjunga pirmautų pasaulyje kibernetinio saugumo srityje, svarbu sukurti plataus užmojo reglamentavimo sistemą;

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

---

[6] OL C 67, 2022 2 8, p. 81.

(9) 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 produktai su skaitmeniniais elementais būtų suprojektuoti ir sukurti laikantis šiame reglamente nustatytų esminių kibernetinio saugumo reikalavimų. Ta pareiga susijusi ir su produktais, kuriuos galima prijungti fiziškai per aparatinės įrangos sąsajas, ir su produktais, kurie prijungiami loginiu būdu, pavyzdžiui, per tinklo lizdus, kanalus, failus, programų sąsajas arba bet kokio kito tipo programinės įrangos sąsają. Kadangi kibernetinės 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 su skaitmeniniais elementais, kurie su kitais įrenginiais ar tinklais yra sujungti tik netiesiogiai, kibernetinį saugumą;

(10) nustatant kibernetinio saugumo reikalavimus, keliamus produktų su skaitmeniniais elementais pateikimui rinkai, siekiama padidinti tų produktų kibernetinį saugumą tiek vartotojams, tiek įmonėms. Tais reikalavimais taip pat bus užtikrinta, kad į kibernetinį saugumą atsižvelgiama visose tiekimo grandinėse ir galutiniai produktai su skaitmeniniais elementais ir jų komponentai taps saugesni. Tai taip pat apima reikalavimus, keliamus produktų su skaitmeniniais elementais, skirtų pažeidžiamiems vartotojams, pavyzdžiui, žaislų ir kūdikių stebėjimo sistemų, pateikimui rinkai. Vartotojų produktai su skaitmeniniais elementais, šiame reglamente priskiriami svarbių produktų su skaitmeniniais elementais kategorijai, kelia didesnę kibernetinio saugumo riziką, nes atlieka funkciją, dėl kurios intensyvumo ir galimybės pakenkti tokių produktų naudotojų sveikatai, saugumui ar saugai kyla didelė neigiamo poveikio rizika, todėl jiems turėtų būti taikoma griežtesnė atitikties vertinimo procedūra. Tai taikoma tokiems produktams kaip išmanieji buitiniai produktai su saugumo funkcijomis, be kita ko, išmaniosioms durų spynoms, kūdikių stebėjimo sistemoms ir signalizacijos sistemoms, prijungtiesiems žaislams ir asmeniniams dėvimiems sveikatos technologijų prietaisams. Be to, griežtesnės atitikties vertinimo procedūros, kurios turi būti taikomos kitiems produktams su skaitmeniniais elementais, kurie šiame reglamente priskiriami prie svarbių arba ypatingos svarbos produktų su skaitmeniniais elementais, padės užkirsti kelią galimam neigiamam pažeidžiamumų išnaudojimo poveikiui vartotojams;

(11) šio reglamento tikslas – užtikrinti aukštą produktų su skaitmeniniais elementais ir jų integruotų nuotolinio duomenų tvarkymo sprendinių kibernetinio saugumo lygį. Tokie nuotolinio duomenų tvarkymo sprendiniai turėtų būti apibrėžiami kaip duomenų tvarkymas per atstumą, kuriam programinę įrangą projektuoja ir kuria atitinkamo produkto su skaitmeniniais elementais gamintojas arba tai daroma jo vardu, ir be kurių toks produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų. Tuo požiūriu užtikrinama, kad gamintojai tinkamai apsaugotų visus tokius produktus, nepriklausomai nuo to, ar duomenys tvarkomi arba saugomi pačiame naudotojo įrenginyje, ar tai nuotoliniu būdu daro gamintojas. Tuo pačiu metu duomenų tvarkymas arba saugojimas per atstumą patenka į šio reglamento taikymo sritį tik tiek, kiek tai būtina, kad produktas su skaitmeniniais elementais galėtų atlikti savo funkcijas. Toks tvarkymas arba saugojimas per atstumą apima atvejus, kai mobiliajai programėlei reikia prieigos prie taikomųjų programų sąsajos arba duomenų bazės, teikiamos naudojantis gamintojo sukurta paslauga. Tokiu atveju paslauga patenka į šio reglamento taikymo sritį kaip nuotolinio duomenų tvarkymo sprendinys. Todėl reikalavimai, susiję su nuotolinio duomenų tvarkymo sprendiniais, patenkančiais į šio reglamento taikymo sritį, neapima techninių, operatyvinių ar organizacinių priemonių, kuriomis siekiama valdyti riziką, kylančią gamintojo tinklų ir informacinių sistemų kaip visumos saugumui;

(12) debesijos sprendiniai yra nuotolinio duomenų tvarkymo sprendiniai, kaip tai suprantama šiame reglamente, tik jei jie atitinka šiame reglamente įtvirtintą apibrėžtį. Pavyzdžiui, į šio reglamento taikymo sritį patenka išmaniųjų buitinių prietaisų gamintojo teikiamos, debesijos pagrindu veikiančios funkcijos, leidžiančios naudotojams nuotoliniu būdu valdyti prietaisą. Priešingai, interneto svetainės, kurios nepalaiko produkto su skaitmeniniais elementais funkcijų, arba debesijos paslaugos, kurios nėra suprojektuotos ir sukurtos produkto su skaitmeniniais elementais gamintojo atsakomybe, nepatenka į šio reglamento taikymo sritį. Direktyva (ES) 2022/2555 taikoma debesijos kompiuterijos paslaugų ir debesijos paslaugų modeliams, pavyzdžiui, paslauginei programinei įrangai (SaaS), paslauginei platformai (PaaS) arba paslauginei infrastruktūrai (IaaS). Debesijos kompiuterijos paslaugas Sąjungoje teikiantiems subjektams, kurie pagal Rekomendacijos 2003/361/EB priedo 2 straipsnį laikomi vidutinėmis įmonėmis arba viršija to straipsnio 1 dalyje nurodytas vidutinėms įmonėms nustatytas viršutines ribas, patenka į tos direktyvos taikymo sritį;

(13) vadovaudamosi šio reglamento tikslu pašalinti kliūtis laisvam produktų su skaitmeniniais elementais judėjimui, valstybės narės neturėtų trukdyti tiekti rinkai šį reglamentą atitinkančius produktus su skaitmeniniais elementais dėl priežasčių, susijusių su šiuo reglamentu reguliuojamais aspektais. Todėl šiuo reglamentu suderintais klausimais valstybės narės negali nustatyti papildomų kibernetinio saugumo reikalavimų, taikomų produktų su skaitmeniniais elementais tiekimui rinkai. Tačiau bet kuris viešasis ar privatusis subjektas be šiame reglamente nustatytų reikalavimų gali nustatyti papildomus reikalavimus, taikomus produktų su skaitmeniniais elementais viešajam pirkimui arba naudojimui konkrečiais tikslais ir todėl gali nuspręsti naudoti produktus su skaitmeniniais elementais, kurie atitinka griežtesnius arba konkretesnius kibernetinio saugumo reikalavimus nei tie, kurie taikomi tiekimui rinkai pagal šį reglamentą. Nedarant poveikio Europos Parlamento ir Tarybos direktyvoms 2014/24/ES[7] ir 2014/25/ES[8], pirkdamos produktus su skaitmeniniais elementais, kurie turi atitikti šiame reglamente nustatytus esminius kibernetinio saugumo reikalavimus, įskaitant reikalavimus dėl pažeidžiamumo valdymo, valstybės narės turėtų užtikrinti, kad į tokius reikalavimus būtų atsižvelgiama viešųjų pirkimų procese ir kad taip pat būtų atsižvelgta į gamintojų gebėjimą veiksmingai taikyti kibernetinio saugumo priemones ir valdyti kibernetines grėsmes.

---

7 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/24/ES dėl viešųjų pirkimų, kuria panaikinama Direktyva 2004/18/EB (OL L 94, 2014 3 28, p. 65).

8 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/25/ES dėl subjektų, vykdančių veiklą vandens, energetikos, transporto ir pašto paslaugų sektoriuose, vykdomų pirkimų, kuria panaikinama Direktyva 2004/17/EB (OL L 94, 2014 3 28, p. 243).

Be to, Direktyvoje (ES) 2022/2555 nustatytos ir tos direktyvos 3 straipsnyje nurodytiems esminiams bei svarbiems subjektams skirtos kibernetinio saugumo rizikos valdymo priemonės, kurios galėtų apimti tiekimo grandinės saugumo priemones, pagal kurias reikalaujama, kad tokie subjektai naudotų produktus su skaitmeniniais elementais, atitinkančius griežtesnius kibernetinio saugumo reikalavimus nei nustatytieji šiame reglamente. Todėl pagal Direktyvą (ES) 2022/2555 ir joje nustatytą minimalaus harmonizavimo principą valstybės narės gali nustatyti papildomus kibernetinio saugumo reikalavimus, taikomus esminiams arba svarbiems subjektams naudojant IRT produktus pagal tą direktyvą, kad būtų užtikrintas aukštesnis kibernetinio saugumo lygis, jei tokie reikalavimai yra suderinami su Sąjungos teisėje nustatytomis valstybių narių pareigomis. Aspektai, kuriems šis reglamentas netaikomas, gali apimti netechninius veiksnius, susijusius su produktais su skaitmeniniais elementais ir jų gamintojais. Todėl valstybės narės gali nustatyti nacionalines priemones, įskaitant apribojimus, taikomus produktams su skaitmeniniais elementais arba tokių produktų tiekėjams, kuriomis būtų atsižvelgiama į netechninius veiksnius. Reikalaujama, kad su tokiais veiksniais susijusios nacionalinės priemonės atitiktų Sąjungos teisę;

(14) šiuo reglamentu neturėtų būti daromas poveikis valstybių narių atsakomybei už nacionalinio saugumo užtikrinimą laikantis Sąjungos teisės. Valstybės narės turėtų turėti galimybę produktams su skaitmeniniais elementais, kurie yra perkami arba naudojami nacionalinio saugumo ar gynybos tikslais, taikyti papildomas priemones, jei tokios priemonės atitinka Sąjungos teisėje nustatytas valstybių narių pareigas;

(15) šis reglamentas ekonominės veiklos vykdytojams taikomas tik dėl produktų su skaitmeniniais elementais, kurie patiekti rinkai, t. y. tiekti platinti arba naudoti Sąjungos rinkoje vykdant komercinę veiklą. Tiekimas vykdant komercinę veiklą gali būti apibūdinamas ne tik kaip užmokesčio už produktą su skaitmeniniais elementais taikymas, bet ir kaip užmokesčio už techninės pagalbos paslaugas taikymas, kai tuo siekiama ne vien atgauti faktines išlaidas, siekiant monetizuoti, pavyzdžiui, teikiant programinės įrangos platformą, per kurią gamintojas gauna pajamų iš kitų paslaugų, kaip naudojimo sąlygą išreiškiant reikalavimą, kad asmens duomenys būtų tvarkomi kitais nei vien programinės įrangos saugumo, suderinamumo ar sąveikos gerinimo tikslais, arba priimant aukas, viršijančias su produkto su skaitmeniniais elementais projektavimu, kūrimu ir teikimu susijusias išlaidas. Aukų priėmimas be ketinimo gauti pelno neturėtų būti laikomas komercine veikla;

(16) produktai su skaitmeniniais elementais, suteikiami teikiant paslaugą, už kurią imamas mokestis tik siekiant padengti faktines išlaidas, tiesiogiai susijusias su tos paslaugos teikimu, pavyzdžiui, tam tikrų viešojo administravimo subjektų teikiamų produktų su skaitmeniniais elementais atveju, vien dėl tų priežasčių neturėtų būti laikomi komercine veikla šio reglamento tikslais. Be to, produktai su skaitmeniniais elementais, kuriuos viešojo administravimo subjektas kuria arba keičia išimtinai savo reikmėms, neturėtų būti laikomi tiekiamais rinkai, kaip tai suprantama šiame reglamente;

(17) programinė įranga ir duomenys, kuriais atvirai dalijamasi ir kurių naudotojai gali laisvai prieiti prie jų arba jų pakeistų versijų, juos naudoti, keisti ir platinti, gali prisidėti prie mokslinių tyrimų ir inovacijų rinkoje. Siekiant skatinti laisvosios ir atvirosios programinės įrangos kūrimą ir diegimą, visų pirma, kai juos atlieka labai mažos įmonės ir mažosios bei vidutinės įmonės, įskaitant startuolius, asmenys, ne pelno organizacijos ir akademinės mokslinių tyrimų organizacijos, taikant šį reglamentą produktams su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga, tiekiama platinti arba naudoti vykdant komercinę veiklą, turėtų būti atsižvelgiama į skirtingų programinės įrangos, platinamos ir kuriamos pagal laisvosios ir atvirosios programinės įrangos licencijas, kūrimo modelių pobūdį;

(18) laisvoji ir atviroji programinė įranga suprantama kaip programinė įranga, kurios pirminiu kodu atvirai dalijamasi ir kurios licencijavimas suteikia visas teises padaryti, kad ji būtų laisvai prieinama, naudojama, keičiama ir pakartotinai platinama. Laisvoji ir atviroji programinė įranga kuriama, techniškai prižiūrima ir platinama atvirai, be kita ko, per interneto platformas. Ekonominės veiklos vykdytojų, kuriems taikomas šis reglamentas, atžvilgiu šis reglamentas turėtų būti taikomas tik laisvajai ir atvirajai programinei įrangai, kuri yra patiekta rinkai ir todėl patiekta platinti ar naudoti vykdant komercinę veiklą. Todėl nustatant tos veiklos komercinį ar nekomercinį pobūdį, neturėtų būti atsižvelgiama vien į aplinkybes, kuriomis produktas su skaitmeniniais elementais buvo sukurtas ar kaip buvo finansuojamas jo kūrimas. Konkrečiau, šio reglamento tikslais ir kiek tai susiję su į jo taikymo sritį patenkančių ekonominės veiklos vykdytojais, siekiant užtikrinti, kad būtų aiškiai atskirti kūrimo ir tiekimo etapai, produktų su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga ir už kuriuos jų gamintojai negauna pelno, teikimas neturėtų būti laikomas komercine veikla. Be to, produktų su skaitmeniniais elementais, kurie laikomi laisvosios ir atvirosios programinės įrangos komponentais, skirtais kitiems gamintojams integruoti į savo produktus su skaitmeniniais elementais, tiekimas turėtų būti laikomas tiekimu rinkai tik jeigu komponentą monetizuoja jo pirminis gamintojas. Pavyzdžiui, vien tai, kad atvirosios programinės įrangos produktas su skaitmeniniais elementais gauna finansinę paramą iš gamintojų arba kad gamintojai prisideda prie tokio produkto kūrimo, savaime nereiškia, kad veikla yra komercinio pobūdžio.

Be to, vien dėl to, kad vykdomi reguliarūs išleidimai, savaime neturėtų būti daroma išvada, kad produktas su skaitmeniniais elementais tiekiamas vykdant komercinę veiklą. Galiausiai, šio reglamento tikslais ne pelno organizacijų vykdomas produktų su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga, kūrimas neturėtų būti laikomas komercine veikla, jeigu organizacija įsteigta taip, kad būtų užtikrinta, jog visos pajamos atskaičius išlaidas būtų naudojamos ne pelno tikslams siekti. Šis reglamentas netaikomas fiziniams ar juridiniams asmenims, kurie pirminiu kodu prisideda prie produktų su skaitmeniniais elementais, laikomais laisvąja ir atvirąja programine įranga, už kuriuos jie nėra atsakingi;

(19) atsižvelgiant į daugelio produktų su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga ir kurie skelbiami, bet nepateikiami rinkai, kaip tai suprantama šiame reglamente, svarbą kibernetiniam saugumui, juridiniams asmenims, kurie nuolat teikia paramą tokių komercinei veiklai skirtų produktų kūrimui ir kurie atlieka pagrindinį vaidmenį užtikrinant tų produktų gyvybingumą (atvirosios programinės įrangos valdytojai), turėtų būti taikoma negriežta ir specialiai pritaikyta reguliavimo tvarka. Atvirosios programinės įrangos valdytojams priskiriami tam tikri fondai ir subjektai, kurie kuria ir skelbia laisvąją ir atvirąją programinę įrangą verslo aplinkoje, įskaitant pelno nesiekiančius subjektus. Reguliavimo tvarkoje turėtų būti atsižvelgiama į jų specifinį pobūdį ir suderinamumą su nustatytų pareigų rūšimi. Ji turėtų būti taikoma tik tiems produktams su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga ir kurie galiausiai yra skirti komercinei veiklai, pavyzdžiui, integravimui į komercines paslaugas arba į monetizuotus produktus su skaitmeniniais elementais. Tos reguliavimo tvarkos tikslais ketinimas integruoti į monetizuotus produktus su skaitmeniniais elementais apima atvejus, kai gamintojai, integruojantys komponentą į savo produktus su skaitmeniniais elementais, reguliariai prisideda prie to komponento kūrimo arba reguliariai teikia finansinę paramą programinės įrangos produkto tęstinumui užtikrinti. Nuolatinės paramos teikimas produkto su skaitmeniniais elementais kūrimui apima, be kita ko, programinės įrangos kūrimo bendradarbiavimo platformų prieglobą ir valdymą, pirminio kodo ar programinės įrangos prieglobą, produktų su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga, administravimą ar valdymą, taip pat vadovavimą tokių produktų kūrimui. Atsižvelgiant į tai, kad pagal negriežtą ir specialiai pritaikytą reguliavimo tvarką subjektams, veikiantiems kaip atvirosios programinės įrangos valdytojai, nėra taikomos tokios pačios pareigos kaip subjektams, veikiantiems kaip gamintojai pagal šį reglamentą, jiems neturėtų būti leidžiama ženklinti CE ženklu produktų su skaitmeniniais elementais, kurių kūrimą jie remia;

(20) vien produktų su skaitmeniniais elementais priegloba atvirose saugyklose, be kita ko, naudojant paketų tvarkytuves ar bendradarbiavimo platformose, savaime nėra produkto su skaitmeniniais elementais tiekimas rinkai. Tokių paslaugų teikėjai turėtų būti laikomi platintojais tik jeigu jie tiekia tokią programinę įrangą rinkai, taigi tiekia ją platinti arba naudoti Sąjungos rinkoje vykdant komercinę veiklą;

(21) siekiant remti ir palengvinti gamintojų, kurie į savo produktus su skaitmeniniais elementais integruoja laisvosios ir atvirosios programinės įrangos komponentus, kuriems netaikomi šiame reglamente nustatyti esminiai kibernetinio saugumo reikalavimai, išsamų patikrinimą, Komisija turėtų galėti nustatyti savanoriškas saugumo patvirtinimo programas arba priimdama deleguotąjį aktą, kuriuo papildomas šis reglamentas, arba prašydama parengti Europos kibernetinio saugumo sertifikavimo schemą pagal Reglamento (ES) 2019/881 48 straipsnį, kurioje būtų atsižvelgiama į laisvosios ir atvirosios programinės įrangos kūrimo modelių ypatumus. Saugumo patvirtinimo programos turėtų būti parengtos taip, kad saugumo patvirtinimą galėtų inicijuoti arba finansuoti ne tik fiziniai ar juridiniai asmenys, kuriantys produktą su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga, arba prisidedantys prie jo kūrimo, bet ir trečiosios šalys, pavyzdžiui, gamintojai, integruojantys tokius produktus į savo produktus su skaitmeniniais elementais, naudotojai arba Sąjungos ir nacionalinės viešojo administravimo institucijos;

(22) atsižvelgiant į šiame reglamente nustatytus viešojo sektoriaus kibernetinio saugumo tikslus ir siekiant pagerinti valstybių narių informuotumą apie padėtį, susijusią su Sąjungos priklausomybe nuo programinės įrangos komponentų, visų pirma nuo potencialiai laisvosios ir atvirosios programinės įrangos komponentų, šiuo reglamentu įsteigta speciali administracinio bendradarbiavimo grupė turėtų galėti nuspręsti bendrai atlikti Sąjungos priklausomybės vertinimą. Rinkos priežiūros institucijos turėtų turėti galimybę reikalauti, kad administracinio bendradarbiavimo grupės nustatytų kategorijų produktų su skaitmeniniais elementais gamintojai pateiktų pagal šį reglamentą jų parengtus programinės įrangos medžiagų žiniaraščius (toliau – PĮMŽ). Siekiant apsaugoti PĮMŽ konfidencialumą, rinkos priežiūros institucijos atitinkamą informaciją apie priklausomybę nuo programinės įrangos turėtų pateikti administracinio bendradarbiavimo grupei anonimizuota ir apibendrinta forma;

(23) šio reglamento įgyvendinimo veiksmingumas taip pat priklausys nuo tinkamų kibernetinio saugumo įgūdžių prieinamumo. Sąjungos lygmeniu įvairiuose programiniuose ir politiniuose dokumentuose, įskaitant 2023 m. balandžio 18 d. Komisijos komunikatą „Kibernetinio saugumo srities talentų trūkumo problemos sprendimas siekiant didinti ES konkurencingumą ir atsparumą bei skatinti jos augimą“ ir 2023 m. gegužės 22 d. Tarybos išvadas dėl ES kibernetinės gynybos politikos, pripažinta, kad Sąjungoje trūksta kibernetinio saugumo įgūdžių ir reikia prioriteto tvarka spręsti tokius uždavinius tiek viešajame, tiek privačiajame sektoriuose. Siekdamos užtikrinti veiksmingą šio reglamento įgyvendinimą, valstybės narės turėtų užtikrinti, kad rinkos priežiūros institucijos ir atitikties vertinimo įstaigos turėtų pakankamai išteklių šiame reglamente nustatytoms savo užduotims atlikti. Tomis priemonėmis turėtų būti didinamas darbo jėgos judumas kibernetinio saugumo srityje ir su juo susijusios karjeros galimybės. Jos taip pat turėtų prisidėti prie to, kad kibernetinio saugumo srities darbo jėga taptų atsparesnė ir įtraukesnė, be kita ko, lyčių požiūriu. Todėl valstybės narės turėtų imtis priemonių užtikrinti, kad tas užduotis vykdytų tinkamai parengti specialistai, turintys reikiamų kibernetinio saugumo įgūdžių. Panašiai ir gamintojai turėtų užtikrinti, kad jų darbuotojai turėtų reikiamų įgūdžių, reikalingų šiame reglamente nustatytoms pareigoms vykdyti. Valstybės narės ir Komisija, atsižvelgdamos į savo prerogatyvas ir kompetenciją bei šiuo reglamentu joms pavestas konkrečias užduotis, turėtų imtis priemonių remti gamintojus, visų pirma labai mažas įmones ir mažąsias bei vidutines įmones, įskaitant startuolius, taip pat ir tose srityse kaip antai įgūdžių ugdymas, kad jie laikytųsi šiuo reglamentu jiems nustatytų pareigų. Be to, kadangi Direktyva (ES) 2022/2555 reikalaujama, kad valstybės narės savo nacionalinėse kibernetinio saugumo strategijose nustatytų politiką, kuria būtų skatinamas ir plėtojamas kibernetinio saugumo ir kibernetinio saugumo įgūdžių mokymas, valstybės narės, priimdamos tokias strategijas, taip pat gali svarstyti galimybę atsižvelgti į su šiuo reglamentu susijusius kibernetinio saugumo įgūdžių poreikius, be kita ko, susijusius su perkvalifikavimu ir kvalifikacijos kėlimu;

(24) saugus internetas yra būtinas ypatingos svarbos infrastruktūros objektų veikimui ir visai visuomenei. Direktyva (ES) 2022/2555 siekiama užtikrinti aukštą paslaugų, kurias teikia tos direktyvos 3 straipsnyje nurodyti esminiai ir svarbūs subjektai, įskaitant skaitmeninės infrastruktūros teikėjus, kurie palaiko pagrindines atvirojo interneto funkcijas, užtikrina interneto prieigą ir teikia 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 (ES) 2022/2555 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;

(25) Europos Parlamento ir Tarybos reglamente (ES) 2017/745[9] nustatomos medicinos priemonių taisyklės, o Europos Parlamento ir Tarybos reglamente (ES) 2017/746[10] nustatomos *in vitro* diagnostikos medicinos priemonių taisyklės. Tais 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. Tie reglamentai taip pat apima tam tikrą neįtaisytąją programinę įrangą ir viso gyvavimo ciklo metodą. Tie 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 priede nustatytus reikalavimus, susijusius su kibernetiniu saugumu. Todėl produktams su skaitmeniniais elementais, kuriems taikomas vienas iš tų reglamentų, šis reglamentas neturėtų būti taikomas;

---

9 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).

10 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).

(26) į šio reglamento taikymo sritį nepatenka išimtinai nacionalinio saugumo ar gynybos tikslais sukurti ar pakeisti produktai su skaitmeniniais elementais arba produktai, specialiai sukurti įslaptintai informacijai tvarkyti. Valstybės narės raginamos užtikrinti tokį patį arba aukštesnį produktų, kuriems taikomas šis reglamentas, apsaugos lygį;

(27) Europos Parlamento ir Tarybos reglamentu (ES) 2019/2144[11] nustatomi transporto priemonių, jų sistemų ir komponentų tipo patvirtinimo reikalavimai, įtvirtinant tam tikrus kibernetinio saugumo reikalavimus, įskaitant reikalavimus dėl sertifikuotos kibernetinio saugumo valdymo sistemos veikimo, programinės įrangos naujinių, kurie apima organizacijų politiką ir kibernetinio saugumo rizikos procesus, susijusius su visu transporto priemonių, įrangos ir paslaugų gyvavimo ciklu, laikantis galiojančių Jungtinių Tautų taisyklių dėl techninių specifikacijų ir kibernetinio saugumo, visų pirma JT taisyklės Nr. 155 dėl vienodų nuostatų dėl transporto priemonių patvirtinimo kibernetinio saugumo ir kibernetinio saugumo valdymo sistemos atžvilgiu, ir nustatant konkrečias atitikties vertinimo procedūras.

---

[11] 2019 m. lapkričio 27 d. Europos Parlamento ir Tarybos reglamentas (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).

Aviacijos srityje pagrindinis Europos Parlamento ir Tarybos reglamento (ES) 2018/1139[12] tikslas – nustatyti ir palaikyti aukštą vienodą civilinės aviacijos saugos lygį Sąjungoje. Juo sukuriama esminių tinkamumo skraidyti reikalavimų, taikomų aeronautikos produktams, dalims ir įrangai, įskaitant programinę įrangą, sistema, į kurią įtraukiamos pareigos apsisaugoti nuo informacijos saugumo grėsmių. Sertifikavimo procesas pagal Reglamentą (ES) 2018/1139 užtikrina šiuo reglamentu siekiamą saugumo užtikrinimo lygį. Todėl produktams su skaitmeniniais elementais, kuriems taikomas Reglamentas (ES) 2019/2144, ir produktams, sertifikuotiems pagal Reglamentą (ES) 2018/1139, šiame reglamente nustatyti esminiai kibernetinio saugumo reikalavimai ir atitikties vertinimo procedūros neturėtų būti taikomi;

---

[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 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).

(28) 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 kibernetinio saugumo reikalavimai. Tokiais atvejais šio reglamento taikymas produktams su skaitmeniniais elementais, kuriems taikomos kitos Sąjungos taisyklės, kuriose nustatomi reikalavimai visai arba daliai rizikos, kuriai taikomi šiame reglamente nustatyti esminiai kibernetinio saugumo reikalavimai, gali būti apribotas arba šis reglamentas gali būti netaikomas, jei toks apribojimas arba netaikymas atitinka bendrą tiems produktams taikomą reguliavimo sistemą ir kai sektorių taisyklėmis užtikrinamas bent toks pats apsaugos lygis kaip ir šiuo reglamentu. Komisijai turėtų būti suteikti įgaliojimai priimti deleguotuosius aktus, siekiant papildyti šį reglamentą, kuriais identifikuojami tokie produktai ir taisyklės. Galiojančių Sąjungos teisės aktų atveju, kai turėtų būti taikomas toks apribojimas ar netaikymas, šiame reglamente nustatomos konkrečios nuostatos, kuriomis paaiškinamas jo ryšys su tais Sąjungos teisės aktais;

(29) siekiant užtikrinti, kad rinkai tiekiamus produktus su skaitmeniniais elementais būtų galima tinkamai sutaisyti ir prailginti jų patvarumą, atsarginėms dalims turėtų būti numatyta išimtis. Ta išimtis turėtų būti taikoma tiek atsarginėms dalims, skirtoms taisyti senus produktus, pateiktus rinkai iki šio reglamento taikymo pradžios dienos, tiek atsarginėms dalims, kurioms jau atlikta atitikties vertinimo procedūra pagal šį reglamentą;

(30) Komisijos deleguotajame reglamente (ES) 2022/30[13] nurodyta, kad tam tikriems radijo įrenginiams taikoma keletas Europos Parlamento ir Tarybos direktyvos 2014/53/ES[14] 3 straipsnio 3 dalies d, e ir f punktuose nustatytų esminių reikalavimų, susijusių su žala tinklui ir netinkamu tinklo išteklių naudojimu, asmens duomenimis ir privatumu bei sukčiavimu. 2022 m. rugpjūčio 5 d. Komisijos įgyvendinimo sprendime C(2022)5637 dėl Europos standartizacijos komitetui ir Europos elektrotechnikos standartizacijos komitetui pateikto standartizacijos prašymo nustatyti reikalavimai konkretiems standartams parengti ir papildomai nurodyta, kaip tie esminiai reikalavimai turėtų būti sprendžiami. Šiame reglamente nustatyti esminiai kibernetinio saugumo 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 kibernetinio saugumo reikalavimai yra suderinti su konkretiems standartams, įtrauktiems į tą standartizacijos prašymą, skirtų reikalavimų tikslais. Todėl, Komisijai panaikinus ar iš dalies pakeitus Deleguotąjį reglamentą (ES) 2022/30 taip, kad jis nustotų būti taikomas tam tikriems produktams, kuriems taikomas šis reglamentas, rengdamos ir plėtodamos darniuosius standartus, padėsiančius įgyvendinti šį reglamentą, Komisija ir Europos standartizacijos organizacijos turėtų atsižvelgti į standartizavimo darbą, atliekamą pagal Įgyvendinimo sprendimą C(2022)5637. Šio reglamento taikymo pereinamuoju laikotarpiu Komisija turėtų pateikti gaires gamintojams, kuriems taikomas šis reglamentas ir kuriems taip pat taikomas Deleguotasis reglamentas (ES) 2022/30, kad būtų lengviau įrodyti atitiktį tiems dviem reglamentams;

---

13 2021 m. spalio 29 d. Komisijos deleguotasis reglamentas (ES) 2022/30, kuriuo papildomos Europos Parlamento ir Tarybos direktyvos 2014/53/ES nuostatos dėl esminių reikalavimų, nurodytų tos direktyvos 3 straipsnio 3 dalies d, e ir f punktuose, taikymo (OL L 7, 2022 1 12, p. 6).

14 2014 m. balandžio 16 d. Europos Parlamento ir Tarybos direktyva 2014/53/ES dėl valstybių narių įstatymų, susijusių su radijo įrenginių tiekimu rinkai, suderinimo, kuria panaikinama Direktyva 1999/5/EB (OL L 153, 2014 5 22, p. 62).

(31) Europos Parlamento ir Tarybos direktyva (ES) 2024/…[15+] papildo šį reglamentą. Toje direktyvoje nustatytos taisyklės dėl atsakomybės už produktus su trūkumais, kad nukentėję asmenys galėtų reikalauti žalos atlyginimo, kai žala padaryta dėl produktų su trūkumais. Joje nustatytas principas, 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, gali kilti gamintojo atsakomybė. Šiame reglamente turėtų būti nustatytos gamintojų pareigos, susijusios su tokių saugumo naujinių teikimu;

---

15 … m. … … d. Europos Parlamento ir Tarybos direktyva (ES) …/… … (OL L …, ELI: …).

\+ OL: prašom tekste įrašyti direktyvos, esančios dokumente (2022/0302(COD)), numerį, o išnašoje – tos direktyvos priėmimo datą, numerį, pavadinimą ir OL nuorodą.

(32) šiuo reglamentu neturėtų būti daromas poveikis Europos Parlamento ir Tarybos reglamentui (ES) 2016/679[16], įskaitant jo nuostatas, susijusias su duomenų apsaugos sertifikavimo mechanizmų ir duomenų apsaugos ženklų bei žymenų sukūrimu, kad būtų galima įrodyti, jog duomenų valdytojų ir tvarkytojų atliekamos tvarkymo operacijos atitinka to reglamento reikalavimus. Tokios operacijos galėtų būti integruotos į produktą su skaitmeniniais elementais. Pagrindiniai Reglamento (ES) 2016/679 elementai yra pritaikytoji ir standartizuotoji duomenų apsauga bei, bendrai, kibernetinis saugumas. Apsaugant vartotojus ir organizacijas nuo kibernetinio saugumo rizikos, šiame reglamente nustatyti esminiai kibernetinio saugumo reikalavimai taip pat turi padėti stiprinti asmens duomenų apsaugą ir asmenų privatumą. Į kibernetinio saugumo aspektų standartizavimo ir sertifikavimo sinergiją turėtų būti atsižvelgiama bendradarbiaujant Komisijai, Europos standartizacijos organizacijoms, Europos Sąjungos kibernetinio saugumo agentūrai (toliau – ENISA), Reglamentu (ES) 2016/679 įsteigtai Europos duomenų apsaugos valdybai ir nacionalinėms duomenų apsaugos priežiūros institucijoms. Taip pat turėtų būti sukurtos sinergijos tarp šio reglamento ir Sąjungos duomenų apsaugos teisės rinkos priežiūros bei vykdymo užtikrinimo srityje. Tuo tikslu pagal šį reglamentą paskirtos nacionalinės rinkos priežiūros institucijos turėtų bendradarbiauti su institucijomis, vykdančiomis Sąjungos duomenų apsaugos teisės taikymo priežiūrą. Pastarosios taip pat turėtų turėti prieigą prie informacijos, susijusios su jų užduočių vykdymu;

---

[16] 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).

(33) tiek, kiek jų produktams taikomas šis reglamentas, europinių skaitmeninės tapatybės dėklių teikėjai, kaip nurodyta Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014[17] 5a straipsnio 2 dalyje, turėtų laikytis ir šiame reglamente nustatytų horizontaliųjų esminių kibernetinio saugumo reikalavimų, ir konkrečių saugumo reikalavimų, nustatytų Reglamento (ES) Nr. 910/2014 5a straipsnyje. Kad būtų lengviau laikytis reikalavimų, dėklių teikėjai turėtų galėti įrodyti, kad Europos skaitmeninės tapatybės dėklės atitinka šiame reglamente ir Reglamente (ES) Nr. 910/2014 nustatytus reikalavimus, atitinkamai sertifikuodami savo produktus pagal Europos kibernetinio saugumo sertifikavimo schemą, nustatytą pagal Reglamentą (ES) 2019/881, kurios atžvilgiu Komisija deleguotaisiais aktais nustatė atitikties šiam reglamentui prezumpciją tiek, kiek sertifikatas arba jo dalys apima tuos reikalavimus;

---

[17] 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (OL L 257, 2014 8 28, p. 73).

(34) projektavimo ir kūrimo etapu integruodami iš trečiųjų šalių gautus komponentus į produktus su skaitmeniniais elementais, gamintojai, siekdami užtikrinti, kad produktai būtų projektuojami, kuriami ir gaminami laikantis šiame reglamente nustatytų esminių kibernetinio saugumo reikalavimų, turėtų atlikti išsamų tų komponentų, įskaitant laisvosios ir atvirosios programinės įrangos komponentus, kurie nebuvo tiekiami rinkai, patikrinimą. Tinkamas išsamaus patikrinimo lygis priklauso nuo su konkrečiu komponentu susijusios kibernetinio saugumo rizikos pobūdžio ir lygio ir tuo tikslu turėtų atsižvelgti į vieną ar daugiau iš šių veiksmų: jei taikytina, patikrinti, ar komponento gamintojas įrodė atitiktį šiam reglamentui, be kita ko, patikrinant, ar komponentas jau paženklintas CE ženklu; patikrinti, ar komponentui reguliariai teikiami saugumo naujiniai, pavyzdžiui, tikrinant jo saugumo naujinių istoriją; patikrinti, ar komponentas neturi pažeidžiamumų, užregistruotų Europos pažeidžiamumo duomenų bazėje, sukurtoje pagal Direktyvos (ES) 2022/2555 12 straipsnio 2 dalį, arba kitose viešai prieinamose pažeidžiamumo duomenų bazėse arba atlikti papildomus saugumo patikrinimus. Šiame reglamente nustatytos pažeidžiamumo valdymo pareigos, kurių gamintojai turi laikytis pateikdami produktą su skaitmeniniais elementais rinkai ir palaikymo laikotarpiu, taikomos visiems produktams su skaitmeniniais elementais, įskaitant visus integruotus komponentus. Jei atlikdamas išsamų patikrinimą produkto su skaitmeniniais elementais gamintojas nustato komponento, įskaitant laisvosios ir atvirosios programinės įrangos komponentą, pažeidžiamumą, jis turėtų informuoti komponentą gaminantį ar techniškai prižiūrintį asmenį ar subjektą, išspręsti ir ištaisyti pažeidžiamumo problemą ir, kai taikytina, pateikti asmeniui ar subjektui taikomą saugumo sprendimą;

(35) iškart po šio reglamento taikymo pereinamojo laikotarpio produkto su skaitmeniniais elementais, į kurį integruotas vienas ar keli komponentai, gauti iš trečiųjų šalių, kurioms taip pat taikomas šis reglamentas, gamintojas, vykdydamas išsamaus patikrinimo pareigą, gali neturėti galimybės patikrinti, ar tų komponentų gamintojai įrodė atitiktį šiam reglamentui, pavyzdžiui, patikrinti, ar komponentai jau paženklinti CE ženklu. Taip gali būti tuo atveju, jeigu komponentai buvo integruoti prieš pradedant taikyti šį reglamentą tų komponentų gamintojams. Tokiu atveju gamintojas, integruojantis tokius komponentus, turėtų atlikti išsamų patikrinimą kitais būdais;

(36) kad produktai su skaitmeniniais elementais galėtų laisvai judėti vidaus rinkoje, jie turėtų būti ženklinami matomu, įskaitomu ir neištrinamu CE ženklu, rodančiu, 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. Be to, prekybos mugėse, parodose ir demonstracijose ar panašiuose renginiuose valstybės narės neturėtų trukdyti pristatyti ar naudoti produkto su skaitmeniniais elementais, kuris neatitinka šio reglamento, įskaitant produkto prototipus, jei tas produktas pateikiamas su matomu ženklu, aiškiai rodančiu, kad produktas neatitinka šio reglamento, ir kad jis nebus tiekiamas rinkai, kol neatitiks šio reglamento;

(37) siekiant užtikrinti, kad prieš atlikdami savo produktų su skaitmeniniais elementais atitikties vertinimą gamintojai galėtų išleisti programinę įrangą bandymo tikslais, valstybės narės neturėtų neleisti pateikti nebaigtos programinės įrangos, pavyzdžiui, alfa versijos, beta versijos ar kandidatinės versijos, su sąlyga, kad nebaigta programinė įranga pateikiama ne ilgesniam laikui nei būtina jai išbandyti 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;

(38) siekiant užtikrinti, kad rinkai pateikti produktai su skaitmeniniais elementais nekeltų kibernetinio saugumo rizikos asmenims ir organizacijoms, tokiems produktams turėtų būti nustatyti esminiai kibernetinio saugumo reikalavimai. Tie esminiai kibernetinio saugumo reikalavimai, įskaitant pažeidžiamumo valdymo reikalavimus, taikomi kiekvienam atskiram rinkai pateikiamam produktui su skaitmeniniais elementais, neatsižvelgiant į tai, ar produktas su skaitmeniniais elementais yra pagamintas kaip atskiras vienetas, ar serijiniu būdu. Pavyzdžiui, produkto rūšies atveju kiekvienas atskiras produktas su skaitmeniniais elementais turėtų būti gavęs visas saugumo pataisas arba naujinius, skirtus atitinkamoms saugumo problemoms spręsti, kai jis pateikiamas rinkai. Jei vėliau daromi produktų su skaitmeniniais elementais pakeitimai fizinėmis ar skaitmeninėmis priemonėmis gamintojo pradiniame rizikos vertinime nenumatytu būdu ir tai galėtų reikšti, kad produktai nebeatitinka atitinkamų esminių kibernetinio saugumo reikalavimų, pakeitimas turėtų būti laikomas esminiu. Pavyzdžiui, taisymai galėtų būti prilyginti techninės priežiūros operacijoms, jei jais nekeičiamas rinkai jau pateiktas produktas su skaitmeniniais elementais taip, kad galėtų būti paveiktas taikytinų reikalavimų laikymasis arba kad galėtų būti pakeista numatytoji paskirtis, dėl kurios produktas buvo įvertintas;

(39) 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 to produkto numatytąją paskirtį ir tie pakeitimai gamintojo nebuvo numatyti pradiniame rizikos vertinime arba kai dėl programinės įrangos naujinio pasikeitė pavojaus pobūdis arba padidėjo kibernetinio saugumo rizikos lygis, o atnaujinta produkto versija pateikiama rinkai. Jei saugumo naujinys, kuriuo siekiama sumažinti produkto su skaitmeniniais elementais kibernetinio saugumo riziką, nekeičia produkto su skaitmeniniais elementais numatytosios paskirties, jis nelaikomas esminiu pakeitimu. Tai paprastai apima atvejus, kai saugumo naujinys susijęs tik su nežymiais pirminio kodo pakeitimais. Pavyzdžiui, taip galėtų būti tuo atveju, kai saugumo naujiniu šalinamas žinomas pažeidžiamumas, be kita ko, keičiant produkto su skaitmeniniais elementais funkcijas ar veikimą, siekiant vienintelio tikslo – sumažinti kibernetinio saugumo rizikos lygį. Panašiai nedidelis funkcijų naujinys, pavyzdžiui, naudotojo sąsajos vizualinis patobulinimas arba naujų piktogramų ar kalbų įtraukimas į ją, paprastai neturėtų būti laikomas esminiu pakeitimu. Ir atvirkščiai – jei funkcijų naujiniu keičiamos pirminės numatytos funkcijos arba produkto su skaitmeniniais elementais rūšis ar veikimas ir jis atitinka anksčiau minėtus kriterijus, jis turėtų būti laikomas esminiu pakeitimu, nes naujų funkcijų įtraukimas paprastai lemia platesnį atakos perimetrą ir taip padidina kibernetinio saugumo riziką. Pavyzdžiui, taip galėtų būti tuo atveju, kai į taikomąją programą įtraukiamas naujas įvesties elementas, dėl kurio gamintojas turi užtikrinti tinkamą įvesties patvirtinimą. Vertinant, ar funkcijos naujinys laikomas esminiu pakeitimu, nesvarbu, ar jis pateikiamas kaip atskiras naujinys, ar kartu su saugumo naujiniu. Komisija turėtų paskelbti gaires, kaip nustatyti, kas yra esminis pakeitimas;

(40) atsižvelgiant į kartotinį programinės įrangos kūrimo pobūdį, gamintojai, pateikę rinkai vėlesnes programinės įrangos produkto versijas dėl vėlesnio esminio to produkto pakeitimo, palaikymo laikotarpiu turėtų galėti teikti saugumo naujinius tik naujausiai rinkai pateiktai programinės įrangos produkto versijai. Jie turėtų turėti galimybę tai daryti tik tuo atveju, jei atitinkamų ankstesnių produkto versijų naudotojai turi galimybę nemokamai naudotis naujausia rinkai pateikta versija ir nepatiria papildomų išlaidų, susijusių su aparatinės ar programinės įrangos aplinkos, kurioje jie naudoja produktą, pritaikymu. Taip galėtų būti, pavyzdžiui, tais atvejais, kai stalinio kompiuterio operacinei sistemai atnaujinti nereikia naujos aparatinės įrangos, pavyzdžiui, greitesnio centrinio procesoriaus ar daugiau atminties. Nepaisant to, palaikymo laikotarpiu gamintojas turėtų toliau laikytis kitų pažeidžiamumo valdymo reikalavimų, pavyzdžiui, taikyti koordinuoto pažeidžiamumų atskleidimo politiką arba priemones, kuriomis būtų sudaromos palankesnės sąlygos dalytis informacija apie galimą visų vėlesnių iš esmės pakeistų programinės įrangos produkto versijų, pateiktų rinkai, pažeidžiamumą. Gamintojai turėtų turėti galimybę atlikti nedidelius saugumo arba funkcijų naujinius, kurie nelaikomi esminiu pakeitimu, tik naujausiai programinės įrangos produkto, kuris nebuvo iš esmės pakeistas, versijai ar subversijai. Tuo pačiu metu, jeigu aparatinės įrangos produktas, pavyzdžiui, išmanusis telefonas, yra nesuderinamas su naujausia operacinės sistemos, su kuria jis iš pradžių buvo pristatytas, versija, gamintojas palaikymo laikotarpiu turėtų toliau teikti saugumo naujinius bent jau naujausiai suderinamai operacinės sistemos versijai;

(41) atsižvelgiant į visuotinai nusistovėjusią Sąjungos derinamaisiais teisės aktais reglamentuojamų produktų esminio pakeitimo koncepciją, jeigu įvyksta esminis pakeitimas, galintis turėti įtakos produkto su skaitmeniniais elementais atitikčiai šio reglamento reikalavimams arba kai pasikeičia to produkto numatytoji paskirtis, tikslinga patikrinti produkto su skaitmeniniais elementais atitiktį ir, jei taikytina, atlikti naują atitikties vertinimą. Kai taikytina, jei gamintojas atlieka atitikties vertinimą, kuriame dalyvauja trečioji šalis, tai trečiajai šaliai turėtų būti pranešta apie pakeitimą, dėl kurio gali atsirasti esminis pakeitimas;

(42) jei produktui su skaitmeniniais elementais taikomas atnaujinimas, techninė priežiūra ir taisymas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2024/1781[18] 2 straipsnio 18, 19 ir 20 punktuose, tai nebūtinai reiškia esminį produkto pakeitimą, pavyzdžiui, jei numatytoji paskirtis nepasikeičia ir funkcijos bei rizikos lygis lieka nepakitę. Tačiau gamintojo atliekamas produkto su skaitmeniniais elementais atnaujinimas gali reikšti produkto projektavimo ir kūrimo pokyčius, todėl gali turėti įtakos jo numatytajai paskirčiai ir atitikčiai šiame reglamente nustatytiems reikalavimams;

---

18 2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1781, kuriuo nustatoma tvarių gaminių ekologinio projektavimo reikalavimų nustatymo sistema, iš dalies keičiami Direktyva (ES) 2020/1828 bei Reglamentas (ES) 2023/1542 ir panaikinama Direktyva 2009/125/EB (OL L, 2024/1781, 2024 6 28, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

(43) produktai su skaitmeniniais elementais turėtų būti laikomi svarbiais, jei neigiamas potencialių produkto pažeidžiamumų išnaudojimo poveikis gali būti didelis taip pat dėl su kibernetiniu saugumu susijusių funkcijų arba funkcijos, dėl kurios kyla didelė neigiamo poveikio rizika, susijusi su jos intensyvumu ir gebėjimu sutrikdyti, kontroliuoti arba padaryti žalos dideliam skaičiui kitų produktų su skaitmeniniais elementais arba jo naudotojų sveikatai, saugumui ar saugai per tiesioginę manipuliaciją, pavyzdžiui, centrinės sistemos funkciją, įskaitant tinklo administravimą, konfigūracijos kontrolę, virtualizavimą arba asmens duomenų tvarkymą. Visų pirma, produktų su skaitmeniniais elementais, kurie turi su kibernetiniu saugumu susijusių funkcijų, pavyzdžiui, sistemos paleidimo tvarkykles, pažeidžiamumai gali sukelti saugumo problemų išplitimą visoje tiekimo grandinėje. Incidento poveikis taip pat gali padidėti, jei produktas pagrindinai atlieka centrinės sistemos funkciją, įskaitant tinklo administravimą, konfigūracijos kontrolę, virtualizavimą ar asmens duomenų tvarkymą;

(44) tam tikrų kategorijų produktams su skaitmeniniais elementais turėtų būti taikomos griežtesnės atitikties vertinimo procedūros, tačiau ir toliau turėtų būti taikomas proporcingumo principas. Tuo tikslu svarbūs produktai su skaitmeniniais elementais turėtų būti suskirstyti į dvi klases, atspindinčias kibernetinio saugumo rizikos lygį, susijusį su tų kategorijų produktais. Incidentas, susijęs su svarbiais produktais su skaitmeniniais elementais, priskiriamais II klasei, galėtų sukelti didesnį neigiamą poveikį nei incidentas, susijęs su svarbiais produktais su skaitmeniniais elementais, priskiriamais I klasei, pavyzdžiui, dėl jų su kibernetiniu saugumu susijusios funkcijos pobūdžio arba kitos funkcijos, dėl kurios kyla didelė neigiamo poveikio rizika, atlikimo. Tokio didesnio neigiamo poveikio požymis – tai, kad II klasei priskiriami produktai su skaitmeniniais elementais gali atlikti su kibernetiniu saugumu susijusias funkcijas arba kitą funkciją, dėl kurios kyla didelė neigiamo poveikio rizika, kuri yra didesnė nei I klasės produktų atveju, arba atitikimas abiem pirmiau nurodytiems kriterijams. Todėl II klasei priskiriamiems svarbiems produktams su skaitmeniniais elementais turėtų būti taikoma griežtesnė atitikties vertinimo procedūra;

(45) šiame reglamente nurodyti svarbūs produktai su skaitmeniniais elementais turėtų būti suprantami kaip produktai, turintys pagrindines šiame reglamente nustatytos svarbių produktų su skaitmeniniais elementais kategorijos funkcijas. Pavyzdžiui, šiame reglamente nustatomos svarbių produktų su skaitmeniniais elementais kategorijos, kurios pagal savo pagrindines funkcijas apibrėžiamos kaip užkardos arba įsibrovimo aptikimo ar prevencijos sistemos, priskiriamos II klasei. Todėl turi būti privalomai atliekamas užkardų ir įsibrovimo aptikimo ar prevencijos sistemų atitikties trečiosios šalies atliekamas vertinimas. Tai netaikoma kitiems produktams su skaitmeniniais elementais, nepriskiriamiems prie svarbių produktų su skaitmeniniais elementais, į kuriuos gali būti integruotos užkardos arba įsibrovimo aptikimo ar prevencijos sistemos. Komisija turėtų priimti įgyvendinimo aktą, kuriuo būtų patikslintas svarbių produktų su skaitmeniniais elementais kategorijų, priskiriamų I ir II klasėms, kaip nustatyta šiame reglamente, techninis aprašymas;

(46) šiame reglamente nustatytos ypatingos svarbos produktų su skaitmeniniais elementais kategorijos turi su kibernetiniu saugumu susijusias funkcijas ir atlieka funkciją, dėl kurios kyla didelė neigiamo poveikio rizika, susijusi su jos intensyvumu ir gebėjimu tiesioginėmis manipuliacijomis sutrikdyti, kontroliuoti arba padaryti žalos dideliam skaičiui kitų produktų su skaitmeniniais elementais. Be to, laikoma, kad esminiai subjektai, nurodyti Direktyvos (ES) 2022/2555 3 straipsnio 1 dalyje, yra kritiškai priklausomi nuo tų kategorijų produktų su skaitmeniniais elementais. Šio reglamento priede nurodytoms ypatingos svarbos produktų su skaitmeniniais elementais kategorijoms dėl jų ypatingos svarbos jau plačiai taikomos įvairios sertifikavimo formos, ir joms taip pat taikoma Europos bendraisiais kriterijais grindžiama kibernetinio saugumo sertifikavimo schema (toliau - EKSS), nustatyta Komisijos įgyvendinimo reglamentu (ES) 2024/482[19]. Todėl, siekiant užtikrinti bendrą tinkamą ypatingos svarbos produktų su skaitmeniniais elementais kibernetinio saugumo apsaugą Sąjungoje, galėtų būti tinkama ir proporcinga deleguotuoju aktu tokių kategorijų produktams taikyti privalomą Europos kibernetinio saugumo sertifikavimą, kai jau įdiegta tuos produktus apimanti atitinkama Europos kibernetinio saugumo sertifikavimo schema, o Komisija atliko numatomo privalomo sertifikavimo galimo poveikio rinkai vertinimą. Atliekant tą vertinimą turėtų būti apsvarstyti ir pasiūlos, ir paklausos aspektai, įskaitant tai, ar yra pakankama atitinkamų produktų su skaitmeniniais elementais paklausa tiek iš valstybių narių, tiek iš naudotojų pusės, kad būtų reikalaujama Europos kibernetinio saugumo sertifikavimo, taip pat į tikslus, kuriems ketinama naudoti produktus su skaitmeniniais elementais, be kita ko, Direktyvos (ES) 2022/2555 3 straipsnio 1 dalyje nurodytų esminių subjektų kritinę priklausomybę nuo tų produktų. Vertinime taip pat turėtų būti analizuojamas galimas privalomo sertifikavimo poveikis tų produktų prieinamumui vidaus rinkoje ir valstybių narių pajėgumai bei pasirengimas įgyvendinti atitinkamas Europos kibernetinio saugumo sertifikavimo schemas;

---

[19] 2024 m. sausio 31 d. Komisijos įgyvendinimo reglamentas (ES) 2024/482, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo (OL L, 2024/482, 2024 2 7, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(47) deleguotuosiuose aktuose, kuriais reikalaujama privalomo Europos kibernetinio saugumo sertifikavimo, turėtų būti nustatyti produktai su skaitmeniniais elementais, turintys pagrindinę šiame reglamente nustatytos ypatingos svarbos produktų su skaitmeniniais elementais kategorijos funkciją, kuriems turi būti taikomas privalomas sertifikavimas, taip pat reikalaujamas saugumo užtikrinimo lygis, kuris turėtų būti bent pakankamai aukštas. Reikalaujamas saugumo užtikrinimo lygis turėtų būti proporcingas su produktu su skaitmeniniais elementais susijusios kibernetinio saugumo rizikos lygiui. Pavyzdžiui, kai produktas su skaitmeniniais elementais turi pagrindinę šiame reglamente nustatytos ypatingos svarbos produktų su skaitmeniniais elementais kategorijos funkciją ir yra skirtas naudoti jautrioje ar ypatingos svarbos aplinkoje, pavyzdžiui, produktų, skirtų naudoti Direktyvos (ES) 2022/2555 3 straipsnio 1 dalyje nurodytiems esminiams subjektams, atveju, gali būti reikalaujama aukščiausio saugumo užtikrinimo lygio;

(48) siekiant užtikrinti bendrą tinkamą produktų su skaitmeniniais elementais, kurie turi pagrindinę šiame reglamente nustatytos ypatingos svarbos produktų su skaitmeniniais elementais kategorijos funkciją, kibernetinio saugumo apsaugą Sąjungoje, Komisijai taip pat turėtų būti suteikti įgaliojimai priimti deleguotuosius aktus, siekiant iš dalies pakeisti šį reglamentą, įtraukiant ypatingos svarbos produktų su skaitmeniniais elementais kategorijas arba pašalinant esamas tokių produktų kategorijas, kurių gamintojams, siekiant įrodyti atitiktį šiam reglamentui, galėtų būti taikomas reikalavimas gauti Europos kibernetinio saugumo sertifikatą pagal Europos kibernetinio saugumo sertifikavimo schemą, laikantis Reglamento (ES) 2019/881. Į tas kategorijas gali būti įtraukta nauja ypatingos svarbos produktų su skaitmeniniais elementais kategorija, jei nuo tokių produktų yra kritiškai priklausomi Direktyvos (ES) 2022/2555 3 straipsnio 1 dalyje nurodyti esminiai subjektai, arba, incidentų poveikio arba pažeidžiamumų, kuriuos galima išnaudoti, egzistavimo atvejais tai galėtų sutrikdyti ypatingos svarbos tiekimo grandines. Vertindama poreikį deleguotuoju aktu įtraukti arba pašalinti esamas ypatingos svarbos produktų su skaitmeniniais elementais kategorijas, Komisija turėtų galėti atsižvelgti į tai, ar valstybės narės nacionaliniu lygmeniu yra nustačiusios produktus su skaitmeniniais elementais, kurie atlieka itin svarbų vaidmenį užtikrinant Direktyvos (ES) 2022/2555 3 straipsnio 1 dalyje nurodytų esminių subjektų atsparumą ir kurie vis dažniau susiduria su tiekimo grandinės kibernetiniais išpuoliais, kurie gali turėti didelį trikdomąjį poveikį. Be to, Komisija turėtų galėti atsižvelgti į Sąjungos lygmeniu koordinuojamo ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimo, atlikto pagal Direktyvos (ES) 2022/2555 22 straipsnį, rezultatus;

(49) Komisija turėtų užtikrinti, kad rengiant šio reglamento įgyvendinimo priemones būtų struktūruotai ir reguliariai konsultuojamasi su įvairiais atitinkamais suinteresuotaisiais subjektais. Tai visų pirma turėtų būti daroma tais atvejais, kai Komisija vertina poreikį galimai atnaujinti svarbių ar ypatingos svarbos produktų su skaitmeniniais elementais kategorijų sąrašus, kai turėtų būti konsultuojamasi su atitinkamais gamintojais ir atsižvelgiama į jų nuomonę, siekiant išanalizuoti kibernetinio saugumo riziką, taip pat tokių produktų kategorijų priskyrimo svarbių ar ypatingos svarbos produktų kategorijai sąnaudų ir naudos pusiausvyrą;

(50) šiuo reglamentu tikslingai siekiama spręsti kibernetinio saugumo riziką. Tačiau produktai su skaitmeniniais elementais gali kelti ir kitą saugumo riziką, kuri gali būti ne visada susijusi su kibernetiniu saugumu, bet gali atsirasti dėl saugumo pažeidimų. Ta rizika turėtų ir toliau būti reglamentuojama atitinkamais kitais nei šis reglamentas Sąjungos derinamaisiais teisės aktais. Jei netaikomi jokie kiti Sąjungos derinamieji teisės aktai, išskyrus šį reglamentą, turėtų būti taikomas Europos Parlamento ir Tarybos reglamentas (ES) 2023/988[20]. Todėl, atsižvelgiant į tikslinį šio reglamento pobūdį, nukrypstant nuo Reglamento (ES) 2023/988 2 straipsnio 1 dalies trečios pastraipos b punkto, Reglamento (ES) 2023/988 III skyriaus 1 skirsnis, V ir VII skyriai ir IX–XI skyriai turėtų būti taikomi produktams su skaitmeniniais elementais, atsižvelgiant į saugumo riziką, kurios šis reglamentas neapima, jei tiems produktams netaikomi konkretūs reikalavimai, nustatyti kituose nei šis reglamentas Sąjungos derinamuosiuose teisės aktuose, kaip tai suprantama Reglamento (ES) 2023/988 3 straipsnio 27 punkte;

---

[20] 2023 m. gegužės 10 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/988 dėl bendros gaminių saugos, kuriuo iš dalies keičiami Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1025/2012 bei Europos Parlamento ir Tarybos direktyva (ES) 2020/1828 ir panaikinamos Europos Parlamento ir Tarybos direktyva 2001/95/EB bei Tarybos direktyva 87/357/EEB (OL L 135, 2023 5 23, p. 1).

(51) produktai su skaitmeniniais elementais, pagal Europos Parlamento ir Tarybos reglamento (ES) 2024/1689[21] 6 straipsnį priskirti didelės rizikos DI sistemoms, kurios patenka į šio reglamento taikymo sritį, turėtų atitikti šiame reglamente nustatytus esminius kibernetinio saugumo reikalavimus. Kai tos didelės rizikos DI sistemos atitinka šiame reglamente nustatytus esminius kibernetinio saugumo reikalavimus, jos turėtų būti laikomos atitinkančiomis Reglamento (ES) 2024/1689 15 straipsnyje nustatytus kibernetinio saugumo reikalavimus tiek, kiek tuos reikalavimus apima pagal šį reglamentą rengiama ES atitikties deklaracija arba jos dalys. Tuo tikslu kibernetinio saugumo rizikų, susijusių su produktu su skaitmeniniais elementais, kuris pagal Reglamentą (ES) 2024/1689 priskiriamas didelės rizikos DI sistemos kategorijai, vertinime, į kurį turi būti atsižvelgiama tokio produkto planavimo, projektavimo, kūrimo, gamybos, pateikimo ir techninės priežiūros etapais, kaip reikalaujama pagal šį reglamentą, turėtų būti atsižvelgiama į riziką DI sistemos kibernetiniam atsparumui, susijusią su leidimo neturinčių trečiųjų šalių bandymais pakeisti jos naudojimą, elgseną ar veikimą, įskaitant konkrečius su DI susijusius pažeidžiamumus, pavyzdžiui, duomenų užkrėtimą arba priešiškas atakas, taip pat, kai taikytina, riziką pagrindinėms teisėms, pagal Reglamentą (ES) 2024/1689. Kalbant apie atitikties vertinimo procedūras, susijusias su esminiais kibernetinio saugumo reikalavimais produktui su skaitmeniniais elementais, kuris patenka į šio reglamento taikymo sritį ir kuris priskiriamas prie didelės rizikos DI sistemų, kaip taisyklė, turėtų būti taikomas Reglamento (ES) 2024/1689 43 straipsnis vietoje atitinkamų šio reglamento nuostatų.

---

[21] 2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1689, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas) (OL L 2024/1689, 2024 7 12, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Tačiau dėl tos taisyklės neturėtų sumažėti būtinas svarbių ar ypatingos svarbos produktų su skaitmeniniais elementais, kaip nurodyta šiame reglamente, užtikrinimo lygis. Todėl, nukrypstant nuo tos taisyklės, didelės rizikos DI sistemoms, kurios patenka į Reglamento (ES) 2024/1689 taikymo sritį ir kurios laikomos svarbiais ar ypatingos svarbos produktais su skaitmeniniais elementais, kaip nurodyta šiame reglamente, ir kurioms taikoma Reglamento (ES) 2024/1689 VI priede nurodyta vidaus kontrole pagrįsto atitikties vertinimo procedūra, turėtų būti taikomas šiame reglamente numatytas atitikties vertinimas tiek, kiek tai susiję su šiame reglamente nustatytais esminiais kibernetinio saugumo reikalavimais. Tokiu atveju visais kitais aspektais, kuriuos apima Reglamentas (ES) 2024/1689, turėtų būti taikomos atitinkamos to reglamento VI priede nustatytos vidaus kontrole pagrįsto atitikties vertinimo nuostatos;

(52) siekiant pagerinti vidaus rinkai pateikiamų produktų su skaitmeniniais elementais saugumą, būtina nustatyti tokiems produktams taikomus esminius kibernetinio saugumo reikalavimus. Tie esminiai kibernetinio saugumo reikalavimai neturėtų daryti poveikio Sąjungos lygmeniu koordinuotiems ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimams, nustatytiems Direktyvos (ES) 2022/2555 22 straipsnyje, per kuriuos atsižvelgiama tiek į techninius ir, jei svarbu, tiek į netechninius rizikos veiksnius, kaip antai nederama trečiosios šalies įtaka tiekėjams. Be to, jais neturėtų būti daromas poveikis valstybių narių prerogatyvoms nustatyti papildomus reikalavimus, kuriais būtų atsižvelgiama į netechninius veiksnius, siekiant užtikrinti aukštą atsparumo lygį, įskaitant apibrėžtus Komisijos rekomendacijoje (ES) 2019/534[22], ES koordinuojamame 5G tinklų kibernetinio saugumo rizikos vertinime ir ES priemonių rinkinyje dėl 5G kibernetinio saugumo, dėl kurio susitarė pagal Direktyvos (ES) 2022/2555 14 straipsnį įsteigta Bendradarbiavimo grupė;

[22] 2019 m. kovo 26 d. Komisijos rekomendacija (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo (OL L 88, 2019 3 29, p. 42).

(53) produktų, kuriems taikomas Europos Parlamento ir Tarybos reglamentas (ES) 2023/1230[23] ir kurie taip pat yra produktai su skaitmeniniais elementais, kaip tai suprantama šiame reglamente, gamintojai turėtų laikytis ir šiame reglamente nustatytų esminių kibernetinio saugumo reikalavimų, ir Reglamente (ES) 2023/1230 nustatytų esminių sveikatos ir saugos reikalavimų. Šiame reglamente nustatytais esminiais kibernetinio saugumo reikalavimais ir tam tikrais esminiais Reglamente (ES) 2023/1230 nustatytais reikalavimais gali būti mažinama panaši kibernetinio saugumo rizika. Todėl laikantis šiame reglamente nustatytų esminių kibernetinio saugumo reikalavimų galėtų būti lengviau laikytis Reglamente (ES) 2023/1230 nustatytų esminių reikalavimų, kurie taip pat apima tam tikrą kibernetinio saugumo riziką, visų pirma to reglamento III priedo 1.1.9 ir 1.2.1 skirsniuose nustatytų reikalavimų, susijusių su apsauga nuo sugadinimo ir valdymo sistemų sauga ir patikimumu. Tokią sinergiją turi įrodyti gamintojas, pavyzdžiui, taikydamas darniuosius standartus ar kitas technines specifikacijas, kai jų yra, apimančius atitinkamus esminius kibernetinio saugumo reikalavimus, atlikus rizikos vertinimą, apimantį tą kibernetinio saugumo riziką. Gamintojas taip pat turėtų laikytis šiame reglamente ir Reglamente (ES) 2023/1230 nustatytų taikytinų atitikties vertinimo procedūrų. Komisija ir Europos standartizacijos organizacijos, atlikdamos parengiamąjį darbą, kuriuo remiamas šio reglamento ir Reglamento (ES) 2023/1230 įgyvendinimas ir susiję standartizacijos procesai, turėtų skatinti nuoseklumą vertinant kibernetinio saugumo riziką ir nustatant, kaip tai rizikai turi būti taikomi darnieji standartai, atsižvelgiant į atitinkamus esminius reikalavimus.

---

[23] 2023 m. birželio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/1230 dėl mašinų, kuriuo iš dalies panaikinama Europos Parlamento ir Tarybos direktyva 2006/42/EB ir Tarybos direktyva 73/361/EEB (OL L 165, 2023 6 29, p. 1).

Visų pirma, Komisija ir Europos standartizacijos organizacijos, rengdamos ir plėtodamos darniuosius standartus, turėtų atsižvelgti į šį reglamentą, kad būtų lengviau įgyvendinti Reglamentą (ES) 2023/1230, visų pirma kiek tai susiję su to reglamento III priedo 1.1.9 ir 1.2.1 skirsniuose nustatytais kibernetinio saugumo aspektais, susijusiais su apsauga nuo sugadinimo ir valdymo sistemų sauga ir patikimumu. Komisija turėtų pateikti gaires, kad padėtų gamintojams, kuriems taikomas šis reglamentas ir taip pat Reglamentas (ES) 2023/1230, visų pirma siekiant sudaryti palankesnes sąlygas įrodyti atitiktį atitinkamiems esminiams reikalavimams, nustatytiems šiame reglamente ir Reglamente (ES) 2023/1230;

(54) siekiant užtikrinti, kad produktai su skaitmeniniais elementais būtų saugūs tiek jų pateikimo rinkai metu, tiek per laikotarpį, kurį numatoma naudoti produktą su skaitmeniniais elementais, būtina nustatyti esminius kibernetinio saugumo reikalavimus, susijusius su pažeidžiamumų valdymu, ir esminius kibernetinio saugumo reikalavimus, susijusius su produktų su skaitmeniniais elementais savybėmis. Nors gamintojai turėtų laikytis visų esminių kibernetinio saugumo reikalavimų, susijusių su pažeidžiamumų valdymu, per visą palaikymo laikotarpį, jie turėtų nustatyti, kurie kiti su produkto savybėmis susiję esminiai kibernetinio saugumo reikalavimai yra svarbūs produkto su atitinkamais skaitmeniniais elementais tipui. Tuo tikslu gamintojai turėtų atlikti kibernetinio saugumo rizikos, susijusios su produktu su skaitmeniniais elementais, vertinimą, kad nustatytų atitinkamą riziką ir atitinkamus esminius kibernetinio saugumo reikalavimus, kad jų produktai su skaitmeniniais elementais būtų tiekiami be žinomų išnaudojamų pažeidžiamumų, kurie galėtų turėti įtakos tų gaminių saugumui, ir būtų deramai taikomi tinkami darnieji standartai, bendrosios specifikacijos arba Europos ar tarptautiniai standartai;

(55) jei produktui su skaitmeniniais elementais netaikomi tam tikri esminiai kibernetinio saugumo reikalavimai, gamintojas į kibernetinio saugumo rizikos vertinimą, įtrauktą į techninius dokumentus, turėtų įtraukti aiškų pagrindimą. Taip galėtų būti tuo atveju, kai esminis kibernetinio saugumo reikalavimas yra nesuderinamas su produkto su skaitmeniniais elementais pobūdžiu. Pavyzdžiui, dėl produkto su skaitmeniniais elementais numatytosios paskirties gali būti, kad gamintojui reikia laikytis plačiai pripažintų sąveikumo standartų, net jei jo saugumo savybės nebelaikomos pažangiausiomis. Panašiai kitais Sąjungos teisės aktais reikalaujama, kad gamintojai taikytų konkrečius sąveikumo reikalavimus. Jei esminis kibernetinio saugumo reikalavimas produktui su skaitmeniniais elementais netaikomas, tačiau gamintojas nustatė su tuo esminiu kibernetinio saugumo reikalavimu susijusią kibernetinio saugumo riziką, jis turėtų imtis priemonių tai rizikai sumažinti kitomis priemonėmis, pavyzdžiui, apribojant gaminio numatytąją paskirtį, kad jis būtų naudojamas tik patikimoje aplinkoje, arba informuodamas naudotojus apie tą riziką;

(56) viena iš svarbiausių priemonių, kurių naudotojai turi imtis, kad nuo kibernetinių išpuolių apsaugotų savo produktus su skaitmeniniais elementais, yra kuo greičiau įdiegti naujausius turimus saugumo naujinius. Todėl gamintojai turėtų projektuoti savo gaminius ir įdiegti procesus taip, kad būtų užtikrinta, jog produktai su skaitmeniniais elementais turėtų funkcijas, leidžiančias automatiškai pranešti apie saugumo naujinius, juos platinti, atsisiųsti ir įdiegti, visų pirma, vartojimo gaminių atveju. Jie taip pat turėtų suteikti galimybę patvirtinti saugumo naujinių atsisiuntimą ir įdiegimą kaip galutinį etapą. Naudotojai turėtų išlaikyti galimybę išjungti automatinius naujinius naudojant aiškų ir lengvai naudojamą mechanizmą, kurį papildo aiškios instrukcijos, kaip naudotojai gali atsisakyti automatinių naujinių. Šio reglamento priede nustatyti reikalavimai, susiję su automatiniais naujiniais, netaikomi produktams su skaitmeniniais elementais, kurie visų pirma yra skirti būti integruotais į kitus gaminius kaip komponentai. Jie taip pat netaikomi produktams su skaitmeniniais elementais, kurių naudotojai pagrįstai nesitiki automatinių atnaujinimų, įskaitant produktus su skaitmeniniais elementais, skirtus naudoti profesionaliuose IRT tinkluose, ypač ypatingos svarbos ir pramoninėje aplinkose, kuriose automatinis atnaujinimas galėtų trukdyti veiklai. Nepriklausomai nuo to, ar produktas su skaitmeniniais elementais sukurtas taip, kad gautų automatinius naujinius, ar ne, jo gamintojas turėtų informuoti naudotojus apie pažeidžiamumą ir nedelsdamas pateikti saugumo naujinius. Jei produktas su skaitmeniniais elementais turi naudotojo sąsają arba panašias technines priemones, leidžiančias tiesioginę sąveiką su jo naudotojais, gamintojas turėtų naudotis tokiomis funkcijomis, kad informuotų naudotojus, kai baigiasi jų produkto su skaitmeniniais elementais palaikymo laikotarpis. Pranešimai turėtų apsiriboti tik tuo, kas būtina siekiant užtikrinti veiksmingą šios informacijos gavimą, ir neturėtų daryti neigiamo poveikio naudotojų patirčiai, susijusiai su produktu su skaitmeniniais elementais;

(57) siekiant padidinti pažeidžiamumo tvarkymo procesų skaidrumą ir užtikrinti, kad nebūtų reikalaujama, jog naudotojai diegtų naujus funkcijų naujinius vien tam, kad gautų naujausius saugumo naujinius, gamintojai turėtų užtikrinti, kai tai techniškai įmanoma, kad nauji saugumo naujiniai būtų teikiami atskirai nuo funkcijų naujinių;

(58) 2023 m. birželio 20 d. Komisijos ir Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai bendrame komunikate „Europos ekonominio saugumo strategija“ nurodyta, kad Sąjunga turi kuo labiau padidinti savo ekonominio atvirumo naudą ir kartu kuo labiau sumažinti riziką, dėl ekonominės priklausomybės kylančią didelės rizikos pardavėjams, taikydama bendrą strateginę ekonominio saugumo sistemą. Priklausomybė nuo didelės rizikos produktų su skaitmeniniais elementais tiekėjų gali kelti strateginę riziką, kuri turi sprendžiama Sąjungos lygmeniu, ypač jei produktai su skaitmeniniais elementais yra skirti Direktyvos (ES) 2022/2555 3 straipsnio 1 dalyje nurodytų esminių subjektų naudojimui. Tokia rizika, be kita ko, gali būti susijusi su gamintojui taikoma jurisdikcija, jo įmonės nuosavybės ypatybėmis ir kontrolės sąsajomis su trečiosios valstybės, kurioje jis yra įsisteigęs, vyriausybe, visų pirma tais atvejais, kai trečioji valstybė vykdo pramoninį šnipinėjimą arba vykdo neatsakingą valstybinę veiklą kibernetinėje erdvėje ir jos teisės aktais leidžiama savavališkai susipažinti su bet kokia įmonės veikla ar duomenimis, įskaitant neskelbtinus komercinius duomenis, ir gali būti nustatytos pareigos žvalgybos tikslais be demokratinės stabdžių ir atsvarų sistemos, priežiūros mechanizmų, tinkamo proceso ar teisės pateikti skundą nepriklausomam teismui arba tribunolui. Nustatant kibernetinio saugumo rizikos, kaip tai suprantama šiame reglamente, dydį, Komisija ir rinkos priežiūros institucijos, vykdydamos šiame reglamente nustatytas savo pareigas, taip pat turėtų apsvarstyti netechninius rizikos veiksnius, visų pirma tuos, kurie buvo nustatyti pagal Direktyvos (ES) 2022/2555 22 straipsnį atlikus Sąjungos lygmens koordinuotus ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimus;

(59) siekiant užtikrinti produktų su skaitmeniniais elementais saugumą po jų pateikimo rinkai, gamintojai turėtų nustatyti palaikymo laikotarpį, kuris turėtų atspindėti numatomą produkto su skaitmeniniais elementais naudojimo laiką. Nustatydamas palaikymo laikotarpį, gamintojas turėtų visų pirma atsižvelgti į pagrįstus naudotojų lūkesčius, produkto pobūdį, taip pat į atitinkamus Sąjungos teisės aktus, pagal kuriuos nustatoma produktų su skaitmeniniais elementais naudojimo trukmė. Gamintojai taip pat turėtų turėti galimybę atsižvelgti į kitus svarbius veiksnius. Kriterijai turėtų būti taikomi taip, kad nustatant palaikymo laikotarpį būtų užtikrintas proporcingumas. Gamintojas, gavęs prašymą, turėtų pateikti rinkos priežiūros institucijoms informaciją, į kurią buvo atsižvelgta nustatant produkto su skaitmeniniais elementais palaikymo laikotarpį;

(60) palaikymo laikotarpis, kuriuo gamintojas užtikrina veiksmingą pažeidžiamumų valdymą, turėtų būti ne trumpesnis kaip penkeri metai, išskyrus atvejus, kai produkto su skaitmeniniais elementais naudojimo trukmė yra trumpesnė nei penkeri metai – tokiu atveju gamintojas turėtų užtikrinti pažeidžiamumo valdymą per tą naudojimo trukmę. Tais atvejais, kai pagrįstai tikimasi, kad produktas su skaitmeniniais elementais bus naudojamas ilgiau nei penkerius metus, kaip dažnai būna aparatinės įrangos komponentų, pavyzdžiui, pagrindinių plokščių ar mikroprocesorių, tinklo prietaisų, pavyzdžiui, maršruto parinktuvų, modemų ar perjungiklių, taip pat programinės įrangos, pavyzdžiui, operacinių sistemų ar vaizdo redagavimo priemonių, atveju, gamintojai turėtų atitinkamai užtikrinti ilgesnius palaikymo laikotarpius. Visų pirma, produktai su skaitmeniniais elementais, skirti naudoti pramoninėje aplinkoje, pavyzdžiui, pramoninės kontrolės sistemos, dažnai naudojami daug ilgesnį laiką. Gamintojas turėtų galėti nustatyti trumpesnį nei penkerių metų palaikymo laikotarpį tik tuo atveju, jei tai pateisinama atitinkamo produkto su skaitmeniniais elementais pobūdžiu ir kai numatoma, kad tas produktas bus naudojamas trumpiau nei penkerius metus – tokiu atveju palaikymo laikotarpis turėtų atitikti numatomą naudojimo laikotarpį. Pavyzdžiui, sąlytį turėjusių asmenų atsekimo programėlės, skirtos naudoti pandemijos metu, naudojimo trukmė galėtų būti apribota tik pandemijos laikotarpiu. Be to, kai kurios taikomosios programos dėl savo pobūdžio gali būti prieinamos tik taikant prenumeratos modelį, visų pirma jeigu pasibaigus prenumeratos galiojimui taikomoji programa tampa neprieinama naudotojui ir todėl ji tampa nebenaudojama;

(61) tais atvejais, kai produktų su skaitmeniniais elementais palaikymo laikotarpiai baigia galioti, siekiant užtikrinti, kad pažeidžiamumus būtų galima pašalinti ir pasibaigus palaikymo laikotarpiui, gamintojai turėtų apsvarstyti galimybę tokių produktų su skaitmeniniais elementais pirminį kodą perduoti kitoms įmonėms, kurios įsipareigoja teikti pažeidžiamumo valdymo paslaugas, arba visuomenei. Kai gamintojai pirminį kodą perduoda kitoms įmonėms, jie turėtų turėti galimybę apsaugoti produkto su skaitmeniniais elementais nuosavybę ir užkirsti kelią pirminio kodo sklaidai visuomenei, pavyzdžiui, sudarydami sutartimi įformintus susitarimus;

(62) siekiant užtikrinti, kad gamintojai visoje Sąjungoje nustatytų panašius palaikymo laikotarpius panašiems produktams su skaitmeniniais elementais, administracinio bendradarbiavimo grupė turėtų skelbti statistinius duomenis apie vidutinius palaikymo laikotarpius, kuriuos gamintojai nustatė tam tikrų kategorijų produktams su skaitmeniniais elementais, ir paskelbti gaires, kuriose būtų nurodyti tinkami tokių kategorijų produktų palaikymo laikotarpiai. Be to, siekiant užtikrinti suderintą požiūrį visoje vidaus rinkoje, Komisija turėtų turėti galimybę priimti deleguotuosius aktus, kuriais būtų nustatyti minimalūs konkrečių kategorijų gaminių palaikymo laikotarpiai, kai iš rinkos priežiūros institucijų pateiktų duomenų matyti, kad gamintojų nustatyti palaikymo laikotarpiai sistemingai neatitinka palaikymo laikotarpių nustatymo kriterijų, nustatytų šiame reglamente, arba kad gamintojai skirtingose valstybėse narėse nepagrįstai nustato skirtingus palaikymo laikotarpius;

(63) gamintojai turėtų įsteigti vieną bendrą kontaktinį punktą, kuris leistų naudotojams lengvai su jais komunikuoti, be kita ko, siekiant teikti ir gauti informaciją apie produkto su skaitmeniniu elementu pažeidžiamumą. Jie turėtų užtikrinti, kad vienas bendras kontaktinis punktas būtų lengvai prieinamas naudotojams, ir aiškiai nurodyti jo prieinamumą, ir kad ši informacija būtų nuolat atnaujinama. Jei gamintojai nusprendžia siūlyti automatines priemones, pavyzdžiui, internetinių pokalbių laukelius, jie taip pat turėtų pasiūlyti telefono numerį arba kitas skaitmenines kontaktines priemones, pavyzdžiui, e. pašto adresą arba kontaktinę formą. Vienas bendras kontaktinis punktas neturėtų būti grindžiamas vien automatinėmis priemonėmis;

(64) gamintojai turėtų tiekti rinkai savo produktus su skaitmeniniais elementais su saugia numatytąja konfigūracija ir teikti saugumo naujinius naudotojams nemokamai. Gamintojai turėtų turėti galimybę nukrypti nuo esminių kibernetinio saugumo reikalavimų tik pagal užsakymą pagamintų produktų, kurie yra pritaikyti konkrečiam verslo klientui pagal konkrečią paskirtį, atvejais ir kai tiek gamintojas, tiek naudotojas aiškiai sutiko su kitokiomis sutarties sąlygomis;

(65) gamintojai per bendrą pranešimų teikimo platformą turėtų tuo pačiu metu pranešti koordinatore paskirtai Reagavimo į kompiuterių saugumo incidentus tarnybai (toliau - CSIRT) ir ENISA apie aktyviai išnaudojamus pažeidžiamumus, esančius produktuose su skaitmeniniais elementais, taip pat apie didelius incidentus, darančius poveikį tų produktų saugumui. Pranešimai turėtų būti teikiami naudojant koordinatore paskirtos CSIRT elektroninio pranešimo galinį įrenginį ir turėtų būti tuo pačiu metu prieinami ENISA;

(66) siekiant užtikrinti, kad koordinatorėmis paskirtos CSIRT ir ENISA turėtų tinkamą pažeidžiamumų apžvalgą ir gautų informaciją, būtiną Direktyvoje (ES) 2022/2555 nustatytoms jų užduotims atlikti, bendram tos direktyvos 3 straipsnyje nurodytų esminių ir svarbių subjektų kibernetinio saugumo lygiui padidinti ir veiksmingam rinkos priežiūros institucijų veikimui užtikrinti, gamintojai turėtų pranešti apie aktyviai išnaudojamus pažeidžiamumus. 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. ENISA, susitarusi su gamintoju, turėtų atskleisti ištaisytus pažeidžiamumus Europos pažeidžiamumų duomenų bazėje, sukurtoje pagal Direktyvos (ES) 2022/2555 12 straipsnio 2 dalį. Europos pažeidžiamumų duomenų bazė padės gamintojams aptikti žinomus išnaudojamus pažeidžiamumus, rastus jų produktuose, siekiant užtikrinti, kad rinkai būtų tiekiami saugūs produktai;

(67) gamintojai taip pat turėtų pranešti koordinatore paskirtai CSIRT ir ENISA apie bet kokį didelį incidentą, darantį poveikį produkto su skaitmeniniais elementais saugumui. Siekdami užtikrinti, kad naudotojai galėtų greitai reaguoti į didelius 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 kibernetinio saugumo rizikos, susisiekdami su naudotojais tiesiogiai;

(68) aktyviai išnaudojami pažeidžiamumai kyla tais atvejais, kai gamintojas nustato, kad saugumo pažeidimą, darantį poveikį jo naudotojams ar bet kuriems kitiems fiziniams ar juridiniams asmenims, padarė piktavalis subjektas, pasinaudojęs vieno iš produktų su skaitmeniniais elementais, kuriuos gamintojas tiekė rinkai, silpnąja vieta. Tokių pažeidžiamumų pavyzdžiai galėtų būti produkto identifikavimo ir tapatumo nustatymo funkcijų trūkumai. Neturėtų būti privaloma pranešti apie nustatytus pažeidžiamumus be piktavalių ketinimų, susijusius su tikslais atlikti sąžiningus bandymus, tyrimą, taisymą ar atskleisti duomenis siekiant skatinti sistemos savininko ir jos naudotojų saugumą ar saugą. Kita vertus, dideli incidentai, darantys poveikį produkto su skaitmeniniais elementais saugumui, kyla tais atvejais, kai kibernetinio saugumo incidentas daro poveikį gamintojo kūrimo, gamybos ar techninės priežiūros procesams taip, kad dėl to galėtų padidėti kibernetinio saugumo rizika naudotojams ar kitiems asmenims. Pavyzdžiui, didelis incidentas galėtų būti situacija, kai užpuolikui pavyksta į sklaidos kanalą, kuriuo gamintojas naudotojams skelbia saugumo naujinius, įterpti piktavališką kodą;

(69) siekiant užtikrinti, kad pranešimus būtų galima greitai išplatinti visoms susijusioms koordinatorėmis paskirtoms CSIRT ir sudaryti sąlygas gamintojams kiekvienu pranešimo proceso etapu pateikti vieną bendrą pranešimą, ENISA turėtų sukurti bendrą pranešimų teikimo platformą su nacionaliniais elektroninio pranešimo galiniais įrenginiais. Tos bendros pranešimų teikimo platformos kasdienę veiklą turėtų valdyti ir prižiūrėti ENISA. Koordinatorėmis paskirtos CSIRT turėtų informuoti savo atitinkamas rinkos priežiūros institucijas apie praneštus pažeidžiamumus ar incidentus. Bendra pranešimų teikimo platforma turėtų būti sukurta taip, kad būtų užtikrintas pranešimų konfidencialumas, visų pirma, kiek tai susiję su pažeidžiamumu, dėl kurio saugumo atnaujinimo dar nėra. Be to, ENISA turėtų nustatyti saugaus ir konfidencialaus informacijos tvarkymo procedūras. Remdamasi surinkta informacija ENISA turėtų kas dvejus metus parengti techninę ataskaitą apie besiformuojančias produktų su skaitmeniniais elementais kibernetinio saugumo rizikos tendencijas ir ją pateikti Bendradarbiavimo grupei, įsteigtai pagal Direktyvos (ES) 2022/2555 14 straipsnį;

(70) išimtinėmis aplinkybėmis ir, visų pirma, gamintojo prašymu koordinatore paskirta CSIRT, kuri pirmoji gavo pranešimą, turėtų galėti nuspręsti atidėti jo platinimą kitoms susijusioms koordinatorėmis paskirtoms CSIRT per bendrą pranešimų teikimo platformą, kai tai galima pagrįsti su kibernetiniu saugumu susijusiomis priežastimis ir tokiu laikotarpiu, kuris yra tikrai būtinas. Koordinatore paskirta CSIRT turėtų nedelsdama informuoti ENISA apie sprendimą atidėti perdavimą ir nurodyti priežastis, taip pat informuoti apie tai, kada ji ketina toliau platinti pranešimą. Komisija, priimdama deleguotąjį aktą, turėtų parengti specifikacijas dėl sąlygų, kuriomis būtų galima taikyti su kibernetiniu saugumu susijusias priežastis, ir, rengdama deleguotojo akto projektą, turėtų bendradarbiauti su CSIRT tinklu, įsteigtu pagal Direktyvos (ES) 2022/2555 15 straipsnį, ir ENISA. Su kibernetiniu saugumu susijusių priežasčių pavyzdžiai apima nuolatinę koordinuoto pažeidžiamumo atskleidimo procedūrą arba situacijas, kai tikėtina, kad gamintojas netrukus turėtų pateikti rizikos mažinimo priemonę, o rizika kibernetiniam saugumui, susijusi su skubiu informacijos platinimu per bendrą pranešimų teikimo platformą, yra didesnė už jos naudą. Koordinatore paskirtos CSIRT prašymu ENISA turėtų galėti padėti tai CSIRT taikyti su kibernetiniu saugumu susijusias priežastis, susijusias su pranešimo platinimo atidėjimu remiantis iš tos CSIRT gauta informacija apie sprendimą atidėti pranešimą dėl tų su kibernetiniu saugumu susijusių priežasčių. Be to, ypač išimtinėmis aplinkybėmis ENISA neturėtų vienu metu gauti visos informacijos apie pranešimą apie aktyviai išnaudojamą pažeidžiamumą.

Taip būtų daroma tuo atveju, kai gamintojas savo pranešime pažymi, kad piktavalis subjektas aktyviai naudojasi pažeidžiamumu, apie kurį pranešta, ir kad, remiantis turima informacija, juo buvo naudojamasi tik CSIRT, kuriai gamintojas pranešė apie pažeidžiamumą, valstybėje narėje, kai bet koks skubus tolesnis pažeidžiamumo, apie kurį pranešta, skleidimas greičiausiai lemtų informacijos, kurios atskleidimas prieštarautų tos valstybės narės esminiams interesams, teikimą arba kai pažeidžiamumas, apie kurį pranešta, kelia neišvengiamą didelę kibernetinio saugumo riziką dėl tolesnio pranešimo platinimo. Tokiais atvejais ENISA tuo pačiu metu galės susipažinti tik su informacija, kad gamintojas pateikė pranešimą, bendra informacija apie atitinkamą produktą su skaitmeniniais elementais, informacija apie bendrą pažeidžiamumo pobūdį ir informacija apie tai, kad gamintojas nurodė tas saugumo priežastis ir kad dėl to visas pranešimo turinys nepateikiamas. Išsamus pranešimas turėtų būti pateiktas ENISA ir kitoms susijusioms koordinatorėmis paskirtoms CSIRT, kai CSIRT, kuri pirmoji gavo pranešimą, nustato, kad tų saugumo priežasčių, susijusių su ypač išimtinėmis aplinkybėmis, nustatytomis šiame reglamente, nebėra. Tais atvejais, kai remdamasi turima informacija ENISA mano, kad esama sisteminės rizikos, darančios poveikį saugumui vidaus rinkoje, ENISA turėtų rekomenduoti pranešimą gavusiai CSIRT išplatinti visą pranešimo tekstą kitoms koordinatorėmis paskirtomis CSIRT ir pačiai ENISA;

(71) kai gamintojai praneša apie aktyviai išnaudojamą pažeidžiamumą arba didelį incidentą, darantį poveikį produkto su skaitmeniniais elementais saugumui, jie turėtų nurodyti, kiek neskelbtina, jų nuomone, yra informacija, kurią jie pateikė. Koordinatore paskirta CSIRT, kuri pirmoji gavo pranešimą, turėtų atsižvelgti į šią informaciją vertindama, ar dėl pranešimo susiklosto išimtinės aplinkybės, pateisinančios pranešimo platinimo kitoms susijusioms koordinatorėmis paskirtoms CSIRT atidėjimą dėl pagrįstų su kibernetiniu saugumu susijusių priežasčių. Ji taip pat turėtų atsižvelgti į tą informaciją vertindama, ar dėl pranešimo apie aktyviai išnaudojamą pažeidžiamumą susidaro ypač išimtinės aplinkybės, pateisinančios tai, kad visas pranešimas ENISA nepateikiamas vienu metu. Galiausiai, koordinatorėmis paskirtos CSIRT turėtų galėti atsižvelgti į tą informaciją nustatydamos tinkamas priemones dėl tokio pažeidžiamumo ir incidentų kylančiai rizikai mažinti;

(72) siekiant supaprastinti informacijos, kurios reikalaujama pagal šį reglamentą, teikimą, atsižvelgiant į kitus papildomus ataskaitų teikimo reikalavimus, nustatytus Sąjungos teisės aktuose, pavyzdžiui, Reglamente (ES) 2016/679, Europos Parlamento ir Tarybos reglamente (ES) 2022/2554[24], Europos Parlamento ir Tarybos direktyvoje 2002/58/EB[25] ir Direktyvoje (ES) 2022/2555, taip pat sumažinti subjektams tenkančią administracinę naštą, valstybės narės raginamos apsvarstyti galimybę nacionaliniu lygmeniu įsteigti vienos bendros prieigos punktus tokių ataskaitų teikimo reikalavimams patenkinti. Tokių vienos bendros prieigos punktų naudojimas pranešimams apie saugumo incidentus teikti pagal Reglamentą (ES) 2016/679 ir Direktyvą 2002/58/EB neturėtų daryti poveikio Reglamento (ES) 2016/679 ir Direktyvos 2002/58/EB nuostatų, visų pirma susijusių su juose nurodytų institucijų nepriklausomumu, taikymui. Kurdama šiame reglamente nurodytą vieną bendrą pranešimų teikimo platformą, ENISA turėtų atsižvelgti į galimybę integruoti šiame reglamente nurodytus nacionalinius elektroninio pranešimo galinius įrenginius į nacionalinius vienos bendros prieigos punktus, kuriuose taip pat gali būti integruojami kiti pranešimai, kurių reikalaujama pagal Sąjungos teisę;

---

[24] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 (OL L 333, 2022 12 27, p. 1).

[25] 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (OL L 201, 2002 7 31, p. 37).

(73) kurdama šiame reglamente nurodytą vieną bendrą ataskaitų teikimo platformą ir siekdama pasinaudoti ankstesne patirtimi, ENISA turėtų konsultuotis su kitomis Sąjungos institucijomis ar agentūromis, valdančiomis platformas ar duomenų bazes, kurioms taikomi griežti saugumo reikalavimai, pavyzdžiui, su Europos Sąjungos didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūra (eu-LISA). ENISA taip pat turėtų išnagrinėti galimą papildomumą su Europos pažeidžiamumų duomenų baze, sukurta pagal Direktyvos (ES) 2022/2555 12 straipsnio 2 dalį;

(74) gamintojai bei kiti fiziniai ir juridiniai asmenys turėtų turėti galimybę koordinatore paskirtai CSIRT arba ENISA savanoriškai pranešti apie bet kokį produkto su skaitmeniniais elementais pažeidžiamumą, kibernetines grėsmes, kurios galėtų turėti įtakos produkto su skaitmeniniais elementais rizikos profiliui, visus incidentus, darančius poveikį produkto su skaitmeniniais elementais saugumui, taip pat apie vos neįvykusius incidentus, dėl kurių galėjo įvykti toks incidentas;

(75) valstybės narės turėtų siekti kuo didesniu mastu reaguoti į iššūkius, su kuriais susiduria pažeidžiamumų tyrėjai, įskaitant jų galimą baudžiamosios atsakomybės riziką, laikantis nacionalinės teisės. Atsižvelgiant į tai, kad pažeidžiamumus tiriantiems fiziniams ir juridiniams asmenims kai kuriose valstybėse narėse gali kilti baudžiamosios ir civilinės atsakomybės rizika, valstybės narės raginamos priimti gaires dėl informacijos saugumo tyrėjų netraukimo baudžiamojon atsakomybėn ir atleidimo nuo civilinės atsakomybės už jų veiklą;

(76) produktų su skaitmeniniais elementais gamintojai turėtų įdiegti koordinuoto pažeidžiamumų atskleidimo politiką, kad asmenys arba subjektai galėtų lengviau tiesiogiai gamintojams arba netiesiogiai pranešti apie pažeidžiamumus, o kai to prašoma anonimiškai – per pagal Direktyvos (ES) 2022/2555 12 straipsnio 1 dalį pažeidžiamumų atskleidimo tikslais koordinatorėmis paskirtas CSIRT. Gamintojų koordinuoto pažeidžiamumų atskleidimo politikoje turėtų būti nurodytas struktūruotas 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. Be to, gamintojai taip pat turėtų apsvarstyti galimybę skelbti savo saugumo politiką kompiuterio skaitomu formatu. 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 koordinuoto pažeidžiamumų atskleidimo politiką, turėtų galėti naudoti programas, kuriomis skatinama pranešti apie pažeidžiamumus užtikrinant, kad asmenys arba subjektai už savo pastangas sulauktų pripažinimo ir kompensacijos. Tos programos – tai vadinamosios atlygio už surastus riktus programos;

(77) kad būtų lengviau atlikti pažeidžiamumų analizę, gamintojai turėtų nustatyti ir dokumentuoti produktuose su skaitmeniniais elementais esančius komponentus, įskaitant parengdami PĮMŽ. PĮMŽ tiems, kurie gamina, perka ir valdo programinę įrangą, gali suteikti informacijos, kuri didina jų supratimą apie tiekimo grandinę, o tai turi daug privalumų – visų pirma tai padeda gamintojams ir naudotojams sekti žinomus naujus atskleistus pažeidžiamumus ir kibernetinio saugumo riziką. Gamintojams ypač svarbu užtikrinti, kad jų produktuose su skaitmeniniais elementais nebūtų pažeidžiamų komponentų, kuriuos sukuria trečiosios šalys. Gamintojai neturėtų būti įpareigoti viešai skelbti PĮMŽ;

(78) pagal naujus sudėtingus verslo modelius, susijusius su pardavimu internetu, internetu veikianti įmonė gali teikti įvairias paslaugas. Priklausomai nuo teikiamų paslaugų, susijusių su konkrečiu produktu su skaitmeniniais elementais, pobūdžio, tas pats subjektas gali priklausyti skirtingoms verslo modelių ar ekonominės veiklos vykdytojų kategorijoms. Jei subjektas teikia tik internetines tarpininkavimo paslaugas konkrečiam produktui su skaitmeniniais elementais ir yra tik elektroninės prekyvietės, kaip apibrėžta Reglamento (ES) 2023/988 3 straipsnio 14 punkte, teikėjas, jis nėra priskiriamas vienai iš šiame reglamente apibrėžtų ekonominės veiklos vykdytojų rūšių. Jei tas pats subjektas yra elektroninės prekyvietės paslaugų teikėjas ir veikia kaip ekonominės veiklos vykdytojas, kaip apibrėžta šiame reglamente, parduodantis konkrečius produktus su skaitmeniniais elementais, jam turėtų būti taikomos pareigos, šiame reglamente nustatytos tos rūšies ekonominės veiklos vykdytojams. Pavyzdžiui, jei elektroninės prekyvietės paslaugos teikėjas taip pat platina produktą su skaitmeniniais elementais, tuomet to produkto pardavimo atžvilgiu jis būtų laikomas platintoju. Panašiai, jei aptariamas subjektas parduoda savo prekių ženklu pažymėtus produktus su skaitmeniniais elementais, jis būtų priskiriamas prie gamintojo ir todėl turėtų laikytis gamintojams taikomų reikalavimų. Be to, kai kurie subjektai gali būti priskiriami prie realizavimo paslaugų teikėjo, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/1020[26] 3 straipsnio 11 punkte, jei jie siūlo tokias paslaugas. Tokius atvejus reikėtų vertinti atsižvelgiant į kiekvieną atvejį atskirai. Atsižvelgiant į svarbų elektroninių prekyviečių vaidmenį įgalinant elektroninę prekybą, turėtų būti stengiamasi, kad jos bendradarbiautų su valstybių narių rinkos priežiūros institucijomis, siekiant padėti užtikrinti, kad elektroninėse prekyvietėse įsigyti produktai su skaitmeniniais elementais atitiktų šiame reglamente nustatytus kibernetinio saugumo reikalavimus;

---

[26] 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).

(79) siekiant palengvinti atitikties šiame reglamente nustatytiems reikalavimams vertinimą, turėtų būti preziumuojama, kad produktai su skaitmeniniais elementais atitinka tuos reikalavimus, kai jie atitinka darniuosius standartus, kuriais šiame reglamente nustatyti esminiai kibernetinio saugumo reikalavimai paverčiami išsamiomis techninėmis specifikacijomis ir kurie priimami pagal Europos Parlamento ir Tarybos reglamentą (ES) Nr. 1025/2012[27]. Tame reglamente numatyta prieštaravimų darniesiems standartams procedūra, taikoma, jei tie standartai nevisiškai atitinka šiame reglamente nustatytus reikalavimus. Standartizacijos procesu turėtų būti užtikrintas subalansuotas interesų atstovavimas ir veiksmingas pilietinės visuomenės suinteresuotųjų subjektų, įskaitant vartotojų organizacijas, dalyvavimas. Taip pat turėtų būtu atsižvelgta į tarptautinius standartus, atitinkančius kibernetinio saugumo apsaugos lygį, kurio siekiama šiame reglamente nustatytais esminiais kibernetinio saugumo reikalavimais, siekiant sudaryti palankesnes sąlygas darniųjų standartų rengimui ir šio reglamento įgyvendinimui, taip pat sudaryti palankesnes sąlygas įmonėms, visų pirma labai mažoms įmonėms ir mažosioms bei vidutinėms įmonėms ir visame pasaulyje veikiančioms įmonėms, laikytis reikalavimų;

[27] 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).

(80) siekiant veiksmingai įgyvendinti šį reglamentą, ypač svarbu, kad šio reglamento taikymo pereinamuoju laikotarpiu būtų laiku parengti darnieji standartai ir kad jie būtų prieinami iki šio reglamento taikymo pradžios dienos. Tai visų pirma taikoma svarbiems produktams su skaitmeniniais elementais, priskiriamiems prie I klasės. Darniųjų standartų buvimas leis tokių produktų gamintojams atlikti atitikties vertinimus taikant vidaus kontrolės procedūrą, todėl gali padėti išvengti atitikties vertinimo įstaigų veiklos kliūčių ir vėlavimų;

(81) Reglamentu (ES) 2019/881 sukuriama savanoriška IRT produktų, IRT procesų ir IRT paslaugų Europos kibernetinio saugumo sertifikavimo sistema. Europos kibernetinio saugumo sertifikavimo schemos suteikia naudotojams bendrą pasitikėjimo naudoti produktus su skaitmeniniais elementais, kurie patenka į šio reglamento taikymo sritį, sistemą. Todėl šiuo reglamentu turėtų būti sukuriama sinergija su Reglamentu (ES) 2019/881. Siekiant palengvinti atitikties šiame reglamente nustatytiems reikalavimams vertinimą, preziumuojama, kad produktai su skaitmeniniais elementais, kurie yra sertifikuoti arba kuriems išduotas atitikties pareiškimas pagal Europos kibernetinio saugumo schemą pagal Reglamentą (ES) 2019/881 ir kuriuos Komisija identifikavo įgyvendinimo akte, atitinka šiame reglamente nustatytus esminius kibernetinio saugumo reikalavimus tiek, kiek Europos 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, be kita ko, rengiant tęstinę Sąjungos darbo programą pagal Reglamentą (ES) 2019/881. Kai reikia naujos schemos, apimančios produktus su skaitmeniniais elementais, be kita ko, siekiant sudaryti palankesnes sąlygas laikytis šio reglamento, Komisija gali prašyti ENISA parengti potencialias schemas pagal Reglamento (ES) 2019/881 48 straipsnį. Tokiose būsimose Europos kibernetinio saugumo sertifikavimo schemose, apimančiose produktus su skaitmeniniais elementais, turėtų būti atsižvelgiama į šiame reglamente nustatytus esminius kibernetinio saugumo reikalavimus ir atitikties vertinimo procedūras ir palengvinamas šio reglamento reikalavimų laikymasis. Europos kibernetinio saugumo sertifikavimo schemų, kurios įsigalioja prieš įsigaliojant šiam reglamentui, atveju gali prireikti papildomų specifikacijų dėl išsamių aspektų, kaip gali būti taikoma atitikties prezumpcija.

Komisijai turėtų būti suteikti įgaliojimai deleguotaisiais aktais nurodyti, kokiomis sąlygomis Europos kibernetinio saugumo sertifikavimo schemos gali būti naudojamos siekiant įrodyti atitiktį šiame reglamente nustatytiems esminiams kibernetinio saugumo reikalavimams. Be to, siekiant išvengti nepagrįstos administracinės naštos , gamintojai neturėtų būti įpareigoti atlikti trečiųjų šalių atitikties atitinkamiems reikalavimams vertinimo, kaip numatyta šiame reglamente, jei pagal tokias Europos kibernetinio saugumo sertifikavimo schemas yra išduotas bent „pakankamai aukšto“ saugumo užtikrinimo lygio Europos kibernetinio saugumo užtikrinimo sertifikatas ;

(82) įsigaliojus Įgyvendinimo reglamentui (ES) 2024/482, susijusiam su į šio reglamento taikymo sritį patenkančiais produktais, pavyzdžiui, aparatinės įrangos saugumo moduliais ir mikroprocesoriais, Komisija turėtų galėti deleguotuoju aktu nurodyti, kaip EUCC suteikia prezumpciją dėl atitikties šio reglamento priede ar jo dalyse nustatytiems esminiams kibernetinio saugumo reikalavimams. Be to, tokiame deleguotajame akte gali būti nurodyta, kaip pagal EUCC išduotas sertifikatas panaikina gamintojų pareigą atlikti trečiųjų šalių vykdomą atitinkamų reikalavimų atitikties vertinimą, kaip to reikalaujama pagal šį reglamentą;

(83) dabartinė Europos standartizacijos sistema, kuri yra grindžiama naujojo požiūrio principais, išdėstytais 1985 m. gegužės 7 d. Tarybos rezoliucijoje dėl naujojo požiūrio į techninį derinimą ir standartus ir Reglamentu (ES) Nr. 1025/2012, yra numatytoji standartų, kuriuose numatoma atitikties atitinkamiems šiame reglamente nustatytiems esminiams kibernetinio saugumo reikalavimams prezumpcija, rengimo sistema. Europos standartai turėtų būti orientuoti į rinką, jais turėtų būti atsižvelgiama į viešąjį interesą ir į politikos tikslus, aiškiai nurodytus Komisijos prašyme vienai ar daugiau Europos standartizacijos organizacijų per nustatytą terminą parengti darniųjų standartų projektus, ir jie turi būti grindžiami bendru sutarimu. Tačiau jei nėra atitinkamų nuorodų į darniuosius standartus, Komisija turėtų galėti priimti įgyvendinimo aktus, kuriais nustatomos šiame reglamente nustatytų esminių kibernetinio saugumo reikalavimų bendrosios specifikacijos, su sąlyga, kad tai darydama ji deramai paisytų standartizacijos organizacijų vaidmens ir funkcijų ir kad tai būtų išimtiniu atveju taikomas atsarginis sprendimas, sudarantis palankesnes sąlygas gamintojui įvykdyti pareigą laikytis tų esminių kibernetinio saugumo reikalavimų tuo atveju, kai standartizacijos procesas sustoja arba kai vėluojama parengti tinkamus darniuosius standartus. Jei toks vėlavimas atsiranda dėl aptariamo standarto techninio sudėtingumo, Komisija, prieš svarstydama, ar reikia nustatyti bendrąsias specifikacijas, turėtų į tai atsižvelgti;

(84) siekiant kuo veiksmingiau nustatyti bendrąsias specifikacijas, kurios apimtų šiame reglamente nustatytus esminius kibernetinio saugumo reikalavimus, Komisija turėtų į šį procesą įtraukti atitinkamus suinteresuotuosius subjektus;

(85) kiek tai susiję su nuorodos į darniuosius standartus paskelbimu *Europos Sąjungos oficialiajame leidinyje* pagal Reglamentą (ES) Nr. 1025/2012, pagrįstas laikotarpis reiškia laikotarpį, per kurį tikimasi *Europos Sąjungos oficialiajame leidinyje* paskelbti nuorodą į standartą, klaidų ištaisymą ar pakeitimą ir kuris neturėtų būti ilgesnis nei vieneri metai nuo Europos standarto parengimo termino, nustatyto pagal Reglamentą (ES) Nr. 1025/2012;

(86) siekiant palengvinti atitikties šiame reglamente nustatytiems esminiams kibernetinio saugumo reikalavimams vertinimą, turėtų būti preziumuojama, kad produktai su skaitmeniniais elementais atitinka tuos reikalavimus, jei jie atitinka Komisijos pagal šį reglamentą priimtas bendrąsias specifikacijas, kad išreikštų išsamias tų reikalavimų technines specifikacijas;

(87) taikant darniuosius standartus, bendrąsias specifikacijas arba Europos kibernetinio saugumo sertifikavimo schemas, priimtas pagal Reglamentą (ES) 2019/881, preziumuojant, kad laikomasi produktams su skaitmeniniais elementais taikomų esminių kibernetinio saugumo reikalavimų, gamintojams bus lengviau atlikti atitikties vertinimą. Jei gamintojas nusprendžia netaikyti tokių priemonių dėl tam tikrų reikalavimų, jis savo techniniuose dokumentuose turi nurodyti, kaip atitiktis užtikrinama kitais būdais. Be to, taikant darniuosius standartus, bendrąsias specifikacijas arba Europos kibernetinio saugumo sertifikavimo schemas, priimtas pagal Reglamentą (ES) 2019/881, preziumuojant, kad gamintojai laikosi reikalavimų, rinkos priežiūros institucijoms būtų lengviau tikrinti produktų su skaitmeniniais elementais atitiktį. Todėl produktų su skaitmeniniais elementais gamintojai skatinami taikyti tokius darniuosius standartus, bendrąsias specifikacijas arba Europos kibernetinio saugumo sertifikavimo schemas;

(88) gamintojai turėtų parengti ES atitikties deklaraciją, kad pateiktų pagal šį reglamentą reikalaujamą informaciją apie produktų su skaitmeniniais elementais atitiktį šiame reglamente nustatytiems esminiams kibernetinio saugumo reikalavimams ir, jei taikytina, kitiems susijusiems Sąjungos derinamiesiems teisės aktams, reglamentuojantiems produktą su skaitmeniniais elementais. 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 visiems susijusiems Sąjungos teisės aktams. Siekiant sumažinti administracinę naštą ekonominės veiklos vykdytojams, turėtų būti įmanoma, kad ta viena ES atitikties deklaracija būtų byla, sudaryta iš atitinkamų atskirų atitikties deklaracijų;

(89) 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[28]. 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 šiame reglamente nustatytiems reikalavimams;

---

[28] 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).

(90) siekiant sudaryti sąlygas ekonominės veiklos vykdytojams įrodyti atitiktį šiame reglamente nustatytiems esminiams kibernetinio saugumo reikalavimams, o rinkos priežiūros institucijoms – užtikrinti, kad rinkai patiekti produktai su skaitmeniniais elementais atitiktų tuos reikalavimus, būtina nustatyti atitikties vertinimo procedūras. Europos Parlamento ir Tarybos sprendime Nr. 768/2008/EB[29] 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 turėtų būti grindžiamos atitikties vertinimo procedūros, tinkamos tikrinti produktų su skaitmeniniais elementais atitiktį šiame reglamente nustatytiems esminiams kibernetinio saugumo reikalavimams. Atliekant atitikties vertinimo procedūras turėtų būti nagrinėjami ir tikrinami tiek su produktu, tiek su procesu susiję reikalavimai, apimantys visą produktų su skaitmeniniais elementais gyvavimo ciklą, įskaitant produkto su skaitmeniniais elementais planavimą, projektavimą, kūrimą ar gamybą, bandymus ir techninę priežiūrą;

[29] 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).

(91) produktų su skaitmeniniais elementais, kurie šiame reglamente nėra išvardyti kaip svarbūs arba ypatingos svarbos produktai su skaitmeniniais elementais, atitikties vertinimą savo atsakomybe gali atlikti gamintojas, taikydamas vidaus kontrolės procedūrą, pagrįstą Sprendimo Nr. 768/2008/EB A moduliu, laikantis šio reglamento. Tai taip pat taikoma tais atvejais, kai gamintojas pasirenka visiškai arba iš dalies netaikyti taikomo darniojo standarto, bendrosios specifikacijos arba Europos kibernetinio saugumo sertifikavimo schemos. Gamintojas gali lanksčiai pasirinkti griežtesnę atitikties vertinimo procedūrą, kurioje dalyvautų trečioji šalis. Pagal vidaus kontrolės atitikties vertinimo procedūrą gamintojas, prisiimdamas visą atsakomybę, užtikrina ir patvirtina, kad produktas su skaitmeniniais elementais ir gamintojo procesai atitinka taikytinus šiame reglamente nustatytus esminius kibernetinio saugumo reikalavimus. Jei svarbus produktas su skaitmeniniais elementais priskiriamas prie I klasės, reikia papildomo užtikrinimo, kad būtų įrodyta atitiktis šiame reglamente nustatytiems esminiams kibernetinio saugumo reikalavimams. Gamintojas turėtų taikyti Komisijos įgyvendinimo akte nurodytus darniuosius standartus, bendrąsias specifikacijas ar Europos kibernetinio saugumo sertifikavimo schemas, priimtas pagal Reglamentą (ES) 2019/881, jei jis nori atlikti atitikties vertinimą savo atsakomybe (A modulis). Jei gamintojas netaiko tokių darniųjų standartų, bendrųjų specifikacijų ar Europos kibernetinio saugumo sertifikavimo schemų, jis turėtų atlikti atitikties vertinimą, kuriame dalyvautų trečioji šalis (paremtą B ir C moduliais arba H moduliu). 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 Nr. 768/2008/EB B ir C moduliais arba H moduliu, kaip tinkamiausios siekiant proporcingai ir veiksmingai įvertinti svarbių 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 svarbių produktų su skaitmeniniais elementais, priskiriamų prie II klasės, naudojimu, atitikties vertinime visada turėtų dalyvauti trečioji šalis, net jei produktas visiškai arba iš dalies atitinka darniuosius standartus, bendrąsias specifikacijas arba Europos kibernetinio saugumo sertifikavimo schemas. Svarbių produktų su skaitmeniniais elementais, kurie gali būti laikomi laisvąja ir atvirąja programine įranga, gamintojai turėtų turėti galimybę laikytis A moduliu grindžiamos vidaus kontrolės procedūros, su sąlyga, kad techniniai dokumentai būtų prieinami visuomenei;

(92) 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 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. Ta veikla turėtų būti laikoma apimančia gamybą, kai taikomi atitinkami atitikties vertinimo moduliai siekiant patikrinti, ar produktas atitinka šiame reglamente nustatytus esminius kibernetinio saugumo reikalavimus projektavimo, kūrimo ir gamybos etapuose;

(93) kalbant apie labai mažas įmones ir mažąsias įmones, siekiant užtikrinti proporcingumą, tikslinga sumažinti administracines išlaidas nedarant poveikio produktų su skaitmeniniais elementais, kurie patenka į šio reglamento taikymo sritį, kibernetinio saugumo apsaugos lygiui arba vienodoms gamintojų sąlygoms. Todėl tikslinga, kad Komisija nustatytų supaprastintą techninių dokumentų formą, skirtą labai mažų įmonių ir mažųjų įmonių poreikiams. Komisijos patvirtinta supaprastinta techninių dokumentų forma turėtų apimti visus taikytinus elementus, susijusius su šiame reglamente nustatytais techniniais dokumentais, ir joje turėtų būti nurodyta, kaip labai maža įmonė arba mažoji įmonė gali glaustai pateikti prašomus elementus, pavyzdžiui, produkto su skaitmeniniais elementais projektavimo, kūrimo ir gamybos aprašymą. Tokiu būdu forma padėtų sumažinti administracinę reikalavimų laikymosi naštą, nes atitinkamoms įmonėms būtų užtikrintas teisinis tikrumas dėl teiktinos informacijos apimties ir išsamumo. Labai mažos įmonės ir mažosios įmonės turėtų turėti galimybę pasirinkti su techniniais dokumentais susijusius taikytinus elementus pateikti išsamiai ir nesinaudoti joms prieinama supaprastinta technine forma;

(94) siekiant skatinti ir apsaugoti inovacijas, svarbu, kad būtų ypač atsižvelgiama į gamintojų, kurie yra labai mažos įmonės, mažosios ar vidutinės įmonės, visų pirma labai mažų įmonių ir mažųjų įmonių, įskaitant startuolius, interesus. Tuo tikslu valstybės narės galėtų parengti iniciatyvas, skirtas gamintojams, kurie yra labai mažos įmonės arba mažosios įmonės, be kita ko, susijusias su mokymu, informuotumo didinimu, informacijos komunikacija, bandymais ir trečiųjų šalių atitikties vertinimo veikla, taip pat apribotos bandomosios aplinkos sukūrimu. Vertimo išlaidos, susijusios su privalomais dokumentais, pavyzdžiui, techniniais dokumentais, naudotojui skirta informacija ir nurodymais, kurių reikalaujama pagal šį reglamentą, ir komunikacija su institucijomis gali lemti dideles išlaidas gamintojams, visų pirma mažesniems gamintojams. Todėl valstybės narės turėtų turėti galimybę laikyti, kad viena iš jų nustatytų ir priimtinų kalbų, vartojamų atitinkamiems tiekėjams rengiant dokumentus ir bendraujant su veiklos vykdytojais, yra ta kalba, kuri yra plačiai suprantama kuo didesniam naudotojų ratui;

(95) siekiant užtikrinti sklandų šio reglamento taikymą, valstybės narės iki šio reglamento taikymo pradžios dienos turėtų stengtis užtikrinti, kad būtų pakankamai notifikuotųjų įstaigų trečiųjų šalių atliekamiems atitikties vertinimams atlikti. Komisija turėtų stengtis padėti valstybėms narėms ir kitoms susijusioms šalims siekti šio tikslo, kad būtų išvengta trukdžių ir kliūčių gamintojams patekti į rinką. Valstybių narių vadovaujama tikslinė mokymo veikla, be kita ko, atitinkamais atvejais padedant Komisijai, gali padėti užtikrinti kvalifikuotų specialistų prieinamumą, be kita ko, remiant notifikuotųjų įstaigų veiklą pagal šį reglamentą. Be to, atsižvelgiant į išlaidas, kurių gali atsirasti dėl trečiosios šalies atitikties vertinimo, reikėtų apsvarstyti galimybę finansuoti Sąjungos ir nacionalinio lygmens iniciatyvas, kuriomis siekiama sumažinti tokias labai mažų įmonių ir mažųjų įmonių išlaidas;

(96) siekiant užtikrinti proporcingumą, atitikties vertinimo įstaigos, nustatydamos mokesčius už atitikties vertinimo procedūras, turėtų atsižvelgti į konkrečius labai mažų įmonių ir mažųjų bei vidutinių įmonių, įskaitant startuolius, interesus ir poreikius. Visų pirma, atitikties vertinimo įstaigos turėtų taikyti atitinkamą šiame reglamente numatytą nagrinėjimo procedūrą ir bandymus taikyti tik tada, kai tai tinkama, ir laikantis rizika grindžiamo požiūrio;

(97) apribotos bandomosios reglamentavimo aplinkos tikslai turėtų būti skatinti įmonių inovacijas ir konkurencingumą sukuriant kontroliuojamą bandymų aplinką prieš pateikiant rinkai produktus su skaitmeniniais elementais. Bandomoji reglamentavimo aplinka turėtų padėti didinti teisinį tikrumą visiems subjektams, kuriems taikomas šis reglamentas, ir palengvinti bei paspartinti produktų su skaitmeniniais elementais patekimą į Sąjungos rinką, visų pirma, kai juos teikia labai mažos įmonės ir mažosios įmonės, įskaitant startuolius;

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

(99) siekiant užtikrinti vienodą kokybės lygį atliekant produktų su skaitmeniniais elementais atitikties vertinimą, reikia taip pat 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;

(100) atitikties vertinimo įstaigos, kurios buvo akredituotos ir notifikuotos pagal Sąjungos teisės aktus, kuriais nustatomi reikalavimai, panašūs į nustatytuosius šiame reglamente, pavyzdžiui, atitikties vertinimo įstaiga, kuri yra notifikuota pagal Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Reglamentą (ES) 2019/881 arba notifikuota pagal Deleguotąjį reglamentą (ES) 2022/30, turėtų būti iš naujo įvertintos ir notifikuotos pagal šį reglamentą. Tačiau, siekiant išvengti nereikalingos finansinės ir administracinės naštos ir užtikrinti sklandų ir savalaikį notifikavimo procesą, atitinkamos institucijos gali nustatyti sąveiką, susijusią su bet kokiais sutampančiais reikalavimais;

(101) Reglamente (EB) Nr. 765/2008 numatytą skaidrią akreditaciją, kuria užtikrinamas būtinas pasitikėjimo atitikties sertifikatais lygis, nacionalinės valdžios 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, jos turėtų pateikti Komisijai ir kitoms valstybėms narėms reikiamus dokumentinius įrodymus, kad įvertintos atitikties vertinimo įstaigos atitinka atitinkamus reguliavimo reikalavimus;

(102) atitikties vertinimo įstaigos dalį savo veiklos, susijusios su atitikties vertinimu, dažnai paveda atlikti subrangovams arba patronuojamai įmonei. Siekiant išsaugoti reikalaujamą rinkai pateiktinų produktų su skaitmeniniais elementais apsaugos lygį, labai svarbu, kad atitikties vertinimą atliekantys subrangovai ir patronuojamosios įmonės atitiktų notifikuotosioms įstaigoms keliamus atitikties vertinimo užduočių atlikimo reikalavimus;

(103) notifikuojančioji institucija turėtų siųsti notifikavimo pranešimą 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;

(104) 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;

(105) 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;

(106) rinkos priežiūra yra svarbi priemonė užtikrinant tinkamą ir vienodą Sąjungos teisės taikymą. Todėl tikslinga sukurti teisinę sistemą, pagal kurią rinkos priežiūra galėtų būti vykdoma tinkamu būdu. Produktams su skaitmeniniais elementais, kurie patenka į šio reglamento taikymo sritį, taikomos Sąjungos rinkos priežiūros ir Sąjungos rinkai tiekiamų produktų kontrolės taisyklės, nustatytos Reglamente (ES) 2019/1020;

(107) pagal Reglamentą (ES) 2019/1020 rinkos priežiūros institucija vykdo rinkos priežiūrą ją paskyrusios valstybės narės teritorijoje. Šiuo reglamentu neturėtų būti draudžiama valstybėms narėms pasirinkti kompetentingų institucijų rinkos priežiūros užduotims vykdyti. Kiekviena valstybė narė savo teritorijoje turėtų paskirti vieną ar daugiau rinkos priežiūros institucijų. Valstybės narės turėtų galėti nuspręsti paskirti bet kurią esamą arba naują instituciją, kuri veiktų kaip rinkos priežiūros institucija, įskaitant kompetentingas institucijas, paskirtas arba įsteigtas pagal Direktyvos (ES) 2022/2555 8 straipsnį, nacionalines kibernetinio saugumo sertifikavimo institucijas, paskirtas pagal Reglamento (ES) 2019/881 58 straipsnį arba rinkos priežiūros institucijas, paskirtas Direktyvos 2014/53/ES tikslais. Ekonominės veiklos vykdytojai turėtų visapusiškai bendradarbiauti su rinkos priežiūros institucijomis ir kitomis kompetentingomis institucijomis. Kiekviena valstybė narė turėtų informuoti Komisiją ir kitas valstybes nares apie savo rinkos priežiūros institucijas ir kiekvienos iš tų institucijų kompetencijos sritis bei užtikrinti būtinus išteklius ir įgūdžius, kad būtų galima vykdyti su šiuo reglamentu susijusias rinkos 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;

(108) siekiant vienodai taikyti šį reglamentą, pagal Reglamento (ES) 2019/1020 30 straipsnio 2 dalį turėtų būti sudaryta speciali administracinio bendradarbiavimo grupė, atsakinga už produktų su skaitmeniniais elementais kibernetinį atsparumą. Administracinio bendradarbiavimo grupę turėtų sudaryti 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, sukurtą pagal Reglamento (ES) 2019/1020 29 straipsnį ir apimantį kiekvienos valstybės narės atstovus, įskaitant kiekvienos bendros ryšių palaikymo tarnybos, nurodytos to reglamento 10 straipsnyje, atstovą ir neprivalomą nacionalinį ekspertą, administracinio bendradarbiavimo grupių pirmininkus ir Komisijos atstovus. Komisija turėtų dalyvauti Sąjungos gaminių atitikties tinklo, jo pogrupių ir administracinio bendradarbiavimo grupės posėdžiuose. Be to, ji turėtų padėti administracinio bendradarbiavimo grupei pasitelkdama vykdomąjį sekretoriatą, teikiantį techninę ir logistinę paramą. Administracinio bendradarbiavimo grupė taip pat gali kviesti nepriklausomus ekspertus dalyvauti ir palaikyti ryšius su kitomis administracinio bendradarbiavimo grupėmis, pavyzdžiui, pagal Direktyvą 2014/53/ES įsteigta grupe;

(109) rinkos priežiūros institucijos, pasitelkdamos pagal šį reglamentą įsteigtą Administracinio bendradarbiavimo grupę, turėtų glaudžiai bendradarbiauti ir turėtų turėti galimybę parengti rekomendacinius dokumentus, kad būtų palengvinta rinkos priežiūros veikla nacionaliniu lygmeniu, pavyzdžiui, kurdamos geriausią praktiką ir rodiklius, skirtus veiksmingai tikrinti produktų su skaitmeniniais elementais atitiktį šiam reglamentui;

(110) siekiant laiku, proporcingai ir veiksmingai taikyti priemones produktams su skaitmeniniais elementais, keliančiais didelę kibernetinio saugumo riziką, reikėtų nustatyti Sąjungos apsaugos procedūrą, pagal kurią suinteresuotosios šalys būtų informuojamos apie priemones, kurių ketinama imtis tokių produktų atžvilgiu. Tai taip pat turėtų suteikti galimybę rinkos priežiūros institucijoms, bendradarbiaujant su atitinkamais ekonominės veiklos vykdytojais, imtis veiksmų ankstesniame etape, kai tai yra būtina. Jei valstybės narės ir Komisija sutaria dėl valstybės narės taikomos priemonės pagrįstumo, neturėtų būti reikalaujama, kad Komisija imtųsi papildomų veiksmų, išskyrus atvejus, kai neatitiktis gali būti susijusi su darniojo standarto trūkumais;

(111) tam tikrais atvejais produktas su skaitmeniniais elementais, kuris atitinka šį reglamentą, vis tiek gali kelti didelę 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 (ES) 2022/2555 3 straipsnio 1 dalyje nurodyti esminiai subjektai, prieinamumui, autentiškumui, vientisumui ar konfidencialumui, arba kitiems viešojo intereso apsaugos aspektams. Todėl būtina nustatyti taisykles, kurios užtikrintų tos rizikos mažinimą. Rinkos priežiūros institucijos turėtų imtis priemonių ir nustatyti ekonominės veiklos vykdytojui reikalavimą užtikrinti, kad, priklausomai nuo rizikos, produktas tos rizikos nebekeltų, būtų atšauktas arba būtų pašalintas. Kai tik rinkos priežiūros institucija apriboja arba uždraudžia laisvą produkto su skaitmeniniais elementais judėjimą tokiu būdu, atitinkama valstybė narė turėtų nedelsdama pranešti Komisijai ir kitoms valstybėms narėms apie laikinąsias priemones nurodydama tokio sprendimo priėmimo priežastis ir pagrindimą. Jei rinkos priežiūros institucija imasi tokių priemonių dėl pavojų keliančių produktų su skaitmeniniais elementais, 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 turėtų apsvarstyti galimybę priimti pasiūlymus peržiūrėti atitinkamus Sąjungos teisės aktus;

(112) jei produktai su skaitmeniniais elementais kelia didelę kibernetinio saugumo riziką ir jei yra priežasčių manyti, kad jie neatitinka šio reglamento, arba jei produktai atitinka šį reglamentą, bet kelia kitą svarbią riziką, pavyzdžiui, pavojų asmenų sveikatai ar saugai, atitikčiai pareigoms pagal Sąjungos ar nacionalinės teisės aktus, kuriais siekiama apsaugoti pagrindines teises, ar paslaugų, kurias per elektroninę informacinę sistemą siūlo Direktyvos (ES) 2022/2555 3 straipsnio 1 dalyje nurodyti esminiai subjektai, prieinamumui, autentiškumui, vientisumui ar konfidencialumui, Komisija turėtų galėti prašyti ENISA atlikti vertinimą. Remdamasi tuo vertinimu Komisija turėtų galėti įgyvendinimo aktais priimti Sąjungos lygmens taisomąsias arba ribojamąsias priemones, įskaitant reikalavimą pašalinti atitinkamus produktus su skaitmeniniais elementais iš rinkos arba atšaukti juos per pagrįstą laikotarpį, atitinkantį rizikos pobūdį. Komisija turėtų galėti pasinaudoti tokia intervencija tik išimtinėmis aplinkybėmis, dėl kurių būtų pateisinama nedelsiant vykdyti intervenciją, kad būtų išsaugotas tinkamas vidaus rinkos veikimas, ir tik tais atvejais, kai rinkos priežiūros institucijos nesiėmė veiksmingų priemonių padėčiai ištaisyti. Tokios išimtinės aplinkybės gali būti ekstremaliosios situacijos, kai, pavyzdžiui, gamintojas ne vienoje valstybėje narėje platina reikalavimų neatitinkantį produktą su skaitmeniniais elementais, kurį pagrindiniuose sektoriuose naudoja ir subjektai, kurie patenka į Direktyvos (ES) 2022/2555 taikymo sritį, nors jame yra žinomų pažeidžiamumų, kuriais naudojasi piktavaliai subjektai ir kuriems ištaisyti gamintojas nepateikia pataisų. Tokiais nepaprastosios padėties atvejais Komisija turėtų galėti įsikišti tik tol, kol trunka išimtinės aplinkybės, ir jei neatitiktis šio reglamento reikalavimams arba svarbi rizika išlieka;

(113) jei yra požymių, kad daugiau nei vienoje valstybėje narėje nesilaikoma šio reglamento, rinkos priežiūros institucijos turėtų galėti vykdyti bendrą veiklą su kitomis institucijomis, kad patikrintų produktų su skaitmeniniais elementais atitiktį ir nustatytų tų produktų kibernetinio saugumo riziką;

(114) tuo pačiu metu atliekami koordinuoti kontrolės veiksmai (toliau - 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 su skaitmeniniais elementais dažnai būdinga kibernetinio saugumo rizika. Be to, nustatant produktų, dėl kurių turi būti atliekamos tikslinės patikros, kategorijas, rinkos priežiūros institucijos taip pat turėtų atsižvelgti į su netechniniais rizikos veiksniais susijusias aplinkybes. Tuo tikslu rinkos priežiūros institucijos turėtų galėti atsižvelgti į Sąjungos lygmeniu koordinuojamų ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimų, atliktų pagal Direktyvos (ES) 2022/2555 22 straipsnį, rezultatus, įskaitant su netechniniais rizikos veiksniais susijusias aplinkybes. ENISA turėtų rinkos priežiūros institucijoms teikti pasiūlymus dėl produktų su skaitmeniniais elementais kategorijų, kurioms galėtų būti organizuojamos tikslinės patikros, remdamasi, be kita ko, ir savo gaunamais pranešimais apie pažeidžiamumus ir incidentus;

(115) atsižvelgiant į savo patirtį ir įgaliojimus, ENISA turėtų galėti remti šio reglamento įgyvendinimo procesą. Visų pirma, ENISA 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, dėl kurių turėtų būti organizuojamos tikslinės patikros. Išimtinėmis aplinkybėmis, Komisijos prašymu ENISA turėtų galėti atlikti konkrečių produktų su skaitmeniniais elementais vertinimus, kai jie kelia didelę kibernetinio saugumo riziką ir kai reikia nedelsiant įsikišti, kad būtų išsaugotas tinkamas vidaus rinkos veikimas;

(116) šiuo reglamentu ENISA pavedamos tam tikros užduotys, kurioms reikia tinkamų tiek ekspertinių žinių, tiek žmogiškųjų išteklių, kad ENISA galėtų tas užduotis vykdyti veiksmingai. Rengdama Sąjungos bendrojo biudžeto projektą Komisija pasiūlys ENISA etatų planui reikalingus biudžeto išteklius pagal Reglamento (ES) 2019/881 29 straipsnyje nustatytą procedūrą. To proceso metu Komisija apsvarstys bendrus ENISA išteklius, kad ji galėtų vykdyti savo užduotis, įskaitant užduotis, pavestas ENISA pagal šį reglamentą;

(117) siekiant užtikrinti, kad, prireikus, būtų galima pritaikyti reglamentavimo sistemą, pagal Sutarties dėl Europos Sąjungos veikimo 290 straipsnį Komisijai turėtų būti deleguoti įgaliojimai priimti aktus dėl priede išvardytų svarbių produktų su skaitmeniniais elementais atnaujinimo. Komisijai turėtų būti deleguoti įgaliojimai 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, jei taikytina, tokio apribojimo taikymo sritį. Komisijai taip pat turėtų būti deleguoti įgaliojimai priimti aktus pagal tą straipsnį dėl galimo įgaliojimų sertifikuoti tam tikrus šio reglamento priede išvardytus ypatingos svarbos produktus su skaitmeniniais elementais suteikimo pagal Europos kibernetinio saugumo sertifikavimo schemą, taip pat dėl ypatingos svarbos produktų su skaitmeniniais elementais sąrašo atnaujinimo remiantis šiame reglamente nustatytais ypatingo svarbumo kriterijais ir dėl pagal Reglamentą (ES) 2019/881 priimtų Europos kibernetinio saugumo sertifikavimo schemų, kurios gali būti naudojamos atitikčiai šio reglamento priede nustatytiems esminiams kibernetinio saugumo reikalavimams ar jų dalims įrodyti, nustatymo. Komisijai taip pat turėtų būti deleguoti įgaliojimai priimti aktus, kuriais būtų nustatytas minimalus palaikymo laikotarpis konkrečioms produktų kategorijoms, kai iš rinkos priežiūros duomenų matyti, kad palaikymo laikotarpiai yra nepakankami, taip pat kuriais nustatomos su kibernetiniu saugumu susijusių priežasčių taikymo sąlygos, susijusios su pranešimų apie aktyviai išnaudojamus pažeidžiamumus perdavimo atidėjimu.

Be to, Komisijai turėtų būti deleguoti įgaliojimai priimti aktus, kuriais nustatomos savanoriškos saugumo patvirtinimo programos, skirtos įvertinti produktų su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga, atitiktį visiems arba tam tikriems šiame reglamente nustatytiems esminiams kibernetinio saugumo reikalavimams ar kitoms pareigoms, taip pat kuriais nustatomas minimalus ES atitikties deklaracijos turinys ir papildomi elementai, kurie turi būti įtraukti į techninius dokumentus . 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[30] 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; Įgaliojimai priimti deleguotuosius aktus pagal šį reglamentą Komisijai turėtų būti suteikti penkerių metų laikotarpiui nuo … [šio reglamento įsigaliojimo diena]. Likus ne mažiau kaip devyniems mėnesiams iki penkerių metų laikotarpio pabaigos Komisija turėtų parengti naudojimosi deleguotaisiais įgaliojimais ataskaitą. Deleguotieji įgaliojimai turėtų būti savaime pratęsiami tokios pačios trukmės laikotarpiams, išskyrus atvejus, kai Europos Parlamentas arba Taryba pareiškia prieštaravimų dėl tokio pratęsimo likus ne mažiau kaip trims mėnesiams iki kiekvieno laikotarpio pabaigos;

[30] OL L 123, 2016 5 12, p. 1.

(118) siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai nustatyti šio reglamento priede nustatytų svarbių produktų su skaitmeniniais elementais kategorijų techninį aprašymą, nustatyti PĮMŽ formatą ir elementus, papildomai patikslinti gamintojų teikiamų pranešimų apie aktyviai išnaudojamus pažeidžiamumus ir didelius incidentus, darančius poveikį produktų su skaitmeniniais elementais saugumui, formatą ir procedūrą, nustatyti bendrąsias specifikacijas, apimančias techninius reikalavimus, kuriais sudaroma galimybė laikytis šio reglamento priede nustatytų esminių kibernetinio saugumo reikalavimų , nustatyti technines specifikacijas etiketėms, piktogramoms arba bet kokiems kitiems su produktų su skaitmeniniais elementais saugumu susijusiems ženklams, jų palaikymo laikotarpį ir mechanizmus, kuriais skatinamas jų naudojimas ir didinamas visuomenės informuotumas apie produktų su skaitmeniniais elementais saugumą, nustatyti supaprastintą dokumentų formą, skirtą labai mažų įmonių ir mažųjų įmonių poreikiams, ir Sąjungos lygmeniu priimti sprendimus dėl taisomųjų arba ribojamųjų priemonių išimtinėmis 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[31];

(119) siekiant užtikrinti pasitikėjimu grindžiamą ir konstruktyvų rinkos priežiūros institucijų bendradarbiavimą Sąjungos ir nacionaliniu lygmenimis, visi subjektai, taikantys šį reglamentą, turėtų laikytis informacijos ir duomenų, gautų vykdant savo užduotis, konfidencialumo;

---

[31] 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(120) 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 nacionalinės teisės aktuose numatomi administracinių baudų dydžiai už šiame reglamente nustatytų pareigų nevykdymą. Priimant sprendimą dėl administracinės baudos dydžio kiekvienu konkrečiu atveju turėtų būti atsižvelgta į visas atitinkamas konkrečios situacijos aplinkybes ir bent jau į šiame reglamente aiškiai nustatytas aplinkybes, įskaitant tai, ar gamintojas yra labai maža įmonė arba mažoji ar vidutinė įmonė, įskaitant startuolius, ir į tai, ar tos pačios arba kitos rinkos priežiūros institucijos jau yra skyrusios administracines baudas tam pačiam ekonominės veiklos vykdytojui už panašų pažeidimą. Tokios aplinkybės galėtų būti sunkinančios tais atvejais, kai tas pats ekonominės veiklos vykdytojas toliau tęsia pažeidimą kitų valstybių narių nei tos, kurioje administracinė bauda jau paskirta, teritorijose, arba lengvinančios, siekiant užtikrinti, kad svarstant skirti bet kokią kitą administracinę baudą, kurią svarsto skirti 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 svarbiomis konkrečiomis aplinkybėmis. Visais tokiais atvejais bendra administracinė bauda, kurią skirtingų valstybių narių rinkos priežiūros institucijos galėtų skirti tam pačiam ekonominės veiklos vykdytojui už tos pačios rūšies pažeidimą, turėtų atitikti proporcingumo principą. Atsižvelgiant į tai, kad administracinės baudos netaikomos labai mažoms įmonėms arba mažosioms įmonėms už tai, kad jos nesilaikė 24 valandų ankstyvojo perspėjimo apie aktyviai išnaudojamą pažeidžiamumą arba didelius incidentus, darančius poveikį produkto su skaitmeniniais elementais saugumui, termino, taip pat atvirosios programinės įrangos valdytojams už bet kokį šio reglamento pažeidimą, ir atsižvelgiant į principą, kad sankcijos turėtų būti veiksmingos, proporcingos ir atgrasomos, valstybės narės tiems subjektams neturėtų skirti kitų rūšių piniginio pobūdžio sankcijų;

(121) jei administracinės baudos skiriamos asmeniui, kuris 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;

(122) valstybės narės, atsižvelgdamos į nacionalines aplinkybes, turėtų išnagrinėti galimybę naudoti pajamas iš šiame reglamente numatytų sankcijų arba jų finansinį ekvivalentą kibernetinio saugumo politikai remti ir kibernetinio saugumo lygiui Sąjungoje didinti, *inter alia*, didinant kvalifikuotų kibernetinio saugumo specialistų skaičių, stiprinant labai mažų įmonių ir mažųjų bei vidutinių įmonių pajėgumą ir didinant visuomenės informuotumą apie kibernetines grėsmes;

(123) palaikydama santykius su trečiosiomis valstybėmis, Sąjunga siekia skatinti tarptautinę prekybą reglamentuojamais produktais. Siekiant palengvinti prekybą, gali būti taikomos įvairios priemonės, įskaitant keletą teisinių priemonių, pavyzdžiui, 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. Tie 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 su keliomis trečiosiomis valstybėmis. Tie abipusio pripažinimo susitarimai sudaromi dėl tam tikrų konkrečių sektorių, kurie skirtingose trečiosiose 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 trečiosiomis valstybėmis partnerėmis, kad kibernetinis atsparumas būtų sustiprintas visame pasaulyje, nes ilgainiui tai prisidės prie stipresnės kibernetinio saugumo sistemos tiek Sąjungos viduje, tiek už jos ribų;

(124) vartotojai turėtų turėti teisę ginti savo teises, susijusias su šiame reglamente ekonominės veiklos vykdytojams nustatytomis pareigomis, pareikšdami atstovaujamuosius ieškinius pagal Europos Parlamento ir Tarybos direktyvą (ES) 2020/1828[32]. Tuo tikslu šiame reglamente turėtų būti nustatyta, kad Direktyva (ES) 2020/1828 taikoma atstovaujamiesiems ieškiniams dėl šio reglamento pažeidimų, kuriais pažeidžiami arba gali būti pažeisti kolektyviniai vartotojų interesai. Todėl tos direktyvos I priedas turėtų būti atitinkamai iš dalies pakeistas. Valstybės narės turi užtikrinti, kad tie pakeitimai būtų atspindėti jų perkėlimo į nacionalinę teisę priemonėse, patvirtintose pagal tą direktyvą, nors nacionalinių perkėlimo į nacionalinę teisę priemonių patvirtinimas tuo atžvilgiu nėra tos direktyvos taikytinumo tiems atstovaujamiesiems ieškiniams sąlyga. Tos direktyvos taikytinumas atstovaujamiesiems ieškiniams, pareikštiems dėl ekonominės veiklos vykdytojų padarytų šio reglamento pažeidimų, kuriais pažeidžiami arba gali būti pažeisti kolektyviniai vartotojų interesai, turėtų prasidėti nuo … [36 mėnesiai nuo šio reglamento įsigaliojimo dienos];

(125) Komisija, konsultuodamasi su atitinkamais suinteresuotaisiais subjektais, turėtų periodiškai vertinti ir peržiūrėti šį reglamentą, visų pirma siekdama nustatyti, ar reikia jį keisti atsižvelgiant į kintančias visuomenines, politines, technologines ar rinkos sąlygas. Šiuo reglamentu bus sudarytos palankesnės sąlygos subjektams, kuriems taikomas Reglamentas (ES) 2022/2554 ir Direktyva (ES) 2022/2555 ir kurie naudoja produktus su skaitmeniniais elementais, laikytis tiekimo grandinės saugumo pareigų. Atlikdama tą periodinę peržiūrą Komisija turėtų įvertinti bendrą Sąjungos kibernetinio saugumo sistemos poveikį;

---

[32] 2020 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva (ES) 2020/1828 dėl atstovaujamųjų ieškinių siekiant apsaugoti vartotojų kolektyvinius interesus, kuria panaikinama Direktyva 2009/22/EB (OL L 409, 2020 12 4, p. 1).

(126) ekonominės veiklos vykdytojams turėtų būti skirta pakankamai laiko prisitaikyti prie šiame reglamente nustatytų reikalavimų. Šis reglamentas turėtų būti taikomas nuo … [36 mėnesiai nuo šio reglamento įsigaliojimo dienos] , išskyrus nuostatas dėl pareigos pranešti apie aktyviai išnaudojamus pažeidžiamumus ir didelius incidentus, darančius poveikį produktų su skaitmeniniais elementais saugumui, kurios turėtų būti taikomos nuo … [21 mėnuo nuo šio reglamento įsigaliojimo dienos], ir nuostatas dėl atitikties vertinimo įstaigų notifikavimo, kurios turėtų būti taikomos nuo … [18 mėnesių nuo šio reglamento įsigaliojimo dienos];

(127) svarbu teikti paramą labai mažoms įmonėms ir mažosioms bei vidutinėms įmonėms, įskaitant startuolius, įgyvendinant šį reglamentą ir kuo labiau sumažinti įgyvendinimo riziką, kylančią dėl žinių ir patirties rinkoje trūkumo, taip pat siekiant sudaryti palankesnes sąlygas gamintojams laikytis šiame reglamente nustatytų pareigų. Pagal Skaitmeninės Europos programą ir kitas atitinkamas Sąjungos programas teikiama finansinė ir techninė parama, kad tos įmonės galėtų prisidėti prie Sąjungos ekonomikos augimo ir bendro kibernetinio saugumo lygio Sąjungoje stiprinimo. Europos kibernetinio saugumo kompetencijos centras ir nacionaliniai koordinavimo centrai, taip pat Komisijos ir valstybių narių Sąjungos ar nacionaliniu lygmeniu įsteigti Europos skaitmeninių inovacijų centrai taip pat galėtų remti įmones ir viešojo sektoriaus organizacijas ir galėtų prisidėti prie šio reglamento įgyvendinimo. Pagal savo atitinkamas misijas ir kompetencijos sritis jie galėtų teikti techninę ir mokslinę paramą labai mažoms įmonėms ir mažosioms bei vidutinėms įmonėms, pavyzdžiui, kai vykdoma bandymų veikla ir trečiųjų šalių atliekami atitikties vertinimai. Jie taip pat galėtų paskatinti diegti priemones, kuriomis būtų palengvintas šio reglamento įgyvendinimas;

(128) be to, valstybės narės turėtų apsvarstyti galimybę imtis papildomų veiksmų, kuriais būtų siekiama teikti gaires ir paramą labai mažoms įmonėms ir mažosioms bei vidutinėms įmonėms, pavyzdžiui, sukurti apribotą bandomąją reglamentavimo aplinką ir specialius komunikacijos kanalus. Siekdamos padidinti kibernetinio saugumo lygį Sąjungoje, valstybės narės taip pat gali apsvarstyti galimybę teikti paramą su skaitmeninių elementų turinčių produktų kibernetiniu saugumu susijusiems pajėgumams ir įgūdžiams plėtoti, ekonominės veiklos vykdytojų, visų pirma labai mažų įmonių ir mažųjų bei vidutinių įmonių, kibernetiniam atsparumui gerinti ir visuomenės informuotumui apie produktų su skaitmeniniais elementais kibernetinį saugumą didinti;

(129) 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 nurodytiems tikslams pasiekti;

(130) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725[33] 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis pateikė nuomonę 2022 m. lapkričio 9 d.[34],

PRIĖMĖ ŠĮ REGLAMENTĄ:

---

33 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).

34 OL C 452, 2022 11 29, p. 23.

I skyrius
Bendrosios nuostatos

1 straipsnis

Dalykas

Šiuo reglamentu nustatoma:

a) produktų su skaitmeniniais elementais tiekimo rinkai taisyklės, siekiant užtikrinti tokių produktų kibernetinį saugumą;

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

c) pažeidžiamumo valdymo procesų, kuriuos gamintojai nustatė, kad užtikrintų produktų su skaitmeniniais elementais kibernetinį saugumą per numatomą produktų naudojimo laikotarpį, esminiai kibernetinio saugumo reikalavimai ir ekonominės veiklos vykdytojų pareigos, susijusios su tais procesais;

d) rinkos priežiūros, įskaitant stebėseną, taisyklės ir šiame straipsnyje nurodytų taisyklių ir reikalavimų vykdymo užtikrinimo nuostatos.

2 straipsnis

Taikymo sritis

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

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. Šis reglamentas netaikomas įrangai, kuriai taikoma Europos Parlamento ir Tarybos direktyva 2014/90/ES[35].

[35] 2014 m. liepos 23 d. Europos Parlamento ir Tarybos direktyva 2014/90/ES dėl laivų įrenginių, kuria panaikinama Tarybos direktyva 96/98/EB (OL L 257, 2014 8 28, p. 146).

5. 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 kibernetinio saugumo reikalavimai, gali būti apribotas arba jis gali būti netaikomas, jei:

   a) toks apribojimas arba toks netaikymas atitinka bendrą tiems produktams taikomą reglamentavimo sistemą, ir

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

   Komisijai pagal 61 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, siekiant šį reglamentą papildyti, kuriais nurodoma, ar toks apribojimas arba netaikymas yra būtinas, nurodomi susiję produktai ir taisyklės, taip pat, jei taikytina, apribojimo taikymo sritis.

6. Šis reglamentas netaikomas atsarginėms dalims, kurios tiekiamos rinkai identiškiems komponentams produktuose su skaitmeniniais elementais pakeisti ir kurios gaminamos pagal tas pačias specifikacijas kaip ir komponentai, kuriuos jomis ketinama pakeisti.

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

8. Šiame reglamente nustatytos pareigos nereiškia, kad bus teikiama informacija, kurios atskleidimas prieštarautų esminiams valstybių narių nacionalinio saugumo, viešojo saugumo ar gynybos interesams.

3 straipsnis

Terminų 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 gamintojas arba tai daroma jo atsakomybe, ir be kurio produktas su skaitmeniniais elementais negalėtų atlikti vienos iš savo funkcijų;

3) kibernetinis saugumas – kibernetinis saugumas, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 1 punkte;

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

5) aparatinė įranga – fizinė elektroninė informacinė sistema ar jos dalys, galinčios apdoroti, saugoti ar perduoti skaitmeninius duomenis;

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

7) elektroninė informacinė sistema – sistema, įskaitant elektros ar elektroninę įrangą, galinti apdoroti, saugoti ar perduoti skaitmeninius duomenis;

8) loginė jungtis – virtuali duomenų jungtis per programinės įrangos sąsają;

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

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

11) galinis įrenginys – bet koks įrenginys, prijungtas prie tinklo ir naudojamas kaip prieigos prie to tinklo priemonė;

12) ekonominės veiklos vykdytojas – gamintojas, įgaliotasis atstovas, importuotojas, platintojas arba kitas fizinis ar juridinis asmuo, kuriam taikomos pareigos, susijusios su produktų su skaitmeniniais elementais gamyba ar produktų su skaitmeniniais elementais tiekimu rinkai, pagal šį reglamentą;

13) 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, monetizavimą arba nemokamai;

14) atvirosios programinės įrangos valdytojas – juridinis asmuo, kuris nėra gamintojas, kurio tikslas ar užduotis – sistemingai nuolat teikti paramą konkrečių produktų su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga ir kurie skirti komercinei veiklai, kūrimui ir kuris užtikrina tų produktų gyvybingumą;

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

16) 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;

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

18) vartotojas – fizinis asmuo, kuris veikia siekdamas tikslų, kurie nėra susiję su to asmens komercine veikla, verslu, amatu ar profesija;

19) labai mažos įmonės, mažosios įmonės ir vidutinės įmonės – atitinkamai labai mažos įmonės, mažosios įmonės ir vidutinės įmonės, kaip apibrėžta Komisijos rekomendacijos 2003/361/EB priede;

20) palaikymo laikotarpis – laikotarpis, per kurį gamintojas privalo užtikrinti, kad produkto su skaitmeniniais elementais pažeidžiamumai būtų valdomi veiksmingai ir laikantis I priedo II dalyje nustatytų esminių kibernetinio saugumo reikalavimų;

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

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

23) 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 aprašymuose ir techniniuose dokumentuose;

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

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

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

27) atitikties vertinimas – tikrinimo, ar įvykdyti I priede nustatyti esminiai kibernetinio saugumo reikalavimai, procesas;

28) atitikties vertinimo įstaiga – atitikties vertinimo įstaiga, kaip apibrėžta Reglamento (EB) Nr. 765/2008 2 straipsnio 13 punkte;

29) notifikuotoji įstaiga – atitikties vertinimo įstaiga, paskirta pagal 43 straipsnį ir kitus atitinkamus Sąjungos derinamuosius teisės aktus;

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

31) CE ženklas – ženklas, kuriuo gamintojas nurodo, kad produktas su skaitmeniniais elementais ir gamintojo įdiegti procesai atitinka I priede nustatytus esminius kibernetinio saugumo reikalavimus ir kitus taikomus Sąjungos derinamuosius teisės aktus, kuriais nustatomas toks ženklinimas;

32) Sąjungos derinamieji teisės aktai – Sąjungos teisės aktai, išvardyti Reglamento (ES) 2019/1020 I priedo sąraše, ir kiti Sąjungos teisės aktai, kuriais suderinamos gaminių, kuriems taikomas tas reglamentas, pardavimo sąlygos;

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

34) tarptautinis standartas – tarptautinis standartas, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkto a papunktyje;

35) Europos standartas – Europos standartas, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkto b papunktyje;

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

37) kibernetinio saugumo rizika – nuostolio arba sutrikimo, kurį sukelia incidentas, potencialas; ji išreiškiama kaip tokio nuostolio arba sutrikimo masto ir to incidento įvykimo tikimybės derinys;

38) didelė 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;

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

40) pažeidžiamumas – produkto su skaitmeniniais elementais silpnoji vieta, jautrumas ar trūkumas, kuriais gali būti pasinaudota kibernetinei grėsmei kelti;

41) pažeidžiamumas, kurį galima išnaudoti – pažeidžiamumas, kurį gali veiksmingai panaudoti priešininkas praktinėmis veiklos sąlygomis;

42) aktyviai išnaudojamas pažeidžiamumas – pažeidžiamumas, kuriuo, kaip matyti iš patikimų įrodymų, piktavalis subjektas pasinaudojo sistemoje be sistemos savininko leidimo;

43) incidentas – incidentas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 6 punkte;

44) incidentas, darantis poveikį produkto su skaitmeniniais elementais saugumui – incidentas, kuris neigiamai veikia arba gali neigiamai paveikti produkto su skaitmeniniais elementais gebėjimą apsaugoti duomenų arba funkcijų prieinamumą, autentiškumą, vientisumą ar konfidencialumą;

45) vos neįvykęs incidentas – vos neįvykęs incidentas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 5 punkte;

46) kibernetinė grėsmė – kibernetinė grėsmė, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 8 punkte;

47) asmens duomenys – asmens duomenys, kaip apibrėžta Reglamento (ES) 2016/679 4 straipsnio 1 punkte;

48) laisvoji ir atviroji programinė įranga – programinė įranga, kurios pirminiu kodu atvirai dalijamasi ir kuri pateikiama pagal laisvąją atvirojo kodo licenciją, kurioje numatytos visos teisės padaryti, kad ji būtų laisvai prieinama, naudojama, keičiama ir pakartotinai platinama;

49) atšaukimas – atšaukimas, kaip apibrėžta Reglamento (ES) 2019/1020 3 straipsnio 22 punkte;

50) pašalinimas – pašalinimas, kaip apibrėžta Reglamento (ES) 2019/1020 3 straipsnio 23 punkte;

51) koordinatore paskirta CSIRT – pagal Direktyvos (ES) 2022/2555 12 straipsnio 1 dalį koordinatore paskirta CSIRT.

4 straipsnis

Laisvas judėjimas

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

2. Prekybos mugėse, parodose ir demonstracijose ar panašiuose renginiuose valstybės narės netrukdo pristatyti ar naudoti produkto su skaitmeniniais elementais, kuris neatitinka šio reglamento, įskaitant produkto prototipus, jei tas produktas pateikiamas su matomu ženklu, aiškiai nurodančiu, kad jis neatitinka šio reglamento, ir nebus tiekiamas rinkai, kol neatitiks šio reglamento.

3. Valstybės narės netrukdo tiekti rinkai nebaigtos programinės įrangos, kuri neatitinka šio reglamento, jei ta programinė įranga tiekiama tik ribotą bandymo tikslais reikalingą laikotarpį su matomu ženklu, aiškiai nurodančiu, jog ji neatitinka šio reglamento ir nebus tiekiama rinkai kitais tikslais, kurie nėra bandymo tikslai.

4. 3 dalis netaikoma saugos komponentams, kaip nurodyta kituose nei šis reglamentas Sąjungos derinamuosiuose teisės aktuose.

5 straipsnis

Produktų su skaitmeniniais elementais viešieji pirkimai arba naudojimas

1. Šiuo reglamentu valstybėms narėms neužkertamas kelias produktams su skaitmeniniais elementais taikyti papildomų kibernetinio saugumo reikalavimų, kai tie produktai perkami arba naudojami konkrečiais tikslais, įskaitant atvejus, kai tie produktai perkami arba naudojami nacionalinio saugumo ar gynybos tikslais, jei tokie reikalavimai dera su Sąjungos teisėje nustatytomis valstybių narių pareigomis ir yra būtini ir proporcingi tiems tikslams pasiekti.

2. Nedarant poveikio direktyvoms 2014/24/ES ir 2014/25/ES, kai perkami produktai su skaitmeniniais elementais, patenkantys į šio reglamento taikymo sritį, valstybės narės užtikrina, kad viešųjų pirkimų procese būtų atsižvelgiama į atitiktį šio reglamento I priede nustatytiems esminiams kibernetinio saugumo reikalavimams, įskaitant gamintojų gebėjimą veiksmingai valdyti pažeidžiamumus.

6 straipsnis

Produktams su skaitmeniniais elementais taikomi reikalavimai

Produktai su skaitmeniniais elementais tiekiami rinkai tik jei:

a) jie atitinka I priedo I dalyje nustatytus esminius kibernetinio saugumo reikalavimus, su sąlyga, kad jie yra tinkamai įrengiami, techniškai prižiūrimi, naudojami pagal numatytąją paskirtį arba tokiomis sąlygomis, kurias galima pagrįstai numatyti, ir, jei taikytina, juose yra įdiegti reikiami saugumo naujiniai, ir

b) gamintojo įdiegti procesai atitinka I priedo II dalyje nustatytus esminius kibernetinio saugumo reikalavimus.

7 straipsnis

Svarbūs produktai su skaitmeniniais elementais

1. Produktai su skaitmeniniais elementais, kurie turi pagrindinę III priede nustatytos produktų kategorijos funkciją, laikomi svarbiais produktais su skaitmeniniais elementais ir jiems taikomos 32 straipsnio 2 ir 3 dalyse nurodytos atitikties vertinimo procedūros. Dėl produkto su skaitmeniniais elementais, kuris turi pagrindinę III priede nustatytos produktų kategorijos funkciją, integravimo, produktui, į kurį jis integruojamas, nėra automatiškai taikomos 32 straipsnio 2 ir 3 dalyse nurodytos atitikties vertinimo procedūros.

2. Šio straipsnio 1 dalyje nurodytos produktų su skaitmeniniais elementais kategorijos, suskirstytos į I ir II klases, kaip nustatyta III priede, turi atitikti bent vieną iš šių kriterijų:

a) produktas su skaitmeniniais elementais visų pirma atlieka funkcijas, kurios yra ypatingos svarbos kitų produktų, tinklų ar paslaugų kibernetiniam saugumui, įskaitant saugaus tapatumo nustatymo ir prieigos užtikrinimą, įsibrovimo prevenciją ir aptikimą, galinių įrenginių saugumą arba tinklo apsaugą;

b) produktas su skaitmeniniais elementais atlieka funkciją, dėl kurios kyla didelė neigiamo poveikio rizika, susijusi su jos intensyvumu ir gebėjimu sutrikdyti, kontroliuoti arba padaryti žalos dideliam skaičiui kitų produktų arba jo naudotojų sveikatai, saugumui ar saugai per tiesioginę manipuliaciją, pavyzdžiui, centrinės sistemos funkciją, įskaitant tinklo administravimą, konfigūracijos kontrolę, virtualizavimą arba asmens duomenų tvarkymą.

3. Komisijai pagal 61 straipsnį suteikiami įgaliojamai priimti deleguotuosius aktus, siekiant iš dalies pakeisti III priedą, kuriais į produktų su skaitmeniniais elementais kategorijų sąrašą įtraukiama nauja kiekvienos produktų klasės kategorija, patikslinama jos apibrėžtis, perkeliama produktų kategorija iš vienos klasės į kitą arba pašalinama esama kategorija iš to sąrašo. Vertindama poreikį iš dalies pakeisti III priede pateiktą sąrašą, Komisija atsižvelgia į su kibernetiniu saugumu susijusias funkcijas arba funkciją ir kibernetinio saugumo rizikos, kurią kelia produktai su skaitmeniniais elementais, lygį, nustatytą pagal šio straipsnio 2 dalyje nurodytus kriterijus.

Šios dalies pirmoje pastraipoje nurodytuose deleguotuosiuose aktuose atitinkamais atvejais nustatomas ne trumpesnis kaip 12 mėnesių pereinamasis laikotarpis, visų pirma tais atvejais, kai į I arba II klasę įtraukiama nauja svarbių produktų su skaitmeniniais elementais kategorija arba tokia kategorija perkeliama iš I klasės į II klasę, kaip nustatyta III priede, prieš pradedant taikyti atitinkamas 32 straipsnio 2 ir 3 dalyse nurodytas atitikties vertinimo procedūras, išskyrus atvejus, kai trumpesnis pereinamasis laikotarpis yra pateisinamas dėl privalomų priežasčių, dėl kurių privaloma skubėti.

4. Ne vėliau kaip … [12 mėnesių nuo šio reglamento įsigaliojimo dienos] Komisija priima įgyvendinimo aktą, kuriuo nustatomas I ir II klasėms, nustatytoms III priede, priskirtų produktų su skaitmeniniais elementais kategorijų techninis aprašymas ir IV priede nustatytų produktų su skaitmeniniais elementais kategorijų techninis aprašymas. Tas įgyvendinimo aktas priimamas laikantis 62 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

8 straipsnis

Ypatingos svarbos produktai su skaitmeniniais elementais

1. Komisijai pagal 61 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, siekiant šį reglamentą papildyti, kuriais nustatoma, kuriems produktams su skaitmeniniais elementais, turintiems pagrindinę šio reglamento IV priede nustatytos produktų kategorijos funkciją, taikomas reikalavimas gauti Europos kibernetinio saugumo sertifikatą, kuriame būtų pažymėta, kad saugumo užtikrinimo lygis yra bent „pakankamai aukštas“ pagal Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Reglamentą (ES) 2019/881, siekiant įrodyti atitiktį šio reglamento I priede arba jo dalyse nustatytiems esminiams kibernetinio saugumo reikalavimams, jei pagal Reglamentą (ES) 2019/881 buvo priimta Europos kibernetinio saugumo sertifikavimo schema, apimanti tų kategorijų produktus su skaitmeniniais elementais, ir gamintojai gali ja naudotis. Tuose deleguotuosiuose aktuose nustatomas reikalaujamas saugumo užtikrinimo lygis, kuris turi būti proporcingas kibernetinio saugumo rizikos, susijusios su produktais su skaitmeniniais elementais, lygiui, ir nustatant tą lygį turi būti atsižvelgiama į tų produktų numatytąją paskirtį, įskaitant Direktyvos (ES) 2022/2555 3 straipsnio 1 dalyje nurodytų esminių subjektų kritinę priklausomybę nuo tų produktų.

   Prieš priimdama tokius deleguotuosius aktus, Komisija įvertina galimą numatomų priemonių poveikį rinkai ir konsultuojasi su atitinkamais suinteresuotaisiais subjektais, įskaitant pagal Reglamentą (ES) 2019/881 įsteigtą Europos kibernetinio saugumo sertifikavimo grupę. Atliekant vertinimą atsižvelgiama į valstybių narių pasirengimą ir pajėgumo įgyvendinti atitinkamą Europos kibernetinio saugumo sertifikavimo schemą lygį. Jei nėra priimta šios dalies pirmoje pastraipoje nurodytų deleguotųjų aktų, produktams su skaitmeniniais elementais, turintiems IV priede nustatytos produktų kategorijos pagrindinę funkciją, taikomos 32 straipsnio 3 dalyje nurodytos atitikties vertinimo procedūros.

Pirmoje pastraipoje nurodytuose deleguotuosiuose aktuose nustatomas ne trumpesnis kaip šešių mėnesių pereinamasis laikotarpis, išskyrus atvejus, kai trumpesnis pereinamasis laikotarpis yra pagrįstas dėl privalomų priežasčių, dėl kurių privaloma skubėti.

2. Komisijai pagal 61 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, siekiant iš dalies pakeisti IV priedą, kuriais įtraukiamos ar pašalinamos ypatingos svarbos produktų su skaitmeniniais elementais kategorijos. Nustatant tokias ypatingos svarbos produktų su skaitmeniniais elementais kategorijas ir reikalaujamą saugumo užtikrinimo lygį pagal šio straipsnio 1 dalį, Komisija atsižvelgia į 7 straipsnio 2 dalyje nurodytus kriterijus ir užtikrina, kad produktų su skaitmeniniais elementais kategorijos atitiktų bent vieną iš šių kriterijų:

a) esama Direktyvos (ES) 2022/2555 3 straipsnyje nurodytų esminių subjektų kritinės priklausomybės nuo konkrečios produktų su skaitmeniniais elementais kategorijos;

b) incidentai ir pažeidžiamumai, kuriuos galima išnaudoti, susiję su konkrečia produktų su skaitmeniniais elementais kategorija, galėtų sukelti didelių ypatingos svarbos tiekimo grandinių sutrikimų visoje vidaus rinkoje.

Prieš priimdama tokius deleguotuosius aktus, Komisija atlieka 1 dalyje nurodyto tipo vertinimą.

Pirmoje pastraipoje nurodytuose deleguotuosiuose aktuose nustatomas ne trumpesnis kaip šešių mėnesių pereinamasis laikotarpis, išskyrus atvejus, kai trumpesnis pereinamasis laikotarpis yra pagrįstas dėl privalomų priežasčių, dėl kurių privaloma skubėti.

9 straipsnis

Konsultacijos su suinteresuotaisiais subjektais

1. Rengiant šio reglamento įgyvendinimo priemones, Komisija konsultuojasi su atitinkamais suinteresuotaisiais subjektais, pavyzdžiui, atitinkamomis valstybių narių institucijomis, privačiojo sektoriaus įmonėmis, įskaitant labai mažas įmones ir mažąsias bei vidutines įmones, atvirosios programinės įrangos bendruomene, vartotojų asociacijomis, akademine bendruomene ir atitinkamomis Sąjungos agentūromis bei organais, taip pat su Sąjungos lygmeniu įsteigtomis ekspertų grupėmis, ir atsižvelgia į jų nuomones. Visų pirma Komisija, kai tinkama, struktūrizuotai konsultuojasi su tais suinteresuotaisiais subjektais ir prašo jų pareikšti nuomonę, kai:

   a) rengiamos 26 straipsnyje nurodytos gairės;

   b) rengiami III priede nustatytų produktų kategorijų techniniai aprašymai pagal 7 straipsnio 4 dalį, vertinamas galimas poreikis atnaujinti produktų kategorijų sąrašą pagal 7 straipsnio 3 dalį ir 8 straipsnio 2 dalį arba atliekamas 8 straipsnio 1 dalyje nurodytas galimo poveikio rinkai vertinimas, nedarant poveikio 61 straipsniui;

   c) atliekamas parengiamasis darbas, susijęs su šio reglamento vertinimu ir peržiūra.

2. Komisija bent kartą per metus rengia reguliarias konsultacijas ir informacines sesijas, kad sužinotų 1 dalyje nurodytų suinteresuotųjų subjektų nuomones apie šio reglamento įgyvendinimą.

10 straipsnis

Įgūdžių stiprinimas kibernetiškai atsparioje skaitmeninėje aplinkoje

Šio reglamento tikslais ir siekiant reaguoti į specialistų poreikius, kad būtų remiamas šio reglamento įgyvendinimas, valstybės narės, kai tinkama, padedamos Komisijos, Europos kibernetinio saugumo kompetencijos centro ir ENISA, kartu visapusiškai atsižvelgdamos į valstybių narių atsakomybę švietimo srityje, propaguoja priemones ir strategijas, kuriomis siekiama:

a) ugdyti kibernetinio saugumo įgūdžius ir kurti organizacines bei technologines priemones, kad būtų užtikrintas pakankamas kvalifikuotų specialistų skaičius, siekiant padėti rinkos priežiūros institucijoms ir atitikties vertinimo įstaigoms vykdyti savo veiklą;

b) didinti privačiojo sektoriaus ir ekonominės veiklos vykdytojų bendradarbiavimą, be kita ko, perkvalifikuojant gamintojų darbuotojus, vartotojus, mokymo paslaugų teikėjus ir viešojo administravimo subjektus arba keliant jų kvalifikaciją ir tokiu būdu didinant galimybes jaunimui gauti darbą kibernetinio saugumo sektoriuje.

11 straipsnis

Bendroji produktų sauga

Nukrypstant nuo Reglamento (ES) 2023/988 2 straipsnio 1 dalies trečios pastraipos b punkto, to reglamento III skyriaus 1 skirsnis, V ir VII skyriai bei IX–XI skyriai taikomi produktams su skaitmeniniais elementais, atsižvelgiant į aspektus ir riziką arba rizikos kategorijas, kuriems netaikomas šis reglamentas, jei tiems produktams netaikomi konkretūs saugos reikalavimai, nustatyti kituose „Sąjungos derinamuosiuose teisės aktuose“, kaip apibrėžta Reglamento (ES) 2023/988 3 straipsnio 27 punkte.

12 straipsnis

Didelės rizikos DI sistemos

1. Nedarant poveikio su tikslumu ir patikimumu susijusiems reikalavimams, nustatytiems Reglamento (ES) 2024/1689 15 straipsnyje, laikoma, kad produktai su skaitmeniniais elementais, kurie patenka į šio reglamento taikymo sritį ir kurie yra priskiriami prie didelės rizikos DI sistemų pagal to reglamento 6 straipsnį, atitinka to reglamento 15 straipsnyje nustatytus kibernetinio saugumo reikalavimus, jei:

    a) tie produktai atitinka I priedo I dalyje nustatytus esminius kibernetinio saugumo reikalavimus;

b) gamintojo įdiegti procesai atitinka I priedo II dalyje nustatytus esminius kibernetinio saugumo reikalavimus, ir

c) pagal šį reglamentą išduota ES atitikties deklaracija įrodoma, kad pasiektas kibernetinio saugumo apsaugos lygis, kurio reikalaujama pagal Reglamento (ES) 2024/1689 15 straipsnį.

2. Šio straipsnio 1 dalyje nurodytiems produktams su skaitmeniniais elementais ir kibernetinio saugumo reikalavimams taikoma atitinkama atitikties vertinimo procedūra, numatyta Reglamento (ES) 2024/1689 43 straipsnyje. To vertinimo tikslais kompetenciją kontroliuoti didelės rizikos DI sistemų atitiktį pagal Reglamentą (ES) 2024/1689 turinčios notifikuotosios įstaigos taip pat turi kompetenciją kontroliuoti didelės rizikos DI sistemų, kurios patenka į šio reglamento taikymo sritį, atitiktį šio reglamento I priede nustatytiems reikalavimams, su sąlyga, kad atliekant notifikavimo pagal Reglamentą (ES) 2024/1689 procedūrą buvo įvertinta tų notifikuotųjų įstaigų atitiktis šio reglamento 39 straipsnyje nustatytiems reikalavimams.

3. Nukrypstant nuo šio straipsnio 2 dalies, šio reglamento III priede išvardytiems svarbiems produktams su skaitmeniniais elementais, kuriems taikomos šio reglamento 32 straipsnio 2 dalies a ir b punktuose bei 3 dalyje nurodytos atitikties vertinimo procedūros, ir šio reglamento IV priede išvardytiems ypatingos svarbos produktams su skaitmeniniais elementais, kuriems taikomas reikalavimas gauti Europos kibernetinio saugumo sertifikatą pagal šio reglamento 8 straipsnio 1 dalį arba, jei jo neturima, kuriems taikomos šio reglamento 32 straipsnio 3 dalyje nurodytos atitikties vertinimo procedūros, ir kurie pagal Reglamento (ES) 2024/1689 6 straipsnį priskiriami prie didelės rizikos DI sistemų ir kuriems taikoma Reglamento (ES) 2024/1689 VI priede nurodyta vidaus kontrole pagrįsta atitikties vertinimo procedūra, šiame reglamente numatytos atitikties vertinimo procedūros taikomos tiek, kiek tai susiję su šiame reglamente nustatytais esminiais kibernetinio saugumo reikalavimais.

4. Šio straipsnio 1 dalyje nurodytų produktų su skaitmeniniais elementais gamintojai gali dalyvauti Reglamento (ES) 2024/1689 57 straipsnyje nurodytoje apribotoje bandomojoje DI reglamentavimo aplinkoje.

II skyrius
Ekonominės veiklos vykdytojų pareigos ir nuostatos, susijusios su laisvąja ir atvirąja programine įranga

13 straipsnis

Gamintojų pareigos

1. Pateikdami produktą su skaitmeniniais elementais rinkai gamintojai užtikrina, kad tas produktas būtų suprojektuotas, sukurtas ir pagamintas laikantis I priedo I dalyje nustatytų esminių kibernetinio saugumo reikalavimų.

2. Siekdami laikytis 1 dalies 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 techninės priežiūros etapuose, kad būtų kuo labiau sumažinta kibernetinio saugumo rizika, išvengta incidentų ir kuo labiau sumažintas jų poveikis, įskaitant atvejus, kai tai susiję su naudotojų sveikata ir sauga.

3. Kibernetinio saugumo rizikos vertinimas dokumentuojamas ir, prireikus, atnaujinamas per palaikymo laikotarpį, kuris turi būti nustatytas pagal šio straipsnio 8 dalį. Tas kibernetinio saugumo rizikos vertinimas apima bent kibernetinio saugumo rizikos analizę, pagrįstą produkto su skaitmeniniais elementais numatytąja paskirtimi ir pagrįstai numatomu naudojimu, taip pat naudojimo sąlygomis, pavyzdžiui, veiklos aplinka arba apsaugomu turtu, atsižvelgiant į tikėtiną produkto naudojimo laikotarpį. Kibernetinio saugumo rizikos vertinime nurodoma, ar ir, jei taip, kokiu būdu atitinkamam produktui su skaitmeniniais elementais taikomi I priedo I dalies 2 punkte nustatyti saugumo reikalavimai ir kaip tie reikalavimai įgyvendinami remiantis kibernetinio saugumo rizikos vertinimu. Jame taip pat nurodoma, kaip gamintojas turi taikyti I priedo I dalies 1 punktą ir I priedo II dalyje nustatytus pažeidžiamumo valdymo reikalavimus.

4. Pateikdamas produktą su skaitmeniniais elementais rinkai gamintojas į pagal 31 straipsnį ir VII priedą reikalaujamus techninius dokumentus įtraukia šio straipsnio 3 dalyje nurodytą kibernetinio saugumo rizikos vertinimą. 12 straipsnyje nurodytų produktų su skaitmeniniais elementais, kuriems taip pat taikomi kiti Sąjungos teisės aktai, atveju kibernetinio saugumo rizikos vertinimas gali būti pagal tuos Sąjungos teisės aktus reikalaujamo rizikos vertinimo dalis. Jei produktui su skaitmeniniais elementais netaikomi tam tikri esminiai kibernetinio saugumo reikalavimai, gamintojas įtraukia tuo tikslu aiškų pagrindimą į techninius dokumentus.

5. Siekdami laikytis 1 dalies gamintojai atlieka išsamų patikrinimą, kai į produktus su skaitmeniniais elementais integruojami iš trečiųjų šalių gauti komponentai, kad tie komponentai nepakenktų produkto su skaitmeniniais elementais kibernetiniam saugumui, be kita ko, kai integruojami laisvosios ir atvirosios programinės įrangos komponentai, kurie netiekiami rinkai vykdant komercinę veiklą.

6. Nustatę pažeidžiamumą komponente, įskaitant atvirojo kodo komponentą, integruotą į produktą su skaitmeniniais elementais, gamintojai praneša apie pažeidžiamumą tą komponentą gaminančiam ar techniškai prižiūrinčiam asmeniui arba subjektui ir sprendžia bei pašalina pažeidžiamumo problemą laikantis I priedo II dalyje nustatytų pažeidžiamumo valdymo reikalavimų. Jei gamintojai yra sukūrę programinės ar aparatinės įrangos pakeitimą to komponento pažeidžiamumo problemai spręsti, jie, kai tinkama, kompiuterio skaitomu formatu dalijasi atitinkamu kodu arba dokumentais su tą komponentą gaminančiu ar techniškai prižiūrinčiu asmeniu arba subjektu.

7. Gamintojai sistemingai, proporcingai kibernetinio saugumo rizikai ir pobūdžiui, dokumentuoja atitinkamus kibernetinio saugumo aspektus, susijusius su produktais su skaitmeniniais elementais, įskaitant pažeidžiamumus, apie kuriuos jie sužino, ir visą aktualią trečiųjų šalių pateiktą informaciją ir, kai taikytina, atnaujina produkto kibernetinio saugumo rizikos vertinimą.

8. Pateikdami produktą su skaitmeniniais elementais rinkai ir per palaikymo laikotarpį gamintojai užtikrina, kad to produkto, įskaitant jo komponentus, pažeidžiamumai būtų veiksmingai valdomi laikantis I priedo II dalyje nustatytų esminių kibernetinio saugumo reikalavimų.

Gamintojai nustato tokį palaikymo laikotarpį, kad jis atspindėtų tikėtiną produkto naudojimo laikotarpį, visų pirma atsižvelgdami į pagrįstus naudotojų lūkesčius, produkto pobūdį, įskaitant jo numatytąją paskirtį, taip pat į atitinkamus Sąjungos teisės aktus, kuriais nustatoma produktų su skaitmeniniais elementais naudojimo trukmė. Nustatydami palaikymo laikotarpį, gamintojai taip pat gali atsižvelgti į produktų su skaitmeniniais elementais, turinčiais panašią funkciją, kuriuos rinkai pateikė kiti gamintojai, palaikymo laikotarpius, veiklos aplinkos prieinamumą, iš trečiųjų šalių gautų pagrindines funkcijas atliekančių integruotų komponentų palaikymo laikotarpius, taip pat į atitinkamas pagal 52 straipsnio 15 dalį įsteigtos specialios administracinio bendradarbiavimo grupės ir Komisijos pateiktas gaires. Į aspektus, į kuriuos turi būti atsižvelgiama nustatant palaikymo laikotarpį, atsižvelgiama taip, kad būtų užtikrintas proporcingumas.

Nedarant poveikio antrai pastraipai, palaikymo laikotarpis turi būti bent penkeri metai. Jei tikėtina, kad produktas su skaitmeniniais elementais bus naudojamas trumpiau nei penkerius metus, palaikymo laikotarpis turi atitikti tikėtiną naudojimo laiką.

Atsižvelgdama į 52 straipsnio 16 dalyje nurodytas administracinio bendradarbiavimo grupės rekomendacijas, Komisija pagal 61 straipsnį gali priimti deleguotuosius aktus, siekiant šį reglamentą papildyti, kuriais nustatomas minimalus palaikymo laikotarpis konkrečioms produktų kategorijoms, jei iš rinkos priežiūros duomenų matyti, kad palaikymo laikotarpiai yra nepakankami.

Gamintojai į VII priede nurodytus techninius dokumentus įtraukia informaciją, į kurią buvo atsižvelgta nustatant produkto su skaitmeniniais elementais palaikymo laikotarpį.

Gamintojai turi turėti tinkamą politiką ir procedūras, įskaitant I priedo II dalies 5 punkte nurodytą koordinuoto pažeidžiamumų atskleidimo politiką, kad tvarkytų ir pašalintų galimus produkto su skaitmeniniais elementais pažeidžiamumus, apie kuriuos pranešė vidiniai arba išoriniai šaltiniai.

9. Gamintojai užtikrina, kad kiekvienas saugumo naujinys, nurodytas I priedo II dalies 8 punkte, kuris naudotojams buvo pateiktas per palaikymo laikotarpį, po jo išleidimo liktų prieinamas ne trumpiau kaip 10 metų arba likusį palaikymo laikotarpio laiką, priklausomai nuo to, kuris terminas yra ilgesnis.

10. Jei gamintojas pateikė rinkai vėlesnių iš esmės pakeistų programinės įrangos produkto versijų, tas gamintojas gali užtikrinti, kad būtų laikomasi I priedo II dalies 2 punkte nustatyto esminio kibernetinio saugumo reikalavimo tik tos versijos, kurią gamintojas paskutinę pateikė rinkai, atveju, jei anksčiau rinkai pateiktų versijų naudotojai gali nemokamai naudotis paskutine rinkai pateikta versija ir nepatiria papildomų išlaidų, kad pritaikytų aparatinės ir programinės įrangos aplinką, kurioje jie naudoja pirminę to produkto versiją.

11. Gamintojai gali laikyti viešuosius programinės įrangos archyvus, kad naudotojams būtų lengviau susipažinti su ankstesnėmis versijomis. Tokiais atvejais naudotojai turi būti aiškiai ir lengvai prieinamu būdu informuojami apie riziką, susijusią su nepalaikomos programinės įrangos naudojimu.

12. Prieš pateikdami produktą su skaitmeniniais elementais rinkai gamintojai parengia 31 straipsnyje nurodytus techninius dokumentus.

Jie atlieka 32 straipsnyje nurodytas pasirinktas atitikties vertinimo procedūras arba paveda jas atlikti.

Jei pagal tą atitikties vertinimo procedūrą įrodyta, kad produktas su skaitmeniniais elementais atitinka I priedo I dalyje nustatytus esminius kibernetinio saugumo reikalavimus ir kad gamintojo įdiegti procesai atitinka I priedo II dalyje nustatytus esminius kibernetinio saugumo reikalavimus, gamintojas parengia ES atitikties deklaraciją pagal 28 straipsnį ir paženklina produktą CE ženklu pagal 30 straipsnį.

13. Gamintojas saugo techninius dokumentus ir ES atitikties deklaraciją bent 10 metų po produkto su skaitmeniniais elementais pateikimo rinkai dienos arba per palaikymo laikotarpį, priklausomai nuo to, kuris terminas yra ilgesnis, kad rinkos priežiūros institucijos galėtų su jais susipažinti.

14. Gamintojai užtikrina, kad būtų nustatytos procedūros, kurias taikant būtų išlaikoma serijinės gamybos būdu gaminamų produktų su skaitmeniniais elementais atitiktis šiam reglamentui. Gamintojai tinkamai atsižvelgia į produkto su skaitmeniniais elementais kūrimo ir gamybos procesų, taip pat projektavimo ir charakteristikų pakeitimus bei į 27 straipsnyje nurodytų darniųjų standartų, Europos kibernetinio saugumo sertifikavimo schemų arba bendrųjų specifikacijų, į kuriuos darant nuorodą deklaruojama produkto su skaitmeniniais elementais atitiktis arba kuriuos taikant tikrinama jo atitiktis, pakeitimus.

15. Gamintojai užtikrina, kad ant jų produktų su skaitmeniniais elementais būtų nurodytas tipo, partijos ar serijos numeris ar kitas elementas, pagal kurį juos galima identifikuoti, arba, jei to neįmanoma padaryti, užtikrina, kad ta informacija būtų pateikta ant jų pakuotės arba prie produkto su skaitmeniniais elementais pridedamame dokumente.

16. Ant produkto su skaitmeniniais elementais, ant jo pakuotės arba prie produkto su skaitmeniniais elementais pridedamame dokumente gamintojas nurodo savo pavadinimą, registruotą prekės pavadinimą arba registruotą prekių ženklą, pašto adresą, e. pašto adresą ar kitus skaitmeninių kontaktų duomenis, taip pat, kai taikytina, interneto svetainę, kuriais naudojantis galima susisiekti su gamintoju. Ta informacija taip pat įtraukiama į naudotojui skirtą informaciją ir instrukcijas, nustatytas II priede. Kontaktiniai duomenys turi būti pateikiami naudotojams ir rinkos priežiūros institucijoms lengvai suprantama kalba.

17. Šio reglamento tikslais gamintojai paskiria vieną bendrą kontaktinį punktą, kad naudotojai galėtų tiesiogiai ir greitai su jais susisiekti, be kita ko, kad būtų lengviau pranešti apie produkto su skaitmeniniais elementais pažeidžiamumus.

Gamintojai užtikrina, kad naudotojai galėtų lengvai nustatyti, kur yra vienas bendras kontaktinis punktas. Gamintojai taip pat nurodo vieną bendrą kontaktinį punktą naudotojui skirtoje informacijoje ir instrukcijose, nustatytose II priede.

Vienas bendras kontaktinis punktas leidžia naudotojams pasirinkti pageidaujamas komunikacijos priemones ir neapriboja tokių priemonių vien automatizuotomis priemonėmis.

18. Gamintojai užtikrina, kad prie produktų su skaitmeniniais elementais būtų pridėta naudotojui skirta informacija ir instrukcijos, nustatytos II priede, popierine arba elektronine forma. Tokia informacija ir instrukcijos pateikiamos tokia kalba, kurią gali lengvai suprasti naudotojai ir rinkos priežiūros institucijos. Jos turi būti aiškios, suprantamos, nesudėtingos ir įskaitomos. Jos turi užtikrinti galimybę saugiai įrengti, eksploatuoti ir naudoti produktus su skaitmeniniais elementais. Gamintojai saugo naudotojui skirtą informaciją ir instrukcijas, nustatytas II priede, bent 10 metų po produkto su skaitmeniniais elementais pateikimo rinkai dienos arba per palaikymo laikotarpį, priklausomai nuo to, kuris terminas yra ilgesnis, kad naudotojai ir nacionalinės rinkos priežiūros institucijos galėtų su jomis susipažinti. Jei tokia informacija ir instrukcijos teikiamos internete, gamintojai užtikrina, kad jos būtų prieinamos, patogios naudotojui ir kad su jomis būtų galima susipažinti internete bent 10 metų po produkto su skaitmeniniais elementais pateikimo rinkai dienos arba per palaikymo laikotarpį, priklausomai nuo to, kuris terminas yra ilgesnis.

19. Gamintojai užtikrina, kad 8 dalyje nurodyto palaikymo laikotarpio pabaigos data, įskaitant bent mėnesį ir metus, būtų aiškiai ir suprantamai nurodyta pirkimo metu lengvai prieinamu būdu ir, kai taikytina, ant produkto su skaitmeniniais elementais, jo pakuotės arba skaitmeninėmis priemonėmis.

Kai tai techniškai įmanoma atsižvelgiant į produkto su skaitmeniniais elementais pobūdį, gamintojai pateikia naudotojams pranešimą, kuriuo jie informuojami, kad atėjo jų produkto su skaitmeniniais elementais palaikymo laikotarpio pabaiga.

20. Gamintojai kartu su produktu su skaitmeniniais elementais pateikia ES atitikties deklaracijos kopiją arba supaprastintą ES atitikties deklaraciją. Jei pateikiama supaprastinta ES atitikties deklaracija, joje turi būti nurodytas tikslus interneto adresas, kuriuo galima gauti visą ES atitikties deklaracijos tekstą.

21. Pateikę produktą su skaitmeniniais elementais rinkai ir per palaikymo laikotarpį, jei gamintojai žino arba turi priežasčių manyti, kad produktas su skaitmeniniais elementais arba gamintojo įdiegti procesai neatitinka I priede nustatytų esminių kibernetinio saugumo reikalavimų, jie nedelsdami imasi taisomųjų priemonių, būtinų to produkto su skaitmeniniais elementais arba gamintojo procesų atitikčiai užtikrinti, arba, prireikus, jį atšaukti ar pašalinti.

22. Gamintojai, gavę pagrįstą rinkos priežiūros institucijos prašymą, pateikia tai institucijai tokia kalba, kurią ta institucija 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 kibernetinio saugumo reikalavimams. Tos institucijos prašymu gamintojai bendradarbiauja su ja dėl visų priemonių, kurių imamasi siekiant pašalinti jų rinkai pateikto produkto su skaitmeniniais elementais keliamą kibernetinio saugumo riziką.

23. Gamintojas, kuris nutraukia savo veiklą ir dėl to negali laikytis šio reglamento, prieš veiklos nutraukimą informuoja atitinkamas rinkos priežiūros institucijas, taip pat visomis turimomis priemonėmis ir, kiek įmanoma, informuoja atitinkamų rinkai pateiktų produktų su skaitmeniniais elementais naudotojus apie tai, kad ketinama nutraukti veiklą.

24. Komisija gali, atsižvelgdama į Europos ar tarptautinius standartus ir geriausią praktiką, įgyvendinimo aktais nustatyti I priedo II dalies 1 punkte nurodyto programinės įrangos medžiagų žiniaraščio formatą ir elementus. Tie įgyvendinimo aktai priimami laikantis 62 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

25. Siekiant įvertinti valstybių narių ir visos Sąjungos priklausomybę nuo programinės įrangos komponentų, visų pirma nuo komponentų, kurie priskiriami prie laisvosios ir atvirosios programinės įrangos, administracinio bendradarbiavimo grupė gali nuspręsti atlikti priklausomybės nuo konkrečių kategorijų produktų su skaitmeniniais elementais Sąjungos mastu vertinimą. Tuo tikslu rinkos priežiūros institucijos gali prašyti tokių kategorijų produktų su skaitmeniniais elementais gamintojų pateikti atitinkamus I priedo II dalies 1 punkte nurodytus programinės įrangos medžiagų žiniaraščius. Remdamosi tokia informacija, rinkos priežiūros institucijos gali pateikti administracinio bendradarbiavimo grupei anoniminę ir apibendrintą informaciją apie priklausomybę nuo programinės įrangos. Administracinio bendradarbiavimo grupė pateikia priklausomybės vertinimo rezultatų ataskaitą Bendradarbiavimo grupei, įsteigtai pagal Direktyvos (ES) 2022/2555 14 straipsnį.

14 straipsnis

Gamintojų pareiga pranešti

1. Gamintojas praneša apie visus aktyviai išnaudojamus produkto su skaitmeniniais elementais pažeidžiamumus, apie kuriuos sužino, tuo pačiu metu koordinatore paskirtai CSIRT pagal šio straipsnio 7 dalį ir ENISA. Gamintojas apie tą aktyviai išnaudojamą pažeidžiamumą praneša per bendrą pranešimų teikimo platformą, sukurtą pagal 16 straipsnį.

2. 1 dalyje nurodyto pranešimo tikslais gamintojas:

   a) nepagrįstai nedelsdamas ir bet kuriuo atveju per 24 valandas nuo tada, kai gamintojas apie jį sužino, pateikia ankstyvąjį perspėjimą apie aktyviai išnaudojamą pažeidžiamumą, nurodydamas, kai taikytina, valstybes nares, kurių teritorijoje, gamintojo žiniomis, jo produktas su skaitmeniniais elementais yra prieinamas;

b) išskyrus atvejus, kai atitinkama informacija jau yra pateikta, nepagrįstai nedelsdamas ir bet kuriuo atveju ne vėliau kaip per 72 valandas nuo tada, kai gamintojas sužino apie aktyviai išnaudojamą pažeidžiamumą, pateikia pranešimą apie pažeidžiamumą, kuriame pateikiama turima bendro pobūdžio informacija apie atitinkamą produktą su skaitmeniniais elementais, bendrą išnaudojimo ir atitinkamo pažeidžiamumo pobūdį, taip pat apie visas taisomąsias ar rizikos mažinimo priemones, kurių imtasi, ir apie taisomąsias ar rizikos mažinimo priemones, kurių gali imtis naudotojai, ir kuriame taip pat nurodoma, kai taikytina, kiek neskelbtina, gamintojo nuomone, yra jo pateikta informacija;

c) išskyrus atvejus, kai atitinkama informacija jau yra pateikta, pateikia galutinį pranešimą ne vėliau kaip per 14 dienų po to, kai buvo imtasi taisomosios ar rizikos mažinimo priemonės, įskaitant bent šią informaciją:

   i) pažeidžiamumo aprašymą, įskaitant jo sunkumą ir poveikį;

   ii) jei turima, informaciją apie bet kurį piktavalį subjektą, kuris išnaudojo arba išnaudoja pažeidžiamumą;

   iii) duomenis apie saugumo naujinius arba kitas taisomąsias priemones, kurių buvo imtasi siekiant pašalinti pažeidžiamumą.

3. Gamintojas praneša apie didelį incidentą, darantį poveikį produkto su skaitmeniniais elementais saugumui, apie kurį sužino, tuo pačiu metu koordinatore paskirtai CSIRT pagal šio straipsnio 7 dalį ir ENISA. Gamintojas apie tą incidentą praneša per bendrą pranešimų teikimo platformą, sukurtą pagal 16 straipsnį.

4. 3 dalyje nurodyto pranešimo tikslais gamintojas:

a) pateikia ankstyvąjį perspėjimą apie didelį incidentą, darantį poveikį produkto su skaitmeniniais elementais saugumui, nepagrįstai nedelsdamas ir bet kuriuo atveju per 24 valandas nuo tada, kai gamintojas apie jį sužino, be kita ko, bent tuo momentu, kai įtariama, kad incidentą sukėlė neteisėti ar piktavališki veiksmai, kuriame taip pat nurodomos, kai taikytina, valstybės narės, kurių teritorijoje, gamintojo žiniomis, jo produktas su skaitmeniniais elementais yra prieinamas;

b) išskyrus atvejus, kai atitinkama informacija jau yra pateikta, nepagrįstai nedelsdamas ir bet kuriuo atveju ne vėliau kaip per 72 valandas nuo tada, kai gamintojas sužino apie incidentą, pateikia pranešimą apie incidentą, kuriame pateikiama turima bendro pobūdžio informacija apie incidentą, pradinį incidento vertinimą, taip pat apie visas taisomąsias ar rizikos mažinimo priemones, kurių imtasi, visas taisomąsias ar rizikos mažinimo priemones, kurių gali imtis naudotojai, ir kuriame taip pat nurodoma, kai taikytina, kiek neskelbtina, gamintojo nuomone, yra jo pateikta informacija;

c) išskyrus atvejus, kai atitinkama informacija jau yra pateikta, pateikia galutinį pranešimą per vieną mėnesį nuo b punkte nurodyto pranešimo apie incidentą pateikimo dienos, įskaitant bent šią informaciją:

i) išsamų incidento, įskaitant jo sunkumą ir poveikį, aprašymą;

ii) grėsmės arba pagrindinės priežasties, dėl kurios incidentas galėjo būti sukeltas, tipą;

iii) taikomas ir įgyvendinamas rizikos mažinimo priemones.

5. 3 dalies tikslais incidentas, darantis poveikį produkto su skaitmeniniais elementais saugumui, laikomas dideliu, jei:

a) jis neigiamai veikia arba gali neigiamai paveikti produkto su skaitmeniniais elementais gebėjimą apsaugoti neskelbtinų ar svarbių duomenų arba funkcijų prieinamumą, autentiškumą, vientisumą ar konfidencialumą, arba

b) jis lėmė arba gali lemti piktavališko kodo įdiegimą į produktą su skaitmeniniais elementais arba produkto su skaitmeniniais elementais naudotojo tinklų ir informacines sistemas ar tokio kodo vykdymą.

6. Prireikus, koordinatore paskirta CSIRT, kuri pirmoji gavo pranešimą, gali paprašyti gamintojų pateikti tarpinį pranešimą apie atitinkamą atnaujintą padėties informaciją apie aktyviai išnaudojamą pažeidžiamumą arba didelį incidentą, darantį poveikį produkto su skaitmeniniais elementais saugumui.

7. Šio straipsnio 1 ir 3 dalyse nurodyti pranešimai teikiami per 16 straipsnyje nurodytą bendrą pranešimų teikimo platformą, naudojant vieną iš 16 straipsnio 1 dalyje nurodytų elektroninio pranešimo galinių įrenginių. Pranešimas pateikiamas naudojant valstybės narės, kurioje yra gamintojo pagrindinė buveinė Sąjungoje, koordinatore paskirtos CSIRT elektroninio pranešimo galinį įrenginį ir jis tuo pačiu metu turi būti prieinamas ENISA.

Šio reglamento tikslais laikoma, kad gamintojo pagrindinė buveinė Sąjungoje yra toje valstybėje narėje, kurioje daugiausia priimami su to gamintojo produktų su skaitmeniniais elementais kibernetiniu saugumu susiję sprendimai. Jei tokios valstybės narės neįmanoma nustatyti, laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje atitinkamas gamintojas turi padalinį, kuriame dirba daugiausia darbuotojų Sąjungoje.

Jei gamintojas neturi pagrindinės buveinės Sąjungoje, jis 1 ir 3 dalyse nurodytus pranešimus pateikia naudodamas valstybės narės, kuri nustatoma laikantis toliau nurodytos tvarkos ir remiantis gamintojo turima informacija, koordinatore paskirtos CSIRT elektroninio pranešimo galinį įrenginį:

a) valstybė narė, kurioje įsisteigęs gamintojo vardu veikiantis įgaliotasis atstovas, atstovaujantis didžiausiam skaičiui to gamintojo produktų su skaitmeniniais elementais;

b) valstybė narė, kurioje įsisteigęs importuotojas, pateikiantis rinkai didžiausią to gamintojo produktų su skaitmeniniais elementais skaičių;

c) valstybė narė, kurioje įsisteigęs platintojas, tiekiantis rinkai didžiausią to gamintojo produktų su skaitmeniniais elementais skaičių;

d) valstybė narė, kurioje yra didžiausias to gamintojo produktų su skaitmeniniais elementais naudotojų skaičius.

Kiek tai susiję su trečios pastraipos d punktu, gamintojas gali pateikti pranešimus, susijusius su bet kokiu vėlesniu aktyviai išnaudojamu pažeidžiamumu arba dideliu incidentu, darančiu poveikį produkto su skaitmeniniais elementais saugumui, tai pačiai koordinatore paskirtai CSIRT, kuriai jis pirmą kartą pateikė pranešimą.

8. Sužinojęs apie aktyviai išnaudojamą pažeidžiamumą arba didelį incidentą, darantį poveikį produkto su skaitmeniniais elementais saugumui, gamintojas informuoja paveiktus produkto su skaitmeniniais elementais naudotojus ir, kai tinkama, visus naudotojus apie tą pažeidžiamumą arba didelį incidentą, ir, jei būtina, apie visas rizikos mažinimo ir taisomąsias priemones, kurių naudotojai gali imtis, kad sumažintų to pažeidžiamumo ar incidento poveikį, kai tinkama, struktūrizuotu, kompiuterio skaitomu formatu, kuris būtų lengvai automatiškai apdorojamas. Jei gamintojas laiku neinformuoja produkto su skaitmeniniais elementais naudotojų, koordinatorėmis paskirtos CSIRT, gavusios pranešimą, gali pateikti tokią informaciją naudotojams, kai manoma, kad tai proporcinga ir būtina siekiant užkirsti kelią to pažeidžiamumo ar incidento poveikiui arba jį sumažinti.

9. Ne vėliau kaip … [12 mėnesių nuo šio reglamento įsigaliojimo dienos] Komisija pagal šio reglamento 61 straipsnį priima deleguotuosius aktus, siekiant šį reglamentą papildyti, kuriais nustatomos sąlygos, kuriomis taikomos su kibernetiniu saugumu susijusios priežastys, dėl kurių atidedamas pranešimų platinimas, kaip nurodyta šio reglamento 16 straipsnio 2 dalyje. Rengdama deleguotųjų aktų projektus Komisija bendradarbiauja su CSIRT tinklu, sukurtu pagal Direktyvos (ES) 2022/2555 15 straipsnį, ir ENISA.

10. Komisija gali įgyvendinimo aktais išsamiau nustatyti šiame straipsnyje ir 15 bei 16 straipsniuose nurodytų pranešimų formatą ir procedūras. Tie įgyvendinimo aktai priimami laikantis 62 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros. Rengdama tų įgyvendinimo aktų projektus Komisija bendradarbiauja su CSIRT tinklu ir ENISA.

15 straipsnis

Savanoriškas pranešimas

1. Gamintojai ir kiti fiziniai ar juridiniai asmenys apie bet kokį produkto su skaitmeniniais elementais pažeidžiamumą ir kibernetines grėsmes, kurios galėtų turėti įtakos produkto su skaitmeniniais elementais rizikos profiliui, gali savanoriškai pranešti koordinatore paskirtai CSIRT arba ENISA.

2. Gamintojai ir kiti fiziniai ar juridiniai asmenys apie bet kokį incidentą, darantį poveikį produkto su skaitmeniniais elementais saugumui, taip pat apie vos neįvykusius įvykius, dėl kurių toks incidentas galėjo įvykti, gali savanoriškai pranešti koordinatore paskirtai CSIRT arba ENISA.

3. Koordinatore paskirta CSIRT arba ENISA tvarko šio straipsnio 1 ir 2 dalyse nurodytus pranešimus laikydamasi 16 straipsnyje nustatytos procedūros.

   Koordinatore paskirta CSIRT gali teikti pirmenybę ne savanoriškų, o privalomų pranešimų tvarkymui.

4. Jei fizinis ar juridinis asmuo, kuris nėra gamintojas, praneša apie aktyviai išnaudojamą pažeidžiamumą arba didelį incidentą, darantį poveikį produkto su skaitmeniniais elementais saugumui pagal 1 arba 2 dalį, koordinatore paskirta CSIRT nepagrįstai nedelsdama apie tai informuoja gamintoją.

5. Koordinatorėmis paskirtos CSIRT ir ENISA užtikrina pranešančiojo fizinio ar juridinio asmens pateiktos informacijos konfidencialumą ir tinkamą apsaugą. Nedarant poveikio nusikalstamų veikų prevencijai, tyrimui, jų atskleidimui ir baudžiamajam persekiojimui už jas, dėl savanoriško pranešimo pranešimą teikiančiam fiziniam ar juridiniam asmeniui nenustatoma jokių papildomų pareigų, kurios jam nebūtų taikomos, jei jis nebūtų pateikęs pranešimo.

16 straipsnis

Bendros pranešimų teikimo platformos sukūrimas

1. 14 straipsnio 1 ir 3 dalyse ir 15 straipsnio 1 ir 2 dalyse nurodytų pranešimų teikimo tikslais ir siekiant supaprastinti gamintojų pareigas teikti pranešimus, ENISA sukuria bendrą pranešimų teikimo platformą. Tos bendros pranešimų teikimo platformos kasdienę veiklą valdo ir prižiūri ENISA. Bendros pranešimų teikimo platformos struktūra sudaro sąlygas valstybėms narėms ir ENISA įdiegti savo elektroninio pranešimo galinius įrenginius.

2. Gavusi pranešimą, koordinatore paskirta CSIRT, kuri pirmoji gavo pranešimą, nedelsdama jį išplatina per bendrą pranešimų teikimo platformą koordinatorėmis paskirtoms CSIRT, kurių teritorijoje, kaip nurodė gamintojas, yra prieinamas tas produktas su skaitmeniniais elementais.

Išimtinėmis aplinkybėmis ir, visų pirma, gamintojo prašymu bei atsižvelgiant į gamintojo pagal šio reglamento 14 straipsnio 2 dalies a punktą nurodytą pateiktos informacijos neskelbtinumo lygį, pranešimo platinimas dėl pagrįstų su kibernetiniu saugumu susijusių priežasčių gali būti atidėtas laikotarpiui, kuris yra tikrai būtinas, įskaitant atvejus, kai pažeidžiamumui taikoma suderinta pažeidžiamumo atskleidimo procedūra, kaip nurodyta Direktyvos (ES) 2022/2555 12 straipsnio 1 dalyje. Jei CSIRT nusprendžia atidėti pranešimą, ji nedelsdama informuoja ENISA apie sprendimą ir pateikia pranešimo atidėjimo pagrindimą, taip pat nurodo, kada ji išplatins pranešimą laikydamasi šioje dalyje nustatytos platinimo procedūros. ENISA gali teikti CSIRT pagalbą su kibernetiniu saugumu susijusių priežasčių nuostatų taikymo srityje, kiek tai susiję su pranešimo platinimo atidėjimu.

Ypatingais išimtiniais atvejais, kai gamintojas 14 straipsnio 2 dalies b punkte nurodytame pranešime nurodo, kad:

a) piktavalis subjektas aktyviai naudojasi pažeidžiamumu, apie kurį pranešta, ir, remiantis turima informacija, juo buvo pasinaudota tik valstybėje narėje, kurios CSIRT yra paskirta koordinatore, kuriai gamintojas pranešė apie pažeidžiamumą;

b) bet koks neatidėliotinas tolesnis pranešimo apie pažeidžiamumą platinimas greičiausiai lemtų informacijos, kurios atskleidimas prieštarautų tos valstybės narės esminiams interesams, teikimą, arba

c) pažeidžiamumas, apie kurį pranešta, kelia neišvengiamą didelę kibernetinio saugumo riziką, kylančią dėl tolesnio pranešimo platinimo,

tik informacija, kad gamintojas pateikė pranešimą, bendroji informacija apie produktą, informacija apie bendrą išnaudojimo pobūdį ir informacija, kad buvo nurodytos su saugumu susijusios priežastys, turi būti pateikta tuo pačiu metu ENISA, kol visas pranešimo tekstas bus išplatintas atitinkamoms CSIRT ir ENISA. Jei, remdamasi ta informacija, ENISA mano, kad esama sisteminės rizikos, turinčios poveikį vidaus rinkos saugumui, ji rekomenduoja pranešimą gavusiai CSIRT išplatinti visą pranešimo tekstą kitoms koordinatorėmis paskirtoms CSIRT ir pačiai ENISA.

3. Gavusios pranešimą apie aktyviai išnaudojamą produkto su skaitmeniniais elementais pažeidžiamumą arba didelį incidentą, darantį poveikį produkto su skaitmeniniais elementais saugumui, koordinatorėmis paskirtos CSIRT savo atitinkamų valstybių narių rinkos priežiūros institucijoms pateikia informaciją, apie kurią joms praneštą ir kurios reikia, kad rinkos priežiūros institucijos galėtų vykdyti savo pareigas pagal šį reglamentą.

4. ENISA imasi tinkamų ir proporcingų techninių, operacinių ir organizacinių priemonių, kad būtų valdoma rizika, kylanti bendros pranešimų teikimo platformos ir per bendrą pranešimų teikimo platformą teikiamos arba platinamos informacijos saugumui. Ji nepagrįstai nedelsdama praneša CSIRT tinklui ir Komisijai apie visus saugumo incidentus, darančius poveikį bendrai pranešimų teikimo platformai.

5. ENISA, bendradarbiaudama su CSIRT tinklu, pateikia ir įgyvendina techninių, operacinių ir organizacinių priemonių, susijusių su 1 dalyje nurodytos bendros pranešimų teikimo platformos sukūrimu, techninė priežiūra ir saugiu eksploatavimu, įskaitant bent saugumo priemones, susijusias su bendros pranešimų teikimo platformos sukūrimu, eksploatavimu ir techninė priežiūra, ir elektroninio pranešimo galinių įrenginių, kuriuos nustatė koordinatorėmis paskirtos CSIRT nacionaliniu lygmeniu, o Sąjungos lygmeniu – ENISA, specifikacijas, įskaitant procedūrinius aspektus, siekiant užtikrinti, kad tais atvejais, kai pažeidžiamumo, apie kurį pranešta, atžvilgiu nėra priimta jokių taisomųjų ar poveikio mažinimo priemonių, informacija apie tą pažeidžiamumą būtų dalijamasi laikantis griežtų saugumo protokolų ir remiantis būtinybės žinoti principu.

6. Jei koordinatore paskirtai CSIRT, vykdant koordinuoto pažeidžiamumų atskleidimo procedūrą, nurodytą Direktyvos (ES) 2022/2555 12 straipsnio 1 dalyje, buvo pranešta apie aktyviai išnaudojamą pažeidžiamumą, koordinatore paskirta CSIRT, kuri pirmoji gavo pranešimą, gali atidėti atitinkamo pranešimo platinimą per bendrą pranešimų teikimo platformą remdamasi pagrįstomis su kibernetiniu saugumu susijusiomis priežastimis ne ilgesniam nei griežtai būtina laikotarpiui iki tol, kol susijusios koordinuoto pažeidžiamumų atskleidimo šalys duos sutikimą atskleisti informaciją. Tuo reikalavimu neužkertamas kelias gamintojams savanoriškai pranešti apie tokį pažeidžiamumą šiame straipsnyje nustatyta tvarka.

17 straipsnis

Kitos su pranešimu susijusios nuostatos

1. ENISA gali pateikti Europos ryšių palaikymo dėl kibernetinių krizių organizaciniam tinklui (EU-CyCLONe), įsteigtam pagal Direktyvos (ES) 2022/2555 16 straipsnį, informaciją, apie kurią pranešta pagal šio reglamento 14 straipsnio 1 ir 3 dalis bei 15 straipsnio 1 ir 2 dalis, jei tokia informacija yra svarbi koordinuotam didelio masto kibernetinio saugumo incidentų ir krizių valdymui operaciniu lygmeniu. Siekdama nustatyti tokią svarbą, ENISA gali atsižvelgti į CSIRT tinklo atliktas technines analizes, jei tokių yra.

2. Kai visuomenės informuotumas yra būtinas siekiant užkirsti kelią dideliam incidentui, darančiam poveikį produkto su skaitmeniniais elementais saugumui, arba jį sušvelninti arba valdyti vykstantį incidentą, arba kai incidento atskleidimas kitu būdu atitinka viešąjį interesą, atitinkamos valstybės narės koordinatore paskirta CSIRT gali, pasikonsultavusi su atitinkamu gamintoju ir, kai tinkama, bendradarbiaudama su ENISA, informuoti visuomenę apie incidentą arba pareikalauti, kad tai padarytų gamintojas.

3. Remdamasi pagal šio reglamento 14 straipsnio 1 ir 3 dalis bei 15 straipsnio 1 ir 2 dalis gautais pranešimais ENISA kas 24 mėnesius parengia techninę ataskaitą apie produktams su skaitmeniniais elementais kylančios kibernetinio saugumo rizikos tendencijas ir pateikia ją Bendradarbiavimo grupei, įsteigtai pagal Direktyvos (ES) 2022/2555 14 straipsnį. Pirmoji tokia ataskaita pateikiama per 24 mėnesius nuo šio reglamento 14 straipsnio 1 ir 3 dalyse nustatytų pareigų taikymo pradžios. ENISA į savo ataskaitą dėl kibernetinio saugumo padėties Sąjungoje pagal Direktyvos (ES) 2022/2555 18 straipsnį įtraukia atitinkamą savo techninių ataskaitų informaciją.

4. Vien dėl pranešimo pagal 14 straipsnio 1 ir 3 dalis arba 15 straipsnio 1 ir 2 dalis veiksmo pranešančiajam negali būti padidinama fizinio ar juridinio asmens atsakomybė.

5. Gavusi saugumo naujinį arba kitokios formos taisomąją ar rizikos mažinimo priemonę, ENISA, susitarusi su atitinkamu produkto su skaitmeniniais elementais gamintoju, į Europos pažeidžiamumo duomenų bazę, sukurtą pagal Direktyvos (ES) 2022/2555 12 straipsnio 2 dalį, įtraukia viešai žinomą pažeidžiamumą, apie kurį pranešta pagal šio reglamento 14 straipsnio 1 dalį arba 15 straipsnio 1 dalį.

6. Koordinatorėmis paskirtos CSIRT teikia pagalbos tarnybos paslaugas, susijusias su pareiga pranešti pagal 14 straipsnį, gamintojams, visų pirma gamintojams, kurie laikomi labai mažomis įmonėmis arba mažosiomis ar vidutinėmis įmonėmis.

18 straipsnis

Įgaliotieji atstovai

1. Gamintojas gali rašytiniu įgaliojimu paskirti įgaliotąjį atstovą.

2. Įgaliotojo atstovo įgaliojimas neapima 13 straipsnio 1–11 dalyse, 13 straipsnio 12 dalies pirmoje pastraipoje ir 13 straipsnio 14 dalyje nustatytų pareigų.

3. Įgaliotasis atstovas atlieka gamintojo suteiktame įgaliojime nustatytas užduotis. Įgaliotasis atstovas, gavęs prašymą, rinkos priežiūros institucijoms pateikia įgaliojimo kopiją. Įgaliojimu įgaliotajam atstovui leidžiama atlikti bent šiuos veiksmus:

a) saugoti 28 straipsnyje nurodytą ES atitikties deklaraciją ir 31 straipsnyje nurodytus techninius dokumentus bent 10 metų po produkto su skaitmeniniais elementais pateikimo rinkai arba palaikymo laikotarpį, priklausomai nuo to, kuris terminas yra ilgesnis, kad rinkos priežiūros institucijos galėtų su jais susipažinti;

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

19 straipsnis

Importuotojų pareigos

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

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

   a) gamintojas būtų atlikęs atitinkamas atitikties vertinimo procedūras, nurodytas 32 straipsnyje;

   b) gamintojas būtų parengęs techninius dokumentus;

   c) produktas su skaitmeniniais elementais būtų paženklintas 30 straipsnyje nurodytu CE ženklu ir prie jo būtų pridedama 13 straipsnio 20 dalyje nurodyta ES atitikties deklaracija bei naudotojams skirta informacija ir naudojimo instrukcijos, nustatytos II priede, ta kalba, kuri yra lengvai suprantama vartotojams ir rinkos priežiūros institucijoms;

   d) gamintojas būtų įvykdęs 13 straipsnio 15, 16 ir 19 dalyse nustatytus reikalavimus.

   Šios dalies tikslais importuotojai turi galėti pateikti būtinus dokumentus, įrodančius, kad įvykdyti šiame straipsnyje nustatyti reikalavimai.

3. Jei importuotojas mano arba turi priežasčių manyti, kad produktas su skaitmeniniais elementais arba gamintojo įdiegti procesai neatitinka šio reglamento, jis neteikia produkto rinkai, kol neužtikrinama to produkto arba gamintojo įdiegtų procesų atitiktis šiam reglamentui. Be to, jei produktas su skaitmeniniais elementais kelia didelę kibernetinio saugumo riziką, importuotojas apie tai informuoja gamintoją ir rinkos priežiūros institucijas.

Jei importuotojas turi priežasčių manyti, kad produktas su skaitmeniniais elementais gali kelti didelę kibernetinio saugumo riziką atsižvelgiant į netechninius rizikos veiksnius, jis apie tai informuoja rinkos priežiūros institucijas. Gavusios tokią informaciją, rinkos priežiūros institucijos taiko 54 straipsnio 2 dalyje nurodytas procedūras.

4. Ant produkto su skaitmeniniais elementais arba ant jo pakuotės ar prie produkto su skaitmeniniais elementais pridedamame dokumente importuotojas nurodo savo pavadinimą, registruotą prekės pavadinimą arba registruotą prekių ženklą, pašto adresą, e. pašto adresą ar kitus skaitmeninių kontaktų duomenis, taip pat, kai taikytina, interneto svetainę, kuriais naudojantis su jais galima susisiekti. Kontaktiniai duomenys turi būti pateikiami naudotojams bei rinkos priežiūros institucijoms lengvai suprantama kalba.

5. Jei importuotojai žino arba turi priežasčių manyti, kad produktas su skaitmeniniais elementais, kurį jie pateikė rinkai, neatitinka šio reglamento, jie nedelsdami imasi taisomųjų priemonių, būtinų to produkto su skaitmeniniais elementais atitikčiai šiam reglamentui užtikrinti, arba, prireikus, jį atšaukti ar pašalinti.

   Sužinoję apie produkto su skaitmeniniais elementais pažeidžiamumą, importuotojai apie tą pažeidžiamumą nedelsdami praneša gamintojui. Be to, jei produktas su skaitmeniniais elementais kelia didelę 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.

6. Importuotojas bent 10 metų po produkto su skaitmeniniais elementais pateikimo rinkai dienos arba per palaikymo laikotarpį, priklausomai nuo to, kuris terminas yra ilgesnis, saugo ES atitikties deklaracijos kopiją, kad rinkos priežiūros institucijos galėtų su ja susipažinti, ir užtikrina, kad tų institucijų prašymu joms galėtų būti pateikti techniniai dokumentai.

7. 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 I dalyje nustatytus esminius kibernetinio saugumo reikalavimus ir kad gamintojo įdiegti procesai atitinka I priedo II dalyje nustatytus esminius kibernetinio saugumo 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 riziką.

8. 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 situaciją atitinkamas rinkos priežiūros institucijas, taip pat, visomis turimomis priemonėmis ir kiek įmanoma, rinkai pateiktų produktų su skaitmeniniais elementais naudotojus.

20 straipsnis

Platintojų pareigos

1. Tiekdami rinkai produktą su skaitmeniniais elementais, platintojai pakankamai rūpestingai laikosi šiame reglamente nustatytų 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 13 straipsnio 15, 16, 18, 19 bei 20 dalyse ir 19 straipsnio 4 dalyje nustatytas pareigas ir pateikė visus būtinus dokumentus platintojui.

3. Jei platintojas, remdamasis savo turima informacija, mano arba turi priežasčių manyti, kad produktas su skaitmeniniais elementais arba gamintojo įdiegti procesai neatitinka I priede nustatytų esminių kibernetinio saugumo reikalavimų, platintojas netiekia produkto su skaitmeniniais elementais rinkai, kol nebus užtikrinta to produkto arba gamintojo įdiegtų procesų atitiktis šiam reglamentui. Be to, jei produktas su skaitmeniniais elementais kelia didelę kibernetinio saugumo riziką, platintojas nepagrįstai nedelsdamas apie tai informuoja gamintoją ir rinkos priežiūros institucijas.

4. Jei platintojai, remdamiesi savo turima informacija, žino arba turi priežasčių manyti, kad produktas su skaitmeniniais elementais, kurį jie tiekė rinkai, arba jo gamintojo įdiegti procesai neatitinka šio reglamento, jie pasirūpina, kad būtų imtasi taisomųjų priemonių, būtinų to produkto su skaitmeniniais elementais arba jo gamintojo įdiegtų procesų atitikčiai užtikrinti, arba, prireikus, jį atšaukti ar pašalinti.

Sužinoję apie produkto su skaitmeniniais elementais pažeidžiamumą, platintojai apie tą pažeidžiamumą nedelsdami praneša gamintojui. Be to, jei produktas su skaitmeniniais elementais kelia didelę 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 šį reglamentą. 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 riziką.

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

21 straipsnis

Atvejai, kuriais importuotojams ir platintojams taikomos gamintojų pareigos

Importuotojas arba platintojas pagal šį reglamentą laikomas gamintoju ir jam taikomi 13 ir 14 straipsniai, jei tas importuotojas ar platintojas pateikia rinkai produktą su skaitmeniniais elementais savo vardu arba naudodamas savo prekių ženklą, arba atlieka jau pateikto rinkai produkto su skaitmeniniais elementais esminį pakeitimą.

22 straipsnis

Kiti atvejai, kuriais taikomos gamintojų pareigos

1. Fizinis ar juridinis asmuo, išskyrus gamintoją, importuotoją ar platintoją, kuris atlieka esminį produkto su skaitmeniniais elementais pakeitimą ir tiekia tą produktą rinkai, pagal šį reglamentą laikomas gamintoju.

2. Asmeniui, nurodytam šio straipsnio 1 dalyje, taikomos 13 ir 14 straipsniuose nustatytos pareigos – jos taikomos tai produkto su skaitmeniniais elementais daliai, kuri yra paveikta esminio pakeitimo, arba visam produktui, jei esminis pakeitimas daro poveikį viso produkto su skaitmeniniais elementais kibernetiniam saugumui.

23 straipsnis

Ekonominės veiklos vykdytojų identifikavimas

1. Ekonominės veiklos vykdytojai, gavę rinkos priežiūros institucijų prašymą , joms teikia šią informaciją:

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

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

2. Ekonominės veiklos vykdytojai 1 dalyje nurodytą informaciją turi galėti pateikti 10 metų po to, kai jiems buvo tiektas produktas su skaitmeniniais elementais, ir 10 metų po to, kai jie tiekė produktą su skaitmeniniais elementais.

24 straipsnis

Atvirosios programinės įrangos valdytojų pareigos

1. Atvirosios programinės įrangos valdytojai įdiegia ir patikrinamu būdu dokumentuoja kibernetinio saugumo politiką, kuria skatinamas saugaus produkto su skaitmeniniais elementais kūrimas ir veiksmingas to produkto kūrėjų vykdomas pažeidžiamumų valdymas. Ta politika taip pat skatinamas savanoriškas to produkto kūrėjų pranešimas apie pažeidžiamumą, kaip nustatyta 15 straipsnyje, ir atsižvelgiama į specifinį atvirosios programinės įrangos valdytojo pobūdį ir jam taikomas teisines bei organizacines priemones. Ta politika visų pirma apima aspektus, susijusius su pažeidžiamumų dokumentavimu, šalinimu ir ištaisymu, ir skatina dalijimąsi informacija apie nustatytus pažeidžiamumus atvirojo kodo bendruomenėje.

2. Rinkos priežiūros institucijų prašymu atvirosios programinės įrangos valdytojai bendradarbiauja su jomis, kad sumažintų produkto su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga, keliamą kibernetinio saugumo riziką.

   Rinkos priežiūros institucijai pateikus pagrįstą prašymą, atvirosios programinės įrangos valdytojai tai institucijai lengvai suprantama kalba popierine arba elektronine forma pateikia 1 dalyje nurodytus dokumentus.

3. 14 straipsnio 1 dalyje nustatytos pareigos taikomos atvirosios programinės įrangos valdytojams tiek, kiek jie dalyvauja kuriant produktus su skaitmeniniais elementais. 14 straipsnio 3 ir 8 dalyse nustatytos pareigos taikomos atvirosios programinės įrangos valdytojams tiek, kiek dideli incidentai, darantys poveikį produktų su skaitmeniniais elementais saugumui, daro poveikį tinklų ir informacinėms sistemoms, kurias atvirosios programinės įrangos valdytojai teikia tokiems produktams kurti.

25 straipsnis

Laisvosios ir atvirosios programinės įrangos saugumo patvirtinimas

Siekiant palengvinti 13 straipsnio 5 dalyje nustatytos išsamaus patikrinimo pareigos vykdymą, visų pirma kiek tai susiję su gamintojais, kurie į savo produktus su skaitmeniniais elementais integruoja laisvosios ir atvirosios programinės įrangos komponentus, Komisijai pagal 61 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, siekiant papildyti šį reglamentą, kuriais nustatomos savanoriškos saugumo patvirtinimo programos, pagal kurias produktų su skaitmeniniais elementais, laikomais laisvąja ir atvirąja programine įranga, kūrėjai ar naudotojai, taip pat kitos trečiosios šalys gali įvertinti tokių produktų atitiktį visiems arba tam tikriems esminiams kibernetinio saugumo reikalavimams ar kitoms pareigoms, nustatytiems šiame reglamente.

26 straipsnis

Gairės

1. Siekiant palengvinti įgyvendinimą ir užtikrinti tokio įgyvendinimo nuoseklumą, Komisija paskelbia gaires, kad padėtų ekonominės veiklos vykdytojams taikyti šį reglamentą, ypatingą dėmesį skiriant palankesnių sąlygų laikytis reikalavimų sudarymui labai mažoms įmonėms ir mažosioms bei vidutinėms įmonėms.

2. Kai Komisija ketina pateikti 1 dalyje nurodytas gaires, ji atsižvelgia bent į šiuos aspektus:

   a) šio reglamento taikymo sritį, ypatingą dėmesį skiriant nuotolinio duomenų tvarkymo sprendimams ir laisvajai bei atvirajai programinei įrangai;

   b) palaikymo laikotarpių taikymą konkrečioms produktų su skaitmeniniais elementais kategorijoms;

   c) gaires, skirtas gamintojams, kuriems taikomas šis reglamentas ir kuriems taip pat taikomi kiti nei šis reglamentas Sąjungos derinamieji teisės aktai arba kiti susiję Sąjungos teisės aktai;

   d) esminio pakeitimo koncepciją.

   Komisija taip pat tvarko lengvai prieinamą pagal šį reglamentą priimtų deleguotųjų ir įgyvendinimo aktų sąrašą.

3. Rengdama gaires pagal šį straipsnį, Komisija konsultuojasi su suinteresuotaisiais subjektais.

III skyrius

Produkto su skaitmeniniais elementais atitiktis

27 straipsnis

Atitikties prezumpcija

1. Preziumuojama, kad jei produktai su skaitmeniniais elementais ir gamintojo įdiegti procesai atitinka darniuosius standartus arba jų dalis, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*, jie atitinka I priede nustatytus esminius kibernetinio saugumo reikalavimus, kuriuos apima tie standartai ar jų dalys.

   Pagal Reglamento (ES) Nr. 1025/2012 10 straipsnio 1 dalį Komisija paprašo vienos ar daugiau Europos standartizacijos organizacijų parengti darniuosius standartus, susijusius su šio reglamento I priede nustatytais esminiais kibernetinio saugumo reikalavimais. Rengdama standartizacijos prašymus dėl šio reglamento, Komisija stengiasi atsižvelgti į esamus arba rengiamus Europos ir tarptautinius kibernetinio saugumo standartus, kad būtų supaprastintas darniųjų standartų rengimas pagal Reglamentą (ES) Nr. 1025/2012.

2. Komisija gali priimti įgyvendinimo aktus, kuriais nustatomos bendrosios specifikacijos, apimančios techninius reikalavimus, kuriais sudaroma galimybė laikytis I priede nustatytų esminių kibernetinio saugumo reikalavimų, taikomų į šio reglamento taikymo sritį patenkantiems produktams su skaitmeniniais elementais.

Tie įgyvendinimo aktai priimami tik tuo atveju, kai tenkinamos šios sąlygos:

a) Komisija pagal Reglamento (ES) Nr. 1025/2012 10 straipsnio 1 dalį yra paprašiusi vienos ar daugiau Europos standartizacijos organizacijų parengti darnųjį standartą, susijusį su I priede nustatytais esminiais kibernetinio saugumo reikalavimais ir:

i) prašymas nebuvo priimtas;

ii) su tuo prašymu susiję darnieji standartai nebuvo pateikti iki termino, nustatyto pagal Reglamento (ES) Nr. 1025/2012 10 straipsnio 1 dalį, arba

iii) darnieji standartai neatitinka prašymo, ir

b) *Europos Sąjungos oficialiajame leidinyje* nėra pagal Reglamentą (ES) Nr. 1025/2012 paskelbta nuoroda į darniuosius standartus, apimančius I priede nustatytus atitinkamus esminius kibernetinio saugumo reikalavimus, ir nenumatoma tokią nuorodą paskelbti per pagrįstą laikotarpį.

Tie įgyvendinimo aktai priimami laikantis 62 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

3. Prieš rengdama šio straipsnio 2 dalyje nurodytą įgyvendinimo akto projektą, Komisija informuoja Reglamento (ES) Nr. 1025/2012 22 straipsnyje nurodytą komitetą apie tai, kad, jos manymu, šio straipsnio 2 dalyje nustatytos sąlygos yra tenkinamos.

4. Rengdama 2 dalyje nurodytą įgyvendinimo akto projektą, Komisija atsižvelgia į atitinkamų įstaigų nuomonę ir tinkamai konsultuojasi su visais atitinkamais suinteresuotaisiais subjektais.

5. Preziumuojama, kad šio straipsnio 2 dalyje nurodytais įgyvendinimo aktais nustatytas bendrąsias specifikacijas ar jų dalis atitinkantys produktai su skaitmeniniais elementais ir gamintojo įdiegti procesai atitinka I priede nustatytus esminius kibernetinio saugumo reikalavimus, kuriuos apima tos bendrosios specifikacijos arba jų dalys.

6. Jei Europos standartizacijos organizacija priima darnųjį standartą ir Komisijai pasiūloma nuorodą į jį paskelbti *Europos Sąjungos oficialiajame leidinyje*, Komisija įvertina darnųjį standartą pagal Reglamentą (ES) Nr. 1025/2012. Jei *Europos Sąjungos oficialiajame leidinyje* paskelbiama darniojo standarto nuoroda, Komisija panaikina šio straipsnio 2 dalyje nurodytus įgyvendinimo aktus arba jų dalis, apimančius tuos pačius esminius kibernetinio saugumo reikalavimus, kaip ir tie, kuriems taikomas tas darnusis standartas.

7. Jei valstybė narė mano, kad bendroji specifikacija nevisiškai atitinka I priede nustatytus esminius kibernetinio saugumo reikalavimus, ji apie tai praneša Komisijai pateikdama išsamų paaiškinimą. Komisija įvertina tą išsamų paaiškinimą ir, jei tinkama, iš dalies pakeičia įgyvendinimo aktą, kuriuo nustatoma atitinkama bendroji specifikacija.

8. Preziumuojama, kad 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 , atitinka I priede nustatytus esminius kibernetinio saugumo reikalavimus tiek, kiek ES atitikties pareiškimas arba Europos kibernetinio saugumo sertifikatas, arba jų dalys, apima tuos reikalavimus.

9. Komisijai pagal šio reglamento 61 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, siekiant šį reglamentą papildyti, kuriais nurodomos Europos kibernetinio saugumo sertifikavimo schemos, priimtos pagal Reglamentą (ES) 2019/881, kurios gali būti naudojamos siekiant įrodyti produktų su skaitmeniniais elementais atitiktį šio reglamento I priede nustatytiems esminiams kibernetinio saugumo reikalavimams ar jų dalims. Be to, Europos kibernetinio saugumo sertifikato, kurio saugumo užtikrinimo lygis yra bent „pakankamai aukštas“, išdavimas pagal tokias schemas panaikina gamintojo pareigą atlikti atitikties atitinkamiems reikalavimams trečiųjų šalių vertinimą, kaip nustatyta šio reglamento 32 straipsnio 2 dalies a ir b punktuose bei 3 dalies a ir b punktuose.

28 straipsnis

ES atitikties deklaracija

1. ES atitikties deklaraciją gamintojai parengia pagal 13 straipsnio 12 dalį ir joje nurodo, kad įrodytas I priede nustatytų taikytinų esminių kibernetinio saugumo reikalavimų įvykdymas.

2. ES atitikties deklaracija parengiama pagal V priede nustatytą pavyzdinę struktūrą, ir joje pateikiami atitinkamose VIII priede nustatytose atitikties vertinimo procedūrose nurodyti elementai. Tokia deklaracija, prireikus, atnaujinama. Ji pateikiama valstybės narės, kurios rinkai pateikiamas arba tiekiamas produktas su skaitmeniniais elementais, reikalaujamomis kalbomis.

13 straipsnio 20 dalyje nurodyta supaprastinta ES atitikties deklaracija parengiama pagal VI priede nustatytą pavyzdinę struktūrą. Ji pateikiama valstybės narės, kurios rinkai pateikiamas arba tiekiamas produktas su skaitmeniniais elementais, reikalaujamomis kalbomis.

3. Jei produktui su skaitmeniniais elementais taikomas daugiau kaip vienas Sąjungos teisės aktas, pagal kurį reikalaujama parengti ES atitikties deklaraciją, dėl visų tokių Sąjungos teisės aktų parengiama viena ES atitikties deklaracija. Toje deklaracijoje nurodomi susiję Sąjungos teisės aktai, įskaitant jų paskelbimo nuorodas.

4. Parengdamas ES atitikties deklaraciją gamintojas prisiima atsakomybę dėl produkto su skaitmeniniais elementais atitikties.

5. Komisijai pagal 61 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, siekiant papildyti šį reglamentą, kuriais prie V priede nustatytos ES atitikties deklaracijos minimalaus turinio pridedami nauji elementai, siekiant atsižvelgti į technologijų raidą.

29 straipsnis

Bendrieji ženklinimo CE ženklu principai

Ženklinimui CE ženklu taikomi bendrieji principai, nustatyti Reglamento (EB) Nr. 765/2008 30 straipsnyje.

30 straipsnis

Ženklinimo CE ženklu taisyklės ir sąlygos

1. Produktas su skaitmeniniais elementais ženklinamas CE ženklu taip, kad jis būtų matomas, įskaitomas ir neištrinamas. Jei taip ženklinti neįmanoma arba negalima dėl produkto su skaitmeniniais elementais pobūdžio, CE ženklas pateikiamas ant pakuotės ir 28 straipsnyje nurodytoje ES atitikties deklaracijoje, pateikiamoje kartu su produktu su skaitmeniniais elementais. Produktų su skaitmeniniais elementais, kurie yra programinės įrangos forma, atveju CE ženklas pateikiamas 28 straipsnyje nurodytoje ES atitikties deklaracijoje arba programinės įrangos produkto interneto svetainėje. Pastaruoju atveju atitinkama interneto svetainės dalis turi būti lengvai ir tiesiogiai prieinama vartotojams.

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 kibernetinio saugumo riziką arba paskirtį, nustatytą 6 dalyje nurodytuose įgyvendinimo aktuose.

4. Po CE ženklo nurodomas notifikuotosios įstaigos identifikacinis numeris, jei ta įstaiga dalyvauja atitikties vertinimo procedūroje, pagrįstoje 32 straipsnyje nurodytu visišku kokybės užtikrinimu (remiantis H moduliu).

   Notifikuotosios įstaigos identifikacinį 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 nei šis reglamentas Sąjungos derinamieji teisės aktai, kuriuose taip pat numatytas ženklinimas CE ženklu, CE ženklu turi būti nurodoma, kad produktas atitinka ir tokiuose kituose Sąjungos derinamuosiuose teisės aktuose nustatytus reikalavimus.

6. Komisija gali įgyvendinimo aktais nustatyti etikečių, piktogramų ar bet kokių kitų su produktų su skaitmeniniais elementais saugumu susijusių ženklų technines specifikacijas, jų palaikymo laikotarpius ir mechanizmus, kuriais skatinamas jų naudojimas ir didinamas visuomenės informuotumas apie produktų su skaitmeniniais elementais saugumą. Rengdama įgyvendinimo aktų projektus, Komisija konsultuojasi su atitinkamais suinteresuotaisiais subjektais ir administracinio bendradarbiavimo grupe, jei ji jau įsteigta pagal 52 straipsnio 15 dalį. Tie įgyvendinimo aktai priimami laikantis 62 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

31 straipsnis

Techniniai dokumentai

1. Techniniuose dokumentuose pateikiami visi svarbūs 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 kibernetinio saugumo reikalavimus. Tuose dokumentuose turi būti bent VII priede nurodyti elementai.

2. Techniniai dokumentai parengiami prieš pateikiant produktą su skaitmeniniais elementais rinkai ir, prireikus, nuolat atnaujinami bent per palaikymo laikotarpį .

3. 12 straipsnyje nurodytų produktų su skaitmeniniais elementais, kuriems taip pat taikomi kiti Sąjungos teisės aktai, kuriuose numatyti techniniai dokumentai, atveju parengiamas vienas techninių dokumentų rinkinys, kuriame pateikiama VII priede nurodyta informacija ir pagal tuos Sąjungos teisės aktus reikalaujama informacija.

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

5. Komisija pagal 61 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, siekiant papildyti šį reglamentą, kuriais pridedami elementai, kurie turi būti įtraukti į VII priede nustatytus techninius dokumentus, atsižvelgiant į technologijų raidą ir pokyčius, su kuriais susiduriama įgyvendinant šį reglamentą. Tuo tikslu Komisija stengiasi užtikrinti, kad administracinė našta, tenkanti labai mažoms įmonėms ir mažosioms bei vidutinėms įmonėms, būtų proporcinga.

32 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 nustatytų esminių kibernetinio saugumo reikalavimų. Gamintojas turi įrodyti atitiktį tiems esminiams kibernetinio saugumo reikalavimams taikydamas bet kurią iš šių procedūrų:

   a) vidaus kontrolės procedūrą (remiantis A moduliu), nustatytą VIII priede;

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

c) visišku kokybės užtikrinimu pagrįstą atitikties vertinimo procedūrą (remiantis H moduliu), nustatytą VIII priede, arba

d) kai yra ir taikytina, Europos kibernetinio saugumo sertifikavimo schemą pagal 27 straipsnio 9 dalį.

2. Jei vertindamas III priede nustatytai I klasei priskiriamo svarbaus produkto su skaitmeniniais elementais ir jo gamintojo įdiegtų procesų atitiktį I priede nustatytiems esminiams kibernetinio saugumo reikalavimams gamintojas netaikė darniųjų standartų, bendrųjų specifikacijų ar Europos kibernetinio saugumo sertifikavimo schemų, kurių saugumo užtikrinimo lygis yra bent „pakankamai aukštas“, kaip nurodyta 27 straipsnyje, arba taikė juos tik iš dalies, arba jei tokių darniųjų standartų, bendrųjų specifikacijų ar Europos kibernetinio saugumo sertifikavimo schemų nėra, atitinkamam produktui su skaitmeniniais elementais ir gamintojo įdiegtiems procesams dėl tų esminių kibernetinio saugumo reikalavimų taikoma bet kuri iš šių procedūrų:

a) ES tipo tyrimo procedūra (remiantis B moduliu), nustatyta VIII priede, ir po to ES tipo atitikties, pagrįstos vidine gamybos kontrole, procedūra (remiantis C moduliu), nustatyta VIII priede, arba

b) visišku kokybės užtikrinimu pagrįsta atitikties vertinimo procedūra (remiantis H moduliu), nustatyta VIII priede.

3. Jei produktas yra III priede nustatytai II klasei priskiriamas svarbus produktas su skaitmeniniais elementais, gamintojas turi įrodyti atitiktį I priede nustatytiems esminiams kibernetinio saugumo reikalavimams taikydamas bet kurią iš šių procedūrų:

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

b) visišku kokybės užtikrinimu pagrįstą atitikties vertinimo procedūrą (remiantis H moduliu), nustatytą VIII priede, arba

c) kai yra ir taikytina, Europos kibernetinio saugumo sertifikavimo schemą pagal šio reglamento 27 straipsnio 9 dalį, kurios saugumo užtikrinimo lygis yra bent „pakankamai aukštas“ pagal Reglamentą (ES) 2019/881.

4. IV priede išvardytų ypatingos svarbos produktų su skaitmeniniais elementais atveju turi būti įrodyta atitiktis I priede nustatytiems esminiams kibernetinio saugumo reikalavimams taikant vieną iš šių procedūrų:

a) Europos kibernetinio saugumo sertifikavimo schemą pagal 8 straipsnio 1 dalį, arba

b) jei netenkinamos 8 straipsnio 1 dalyje nustatytos sąlygos, bet kurią iš šio straipsnio 3 dalyje nurodytų procedūrų.

5. Produktų su skaitmeniniais elementais, kurie laikomi laisvąja ir atvirąja programine įranga, priskiriamų prie III priede nustatytų kategorijų, gamintojai turi gebėti įrodyti atitiktį I priede nustatytiems esminiams kibernetinio saugumo reikalavimams taikant vieną iš šio straipsnio 1 dalyje nurodytų procedūrų, su sąlyga, kad 31 straipsnyje nurodyti techniniai dokumentai yra viešai prieinami tų produktų pateikimo rinkai metu.

6. Nustatant mokesčius už atitikties vertinimo procedūras atsižvelgiama į konkrečius labai mažų įmonių ir mažųjų bei vidutinių įmonių, įskaitant startuolius, interesus ir poreikius ir tie mokesčiai sumažinami proporcingai jų konkretiems interesams ir poreikiams.

33 straipsnis

Paramos priemonės labai mažoms įmonėms ir mažosioms bei vidutinėms įmonėms, įskaitant startuolius

1. Valstybės narės, kai tinkama, imasi toliau nurodytų veiksmų, pritaikytų labai mažų ir mažųjų įmonių poreikiams:

   a) organizuoja specialią informuotumo didinimo ir mokymo veiklą apie šio reglamento taikymą;

b) sukuria specialų komunikacijos su labai mažomis ir mažosiomis įmonėmis ir, kai tinkama, su vietos valdžios institucijomis kanalą, kuriuo teikiamos konsultacijos ir atsakoma į užklausas dėl šio reglamento įgyvendinimo;

c) remia bandymo ir atitikties vertinimo veiklą, be kita ko, kai aktualu, padedant Europos kibernetinio saugumo kompetencijos centrui.

2. Kai tikslinga, valstybės narės gali sukurti apribotą bandomąją kibernetinio atsparumo reglamentavimo aplinką. Tokioje apribotoje bandomojoje reglamentavimo aplinkoje nustatoma kontroliuojama novatoriškų produktų su skaitmeniniais elementais bandymų aplinka siekiant palengvinti jų kūrimą, projektavimą, tvirtinimą ir bandymą atitikties šiam reglamentui tikslais ribotą laikotarpį iki jų pateikimo rinkai. Komisija ir, kai tinkama, ENISA gali teikti techninę paramą, konsultacijas ir priemones, susijusias su apribotos bandomosios reglamentavimo aplinkos sukūrimu ir veikimu. Apribota bandomoji reglamentavimo aplinka sukuriama rinkos priežiūros institucijoms tiesiogiai prižiūrint, vadovaujant ir remiant. Valstybės narės per administracinio bendradarbiavimo grupę informuoja Komisiją ir kitas rinkos priežiūros institucijas apie apribotos bandomosios reglamentavimo aplinkos sukūrimą. Apribota bandomoji reglamentavimo aplinka nedaro poveikio su priežiūra ir taisomaisiais veiksmais susijusiems kompetentingų institucijų įgaliojimams. Valstybės narės užtikrina atvirą, sąžiningą ir skaidrią prieigą prie apribotos bandomosios reglamentavimo aplinkos ir, visų pirma, palengvina prieigą labai mažoms įmonėms ir mažosioms įmonėms, įskaitant startuolius.

3. Pagal 26 straipsnį Komisija teikia labai mažoms įmonėms ir mažosioms bei vidutinėms įmonėms gaires dėl šio reglamento įgyvendinimo.

4. Komisija skelbia apie galimybes gauti finansinę paramą pagal esamų Sąjungos programų reglamentavimo sistemą, visų pirma, siekdama palengvinti finansinę naštą labai mažoms įmonėms ir mažosioms įmonėms.

5. Labai mažos įmonės ir mažosios įmonės visus VII priede nurodytų techninių dokumentų elementus gali pateikti supaprastinta forma. Šiuo tikslu Komisija įgyvendinimo aktais nustato supaprastintą techninių dokumentų formą, pritaikytą labai mažų ir mažųjų įmonių poreikiams, įskaitant tai, kaip turi būti pateikti VII priede nustatyti elementai. Jei labai maža įmonė arba mažoji įmonė nusprendžia pateikti VII priede nustatytą informaciją supaprastinta tvarka, ji naudoja šioje dalyje nurodytą formą. Notifikuotosios įstaigos pripažįsta tą formą atitikties vertinimo tikslais.

Tie įgyvendinimo aktai priimami laikantis 62 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

34 straipsnis

Abipusio pripažinimo susitarimai

Atsižvelgiant į trečiosios valstybės techninę pažangą ir požiūrį į atitikties vertinimą, Sąjunga gali sudaryti su trečiosiomis valstybėmis abipusio pripažinimo susitarimus pagal SESV 218 straipsnį, kad paskatintų ir palengvintų tarptautinę prekybą.

IV skyrius

Atitikties vertinimo įstaigų notifikavimas

35 straipsnis

Notifikavimas

1. Valstybės narės notifikuoja Komisijai ir kitoms valstybėms narėms įstaigas, įgaliotas atlikti atitikties vertinimą pagal šį reglamentą.

2. Valstybės narės ne vėliau kaip … [24 mėnesiai nuo šio reglamento įsigaliojimo dienos] siekia užtikrinti, kad Sąjungoje būtų pakankamai notifikuotųjų įstaigų atitikties vertinimams atlikti siekiant išvengti kliūčių ir trukdymų patekti į rinką.

36 straipsnis

Notifikuojančiosios institucijos

1. Kiekviena valstybės narė paskiria notifikuojančiąją instituciją, atsakingą už tai, kad būtų nustatytos ir taikomos reikiamos procedūros, pagal kurias įvertinamos ir paskiriamos atitikties vertinimo įstaigos, atliekama jų notifikavimo procedūra ir vykdoma jų stebėsena, apimanti 41 straipsnio laikymąsi.

2. Valstybės narės gali nuspręsti, kad 1 dalyje nurodytą vertinimą ir stebėseną turi vykdyti nacionalinė akreditacijos įstaiga, kaip tai suprantama Reglamente (EB) Nr. 765/2008 ir laikantis to reglamento.

3. Jei notifikuojančioji institucija šio straipsnio 1 dalyje nurodytą vertinimą, notifikavimą ar stebėseną deleguoja arba kitaip paveda vykdyti įstaigai, kuri nėra vyriausybinis subjektas, ta įstaiga turi būti teisės subjektas ir *mutatis mutandis* turi laikytis 37 straipsnio. Be to, ji turi turėti su jos veikla susijusios atsakomybės draudimą.

4. Notifikuojančioji institucija prisiima visą atsakomybę už 3 dalyje nurodytos įstaigos atliekamas užduotis.

37 straipsnis

Notifikuojančiosioms institucijoms taikomi reikalavimai

1. Notifikuojančioji institucija įsteigiama taip, kad nekiltų jos ir atitikties vertinimo įstaigų interesų konfliktas.

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. Notifikuojančioji institucija turi turėti pakankamai kompetentingų darbuotojų, kad jos užduotys būtų atliekamos tinkamai.

38 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 užtikrina, kad 1 dalyje nurodyta informacija būtų viešai prieinama.

39 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 teisinį subjektiškumą.

3. Atitikties vertinimo įstaiga turi būti trečiosios šalies įstaiga, nepriklausoma nuo organizacijos ar produkto su skaitmeniniais elementais, kurį ji vertina.

   Įstaiga, priklausanti verslo asociacijai arba profesinei federacijai, atstovaujančiai įmonės, susijusios su jos vertinamų produktų su skaitmeniniais elementais projektavimu, kūrimu, gamyba, tiekimu, surinkimu, naudojimu ar techninе priežiūra, gali būti laikoma tokia trečiosios šalies įstaiga, jei įrodoma, kad ji yra nepriklausoma ir nėra jokio interesų konflikto.

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

Atitikties vertinimo įstaiga, jos vyresnioji vadovybė ir už atitikties vertinimo užduotis atsakingi darbuotojai negali tiesiogiai dalyvauti projektuojant, kuriant, gaminant, importuojant, platinant, parduodant, montuojant, naudojant produktus su skaitmeniniais elementais, kuriuos jie vertina, ar atliekant techninę jų priežiūrą, taip pat negali atstovauti tokia veikla užsiimančioms šalims. Jos negali imtis 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 patronuojamųjų bendrovių 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, ir turi turėti reikiamą konkrečios srities techninę kompetenciją bei nepasiduoti jokiam spaudimui ir paskatoms, visų pirma finansinėms, kurie galėtų paveikti jų sprendimą ar 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 VIII 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:

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

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

c) reikiamas 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.

Atitikties vertinimo įstaiga turi turėti priemonių, būtinų su atitikties vertinimo veikla susijusioms techninėms ir administracinėms užduotims tinkamai atlikti, ir galimybę naudotis visa reikiama įranga ar infrastruktūra.

7. Už atitikties vertinimo veiklą atsakingi darbuotojai turi:

a) turėti tinkamą techninį ir profesinį parengimą, apimantį visą atitikties vertinimo veiklą, dėl kurios atitikties vertinimo įstaiga buvo notifikuota;

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

c) turėti tinkamų žinių ir išmanyti I priede nustatytus esminius kibernetinio saugumo reikalavimus, taikomus darniuosius standartus ir bendrąsias specifikacijas, taip pat atitinkamas Sąjungos derinamųjų teisės aktų ir įgyvendinimo aktų nuostatas;

d) turėti gebėjimų rengti sertifikatus, daryti duomenų įrašus ir rengti ataskaitas, kuriais įrodoma, kad buvo atliktas vertinimas.

8. Turi būti užtikrintas atitikties vertinimo įstaigų, jų vyresniosios vadovybės ir vertinimą atliekančių darbuotojų nešališkumas.

Atitikties vertinimo įstaigos vyresniosios vadovybės 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 jų valstybė narė 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 VIII priedą arba bet kurią nacionalinės teisės nuostatą, kuria jis įgyvendinamas, išskyrus atvejus, susijusius su valstybės narės, kurioje vykdoma jų 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 pagal 51 straipsnį sukurtos notifikuotųjų įstaigų koordinavimo grupės veikloje arba užtikrina, kad vertinimą atliekantys jų darbuotojai būtų apie tą veiklą informuoti, ir tos grupės priimtus administracinius sprendimus ir parengtus dokumentus taiko kaip bendrąsias gaires.

12. Atitikties vertinimo įstaigos veikia vadovaudamosi nuosekliomis, sąžiningomis, proporcingomis ir pagrįstomis sąlygomis, vengdamos nereikalingos naštos ekonominės veiklos vykdytojams, ypač atsižvelgiant į labai mažų įmonių ir mažųjų bei vidutinių įmonių interesus dėl mokesčių.

40 straipsnis

Notifikuotųjų įstaigų atitikties prezumpcija

Jei atitikties vertinimo įstaiga įrodo, kad atitinka kriterijus, nustatytus atitinkamuose darniuosiuose standartuose arba jų dalyse, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*, preziumuojama, kad ji atitinka 39 straipsnyje nustatytus reikalavimus tiek, kiek juos apima taikomi darnieji standartai.

41 straipsnis

Notifikuotųjų įstaigų patronuojamosios įmonės ir subranga

1. Jei notifikuotoji įstaiga konkrečias su atitikties vertinimu susijusias užduotis paveda atlikti subrangovui ar patronuojamajai įmonei, ji užtikrina, kad tas subrangovas arba patronuojamoji įmonė atitiktų 39 straipsnyje nustatytus reikalavimus, ir apie tai informuoja notifikuojančiąją instituciją.

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

3. Pavesti darbą subrangovui arba patronuojamai įmonei galima tik gavus gamintojo sutikimą.

4. Notifikuotosios įstaigos saugo aktualius dokumentus, susijusius su subrangovo ar patronuojamosios įmonės kvalifikacijos įvertinimu ir jų pagal šį reglamentą atliktu darbu, kad notifikuojančioji institucija galėtų su jais susipažinti.

42 straipsnis

Notifikavimo paraiška

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

2. Prie tos paraiškos pridedamas atitikties vertinimo veiklos, atitikties vertinimo procedūros arba procedūrų ir produkto arba produktų su skaitmeniniais elementais, kuriuos vertinti ta įstaiga teigia turinti kompetencijos, aprašymas, taip pat, kai taikytina, nacionalinės akreditacijos įstaigos išduotas akreditacijos pažymėjimas, kuriuo patvirtinama, kad atitikties vertinimo įstaiga atitinka 39 straipsnyje nustatytus reikalavimus.

3. Jei tam tikra atitikties vertinimo įstaiga negali pateikti akreditacijos pažymėjimo, ji pateikia notifikuojančiajai institucijai visus dokumentinius įrodymus, būtinus jos atitikčiai 39 straipsnyje nustatytiems reikalavimams patikrinti, patvirtinti ir reguliariai stebėti.

43 straipsnis

Notifikavimo procedūra

1. Notifikuojančiosios institucijos notifikuoja tik tas atitikties vertinimo įstaigas, kurios atitinka 39 straipsnyje nustatytus reikalavimus.

2. Notifikuojančioji institucija teikia notifikavimo pranešimus Komisijai ir kitoms valstybėms narėms naudodama Komisijos sukurtą ir administruojamą Naujojo požiūrio notifikuotųjų ir paskirtų organizacijų informacinę sistemą“.

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

4. Jei notifikavimas nėra grindžiamas akreditacijos pažymėjimu, kaip nurodyta 42 straipsnio 2 dalyje, notifikuojančioji institucija Komisijai ir kitoms valstybėms narėms pateikia dokumentinius įrodymus, kuriais patvirtinama atitikties vertinimo įstaigos kompetencija ir tai, kad yra nustatyta reguliarų tos įstaigos stebėjimą ir jos tolesnę atitiktį 39 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, arba per du mėnesius po notifikavimo, jeigu nesinaudojama akreditacijos pažymėjimu, nepareiškia prieštaravimų.

   Tik tokia įstaiga laikoma notifikuotąja įstaiga pagal šį reglamentą.

6. Komisijai ir kitoms valstybėms narėms pranešama apie visus susijusius vėlesnius notifikavimo pranešimo pakeitimus.

44 straipsnis

Notifikuotųjų įstaigų identifikaciniai numeriai ir sąrašai

1. Komisija suteikia notifikuotajai įstaigai identifikacinį numerį.

   Komisija suteikia tik vieną identifikacinį numerį net ir tuo atveju, kai apie įstaigą yra notifikuota pagal kelis Sąjungos teisės aktus.

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

   Komisija užtikrina, kad tas sąrašas būtų nuolat atnaujinamas.

45 straipsnis

Notifikavimų pakeitimai

1. Kai notifikuojančioji institucija išsiaiškina arba yra informuojama, kad notifikuotoji įstaiga nebeatitinka 39 straipsnyje nustatytų reikalavimų arba kad ji nevykdo savo pareigų, notifikuojančioji institucija atitinkamai apriboja, laikinai sustabdo arba panaikina notifikavimo galiojimą, atsižvelgdama į tų reikalavimų nesilaikymo arba pareigų nevykdymo sunkumą. Apie tai ji atitinkamai nedelsdama informuoja Komisiją ir kitas valstybes nares.

2. Jei notifikavimo galiojimas apribojamas, laikinai sustabdomas arba panaikinamas, arba jei notifikuotoji įstaiga nutraukia veiklą, notifikuojančioji valstybė narė imasi tinkamų priemonių siekdama užtikrinti, kad tos įstaigos bylas tvarkytų kita notifikuotoji įstaiga arba jos būtų saugomos, kad su jomis galėtų susipažinti prašymą pateikusios atsakingos notifikuojančiosios institucijos ir rinkos priežiūros institucijos.

46 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 notifikavimo pagrindu arba atitinkamos įstaigos kompetencijos užtikrinimu.

3. Komisija užtikrina, kad visa neskelbtina informacija, gauta jai atliekant tyrimą, būtų tvarkoma konfidencialiai.

4. Jei Komisija sužino, kad notifikuotoji įstaiga neatitinka arba nebeatitinka jos notifikavimo reikalavimų, ji atitinkamai informuoja notifikuojančiąja valstybę narę ir paprašo imtis būtinų taisomųjų priemonių, įskaitant, jei būtina, notifikavimo panaikinimą.

47 straipsnis

Notifikuotųjų įstaigų su veikla susijusios pareigos

1. Notifikuotosios įstaigos atlieka atitikties vertinimus pagal 32 straipsnyje ir VIII priede numatytas atitikties vertinimo procedūras.

2. Atitikties vertinimai atliekami proporcingai, siekiant išvengti nereikalingos naštos ekonominės veiklos vykdytojams. Atitikties vertinimo įstaigos atlieka savo veiklą tinkamai atsižvelgdamos į įmonių dydį, visų pirma į labai mažas įmones ir mažąsias bei vidutines įmones, jų veiklos sektorių, jų struktūrą, atitinkamos produktų su skaitmeniniais elementais rūšies ir technologijos sudėtingumo laipsnį bei kibernetinio saugumo rizikos lygį 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 produktų su skaitmeniniais elementais atitiktis šiam reglamentui.

4. Kai notifikuotoji įstaiga nustato, kad gamintojas neįvykdė I priede, atitinkamuose darniuosiuose standartuose arba bendrosiose specifikacijose nustatytų reikalavimų, kaip nurodyta 27 straipsnyje, ji reikalauja, kad tas gamintojas imtųsi tinkamų taisomųjų priemonių, ir neišduoda atitikties sertifikato.

5. Jei sertifikatą išdavusi notifikuotoji įstaiga, vykdydama atitikties stebėseną, nustato, kad produktas su skaitmeniniais elementais nebeatitinka šiame reglamente nustatytų reikalavimų, ji reikalauja, kad gamintojas imtųsi tinkamų taisomųjų priemonių, ir, jei būtina, laikinai sustabdo arba panaikina sertifikato galiojimą.

6. Jei taisomųjų priemonių nesiimama arba jos nedaro reikalaujamo poveikio, notifikuotoji įstaiga prireikus apriboja, laikinai sustabdo arba panaikina sertifikatų galiojimą.

48 straipsnis

Notifikuotųjų įstaigų sprendimų apskundimas

Valstybės narės užtikrina, kad būtų nustatyta skundų dėl notifikuotųjų įstaigų sprendimų teikimo tvarka.

49 straipsnis

Notifikuotųjų įstaigų pareiga informuoti

1. Notifikuotosios įstaigos informuoja notifikuojančiąją instituciją apie:

   a) kiekvieną atsisakymą išduoti sertifikatą, sertifikato galiojimo apribojimą, laikiną 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, atsižvelgiant į notifikavimo taikymo sritį, 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 su skaitmeniniais elementais atitikties vertinimo veiklą, teikia susijusią informaciją klausimais, susijusiais su neigiamais ir, jei prašoma, teigiamais atitikties vertinimo rezultatais.

50 straipsnis

Keitimasis patirtimi

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

51 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 notifikuotosios įstaigos tiesiogiai ar per paskirtuosius atstovus dalyvautų tos grupės veikloje.

V skyrius

Rinkos priežiūra ir vykdymo užtikrinimas

52 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. Pagal šio straipsnio 2 dalį paskirtos rinkos priežiūros institucijos taip pat atsako už rinkos priežiūros veiklos, susijusios su 24 straipsnyje nustatytomis atvirosios programinės įrangos valdytojų pareigomis, vykdymą. Jei rinkos priežiūros institucija nustato, kad atvirosios programinės įrangos valdytojas nesilaiko tame straipsnyje nustatytų pareigų, ji reikalauja, jog atvirosios programinės įrangos valdytojas užtikrintų, kad būtų imtasi visų tinkamų taisomųjų veiksmų. Atvirosios programinės įrangos valdytojai užtikrina, kad būtų imtasi visų tinkamų taisomųjų veiksmų, susijusių su jų pareigomis pagal šį reglamentą.

4. 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 vykdomos pareigos pranešti pagal šio reglamento 14 straipsnį, paskirtosios rinkos priežiūros institucijos reguliariai bendradarbiauja ir keičiasi informacija su koordinatorėmis paskirtomis CSIRT ir ENISA.

5. Rinkos priežiūros institucijos gali prašyti koordinatore paskirtos CSIRT arba ENISA teikti technines konsultacijas su šio reglamento įgyvendinimu ir vykdymo užtikrinimu susijusiais klausimais. Vykdydamos tyrimą pagal 54 straipsnį, rinkos priežiūros institucijos gali prašyti koordinatore paskirtos CSIRT arba ENISA pateikti analizę, kuri padėtų įvertinti produktų su skaitmeniniais elementais atitiktį.

6. Prireikus, rinkos priežiūros institucijos bendradarbiauja su kitomis rinkos priežiūros institucijomis, paskirtomis pagal kitus nei šis reglamentas Sąjungos derinamuosius teisės aktus, ir reguliariai keičiasi informacija.

7. Rinkos priežiūros institucijos, kai tinkama, bendradarbiauja su institucijomis, atsakingomis už Sąjungos duomenų apsaugos teisės priežiūrą. Toks bendradarbiavimas apima tų institucijų informavimą apie bet kokius nustatytus faktus, susijusius su jų pareigų pagal jų kompetenciją vykdymu, įskaitant teikiant rekomendacijas ir konsultacijas pagal 10 dalį, jei tokios rekomendacijos ir konsultacijos yra susiję su asmens duomenų tvarkymu.

   Institucijos, atsakingos už Sąjungos duomenų apsaugos teisės priežiūrą, turi turėti įgaliojimus 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 informuoja atitinkamos valstybės narės paskirtąsias rinkos priežiūros institucijas.

8. Valstybės narės užtikrina, kad paskirtosioms rinkos priežiūros institucijoms būtų suteikta pakankamai finansinių ir techninių išteklių, įskaitant, kai tinkama, automatizuoto tvarkymo priemones, taip pat žmogiškųjų išteklių su reikiamais kibernetinio saugumo įgūdžiais jų užduotims pagal šį reglamentą vykdyti.

9. Komisija skatina ir palengvina paskirtųjų rinkos priežiūros institucijų keitimąsi patirtimi.

10. Rinkos priežiūros institucijos, padedamos Komisijos ir, kai tinkama, CSIRT ir ENISA, gali teikti rekomendacijas ir konsultacijas ekonominės veiklos vykdytojams dėl šio reglamento įgyvendinimo.

11. Rinkos priežiūros institucijos informuoja vartotojus apie tai, kur pateikti skundus, kurie rodytų šio reglamento nesilaikymą, pagal Reglamento (ES) 2019/1020 11 straipsnį, ir teikia vartotojams informaciją apie tai, kur ir kaip naudotis mechanizmais, kad būtų lengviau pranešti apie pažeidžiamumus, incidentus ir kibernetines grėsmes, kurie gali daryti poveikį produktams su skaitmeniniais elementais.

12. Rinkos priežiūros institucijos, kai aktualu, sudaro palankesnes sąlygas bendradarbiauti su suinteresuotaisiais subjektais, įskaitant mokslo, tyrimų ir vartotojų organizacijas.

13. Rinkos priežiūros institucijos kartą per metus perduoda 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.

14. Produktų su skaitmeniniais elementais, kurie patenka į šio reglamento taikymo sritį ir pagal Reglamento (ES) 2024/1689 6 straipsnį priskiriami prie didelės rizikos DI sistemų, atveju Reglamento (ES) 2024/1689 tikslais paskirtos rinkos priežiūros institucijos yra institucijos, atsakingos už rinkos priežiūros veiklą, kurią reikalaujama vykdyti pagal šį reglamentą. Pagal Reglamentą (ES) 2024/1689 paskirtos rinkos priežiūros institucijos, prireikus, bendradarbiauja su pagal šį reglamentą paskirtomis rinkos priežiūros institucijomis, o dėl pareigos pranešti vykdymo pagal šio reglamento 14 straipsnį priežiūros – su koordinatorėmis paskirtomis CSIRT ir ENISA. Pagal Reglamentą (ES) 2024/1689 paskirtos rinkos priežiūros institucijos pagal šį reglamentą paskirtas rinkos priežiūros institucijas visų pirma informuoja apie visus nustatytus faktus, kurie yra svarbūs su šio reglamento įgyvendinimu susijusių jų užduočių vykdymui.

15. Siekiant vienodai taikyti šį reglamentą, sudaroma administracinio bendradarbiavimo grupė pagal Reglamento (ES) 2019/1020 30 straipsnio 2 dalį. Administracinio bendradarbiavimo grupę sudaro paskirtų rinkos priežiūros institucijų ir, jei tinkama, bendrų ryšių palaikymo tarnybų atstovai. Administracinio bendradarbiavimo grupė taip pat sprendžia konkrečius klausimus dėl rinkos priežiūros veiklos, susijusios su atvirosios programinės įrangos valdytojams nustatytomis pareigomis.

16. Rinkos priežiūros institucijos vykdo stebėseną, kaip gamintojai, nustatydami savo produktų su skaitmeniniais elementais palaikymo laikotarpį, taikė 13 straipsnio 8 dalyje nurodytus kriterijus.

Administracinio bendradarbiavimo grupė viešai prieinama ir patogia naudoti forma skelbia atitinkamus statistinius duomenis apie produktų su skaitmeniniais elementais kategorijas, įskaitant vidutinius palaikymo laikotarpius, kuriuos gamintojas nustato pagal 13 straipsnio 8 dalį, taip pat parengia gaires, kuriose nurodomi orientaciniai produktų su skaitmeniniais elementais kategorijoms taikomi palaikymo laikotarpiai.

Jei iš duomenų matyti, kad konkrečių kategorijų produktų su skaitmeniniais elementais palaikymo laikotarpiai yra nepakankami, administracinio bendradarbiavimo grupė gali rekomenduoti rinkos priežiūros institucijoms sutelkti dėmesį į tokių kategorijų produktus su skaitmeniniais elementais.

53 straipsnis

Prieiga prie duomenų ir dokumentų

Kai reikia įvertinti produktų su skaitmeniniais elementais ir jų gamintojų įdiegtų procesų atitiktį I priede nustatytiems esminiams kibernetinio saugumo reikalavimams, rinkos priežiūros institucijoms, pateikus pagrįstą prašymą, joms lengvai suprantama kalba suteikiama prieiga prie duomenų, kurių reikia tokių produktų projektavimui, kūrimui, gamybai ir pažeidžiamumų valdymui įvertinti, įskaitant susijusius atitinkamo ekonominės veiklos vykdytojo vidaus dokumentus.

54 straipsnis

Nacionaliniu lygmeniu taikoma procedūra dėl produktų su skaitmeniniais elementais, keliančių didelę kibernetinio saugumo riziką

1. Jei valstybės narės rinkos priežiūros institucija turi pakankamų priežasčių manyti, kad produktas su skaitmeniniais elementais, įskaitant jo pažeidžiamumų valdymą, kelia didelę kibernetinio saugumo riziką, ji, nepagrįstai nedelsdama ir, kai tikslinga, bendradarbiaudama su atitinkama CSIRT, atlieka atitinkamo produkto su skaitmeniniais elementais atitikties visiems šiame reglamente nustatytiems reikalavimams vertinimą. Atitinkami ekonominės veiklos vykdytojai, prireikus, bendradarbiauja su rinkos priežiūros institucija.

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

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

2. Nustatant šio straipsnio 1 dalyje nurodytos kibernetinio saugumo rizikos dydį, rinkos priežiūros institucijos taip pat apsvarsto netechninius rizikos veiksnius, visų pirma tuos, kurie buvo nustatyti pagal Direktyvos (ES) 2022/2555 22 straipsnį atlikus Sąjungos lygmens koordinuotus ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimus. Jei rinkos priežiūros institucija turi pakankamai priežasčių manyti, kad produktas su skaitmeniniais elementais kelia didelę kibernetinio saugumo riziką dėl netechninių rizikos veiksnių, ji informuoja pagal Direktyvos (ES) 2022/2555 8 straipsnį paskirtas arba įsteigtas kompetentingas institucijas ir, kai būtina, su jomis bendradarbiauja.

3. 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 ekonominės veiklos vykdytojas.

4. Ekonominės veiklos vykdytojas užtikrina, kad visų tinkamų taisomųjų veiksmų būtų imtasi dėl visų susijusių produktų su skaitmeniniais elementais, kuriuos jis patiekė rinkai visoje Sąjungoje.

5. Jei per 1 dalies antroje pastraipoje nurodytą laikotarpį ekonominės veiklos vykdytojas nesiima tinkamų taisomųjų veiksmų, rinkos priežiūros institucija imasi visų tinkamų laikinųjų priemonių, kad būtų uždraustas arba apribotas produkto su skaitmeniniais elementais tiekimas jo nacionalinei rinkai, kad jis būtų pašalintas iš tos rinkos arba atšauktas.

   Apie tokias priemones ta institucija nedelsdama praneša Komisijai ir kitoms valstybėms narėms.

6. 5 dalyje nurodyta informacija apima visus turimus duomenis, visų pirma duomenis, reikalingus reikalavimų neatitinkančiam produktui su skaitmeniniais elementais, to produkto su skaitmeniniais elementais kilmei, tariamos neatitikties ir keliamos rizikos pobūdžiui, nacionaliniu lygmeniu taikomų priemonių pobūdžiui ir trukmei bei atitinkamo ekonominės veiklos vykdytojo pateiktiems argumentams nustatyti. Visų pirma, rinkos priežiūros institucija nurodo, ar neatitiktis sietina su viena ar daugiau iš šių priežasčių:

   a) produkto su skaitmeniniais elementais arba gamintojo įdiegtų procesų neatitiktimi I priede nustatytiems esminiams kibernetinio saugumo reikalavimams;

   b) 27 straipsnyje nurodytų darniųjų standartų, Europos kibernetinio saugumo sertifikavimo schemų ar bendrųjų specifikacijų trūkumais.

7. Valstybių narių rinkos priežiūros institucijos, išskyrus procedūrą inicijavusios valstybės narės rinkos priežiūros instituciją, nedelsdamos praneša Komisijai ir kitoms valstybėms narėms apie visas priemones, kurių ėmėsi, ir pateikia visą turimą papildomą informaciją, susijusią su atitinkamo produkto su skaitmeniniais elementais neatitiktimi, ir, jei nesutinka su nacionaline priemone, apie kurią pranešta, savo prieštaravimus.

8. Jei per tris mėnesius nuo šio straipsnio 5 dalyje nurodyto pranešimo gavimo dienos nei kuri nors valstybė narė, nei Komisija nepareiškia prieštaravimų dėl laikinosios priemonės, kurios ėmėsi valstybė narė, ta priemonė laikoma pagrįsta. Tai nedaro poveikio atitinkamo ekonominės veiklos vykdytojo procesinėms teisėms pagal Reglamento (ES) 2019/1020 18 straipsnį.

9. Visų valstybių narių rinkos priežiūros institucijos užtikrina, kad atitinkamam produktui su skaitmeniniais elementais nedelsiant būtų taikomos tinkamos ribojamosios priemonės, pavyzdžiui, tas produktas būtų pašalintas iš jų rinkos.

55 straipsnis

Sąjungos apsaugos procedūra

1. Jei per tris mėnesius nuo 54 straipsnio 5 dalyje nurodyto pranešimo gavimo dienos kuri nors valstybė narė pareiškia prieštaravimų dėl priemonės, kurios ėmėsi kita valstybė narė, arba jei Komisija mano, kad priemonė prieštarauja Sąjungos teisei, Komisija nedelsdama pradeda konsultacijas su atitinkama valstybe nare ir ekonominės veiklos vykdytoju ar vykdytojais ir įvertina nacionalinę priemonę. Remdamasi to vertinimo rezultatais, Komisija per devynis mėnesius nuo 54 straipsnio 5 dalyje nurodyto pranešimo dienos nusprendžia, ar nacionalinė priemonė yra pagrįsta, ar ne, ir apie tą sprendimą praneša atitinkamai valstybei narei.

2. Jei nacionalinė priemonė yra 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 yra laikoma nepagrįsta, atitinkama valstybė narė tą priemonę atšaukia.

3. Jei nacionalinė priemonė laikoma pagrįsta, o produkto su skaitmeniniais elementais neatitiktis siejama su darniųjų standartų trūkumais, Komisija taiko Reglamento (ES) Nr. 1025/2012 11 straipsnyje numatytą procedūrą.

4. Jei nacionalinė priemonė laikoma pagrįsta, o produkto su skaitmeniniais elementais neatitiktis siejama su 27 straipsnyje nurodytos Europos kibernetinio saugumo sertifikavimo sistemos trūkumais, Komisija svarsto, ar iš dalies pakeisti arba panaikinti pagal 27 straipsnio 9 dalį priimtą deleguotąjį aktą, kuriame nurodoma tos sertifikavimo sistemos atitikties prezumpcija.

5. Jei nacionalinė priemonė laikoma pagrįsta, o produkto su skaitmeniniais elementais neatitiktis siejama su 27 straipsnyje nurodytų bendrųjų specifikacijų trūkumais, Komisija svarsto, ar iš dalies pakeisti arba panaikinti pagal 27 straipsnio 2 dalį priimtą įgyvendinimo aktą, kuriame nustatomos tos bendrosios specifikacijos.

56 straipsnis

Sąjungos lygmeniu taikoma procedūra dėl produktų su skaitmeniniais elementais, keliančių didelę kibernetinio saugumo riziką

1. Jei Komisija turi pakankamai priežasčių manyti, įskaitant remdamasi ENISA pateikta informacija, kad produktas su skaitmeniniais elementais, kuris kelia didelę kibernetinio saugumo riziką, neatitinka šiame reglamente nustatytų reikalavimų, ji apie tai informuoja atitinkamas rinkos priežiūros institucijas. Jei rinkos priežiūros institucijos atlieka to produkto su skaitmeniniais elementais, kuris gali kelti didelę kibernetinio saugumo riziką, vertinimą, susijusį su jo atitiktimi šiame reglamente nustatytiems reikalavimams, taikomos 54 ir 55 straipsniuose nurodytos procedūros.

2. Jei Komisija turi pakankamai priežasčių manyti, kad produktas su skaitmeniniais elementais kelia didelę kibernetinio saugumo riziką dėl netechninių rizikos veiksnių, ji informuoja atitinkamas rinkos priežiūros institucijas ir, kai taikytina, pagal Direktyvos (ES) 2022/2555 8 straipsnį paskirtas arba įsteigtas kompetentingas institucijas ir, kai būtina, su jomis bendradarbiauja. Komisija taip pat apsvarsto nustatytos rizikos, susijusios su tuo produktu su skaitmeniniais elementais, svarbą, vykdydama savo užduotis, susijusias su Direktyvos (ES) 2022/2555 22 straipsnyje numatytais koordinuotais Sąjungos lygmens ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimais, ir, kai būtina, konsultuojasi su Bendradarbiavimo grupe, įsteigta pagal Direktyvos (ES) 2022/2555 14 straipsnį, ir ENISA.

3. Aplinkybėmis, kurios pateisina neatidėliotiną intervenciją siekiant išsaugoti tinkamą vidaus rinkos veikimą, ir jei Komisija turi pakankamai priežasčių manyti, kad 1 dalyje nurodytas produktas su skaitmeniniais elementais vis dar neatitinka šiame reglamente nustatytų reikalavimų, o atitinkamos rinkos priežiūros institucijos nesiėmė jokių veiksmingų priemonių, Komisija atlieka atitikties vertinimą ir gali prašyti ENISA atlikti tą vertinimą pagrindžiančią analizę. Komisija apie tai informuoja atitinkamas rinkos priežiūros institucijas. Atitinkami ekonominės veiklos vykdytojai, kai būtina, bendradarbiauja su ENISA.

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

5. Remdamasi šio straipsnio 4 dalyje nurodytomis konsultacijomis Komisija gali priimti įgyvendinimo aktus dėl taisomųjų arba ribojamųjų priemonių Sąjungos lygmeniu nustatymo, įskaitant reikalavimą pašalinti atitinkamus produktus su skaitmeniniais elementais iš rinkos arba atšaukti juos per pagrįstą laikotarpį, nustatytą atsižvelgiant į rizikos pobūdį. Tie įgyvendinimo aktai priimami laikantis 62 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

6. Komisija apie 5 dalyje nurodytus įgyvendinimo aktus nedelsdama praneša atitinkamam ekonominės veiklos vykdytojui ar vykdytojams. Valstybės narės nedelsdamos įgyvendina tuos įgyvendinimo aktus ir atitinkamai informuoja Komisiją.

7. 3–6 dalys taikomos tiek laiko, kiek trunka išimtinė situacija, pateisinanti Komisijos įsikišimą, jei ir toliau neužtikrinama produkto su skaitmeniniais elementais atitiktis šiam reglamentui.

57 straipsnis

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

1. Valstybės narės rinkos priežiūros institucija reikalauja, kad ekonominės veiklos vykdytojas imtųsi visų tinkamų priemonių, jei ji, atlikusi vertinimą pagal 54 straipsnį, nustato, kad nepaisant to, jog produktas su skaitmeniniais elementais ir gamintojo įdiegti procesai atitinka šį reglamentą, jis kelia didelę kibernetinio saugumo riziką ir riziką:

   a) asmenų sveikatai ar saugai;

   b) pareigų vykdymui pagal Sąjungos ar nacionalinę teisę, kuria siekiama apsaugoti pagrindines teises;

c) paslaugų, kurias per elektroninę informacinę sistemą siūlo Direktyvos (ES) 2022/2555 3 straipsnio 1 dalyje nurodyti esminiai subjektai, prieinamumui, autentiškumui, vientisumui ar konfidencialumui, arba

d) kitiems viešojo intereso apsaugos aspektams.

Pirmoje pastraipoje nurodytos priemonės gali apimti priemones, kuriomis užtikrinama, kad atitinkamas produktas su skaitmeniniais elementais ir gamintojo įdiegti procesai nebekeltų atitinkamos rizikos, kai jis tiekiamas rinkai, jog atitinkamas produktas su skaitmeniniais elementais būtų pašalintas iš rinkos arba atšauktas, ir kad tos priemonės būtų proporcingos tos rizikos pobūdžiui.

2. Gamintojas arba kiti atitinkami ekonominės veiklos vykdytojai užtikrina, kad taisomųjų veiksmų dėl produktų su skaitmeniniais elementais, kuriuos jie patiekė rinkai visoje Sąjungoje, būtų imtasi per 1 dalyje nurodytos valstybės narės rinkos priežiūros institucijos nustatytą terminą.

3. Valstybė narė nedelsdama informuoja Komisiją ir kitas valstybes nares apie priemones, kurių imtasi pagal 1 dalį. Ta informacija apima visus turimus duomenis, visų pirma, atitinkamam produktui su skaitmeniniais elementais identifikuoti būtinus duomenis, tų produktų su skaitmeniniais elementais kilmę ir tiekimo grandinę, susijusios rizikos pobūdį ir nacionalinių priemonių, kurių imtasi, pobūdį bei trukmę.

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

5. Komisija 4 dalyje nurodytą sprendimą skiria valstybėms narėms.

6. Jei Komisija turi pakankamai priežasčių manyti, be kita ko remdamasi ENISA pateikta informacija, kad produktas su skaitmeniniais elementais nors ir atitinka šio reglamento reikalavimus, tačiau kelia šio straipsnio 1 dalyje nurodytą riziką, ji informuoja atitinkamą rinkos priežiūros instituciją ar institucijas ir gali jų prašyti atlikti vertinimą ir laikytis 54 straipsnyje bei šio straipsnio 1, 2 ir 3 dalyse nurodytų procedūrų.

7. Aplinkybėmis, kuriomis pateisinama neatidėliotina intervencija siekiant išsaugoti tinkamą vidaus rinkos veikimą, ir kai Komisija turi pakankamai priežasčių manyti, kad 6 dalyje nurodytas produktas su skaitmeniniais elementais vis dar kelia 1 dalyje nurodytą riziką, o atitinkamos rinkos priežiūros institucijos nesiėmė jokių veiksmingų priemonių, Komisija atlieka to produkto su skaitmeniniais elementais keliamos rizikos vertinimą ir gali nurodyti ENISA atlikti tą vertinimą pagrindžiančią analizę bei apie tai informuoja atitinkamas rinkos priežiūros institucijas. Atitinkami ekonominės veiklos vykdytojai, kai būtina, bendradarbiauja su ENISA.

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

9. Remdamasi šio straipsnio 8 dalyje nurodytomis konsultacijomis Komisija gali priimti įgyvendinimo aktus, kuriais nusprendžiama Sąjungos lygmeniu taikyti taisomąsias arba ribojamąsias priemones, įskaitant reikalavimą pašalinti atitinkamus produktus su skaitmeniniais elementais iš rinkos arba atšaukti juos per pagrįstą laikotarpį, nustatytą atsižvelgiant į rizikos pobūdį. Tie įgyvendinimo aktai priimami laikantis 62 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

10. Komisija apie 9 dalyje nurodytus įgyvendinimo aktus nedelsdama praneša atitinkamam ekonominės veiklos vykdytojui ar vykdytojams. Valstybės narės nedelsdamos įgyvendina tuos įgyvendinimo aktus ir apie tai atitinkamai informuoja Komisiją.

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

58 straipsnis

Oficiali neatitiktis

1. Valstybės narės rinkos priežiūros institucija reikalauja, kad atitinkamas gamintojas pašalintų atitinkamą neatitiktį, jei ji padaro vieną iš šių išvadų:

a) CE ženklu buvo ženklinama pažeidžiant 29 ir 30 straipsnius;

b) nebuvo ženklinama CE ženklu;

c) neparengta ES atitikties deklaracija;

d) ES atitikties deklaracija parengta netinkamai;

e) nepažymėta atitikties vertinimo procedūroje dalyvaujančios notifikuotosios įstaigos identifikaciniu numeriu, kai taikytina;

f) nėra techninių dokumentų arba jie yra neišsamūs.

2. Jei 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 jis būtų atšauktas arba pašalintas iš rinkos.

59 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 su skaitmeniniais elementais, kurie dažnai kelia kibernetinio saugumo riziką.

2. Komisija arba ENISA pasiūlo bendrą veiklą, skirtą atitikčiai šio reglamento reikalavimams patikrinti, kurią vykdo rinkos priežiūros institucijos remdamosi įrodymais arba informacija apie galimą produktų su skaitmeniniais elementais, kurie patenka į šio reglamento taikymo sritį, neatitiktį šiame reglamente nustatytiems reikalavimams keliose valstybėse narėse.

3. Rinkos priežiūros institucijos ir, kai taikytina, Komisija 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 bendrai 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.

60 straipsnis

Tikslinės patikros

1. Rinkos priežiūros institucijos nusprendžia 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. Tos tikslinės patikros gali apimti produktų su skaitmeniniais elementais, įsigytų neatskleidus tapatybės, tikrinimą.

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

3. Jei ENISA, vykdydama savo užduotis , taip pat remdamasi pagal 14 straipsnio 1 ir 3 dalis gautais pranešimais, nustato produktų su skaitmeniniais elementais kategorijas, dėl kurių gali būti organizuojamos patikros, ji pateikia pasiūlymą dėl tikslinės patikros šio straipsnio 2 dalyje nurodytam koordinatoriui, kad jį apsvarstytų rinkos priežiūros institucijos.

4. Vykdydamos tikslines patikras jose dalyvaujančios rinkos priežiūros institucijos gali naudotis 52–58 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

61 straipsnis

Naudojimasis įgaliojimais

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

2. 2 straipsnio 5 dalies antroje pastraipoje, 7 straipsnio 3 dalyje, 8 straipsnio 1 ir 2 dalyse, 13 straipsnio 8 dalies ketvirtoje pastraipoje, 14 straipsnio 9 dalyje, 25 straipsnyje, 27 straipsnio 9 dalyje, 28 straipsnio 5 dalyje ir 31 straipsnio 5 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo … [šio reglamento įsigaliojimo diena]. Likus ne mažiau kaip devyniems mėnesiams iki penkerių metų laikotarpio pabaigos Komisija parengia naudojimosi deleguotaisiais įgaliojimais ataskaitą. Deleguotieji įgaliojimai savaime pratęsiami tokios pačios trukmės laikotarpiams, išskyrus atvejus, kai Europos Parlamentas arba Taryba pareiškia prieštaravimų dėl tokio pratęsimo likus ne mažiau kaip trims mėnesiams iki kiekvieno laikotarpio pabaigos.

3. Europos Parlamentas arba Taryba gali bet kada atšaukti 2 straipsnio 5 dalies antroje pastraipoje, 7 straipsnio 3 dalyje, 8 straipsnio 1 ir 2 dalyse, 13 straipsnio 8 dalies ketvirtoje pastraipoje, 14 straipsnio 9 dalyje, 25 straipsnyje, 27 straipsnio 9 dalyje, 28 straipsnio 5 dalyje ir 31 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. Apie priimtą deleguotąjį aktą Komisija nedelsdama vienu metu praneša Europos Parlamentui ir Tarybai.

6. Pagal 2 straipsnio 5 dalies antrą pastraipą, 7 straipsnio 3 dalį, 8 straipsnio 1 arba 2 dalis, 13 straipsnio 8 dalies ketvirtą pastraipą, 14 straipsnio 9 dalį, 25 straipsnį, 27 straipsnio 9 dalį, 28 straipsnio 5 dalį arba 31 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 dviem mėnesiais.

62 straipsnis

Komiteto procedūra

1. Komisijai padeda komitetas. Tas komitetas – tai komitetas, kaip tai suprantama 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

63 straipsnis

Konfidencialumas

1. Visos šį reglamentą taikant dalyvaujančios 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 (ES) 2016/943[36] 5 straipsnyje nurodytus atvejus;

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

   c) viešojo ir nacionalinio saugumo interesai;

   d) baudžiamojo ar administracinio proceso vientisumas.

[36] 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).

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.

64 straipsnis

Sankcijos

1. Valstybės narės nustato sankcijų, taikomų pažeidus šį reglamentą, taisykles ir imasi visų būtinų priemonių užtikrinti, kad šios sankcijos būtų įgyvendinamos. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos. Valstybės narės nedelsdamos praneša apie tas taisykles ir priemones Komisijai ir nedelsdamos jai praneša apie visus vėlesnius joms įtakos turinčius pakeitimus.

2. Už I priede nustatytų esminių kibernetinio saugumo reikalavimų ir 13 bei 14 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, atsižvelgiant į tai, kuri suma yra didesnė.

3. Už 18–23 straipsniuose, 28 straipsnyje, 30 straipsnio 1–4 dalyse, 31 straipsnio 1–4 dalyse, 32 straipsnio 1, 2 ir 3 dalyse, 33 straipsnio 5 dalyje ir 39, 41, 47, 49 ir 53 straipsniuose nustatytų pareigų 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, atsižvelgiant į tai, kuri suma yra didesnė.

4. 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, atsižvelgiant į tai, kuri suma yra didesnė.

5. Sprendžiant dėl administracinės baudos dydžio kiekvienu konkrečiu atveju atsižvelgiama į visas svarbias konkrečios situacijos aplinkybes ir tinkamai atsižvelgiama į šiuos dalykus:

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

   b) ar tos pačios arba kitos rinkos priežiūros institucijos jau skyrė administracines baudas tam pačiam ekonominės veiklos vykdytojui už panašų pažeidimą;

   c) pažeidimą padariusio ekonominės veiklos vykdytojo dydį, visų pirma kiek tai susiję su labai mažomis įmonėmis ir mažosiomis bei vidutinėmis įmonėmis, įskaitant startuolius, ir rinkos dalį.

6. Administracines baudas skiriančios rinkos priežiūros institucijos informacija apie tų baudų taikymą dalijasi su kitų valstybių narių rinkos priežiūros institucijomis per Reglamento (ES) 2019/1020 34 straipsnyje nurodytą informacinę ir komunikacijos sistemą.

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

8. 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.

9. 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.

10. Nukrypstant nuo 3–9 dalių, tose dalyse nurodytos administracinės baudos netaikomos:

    a) gamintojams, kurie laikomi labai mažomis įmonėmis arba mažomis įmonėmis, nesilaikantiems 14 straipsnio 2 dalies a punkte arba 14 straipsnio 4 dalies a punkte nurodyto termino;

    b) atvirosios programinės įrangos valdytojams už šio reglamento pažeidimus.

65 straipsnis

Atstovaujamieji ieškiniai

Atstovaujamiesiems ieškiniams, pareikštiems dėl ekonominės veiklos vykdytojų padarytų šio reglamento pažeidimų, kurie daro arba gali daryti žalą kolektyviniams vartotojų interesams, taikoma Direktyva (ES) 2020/1828.

VIII skyrius

Pereinamojo laikotarpio ir baigiamosios nuostatos

66 straipsnis

Reglamento (ES) 2019/1020 dalinis pakeitimas

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

„XX[+]. Europos Parlamento ir Tarybos reglamentas (ES) 2024/…[*++].

---

[*] … m. … … d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/… dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas) (OL …, ELI: …).“.

[+] OL: prašom tekste įrašyti Reglamento (ES) 2019/1020 I priede esančio sąrašo sekantį skaičių eilės tvarka.

[++] OL: prašom tekste įrašyti reglamento, esančio dokumente PE-CONS 100/23 (2022/0272(COD)), numerį, o išnašoje – to reglamento priėmimo datą, numerį ir OL nuorodą.

67 straipsnis

Direktyvos (ES) 2020/1828 dalinis pakeitimas

Direktyvos (ES) 2020/1828 I priedas papildomas šiuo punktu:

„XX[+]. Europos Parlamento ir Tarybos reglamentas (ES) 2024/…[*++].

---

[*] … m. … … d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/… dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas) (OL …, ELI: …).“.

[+] OL: prašom įrašyti tekste Direktyvos (ES) 2020/1828 I priedo sąrašo sekantį skaičių eilės tvarka.

[++] OL: prašom tekste įrašyti reglamento, esančio dokumente PE-CONS 100/23 (2022/0272(COD)), numerį, o išnašoje – to reglamento priėmimo datą, numerį ir OL nuorodą.

68 straipsnis

Reglamento (ES) Nr. 168/2013 dalinis pakeitimas

Europos Parlamento ir Tarybos reglamento (ES) Nr. 168/2013[37] II priedas iš dalies keičiamas taip:

C1 dalies lentelėje įterpiama ši eilutė:

„

XX+	18	Transporto priemonės apsauga nuo kibernetinių išpuolių		x	x	x	x	x	x	x	x	x	x	x	x	x	x

“.

[37] 2013 m. sausio 15 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 168/2013 dėl dviračių ir triračių transporto priemonių bei keturračių patvirtinimo ir rinkos priežiūros (OL L 60, 2013 3 2, p. 52).

+ OL: prašom tekste įrašyti Reglamento (ES) Nr. 168/2013 II priede po antrašte C1 sekantį skaičių eilės tvarka.

69 straipsnis

Pereinamojo laikotarpio nuostatos

1. ES tipo tyrimo sertifikatai ir patvirtinimo sprendimai dėl produktų su skaitmeniniais elementais, kuriems taikomi kiti nei šis reglamentas Sąjungos derinamieji teisės aktai, kibernetinio saugumo reikalavimų galioja iki …[42 mėnesiai nuo šio reglamento įsigaliojimo dienos], išskyrus atvejus, kai jie nustoja galioti anksčiau nei tą datą arba kai tuose kituose Sąjungos derinamuosiuose teisės aktuose nurodyta kitaip – tokiu atveju jie galioja tiek, kiek nurodyta tuose teisės aktuose.

2. Produktams su skaitmeniniais elementais, pateiktiems rinkai anksčiau nei **…** [36 mėnesiai nuo šio reglamento įsigaliojimo dienos], šiame reglamente nustatyti reikalavimai taikomi tik tuo atveju, jei nuo tos datos padarytas esminis tų produktų pakeitimas.

3. Nukrypstant nuo šio straipsnio 2 dalies, 14 straipsnyje nustatytos pareigos taikomos visiems produktams su skaitmeniniais elementais, kurie patenka į šio reglamento taikymo sritį ir kurie rinkai buvo pateikti anksčiau nei **…** [36 mėnesiai nuo šio reglamento įsigaliojimo dienos].

70 straipsnis

Vertinimas ir peržiūra

1. Ne vėliau kaip … [72 mėnesiai nuo šio reglamento įsigaliojimo dienos], o vėliau - kas ketverius metus, Komisija pateikia Europos Parlamentui ir Tarybai šio reglamento vertinimo ir peržiūros ataskaitą. Tos ataskaitos skelbiamos viešai.

2. Ne vėliau kaip … [45 mėnesiai nuo šio reglamento įsigaliojimo dienos] Komisija, pasikonsultavusi su ENISA ir CSIRT tinklu, pateikia Europos Parlamentui ir Tarybai ataskaitą, kurioje įvertinamas 16 straipsnyje nustatytos bendrosios pranešimų teikimo platformos veiksmingumas, taip pat 16 straipsnio 2 dalyje nurodytų su kibernetiniu saugumu susijusių priežasčių, kurias taiko koordinatorėmis paskirtos CSIRT, taikymo poveikis bendros ataskaitų teikimo platformos veiksmingumui, kiek tai susiję su gautų pranešimų savalaikiu platinimu kitoms atitinkamoms CSIRT.

71 straipsnis

Įsigaliojimas ir taikymas

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

2. Šis reglamentas taikomas nuo … [36 mėnesiai nuo šio reglamento įsigaliojimo dienos].

   Tačiau 14 straipsnis taikomas nuo … [21 mėnuo nuo šio reglamento įsigaliojimo dienos], o IV skyrius (35–51 straipsniai) – nuo … [18 mėnesių nuo šio reglamento įsigaliojimo dienos].

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta … …

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

I PRIEDAS

ESMINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI

I dalis Kibernetinio saugumo reikalavimai, susiję su produktų su skaitmeniniais elementais savybėmis

1) Produktai su skaitmeniniais elementais projektuojami, kuriami ir gaminami taip, kad, atsižvelgiant į riziką, būtų užtikrintas tinkamas kibernetinio saugumo lygis.

2) Remiantis 13 straipsnio 2 dalyje nurodytu kibernetinio saugumo rizikos vertinimu, kai taikytina, produktams su skaitmeniniais elementais turi būti būdingos šios savybės:

   a) jie tiekiami rinkai be jokio žinomo pažeidžiamumo, kurį būtų galima išnaudoti;

   b) jie tiekiami rinkai su saugia numatytąja konfigūracija, išskyrus atvejus, jei produktą su skaitmeniniais elementais gaminant pagal užsakymą gamintojas ir verslo klientas susitaria kitaip, įskaitant galimybę atkurti pradinę gaminio būseną;

   c) užtikrinama, kad pažeidžiamumą būtų galima pašalinti saugumo naujiniais, įskaitant, kai taikytina, automatinius saugumo naujinius, diegiamus per tinkamą laikotarpį, taikant numatytąjį nustatymą, su aiškiu ir lengvai naudojamu atsisakymo mechanizmu, pranešant naudotojams apie esamus naujinius ir numatant galimybę juos laikinai atidėti;

d) juose užtikrinama apsauga nuo neteisėtos prieigos atitinkamais kontrolės mechanizmais, įskaitant atpažinimo, tapatybės ar prieigos valdymo sistemas ir pranešimus apie galimą neteisėtą prieigą, bet jomis neapsiribojant;

e) juose užtikrinamas saugomų, perduodamų ar kitaip apdorojamų asmens ar kitų duomenų konfidencialumas, pavyzdžiui, užšifruojant atitinkamus duomenis pažangiausiomis priemonėmis, kai šie duomenys saugomi arba perduodami, taip pat naudojant kitas technines priemones;

f) juose užtikrinama saugomų, perduodamų ar kitaip tvarkomų asmens ar kitų duomenų, komandų, programų ir konfigūracijos vientisumo apsauga nuo bet kokių manipuliacijų ar pakeitimų, kurioms naudotojas nesuteikė leidimo, ir pranešama apie pažeidimus;

g) juose tvarkomi tik tie asmens ar kiti duomenys, kurie yra tinkami, svarbūs ir apsiriboja tik tuo, kas būtina pagal produkto su skaitmeniniais elementais naudojimo numatomąją paskirtį (duomenų kiekio mažinimas);

h) juose užtikrinama galimybė naudotis esminėmis ir pagrindinėmis funkcijomis, taip pat po incidento, taikant atsparumo paslaugos trikdymo atakoms ir jų padarinių mažinimo priemones;

i) kuo labiau sumažinamas pačių produktų arba prijungtųjų įrenginių neigiamas poveikis kitų įrenginių ar tinklų teikiamų paslaugų prieinamumui;

j) jie projektuojami, kuriami ir gaminami taip, kad būtų apribotos atakos pažeidžiamos sritys, įskaitant išorines sąsajas;

k) jie projektuojami, kuriami ir gaminami taip, kad būtų sumažintas incidento poveikis, naudojant atitinkamus galimybės išnaudoti pažeidžiamas vietas mažinimo mechanizmus ir metodus;

l) jie teikia su saugumu susijusią informaciją, įrašant arba stebint atitinkamą vidinę veiklą, įskaitant prieigą prie duomenų, paslaugų ar funkcijų arba jų pakeitimą, suteikiant naudotojui galimybę pasinaudoti atsisakymo mechanizmu;

m) jie suteikia naudotojams galimybę saugiai ir lengvai visam laikui pašalinti visus duomenis ir nustatymus ir, kai tokius duomenis galima perkelti į kitus produktus ar sistemas, užtikrinti, kad tai būtų daroma saugiai.

II dalis Pažeidžiamumo valdymo reikalavimai

Produktų su skaitmeniniais elementais gamintojai:

1) nustato ir dokumentuoja produktų su skaitmeniniais elementais pažeidžiamumą ir komponentus, taip pat parengdami programinės įrangos medžiagų žiniaraštį įprastu ir kompiuterio skaitomu formatu, apimantį bent jau produktų aukščiausio lygio priklausomybes;

2) dėl produktams su skaitmeniniais elementais keliamos rizikos nedelsdami pašalina ir ištaiso pažeidžiamumo veiksnius, taip pat teikdami saugumo naujinius; kai techniškai įmanoma, nauji saugumo naujiniai teikiami atskirai nuo funkcijų naujinių;

3) taiko veiksmingus ir reguliarius produkto su skaitmeniniais elementais saugumo bandymus ir peržiūras;

4) kai tik saugumo naujinys tampa prieinamas, dalinasi ir viešai atskleidžia informaciją apie pašalintus pažeidžiamumo veiksnius, taip pat pateikdami pažeidžiamumo aprašymą, informaciją, leidžiančią naudotojams identifikuoti paveiktą produktą su skaitmeniniais elementais, pažeidžiamumo poveikį, jo sunkumą ir informaciją, padedančią naudotojams pašalinti pažeidžiamumo priežastis; tinkamai pagrįstais atvejais, kai gamintojai mano, kad paskelbimo saugumo rizika nusveria saugumo naudą, jie gali atidėti viešą informacijos apie pašalintą pažeidžiamumo veiksnį paskelbimą tol, kol naudotojams bus suteikta galimybė taikyti atitinkamą pataisą;

5) taiko koordinuoto pažeidžiamumo atskleidimo politiką ir užtikrina jos vykdymą;

6) imasi priemonių, kad palengvintų keitimąsi informacija apie galimą jų produkto su skaitmeniniais elementais ir tame produkte esančių trečiųjų šalių komponentų pažeidžiamumą, taip pat nurodydami kontaktinį adresą pranešimams apie produkte su skaitmeniniais elementais aptiktus pažeidžiamumo veiksnius;

7) numato produktų su skaitmeniniais elementais saugumo naujinių saugaus platinimo mechanizmus, siekiant užtikrinti, kad pažeidžiamumas būtų laiku ir, jei įmanoma naudojant saugumo naujinius, automatiškai ištaisytas arba būtų sumažintas jo poveikis;

8) užtikrina, kad atsiradus saugumo naujiniams, skirtiems nustatytoms saugumo problemoms spręsti, jie būtų nedelsiant ir, jeigu produktą su skaitmeniniais elementais gaminant pagal užsakymą gamintojas ir verslo klientas nesusitarė kitaip, nemokamai išplatinti kartu su patariamosiomis žinutėmis, suteikiančiomis naudotojams atitinkamą informaciją, įskaitant informaciją apie veiksmus, kurių gali reikėti imtis.

II PRIEDAS

NAUDOTOJUI SKIRTA INFORMACIJA IR INSTRUKCIJOS

Kartu su produktu su skaitmeniniais elementais turi būti pateikiama bent ši informacija:

1. gamintojo pavadinimas, registruotas prekės pavadinimas arba registruotasis prekių ženklas ir pašto adresas, e. pašto adresas ar kita skaitmeninė kontaktinė informacija, taip pat, jei yra, interneto svetainė, kurioje su gamintoju galima susisiekti;

2. vienas kontaktinis punktas, kuriame galima pranešti ir gauti informaciją apie su kibernetiniu saugumu susijusį produkto su skaitmeniniais elementais pažeidžiamumą, ir kur galima rasti gamintojo politiką dėl koordinuoto pažeidžiamumo atskleidimo;

3. pavadinimas, tipas ir visa papildoma informacija, leidžianti vienareikšmiškai identifikuoti produktą su skaitmeniniais elementais;

4. produkto su skaitmeniniais elementais numatytoji paskirtis, įskaitant gamintojo teikiamą saugumo aplinką, taip pat esminės produkto funkcijos ir informacija apie saugumo savybes;

5. visos žinomos ir numatomos aplinkybės, susijusios su produkto su skaitmeniniais elementais naudojimu pagal numatytąją paskirtį arba pagrįstai numatomo netinkamo naudojimo sąlygomis, dėl kurio gali kilti didelė kibernetinio saugumo rizika;

6. kai taikytina, interneto adresas, kuriuo galima gauti prieigą prie ES atitikties deklaracijos;

7. gamintojo siūlomo techninio saugumo palaikymo rūšis ir palaikymo laikotarpio galutinis terminas, per kurį naudotojai gali tikėtis, kad pažeidžiamumas bus tvarkomas, ir gauti saugumo naujinius;

8. išsamios instrukcijos arba interneto adresas, nukreipiantis į tokias išsamias instrukcijas ir informaciją:

   a) būtinos priemonės produkto su skaitmeniniais elementais pradinio paleidimo metu ir per visą jo naudojimo trukmę, kad būtų užtikrintas jo saugus naudojimas;

   b) kaip produkto su skaitmeniniais elementais pakeitimai gali paveikti duomenų saugumą;

   c) kaip galima įdiegti su saugumu susijusius naujinius;

   d) kaip saugiai nutraukti produkto su skaitmeniniais elementais naudojimą, įskaitant informaciją apie tai, kaip galima saugiai pašalinti naudotojo duomenis;

   e) kaip galima išjungti numatytąjį nustatymą, leidžiantį automatiškai įdiegti saugumo naujinius, kaip reikalaujama I priedo I dalies 2 punkto c papunktyje;

   f) jei produktas su skaitmeniniais elementais yra skirtas integruoti į kitus produktus su skaitmeniniais elementais – informacija, būtina, kad integratorius atitiktų I priede nustatytus esminius kibernetinio saugumo reikalavimus ir VII priede nustatytus dokumentų reikalavimus.

9. Jei gamintojas nusprendžia pateikti naudotojui programinės įrangos medžiagų žiniaraštį, informacija apie tai, kur tą programinės įrangos medžiagų žiniaraštį galima rasti.

III PRIEDAS

SVARBŪS PRODUKTAI SU SKAITMENINIAIS ELEMENTAIS

I klasė

1. Tapatybės valdymo sistemos ir privilegijuotos prieigos valdymo programinė ir aparatinė įranga, įskaitant tapatumo nustatymo ir prieigos kontrolės skaitytuvus, be kita ko, biometrinius skaitytuvus;

2. atskiros ir įterptosios naršyklės;

3. slaptažodžių tvarkyklės;

4. programinė įranga, kuri ieško, šalina arba izoliuoja kenkimo programinę įrangą;

5. produktai su skaitmeniniais elementais, atliekantys virtualiojo privataus tinklo (VPN) funkciją;

6. tinklo valdymo sistemos;

7. saugumo informacijos ir įvykių valdymo (SIEM) sistemos;

8. sistemos paleidimo tvarkyklės;

9. viešojo rakto infrastruktūra ir skaitmeninių sertifikatų išdavimo programinė įranga;

10. fizinės ir virtualiosios tinklo sąsajos;

11. operacinės sistemos ;

12. maršruto parinktuvai, modemai, skirti prisijungti prie interneto, ir jungikliai ;

13. mikroprocesoriai, turintys su saugumu susijusių funkcijų;

14. mikrovaldikliai, turintys su saugumu susijusių funkcijų;

15. konkrečios paskirties integriniai grandynai (ASIC) ir programuojamosios loginės matricos (FPGA), turinčios su saugumu susijusių funkcijų;

16. išmanieji namų bendrosios paskirties virtualūs asistentai;

17. išmanieji namų produktai, turintys su saugumu susijusių funkcijų, įskaitant išmaniąsias durų spynas, saugumo kameras, kūdikių stebėjimo sistemas ir signalizacijos sistemas;

18. prie interneto prijungti žaislai, kuriems taikoma Europos Parlamento ir Tarybos direktyva 2009/48/EB[1] ir kurie turi socialinių interaktyvių funkcijų (pavyzdžiui, kalbėjimo ar filmavimo) arba buvimo vietos sekimo funkcijų;

19. asmeniniai dėvimi gaminiai, kurie yra dėvimi arba tvirtinami ant žmogaus kūno ir kurie turi sveikatos stebėsenos (pavyzdžiui, sekimo) paskirtį bei kuriems netaikomas Reglamentas (ES) 2017/745 arba Reglamentas (ES) 2017/746, arba asmeniniai dėvimi gaminiai, kurie skirti naudoti vaikams.

II klasė

1. Hipervizoriai ir sudėtinių rodinių vykdymo sistemos, padedantys virtualizuoti operacines sistemas ir panašias aplinkas;

2. užkardos, įsibrovimo aptikimo ir prevencijos sistemos ;

3. klastojimui atsparūs mikroprocesoriai;

4. klastojimui atsparūs mikrovaldikliai.

---

[1] 2009 m. birželio 18 d. Europos Parlamento ir Tarybos direktyva 2009/48/EB dėl žaislų saugos (OL L 170, 2009 6 30, p. 1).

IV PRIEDAS

YPATINGOS SVARBOS PRODUKTAI SU SKAITMENINIAIS ELEMENTAIS

1. Aparatinės įrangos prietaisai su seifais;

2. išmaniųjų skaitiklių tinklų sietuvai, naudojami pažangiosiose matavimo sistemose, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2019/944[1] 2 straipsnio 23 punkte, ir kiti pažangieji saugumo prietaisai, be kita ko, skirti saugiam kriptografiniam apdorojimui;

3. išmaniosios kortelės arba panašūs prietaisai, įskaitant saugiuosius elementus.

---

[1] 2019 m. birželio 5 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/944 dėl elektros energijos vidaus rinkos bendrųjų taisyklių, kuria iš dalies keičiama Direktyva 2012/27/ES (OL L 158, 2019 6 14, p. 125).

V PRIEDAS

ES ATITIKTIES DEKLARACIJA

28 straipsnyje nurodytoje ES atitikties deklaracijoje pateikiama visa toliau nurodyta informacija:

1. pavadinimas, tipas ir visa papildoma informacija, leidžianti vienareikšmiškai identifikuoti produktą su skaitmeniniais elementais;

2. gamintojo arba jo įgaliotojo atstovo pavadinimas ir adresas;

3. patvirtinimas, kad ES atitikties deklaracija išduota tik teikėjo atsakomybe;

4. deklaracijos objektas (produkto su skaitmeniniais elementais identifikavimo informacija, pagal kurią jį būtų galima atsekti; kai tikslinga, galima pateikti nuotrauką);

5. pareiškimas, kad pirmiau apibūdintas deklaracijos objektas atitinka atitinkamus Sąjungos derinamuosius teisės aktus;

6. nuorodos į atitinkamą naudojamą darnųjį standartą arba kitą bendrąją specifikaciją arba kibernetinio saugumo sertifikavimą, kurių atžvilgiu deklaruota atitiktis;

7. kai taikytina, notifikuotosios įstaigos pavadinimas ir numeris, atliktos atitikties vertinimo procedūros aprašymas ir išduoto sertifikato identifikavimo duomenys;

8. papildoma informacija:

subjekto, kurio vardu pasirašoma, pavadinimas: ……

(išdavimo data ir vieta):

(vardas ir pavardė, pareigos) (parašas):

VI PRIEDAS

SUPAPRASTINTA ES ATITIKTIES DEKLARACIJA

Supaprastinta ES atitikties deklaracija, nurodyta 13 straipsnio 20 dalyje, formuluojama taip:

Aš, [gamintojo pavadinimas], patvirtinu, kad produkto su skaitmeniniais elementais tipas [produkto su skaitmeniniu elementu tipo pavadinimas] atitinka Europos Parlamento ir Tarybos reglamentą (ES) …/…[1].

Visas ES atitikties deklaracijos tekstas prieinamas šiuo interneto adresu:

---

[1] OL: prašom tekste įrašyti reglamento, esančio dokumente PE-CONS Nr/MM (2022/0272(COD)), numerį.

VII PRIEDAS

TECHNINIŲ DOKUMENTŲ TURINYS

31 straipsnyje nurodytuose techniniuose dokumentuose pateikiama bent ši informacija, taikoma atitinkamam produktui su skaitmeniniais elementais:

1. bendras produkto su skaitmeniniais elementais aprašymas, apimantis:

   a) jo numatytąją paskirtį;

   b) programinės įrangos versiją, turinčią įtakos atitikčiai esminiams kibernetinio saugumo reikalavimams;

   c) jei produktas su skaitmeniniais elementais yra aparatinės įrangos produktas, nuotraukas ar iliustracijas, kuriose matosi išorinės savybės, ženklinimas ir vidinis išdėstymas;

   d) naudotojui skirtą informaciją ir instrukcijas, kaip nustatyta II priede;

2. produkto su skaitmeniniais elementais projektavimo, kūrimo ir gamybos bei pažeidžiamumo valdymo procesų aprašymas, apimantis:

   a) būtiną informaciją apie produkto su skaitmeniniais elementais projektavimą ir kūrimą, įskaitant, kai taikytina, brėžinius ir schemas ir sistemos architektūros aprašymą, paaiškinantį, kaip programinės įrangos komponentai vienas kitą papildo arba sąveikauja ir integruojami į bendrą apdorojimą;

b) būtiną informaciją apie gamintojo įdiegtus pažeidžiamumo valdymo procesus ir jų specifikacijas, įskaitant programinės įrangos medžiagų žiniaraštį, koordinuoto pažeidžiamumo atskleidimo politiką, kontaktinio adreso pateikimo pranešimams apie pažeidžiamumą įrodymą ir techninių sprendimų, pasirinktų saugiam naujinių paskirstymui, aprašymą;

c) būtiną produkto su skaitmeniniais elementais gamybos ir stebėsenos procesų informaciją ir specifikacijas bei tų procesų patvirtinimą;

3. kibernetinio saugumo rizikos, į kurią atsižvelgiant produktas su skaitmeniniais elementais yra suprojektuotas, sukurtas, pagamintas, pristatytas ir techniškai prižiūrimas, vertinimas pagal 13 straipsnį, įskaitant vertinimą, kaip taikomi I priedo I dalyje nustatyti esminiai kibernetinio saugumo reikalavimai;

4. susijusi informacija, į kurią buvo atsižvelgta nustatant produkto su skaitmeniniais elementais palaikymo laikotarpį pagal 13 straipsnio 8 dalį;

5. visiškai arba iš dalies taikomų darniųjų standartų, kurių nuorodos paskelbtos *Europos Sąjungos oficialiajame leidinyje*, bendrųjų specifikacijų, nurodytų šio reglamento 27 straipsnyje, arba pagal Reglamentą (ES) 2019/881 patvirtintų Europos kibernetinio saugumo sertifikavimo schemų sąrašas, kaip nustatyta šio reglamento 27 straipsnio 8 dalyje, ir, jei tie darnieji standartai, bendrosios specifikacijos ar Europos kibernetinio saugumo sertifikavimo schemos nebuvo taikomos, sprendinių, taikytų siekiant užtikrinti atitiktį I priedo I ir II dalyse nustatytiems esminiams kibernetinio saugumo reikalavimams, aprašymas, įskaitant taikytų kitų susijusių techninių specifikacijų sąrašą. Jei darnieji standartai, bendrosios specifikacijos ar Europos kibernetinio saugumo sertifikavimo schemos buvo taikomi iš dalies, techniniuose dokumentuose nurodomos dalys, kurios buvo taikomos;

6. bandymų, atliktų siekiant patikrinti produkto su skaitmeniniais elementais ir pažeidžiamumo valdymo procesų atitiktį taikytiniems I priedo I ir II dalyse nustatytiems esminiams kibernetinio saugumo reikalavimams, ataskaitos;

7. ES atitikties deklaracijos kopija;

8. jei taikytina, programinės įrangos medžiagų žiniaraštis pagal pagrįstą rinkos priežiūros institucijos prašymą, jeigu tai yra būtina, kad ši institucija galėtų patikrinti, kaip laikomasi I priede nustatytų esminių kibernetinio saugumo reikalavimų.

VIII PRIEDAS

ATITIKTIES VERTINIMO PROCEDŪROS

I dalis Atitikties vertinimo procedūra, pagrįsta vidaus kontrole (remiantis A moduliu)

1. Vidaus kontrolė yra atitikties vertinimo procedūra, pagal kurią gamintojas įvykdo šios dalies 2, 3 ir 4 punktuose nustatytas pareigas ir, prisiimdamas visą atsakomybę, užtikrina ir pareiškia, kad produktai su skaitmeniniais elementais atitinka visus I priedo I dalyje nustatytus esminius kibernetinio saugumo reikalavimus, o gamintojas atitinka I priedo II dalyje nustatytus esminius kibernetinio saugumo reikalavimus.

2. Gamintojas parengia VII priede aprašytus techninius dokumentus.

3. Produktų su skaitmeniniais elementais projektavimas, kūrimas, gamyba ir pažeidžiamumo valdymas

   Gamintojas imasi visų būtinų priemonių, kad projektavimo, kūrimo, gamybos ir pažeidžiamumo valdymo procesai bei jų stebėsena užtikrintų pagamintų ar sukurtų produktų su skaitmeniniais elementais bei gamintojo įdiegtų procesų atitiktį I priedo I ir II dalyse nustatytiems esminiams kibernetinio saugumo reikalavimams.

4. Atitikties ženklas ir atitikties deklaracija

4.1. Kiekvieną atskirą produktą su skaitmeniniais elementais, kuris atitinka taikytinus šiame reglamente nustatytus reikalavimus, gamintojas paženklina CE ženklu.

4.2. Gamintojas parengia rašytinę kiekvieno produkto su skaitmeniniais elementais ES atitikties deklaraciją pagal 28 straipsnį ir kartu su techniniais dokumentais saugo ją 10 metų po produkto su skaitmeniniais elementais pateikimo rinkai dienos arba palaikymo laikotarpį, priklausomai nuo to, kuris terminas yra ilgesnis, kad nacionalinės institucijos galėtų su jais susipažinti. ES atitikties deklaracijoje identifikuojamas produktas su skaitmeniniais elementais, kuriam ji buvo parengta. ES atitikties deklaracijos kopija pateikiama atitinkamoms institucijoms jų prašymu.

5. Įgaliotieji atstovai

4 punkte nustatytas gamintojo pareigas jo vardu ir jo atsakomybe gali vykdyti jo įgaliotasis atstovas, jei atitinkamos pareigos yra nurodytos įgaliojime.

II dalis ES tipo tyrimas (remiantis B moduliu)

1. ES tipo tyrimas yra dalis atitikties vertinimo procedūros, pagal kurią notifikuotoji įstaiga nagrinėja produkto su skaitmeniniais elementais techninį projektą ir kūrimą bei gamintojo įdiegtus pažeidžiamumo valdymo procesus ir patvirtina, kad produktas su skaitmeniniais elementais atitinka I priedo I dalyje nustatytus esminius kibernetinio saugumo reikalavimus, o gamintojas atitinka I priedo II dalyje nustatytus esminius kibernetinio saugumo reikalavimus.

2. ES tipo tyrimas atliekamas kaip produkto su skaitmeniniais elementais techninio projekto ir kūrimo atitikties vertinimas atliekant techninių dokumentų ir 3 punkte nurodytų patvirtinamųjų duomenų tyrimą ir vienos ar daugiau svarbiausių produkto dalių pavyzdžių tyrimą (apimantį produkcijos tipą ir projekto tipą).

3. Gamintojas vienai jo pasirinktai notifikuotajai įstaigai pateikia ES tipo tyrimo paraišką.

   Paraiškoje pateikiama:

   3.1. gamintojo pavadinimas ir adresas ir, jei paraišką pateikia jo įgaliotasis atstovas, to atstovo pavadinimas ir adresas;

3.2. rašytinis pareiškimas, kad tokia pati paraiška nėra pateikta jokiai kitai notifikuotajai įstaigai;

3.3. techniniai dokumentai, kurie suteikia galimybę įvertinti produkto su skaitmeniniais elementais atitiktį taikytiniems I priedo I dalyje nustatytiems esminiams kibernetinio saugumo reikalavimams ir I priedo II dalyje nustatytus gamintojo pažeidžiamumo valdymo procesus ir kurie apima tinkamą rizikos analizę ir vertinimą. Techniniuose dokumentuose nurodomi taikytini reikalavimai, ir tie dokumentai, kiek reikia vertinimui, apima produkto su skaitmeniniais elementais projektavimą, gamybą ir veikimą. Kai taikytina, techniniuose dokumentuose pateikiami bent VII priede nurodyti elementai;

3.4. duomenys, patvirtinantys techninio projekto ir kūrimo sprendimų bei pažeidžiamumo valdymo procesų tinkamumą. Pateikiant šiuos patvirtinamuosius duomenis nurodomi visi naudoti dokumentai, ypač jei atitinkami darnieji standartai arba techninės specifikacijos buvo taikyti nepilnai. Prireikus, į patvirtinamuosius duomenis įtraukiami atitinkamoje gamintojo laboratorijoje arba kitoje bandymų laboratorijoje jo vardu ir jo atsakomybe atliktų bandymų rezultatai.

4. Notifikuotoji įstaiga:

4.1. išnagrinėja techninius dokumentus ir patvirtinamuosius duomenis, kad įvertintų produkto su skaitmeniniais elementais techninio projekto ir kūrimo atitiktį I priedo I dalyje nustatytiems esminiams kibernetinio saugumo reikalavimams ir gamintojo įdiegtų pažeidžiamumo valdymo procesų atitiktį I priedo II dalyje nustatytiems esminiams kibernetinio saugumo reikalavimams;

4.2. patikrina, ar pavyzdžiai sukurti arba pagaminti pagal techninius dokumentus, ir nustato, kurie elementai suprojektuoti ir sukurti pagal taikytinas atitinkamų darniųjų standartų arba techninių specifikacijų nuostatas ir kurie elementai suprojektuoti ir sukurti netaikant atitinkamų tų standartų nuostatų;

4.3. jei dėl I priede nurodytų reikalavimų gamintojas pasirinko taikyti atitinkamuose darniuosiuose standartuose arba techninėse specifikacijose nustatytus sprendimus – atlieka reikiamus tyrimus ir bandymus arba paveda juos atlikti, kad patikrintų, jog tie sprendimai taikyti tinkamai;

4.4. jei dėl I priede nurodytų reikalavimų susijusiuose darniuosiuose standartuose arba techninėse specifikacijose nustatyti sprendimai nebuvo taikomi – atlieka reikiamus tyrimus ir bandymus arba paveda juos atlikti, kad patikrintų, jog gamintojo pasirinkti sprendimai atitinka susijusius esminius kibernetinio saugumo reikalavimus;

4.5. susitaria su gamintoju dėl vietos, kurioje bus atliekami tyrimai ir bandymai.

5. Notifikuotoji įstaiga parengia vertinimo ataskaitą, kurioje registruojami pagal 4 punktą atliekami veiksmai ir jų rezultatai. Nedarant poveikio jos pareigoms notifikuojančiųjų institucijų atžvilgiu, notifikuotoji įstaiga visą tos ataskaitos turinį arba jos dalį paskelbia tik gavusi gamintojo sutikimą.

6. Kai tipas ir pažeidžiamumo valdymo procesai atitinka I priede nustatytus esminius kibernetinio saugumo reikalavimus, notifikuotoji įstaiga išduoda gamintojui ES tipo tyrimo sertifikatą. Sertifikate nurodomas gamintojo pavadinimas ir adresas, tyrimo išvados, sertifikato galiojimo sąlygos (jei yra) ir duomenys, reikalingi patvirtintam tipui ir pažeidžiamumo valdymo procesams identifikuoti. Prie sertifikato gali būti pridedamas vienas arba daugiau priedų.

Sertifikate ir jo prieduose turi būti visa susijusi informacija, kuria remiantis būtų galima įvertinti pagamintų ar sukurtų produktų su skaitmeniniais elementais atitiktį ištirtam tipui ir pažeidžiamumo valdymo procesams bei atlikti naudojamų produktų kontrolę.

Kai tipas ir pažeidžiamumo valdymo procesai neatitinka taikytinų I priede nustatytų esminių kibernetinio saugumo reikalavimų, notifikuotoji įstaiga turi atsisakyti išduoti ES tipo tyrimo sertifikatą ir apie tai pranešti pareiškėjui, nurodydama išsamias atsisakymo priežastis.

7. Notifikuotoji įstaiga seka visuotinai pripažįstamas mokslo ir technikos naujoves, kurios rodo, kad patvirtintas tipas ir pažeidžiamumo valdymo procesai gali nebeatitikti taikytinų I priede nustatytų esminių kibernetinio saugumo reikalavimų, ir sprendžia, ar dėl tokių pokyčių būtina atlikti papildomus tyrimus. Jei taip, notifikuotoji įstaiga apie tai praneša gamintojui.

Gamintojas informuoja notifikuotąją įstaigą, kuri saugo su ES tipo tyrimo sertifikatu susijusius techninius dokumentus, apie visus patvirtinto tipo ir pažeidžiamumo valdymo procesų pakeitimus, kurie gali daryti poveikį atitikčiai I priede nustatytiems esminiams kibernetinio saugumo reikalavimams arba sertifikato galiojimo sąlygoms. Tokiems pakeitimams reikalingas papildomas patvirtinimas, išduodamas kaip pirminio ES tipo tyrimo sertifikato papildymas.

8. Notifikuotoji įstaiga atlieka periodinius auditus, siekdama užtikrinti, kad I priedo II dalyje nustatyti pažeidžiamumo valdymo procesai būtų įgyvendinami tinkamai.

9. Kiekviena notifikuotoji įstaiga praneša notifikuojančiosioms institucijoms apie savo išduotus arba panaikintus ES tipo tyrimo sertifikatus ir jų papildymus ir periodiškai arba gavusi prašymą pateikia joms sertifikatų ir jų papildymų, kuriuos išduoti ji atsisakė arba kurių galiojimą laikinai sustabdė ar kitaip apribojo, sąrašą.

Kiekviena notifikuotoji įstaiga informuoja kitas notifikuotąsias įstaigas apie ES tipo tyrimo sertifikatus ir jų papildymus, kuriuos ji atsisakė išduoti, panaikino, laikinai sustabdė ar kitaip apribojo jų galiojimą, o gavusi prašymą – ir apie išduotus sertifikatus ir jų papildymus.

Komisija, valstybės narės ir kitos notifikuotosios įstaigos gali, pateikusios prašymą, gauti ES tipo tyrimo sertifikatų ir visų jų papildymų kopijas. Komisija ir valstybės narės gali, pateikusios prašymą, gauti techninių dokumentų kopiją ir notifikuotosios įstaigos atliktų tyrimų rezultatus. Notifikuotoji įstaiga saugo ES tipo tyrimo sertifikato, jo priedų ir papildymų kopijas, taip pat techninę bylą su gamintojo pateiktais dokumentais iki sertifikato galiojimo pabaigos.

10. Gamintojas saugo ES tipo tyrimo sertifikato, jo priedų bei papildymų kopijas ir techninius dokumentus 10 metų po produkto su skaitmeniniais elementais pateikimo rinkai dienos arba per palaikymo laikotarpį, priklausomai nuo to, kuris terminas yra ilgesnis, kad nacionalinės institucijos galėtų su jais susipažinti.

11. Gamintojo įgaliotasis atstovas gali pateikti 3 punkte nurodytą paraišką ir vykdyti 7 ir 10 punktuose nustatytas pareigas, jei atitinkamos pareigos yra nurodytos įgaliojime.

III dalis Gamybos vidaus kontrole pagrįsta atitiktis tipui (remiantis C moduliu)

1. Gamybos vidaus kontrole pagrįsta tipo atitiktis – tai atitikties vertinimo procedūros dalis, kurios metu gamintojas įvykdo šios dalies 2 ir 3 punktuose nustatytas pareigas, taip pat užtikrina ir patvirtina, kad atitinkami produktai su skaitmeniniais elementais atitinka ES tipo tyrimo sertifikate aprašytą tipą bei I priedo I dalyje nustatytus esminius kibernetinio saugumo reikalavimus ir kad gamintojas atitinka I priedo II dalyje nustatytus esminius kibernetinio saugumo reikalavimus.

2. Gamyba

Gamintojas imasi visų būtinų priemonių, kad vykdant gamybą ir jos stebėseną būtų užtikrinta pagamintų produktų su skaitmeniniais elementais atitiktis ES tipo tyrimo sertifikate aprašytam patvirtintam tipui bei I priedo I dalyje nustatytiems esminiams kibernetinio saugumo reikalavimams, taip pat užtikrinta gamintojo atitiktis I priedo II dalyje nustatytiems esminiams kibernetinio saugumo reikalavimams.

3. Atitikties ženklas ir atitikties deklaracija

3.1. Kiekvieną produktą su skaitmeniniais elementais, atitinkantį ES tipo tyrimo sertifikate aprašytą tipą ir teisės akte nustatytus taikytinus reikalavimus, gamintojas paženklina CE ženklu.

3.2. Gamintojas parengia rašytinę produkto modelio atitikties deklaraciją ir saugo ją 10 metų nuo produkto su skaitmeniniais elementais pateikimo rinkai arba per palaikymo laikotarpį, priklausomai nuo to, kuris terminas yra ilgesnis, kad nacionalinės institucijos galėtų su jais susipažinti. Atitikties deklaracijoje identifikuojamas produkto modelis, kuriam ji buvo parengta. Atitikties deklaracijos kopija pateikiama atitinkamoms institucijoms jų prašymu.

4. Įgaliotasis atstovas

3 punkte nustatytas gamintojo pareigas jo vardu ir jo atsakomybe gali vykdyti jo įgaliotasis atstovas, jei atitinkamos pareigos yra nurodytos įgaliojime.

IV dalis Visišku kokybės užtikrinimu pagrįsta atitiktis (remiantis H moduliu)

1. Visišku kokybės užtikrinimu pagrįsta atitiktis yra atitikties vertinimo procedūra, pagal kurią gamintojas įvykdo šios dalies 2 ir 5 punktuose nustatytas pareigas ir, prisiimdamas visą atsakomybę, užtikrina ir pareiškia, kad atitinkami produktai su skaitmeniniais elementais arba produktų kategorijos atitinka I priedo I dalyje nustatytus esminius kibernetinio saugumo reikalavimus ir kad gamintojo įdiegti pažeidžiamumo valdymo procesai atitinka I priedo II dalyje nustatytus reikalavimus.

2. Produktų su skaitmeniniais elementais projektavimas, kūrimas, gamyba ir pažeidžiamumo valdymas

Gamintojas valdo 3 punkte nurodytą patvirtintą atitinkamų produktų su skaitmeniniais elementais projektavimo, kūrimo ir galutinio gaminio patikros bei bandymų kokybės sistemą bei pažeidžiamumo valdymo kokybės sistemą, palaiko jos veiksmingumą per visą palaikymo laikotarpį ir jam taikoma 4 punkte nustatyta priežiūra.

3. Kokybės sistema

3.1. Gamintojas jo pasirinktai notifikuotajai įstaigai pateikia paraišką įvertinti jo kokybės sistemą, kurią jis taiko atitinkamiems produktams su skaitmeniniais elementais.

Paraiškoje pateikiama:

– gamintojo pavadinimas ir adresas ir, jei paraišką pateikia jo įgaliotasis atstovas, to atstovo pavadinimas ir adresas;

– techniniai dokumentai, parengti vienam kiekvienos numatytų gaminti ar kurti produktų su skaitmeniniais elementais kategorijos modeliui. Jei taikytina, techniniuose dokumentuose pateikiami bent VII priede nurodyti elementai;

– dokumentai dėl kokybės sistemos, ir

– rašytinis pareiškimas, kad tokia pati paraiška nėra pateikta jokiai kitai notifikuotajai įstaigai.

3.2. Kokybės sistema turi užtikrinti produktų su skaitmeniniais elementais atitiktį I priedo I dalyje nustatytiems esminiams kibernetinio saugumo reikalavimams ir gamintojo įdiegtų pažeidžiamumo valdymo procesų atitiktį I priedo II dalyje nustatytiems reikalavimams.

Visi gamintojo priimti elementai, reikalavimai ir nuostatos sistemingai ir tvarkingai dokumentuojami – rengiamos rašytinės strategijos, procedūros ir instrukcijos. Kokybės sistemos dokumentai parengiami taip, kad jais remiantis būtų galima vienodai aiškinti kokybės programas, planus, vadovus ir įrašus.

Visų pirma, juose tinkamai aprašoma:

– kokybės valdymo tikslai ir organizacinė struktūra, vadovybės pareigos ir įgaliojimai, susiję su projektavimu, kūrimu, produkto kokybe ir pažeidžiamumo valdymu;

– techninio projekto ir kūrimo specifikacijos, įskaitant standartus, kurie bus taikomi, ir, jeigu atitinkami darnieji standartai arba techninės specifikacijos bus taikomi tik iš dalies, priemonės, kuriomis bus siekiama užtikrinti I priedo I dalyje nustatytų produktams su skaitmeniniais elementais taikomų esminių kibernetinio saugumo reikalavimų vykdymą;

– procedūrų specifikacijos, įskaitant standartus, kurie bus taikomi, ir, jeigu atitinkami darnieji standartai arba techninės specifikacijos bus taikomi tik iš dalies, priemonės, kuriomis bus siekiama užtikrinti I priedo II dalyje nustatytų gamintojui taikomų esminių kibernetinio saugumo reikalavimų vykdymą;

– projekto ir kūrimo kontrolės bei projekto ir kūrimo patikros būdai, procesai ir sistemingi veiksmai, kurie bus taikomi projektuojant ir kuriant nagrinėjamai gaminių kategorijai priklausančius produktus su skaitmeniniais elementais;

– atitinkami gamybos, kokybės kontrolės ir kokybės užtikrinimo metodai, procesai ir sistemingi veiksmai, kurie bus taikomi;

– tyrimai ir bandymai, kurie bus atliekami prieš gamybą, gamybos metu ir po jos, ir jų atlikimo dažnumas;

– kokybės įrašai, kaip antai patikrinimų ataskaitos, bandymų ir kalibravimo duomenys bei atitinkamo personalo kvalifikacijos ataskaitos;

– priemonės, skirtos stebėti, ar užtikrinama reikiama projekto ir produktų kokybė ir ar efektyviai veikia kokybės sistema.

3.3. Notifikuotoji įstaiga vertina kokybės sistemą ir nustato, ar ji atitinka 3.2 punkte nurodytus reikalavimus.

Ji preziumuoja, kad tuos reikalavimus atitinka tie kokybės sistemos elementai, kurie atitinka susijusį darnųjį standartą arba techninę specifikaciją įgyvendinančio nacionalinio standarto atitinkamas specifikacijas.

Be kokybės valdymo sistemų srities patirties, audito grupėje turi būti bent vienas narys, turintis atitinkamų produktų vertinimo patirties ir išmanantis atitinkamo produkto technologiją, ir audito grupė privalo žinoti taikytinus šiame reglamente nustatytus reikalavimus. Audito procedūros dalis yra vertinimas lankantis gamintojo patalpose, jei jis turi patalpas. Audito grupė peržiūri 3.1 punkto antroje įtraukoje nustatytus techninius dokumentus, kad patikrintų gamintojo gebėjimą identifikuoti taikytinus šiame reglamente nustatytus reikalavimus ir atlikti reikiamus tyrimus, kad užtikrintų produkto su skaitmeniniais elementais atitiktį tiems reikalavimams.

Apie sprendimą pranešama gamintojui arba jo įgaliotajam atstovui.

Pranešime pateikiamos audito išvados ir pagrįstas įvertinimo sprendimas.

3.4. Gamintojas įsipareigoja vykdyti su patvirtinta kokybės sistema susijusias pareigas ir užtikrinti, kad sistema toliau veiktų tinkamai ir veiksmingai.

3.5. Gamintojas informuoja kokybės sistemą patvirtinusią notifikuotąją įstaigą apie visus numatomus kokybės sistemos pakeitimus.

Notifikuotoji įstaiga įvertina siūlomus pakeitimus ir nusprendžia, ar pakeista kokybės sistema toliau atitinka 3.2 punkte nurodytus reikalavimus, ar reikia ją iš naujo įvertinti.

Apie savo sprendimą ji praneša gamintojui. Pranešime pateikiamos nagrinėjimo išvados ir pagrįstas sprendimas dėl įvertinimo.

4. Notifikuotosios įstaigos atsakomybe atliekama priežiūra

4.1. Priežiūros tikslas – įsitikinti, ar gamintojas deramai vykdo pareigas, susijusias su patvirtinta kokybės sistema.

4.2. Gamintojas leidžia notifikuotajai įstaigai vertinimo tikslais patekti į projektavimo, kūrimo, gamybos, tikrinimo, bandymų bei sandėliavimo vietas, taip pat suteikia jai visą būtiną informaciją, visų pirma:

– kokybės sistemos dokumentus;

– projektui skirtoje kokybės sistemos dalyje numatytus kokybės įrašus, pavyzdžiui, analizių, skaičiavimų ir bandymų rezultatus;

– gamybai skirtoje kokybės sistemos dalyje numatytus kokybės įrašus, pavyzdžiui, tikrinimų ataskaitas ir bandymų duomenis, kalibravimo duomenis ir susijusio personalo kvalifikacijos ataskaitas.

4.3. Notifikuotoji įstaiga atlieka periodinius auditus, kad galėtų įsitikinti, ar gamintojas techniškai prižiūri ir taiko kokybės sistemą, ir pateikia audito ataskaitą gamintojui.

5. Atitikties ženklas ir atitikties deklaracija

5.1. Kiekvieną atskirą produktą su skaitmeniniais elementais, kuris atitinka šio reglamento I priedo I dalyje nustatytus reikalavimus, gamintojas paženklina CE ženklu ir, 3.1 punkte nurodytos notifikuotosios įstaigos atsakomybe, šios įstaigos identifikaciniu numeriu.

5.2. Gamintojas parengia rašytinę kiekvieno produkto modelio atitikties deklaraciją ir saugo ją 10 metų nuo produkto su skaitmeniniais elementais pateikimo rinkai arba per palaikymo laikotarpį, priklausomai nuo to, kuris terminas yra ilgesnis, kad ją būtų galima pateikti nacionalinėms institucijoms. Atitikties deklaracijoje identifikuojamas produkto modelis, kuriam ji buvo parengta.

Atitikties deklaracijos kopija pateikiama atitinkamoms institucijoms jų prašymu.

6. Gamintojas ne trumpiau kaip 10 metų po produkto su skaitmeniniais elementais pateikimo rinkai dienos arba palaikymo laikotarpį, priklausomai nuo to, kuris terminas yra ilgesnis, saugo toliau nurodytus dokumentus, kad nacionalinės institucijos galėtų su jais susipažinti:

6.1. 3.1 punkte nurodytus techninius dokumentus;

6.2. dokumentus, susijusius su 3.1 punkte nurodyta kokybės sistema;

6.3. informaciją apie 3.5 punkte nurodytus patvirtintus pakeitimus;

6.4. notifikuotosios įstaigos sprendimus ir ataskaitas, nurodytas 3.5 ir 4.3 punktuose.

7. Kiekviena notifikuotoji įstaiga savo notifikuojančiąsias institucijas informuoja apie išduotus arba panaikintus kokybės sistemos patvirtinimus ir periodiškai arba gavusi prašymą notifikuojančiosioms institucijoms pateikia kokybės sistemos patvirtinimų, kuriuos išduoti ji atsisakė arba kurių galiojimą laikinai sustabdė ar kitaip apribojo, sąrašą.

Kiekviena notifikuotoji įstaiga kitas notifikuotąsias įstaigas informuoja apie kokybės sistemų patvirtinimus, kuriuos ji atsisakė išduoti, panaikino arba kurių galiojimą laikinai sustabdė, o gavusi prašymą – ir apie išduotus kokybės sistemų patvirtinimus.

8. Įgaliotasis atstovas

3.1, 3.5, 5 ir 6 punktuose nustatytas gamintojo pareigas jo vardu ir jo atsakomybe gali vykdyti jo įgaliotasis atstovas, jei atitinkamos pareigos nurodytos įgaliojime.

Dėl šio akto buvo padarytas pareiškimas; jį galima rasti [OL: prašom įrašyti OL C, XXX, 2024 XX XX, p. XX] ir šioje tinklapio nuorodoje [OL: prašom įrašyti tinklapio nuorodą į pareiškimą].