Europos Sąjungos
oficialusis leidinys

L 333

Leidimas
lietuvių kalba

Teisės aktai

65 metai

2022 m. gruodžio 27 d.

Turinys

[1] Tekstas svarbus EEE.

LT

I

(Įstatymo galią turintys teisės aktai)

REGLAMENTAI

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (ES) 2022/2554

2022 m. gruodžio 14 d.

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

(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 Centrinio Banko nuomonę ([1]),

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę ([2]),

laikydamiesi įprastos teisėkūros procedūros ([3]),

kadangi:

(1) skaitmeniniame amžiuje informacinėmis ir ryšių technologijomis (IRT) palaikomos sudėtingos sistemos, naudojamos kasdienei veiklai. Jos padeda veikti pagrindiniams mūsų ekonomikos sektoriams, įskaitant finansų sektorių, ir stiprina bendrosios rinkos veikimą. Didesnė skaitmenizacija ir daugiau tarpusavio sąsajų taip pat didina IRT riziką, todėl visa visuomenė ir konkrečiai finansų sistema, tampa labiau pažeidžiama kibernetinių grėsmių ar IRT sutrikimų atžvilgiu. Nors plačiai paplitęs IRT sistemų naudojimas ir didelė skaitmenizacija bei junglumas šiandien yra pagrindiniai Sąjungos finansų sektoriaus subjektų veiklos bruožai, jų skaitmeninio atsparumo klausimą vis dar reikia geriau spręsti ir integruoti į jų platesnes veiklos sistemas;

(2) per pastaruosius dešimtmečius IRT naudojimas įgijo esminį vaidmenį teikiant finansines paslaugas ir pasiekė tokį tašką, kad dabar yra ypatingai svarbus visų finansų sektoriaus subjektų įprastų kasdienių funkcijų vykdymui. Dabar skaitmenizacija apima, pavyzdžiui, mokėjimus – juos atliekant vis dažniau atsisakoma grynųjų pinigų ir popierinių metodų, kuriuos keičia naudojami skaitmeniniai sprendimai, taip pat vertybinių popierių tarpuskaitą ir atsiskaitymą, elektroninę ir algoritminę prekybą, skolinimo ir finansavimo operacijas, tarpusavio finansavimą, kredito reitingus, reikalavimų išmokėti draudimo išmoką administravimą ir netiesioginio aptarnavimo padalinio

([1]) OL C 343, 2021 8 26, p. 1.
([2]) OL C 155, 2021 4 30, p. 38.
([3]) 2022 m. lapkričio 10 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2022 m. lapkričio 28 d. Tarybos sprendimas.

operacijas. Draudimo sektoriuje dėl IRT technologijų taip pat įvyko transformacija, pradedant internetu savo paslaugas teikiančių draudimo tarpininkų, veikiančių naudojant „InsurTech“, atsiradimu, ir baigiant skaitmenine draudimo veikla. Finansų sektorius ne tik visas tapo iš esmės skaitmeninis, bet skaitmenizacija padidino tarpusavio sąsajas ir priklausomybę pačiame finansų sektoriuje ir sąsajas su infrastruktūrą ir paslaugas teikiančiomis trečiosiomis šalimis bei priklausomybę nuo jų;

(3) 2020 m. ataskaitoje dėl sisteminės kibernetinės rizikos Europos sisteminės rizikos valdyba (ESRV) dar kartą patvirtino, kad dabartinis didelis finansų sektoriaus subjektų, finansų rinkų ir finansų rinkų infrastruktūrų tarpusavio susietumas, ypač jų IRT sistemų tarpusavio priklausomybė, galėtų virsti sisteminiu pažeidžiamumu, nes vienoje vietoje kilę kibernetiniai incidentai, nevaržomi jokių geografinių ribų, iš bet kurio iš apytikriai 22 000 Sąjungos finansų sektoriaus subjektų galėtų greitai išplisti į visą finansų sistemą. Rimti IRT pažeidimai, kylantys finansų sektoriuje, daro poveikį ne tik finansų sektoriaus subjektams. Jie taip pat sudaro sąlygas vienoje vietoje atsiradusiems pažeidžiamumams plisti finansiniais perdavimo kanalais ir gali turėti neigiamų padarinių Sąjungos finansų sistemos stabilumui, pavyzdžiui, mažinti likvidumą ir apskritai pasikliovimą ir pasitikėjimą finansų rinkomis;

(4) pastaraisiais metais IRT rizika sulaukė tarptautinių, Sąjungos ir nacionalinių politikos formuotojų, reguliavimo institucijų ir standartus nustatančių įstaigų dėmesio, siekiant stiprinti skaitmeninį atsparumą, nustatyti standartus ir koordinuoti reguliavimo ar priežiūros darbą. Tarptautiniu lygmeniu Bazelio bankų priežiūros komitetas, Mokėjimo ir rinkos infrastruktūrų komitetas, Finansinio stabilumo taryba, Finansinio stabilumo institutas, taip pat G7 ir G20 siekia įvairių jurisdikciją turinčių subjektų kompetentingoms institucijoms ir rinkos operatoriams suteikti priemonių jų finansų sistemų atsparumui stiprinti. Tą darbą taip pat paskatino poreikis tinkamai vertinti IRT riziką glaudžiai tarpusavyje susijusios pasaulinės finansų sistemos kontekste ir siekti didesnio atitinkamos geriausios praktikos nuoseklumo;

(5) nepaisant Sąjungos ir nacionalinių tikslinių politikos ir teisėkūros iniciatyvų, IRT rizika ir toliau kelia sunkumų Sąjungos finansų sistemos veiklos atsparumui, efektyvumui ir stabilumui. Po 2008 m. finansų krizės vykdytomis reformomis visų pirma buvo didinamas Sąjungos finansų sektoriaus finansinis atsparumas ir siekta ekonominiu, prudenciniu ir elgesio rinkoje požiūriu apsaugoti Sąjungos konkurencingumą ir stabilumą. Nors IRT saugumas ir skaitmeninis atsparumas yra operacinės rizikos dalis, jiems po finansų krizės įgyvendinamoje reguliavimo darbotvarkėje teko mažiau dėmesio ir jie buvo plėtojami tik kai kuriose Sąjungos finansinių paslaugų politikos ir reglamentavimo aplinkos srityse arba tik keliose valstybėse narėse;

(6) Komisija savo 2018 m. kovo 8 d. komunikate „*FinTech*“ srities veiksmų planas: konkurencingesnis ir novatoriškesnis Europos finansų sektorius“ pabrėžė, kad itin svarbu, jog Sąjungos finansų sektorius taptų atsparesnis, be kita ko, veiklos požiūriu, kad būtų užtikrinta jo technologinė sauga ir geras veikimas, greitas veiklos atkūrimas po IRT pažeidimų ir incidentų, taip galiausiai sudarant sąlygas veiksmingai ir sklandžiai teikti finansines paslaugas visoje Sąjungoje, be kita ko, esant nepalankioms sąlygoms, kartu išsaugant vartotojų ir rinkos pasitikėjimą ir kliovimąsi;

(7) 2019 m. balandžio mėn. Europos Parlamento ir Tarybos reglamentu (ES) Nr. 1093/2010 ([4]) įsteigta Europos priežiūros institucija (Europos bankininkystės institucija) (EBI), Europos Parlamento ir Tarybos reglamentu (ES) Nr. 1094/2010 ([5]) įsteigta *Europos* priežiūros institucija (Europos draudimo ir profesinių pensijų institucija) (EIOPA)

([4]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1093/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos bankininkystės institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/78/EB (OL L 331, 2010 12 15, p. 12).

([5]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1094/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos draudimo ir profesinių pensijų institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/79/EB (OL L 331, 2010 12 15, p. 48).

ir Europos Parlamento ir Tarybos reglamentu (ES) Nr. 1095/2010 ([6]) įsteigta Europos priežiūros institucija (Europos vertybinių popierių ir rinkų institucija) (ESMA) (kartu vadinamos Europos priežiūros institucijomis arba EPI) kartu paskelbė technines rekomendacijas, kuriose paragino laikytis nuoseklaus požiūrio į IRT riziką finansų srityje ir rekomendavo proporcingai didinti finansinių paslaugų sektoriaus skaitmeninės veiklos atsparumą įgyvendinant Sąjungos konkrečiam sektoriui skirtą iniciatyvą;

(8) Sąjungos finansų sektorių reglamentuoja bendras taisyklių sąvadas ir reguliuoja Europos finansų priežiūros institucijų sistema. Vis dėlto su skaitmeninės veiklos atsparumu ir IRT saugumu susijusios nuostatos dar nėra visiškai arba nuosekliai suderintos, nors skaitmeninės veiklos atsparumas yra gyvybiškai svarbus norint užtikrinti finansinį stabilumą ir rinkos vientisumą skaitmeniniame amžiuje ir ne mažiau svarbus nei, pavyzdžiui, bendrieji prudenciniai ar elgesio rinkoje standartai. Todėl bendras taisyklių sąvadas ir priežiūros sistema turėtų būti plėtojami, kad apimtų ir skaitmeninės veiklos atsparumą, stiprinant kompetentingų institucijų įgaliojimus, kad joms būtų sudaromos sąlygos prižiūrėti IRT rizikos finansų sektoriuje valdymą, siekiant apsaugoti vidaus rinkos vientisumą ir efektyvumą bei sudaryti palankesnes sąlygas tvarkingam jos veikimui;

(9) dėl teisės aktų skirtumų ir nevienodų nacionalinių reguliavimo ar priežiūros metodų, susijusių su IRT rizika, atsiranda kliūčių finansinių paslaugų vidaus rinkos veikimui, o dėl jų tarpvalstybinę veiklą vykdantiems finansų sektoriaus subjektams trukdoma sklandžiai naudotis įsisteigimo ir paslaugų teikimo laisve. Taip pat galėtų būti iškraipoma tos pačios rūšies finansų sektoriaus subjektų, veikiančių skirtingose valstybėse narėse, konkurencija. Taip yra visų pirma tose srityse, kuriose Sąjungos vykdomo suderinimo mastas buvo labai nedidelis, pavyzdžiui, skaitmeninės veiklos atsparumo testavimo srityje, arba jo visai nebuvo, pavyzdžiui, trečiosios šalies keliamos IRT rizikos stebėsenos srityje. Dėl numatomų pokyčių nacionaliniu lygmeniu atsirandantys skirtumai galėtų sukelti papildomų kliūčių vidaus rinkos veikimui, o tai pakenktų rinkos dalyviams ir finansiniam stabilumui;

(10) iki šiol su IRT rizika susijusios nuostatos Sąjungos lygmeniu nustatytos tik iš dalies, todėl svarbiose srityse, pavyzdžiui, pranešimų apie su IRT susijusius incidentus ir skaitmeninės veiklos atsparumo testavimo srityse, esama spragų arba dubliavimosi, o dėl priimamų skirtingų nacionalinių taisyklių arba ekonomiškai neefektyvaus besidubliuojančių taisyklių taikymo atsiranda nenuoseklumų. Tai ypač kenkia tokiam intensyviam IRT naudotojui, koks yra finansų sektorius, nes technologijų rizika neturi sienų, o finansų sektoriaus paslaugos tarpvalstybiniu mastu plačiai teikiamos Sąjungoje ir už jos ribų. Atskiri finansų sektoriaus subjektai, veikiantys tarpvalstybiniu mastu arba turintys kelis veiklos leidimus (pvz., vienas finansų sektoriaus subjektas gali turėti bankininkystės, investicinės įmonės ir mokėjimo įstaigos licenciją, kurių kiekviena yra išduota vienos ar kelių valstybių narių skirtingų kompetentingų institucijų), susiduria su veiklos sunkumais norėdami savarankiškai ir nuosekliu ekonomiškai efektyviu būdu mažinti IRT riziką ir švelninti IRT incidentų neigiamą poveikį;

(11) kadangi bendras taisyklių sąvadas nebuvo papildytas išsamia IRT arba operacinės rizikos sistema, būtina toliau derinti pagrindinius skaitmeninės veiklos atsparumo reikalavimus, taikomus visiems finansų sektoriaus subjektams. Finansų subjektų IRT pajėgumų ir bendro atsparumo, besiremiančių tais pagrindiniais reikalavimais, kad nenukentėtų veiklos sutrikdymo atvejais, plėtra padėtų išsaugoti Sąjungos finansų rinkų stabilumą bei vientisumą ir tokiu būdu užtikrinti aukštą investuotojų ir vartotojų apsaugos lygį Sąjungoje. Kadangi šiuo reglamentu siekiama prisidėti prie sklandaus vidaus rinkos veikimo, jis turėtų būti grindžiamas Sutarties dėl Europos Sąjungos veikimo (SESV) 114 straipsnio nuostatomis, atsižvelgiant į jų aiškinimą pagal nusistovėjusią Europos Sąjungos Teisingumo Teismo (toliau – Teisingumo Teismas) jurisprudenciją;

(12) šiuo reglamentu siekiama konsoliduoti ir atnaujinti IRT rizikos reikalavimus, priklausančius operacinės rizikos reikalavimams, kurie iki šiol buvo atskirai aptariami skirtinguose Sąjungos teisės aktuose. Nors tuose aktuose buvo numatytos pagrindinės finansinės rizikos kategorijos (pvz., kredito rizika, rinkos rizika, sandorio šalies kredito rizika ir likvidumo rizika, elgesio rinkoje rizika), juos priimant nebuvo išsamiai atsižvelgta į visus veiklos atsparumo komponentus. Toliau plėtojant operacinės rizikos taisykles tuose Sąjungos teisės aktuose dažnai pirmenybė teikta tradiciniam kiekybiniam rizikos mažinimo metodui (t. y. nustatant kapitalo reikalavimus IRT rizikai padengti), o ne tikslinėms kokybinėms taisyklėms, skirtomis apsaugos nuo su IRT susijusių incidentų, jų aptikimo, izoliavimo,

([6]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1095/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos vertybinių popierių ir rinkų institucija) ir iš dalies keičiamas Sprendimas Nr. 716/2009/EB bei panaikinamas Komisijos sprendimas 2009/77/EB (OL L 331, 2010 12 15, p. 84).

veiklos atkūrimo ir ištaisymo pajėgumams arba pranešimų teikimo ir skaitmeninio testavimo pajėgumams. Tie aktai visų pirma buvo skirti esminėms prudencinės priežiūros, rinkos vientisumo ar elgesio taisyklėms nustatyti ir atnaujinti. Visos nuostatos, susijusios su skaitmenine rizika finansų sektoriuje, turėtų būti pirmą kartą nuosekliai išdėstytos viename teisėkūros procedūra priimame akte, taip konsoliduojant ir atnaujinant skirtingas su IRT rizika susijusias taisykles. Taigi šiuo reglamentu užpildomos kai kurių ankstesnių teisės aktų spragos arba pašalinamas jų nenuoseklumas, įskaitant juose vartojamą terminiją, o IRT rizika aiškiai įvardijama numatant tikslines IRT rizikos valdymo pajėgumų, pranešimų apie incidentus teikimo, veiklos atsparumo testavimo bei trečiosios šalies keliamos IRT rizikos stebėsenos taisykles. Todėl šiuo reglamentu taip pat turėtų būti didinamas informuotumas apie IRT riziką ir pripažįstama, kad IRT incidentai ir veiklos atsparumo stoka gali pakenkti finansų sektoriaus subjektų patikimumui;

(13) finansų sektoriaus subjektai, mažindami IRT riziką, turėtų laikytis to paties požiūrio ir tų pačių principais grindžiamų taisyklių, atsižvelgdami į savo dydį bei bendrą rizikos profilį ir į savo paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą. Nuoseklumas padeda didinti pasitikėjimą finansų sistema ir išsaugoti jos stabilumą, ypač esant didelei priklausomybei nuo IRT sistemų, platformų ir infrastruktūrų, dėl kurios kyla didesnė skaitmeninė rizika. Laikantis bazinės kibernetinės higienos taip pat turėtų būti išvengta didelių ekonomikai tenkančių išlaidų, nes būtų kuo labiau sumažintas IRT sutrikimų poveikis ir išlaidos;

(14) reglamentu padedama mažinti reglamentavimo sudėtingumą, skatinama priežiūros konvergencija ir didinamas teisinis tikrumas, taip pat prisidedama prie reikalavimų laikymosi išlaidų, visų pirma patiriamų tarpvalstybiniu mastu veikiančių finansų sektoriaus subjektų, apribojimo ir konkurencijos iškraipymo mažinimo. Todėl norint užtikrinti vienodą ir nuoseklų visų IRT rizikos valdymo komponentų taikymą Sąjungos finansų sektoriuje sukuriant bendrą finansų sektoriaus subjektų skaitmeninės veiklos atsparumo sistemą tinkamiausia priemonė yra reglamentas;

(15) Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 ([7]) buvo pirmoji Sąjungos lygmeniu priimta horizontalioji kibernetinio saugumo sistema, taip pat taikoma trijų rūšių finansų sektoriaus subjektams, t. y. kredito įstaigoms, prekybos vietoms ir pagrindinėms sandorio šalims. Tačiau, kadangi Direktyvoje (ES) 2016/1148 buvo nustatytas esminių paslaugų operatorių identifikavimo nacionaliniu lygmeniu mechanizmas, tik tam tikros kredito įstaigos, prekybos vietos ir pagrindinės sandorio šalys, kurios buvo nurodytos valstybių narių, praktiškai pateko į jos taikymo sritį, ir todėl turėjo laikytis joje nustatytų IRT saugumo ir panešimo apie incidentus reikalavimų. Europos Parlamento ir Tarybos direktyvoje (ES) 2022/2555 ([8]) nustatytas vienodas kriterijus, pagal kurį nustatoma, kurie subjektai patenka į jos taikymo sritį (dydžio ribojimo taisyklė), kartu jos taikymo srityje išlaikant visų trijų rūšių finansų sektoriaus subjektus;

(16) tačiau, kadangi nustatant reikalavimus, taikomus IRT rizikos valdymui ir pranešimų apie su IRT susijusius incidentus teikimui, kurie yra griežtesni, palyginti su nustatytaisiais galiojančiuose Sąjungos finansinių paslaugų teisės aktuose, šiuo reglamentu didinamas įvairių skaitmeninio atsparumo komponentų suderinimas, didinant šį suderinimo lygį kartu didinamas suderinimas ir palyginti su Direktyvoje (ES) 2022/2555 nustatytais reikalavimais. Todėl Direktyvos (ES) 2022/2555 atžvilgiu šis reglamentas yra *lex specialis*. Tuo pat metu labai svarbu išlaikyti tvirtą finansų sektoriaus ir Sąjungos horizontaliosios kibernetinio saugumo sistemos sąryšį, kaip tai šiuo metu nustatyta Direktyvoje (ES) 2022/2555, kad būtų užtikrintas nuoseklumas su valstybių narių priimamomis kibernetinio saugumo strategijomis, o finansų priežiūros institucijos galėtų būti informuotos apie kibernetinius incidentus, darančius poveikį kitiems sektoriams, kuriems taikoma ta direktyva;

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

([8]) 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) (žr. šio Oficialiojo leidinio p. 80).

(17) pagal Europos Sąjungos sutarties 4 straipsnio 2 dalį ir nedarant poveikio Teisingumo Teismo atliekamai teisminei peržiūrai, šiuo reglamentu neturėtų būti daromas poveikis valstybių narių atsakomybei, susijusiai su esminėmis valstybės funkcijomis visuomenės saugumo, gynybos ir nacionalinio saugumo užtikrinimo srityse pavyzdžiui, informacijos, kuri prieštarautų nacionalinio saugumo užtikrinimui, teikimo atveju;

(18) siekiant sudaryti sąlygas tarpsektoriniam mokymuisi ir veiksmingai pasinaudoti kitų sektorių patirtimi kovojant su kibernetinėmis grėsmėmis, Direktyvoje (ES) 2022/2555 nurodyti finansų sektoriaus subjektai turėtų likti tos direktyvos „ekosistemos“ (pavyzdžiui, bendradarbiavimo grupės ir reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT)) dalimi. EPI ir nacionalinėms kompetentingoms institucijoms turėtų būti suteikta galimybė dalyvauti strateginėse politikos diskusijose ir bendradarbiavimo grupės, įsteigtos pagal tą direktyvą, techniniame darbe bei keistis informacija ir toliau bendradarbiauti su bendraisiais informaciniais centrais, paskirtais arba įsteigtais pagal tą direktyvą. Pagal šį reglamentą kompetentingos institucijos taip pat turėtų konsultuotis ir bendradarbiauti su CSIRT. Kompetentingos institucijos taip pat turėti galimybę pagal Direktyvą (ES) 2022/2555 paskirtų ar įsteigtų kompetentingų institucijų prašyti techninių konsultacijų ir nustatyti bendradarbiavimo tvarką, kuria siekiama užtikrinti veiksmingus ir greitą reagavimą užtikrinančius koordinavimo mechanizmus;

(19) atsižvelgiant į tvirtas finansų sektoriaus subjektų skaitmeninio atsparumo ir fizinio atsparumo sąsajas, šiame reglamente ir Europos Parlamento ir Tarybos direktyvoje (ES) 2022/2557 ([9]) būtina laikytis nuoseklaus požiūrio į ypatingos svarbos subjektų atsparumą. Atsižvelgiant į tai, kad finansų sektoriaus subjektų fizinio atsparumo klausimai visapusiškai sprendžiami taikant IRT rizikos valdymo pareigas ir pareigas pranešti, kurioms taikomas šis reglamentas, Direktyvos (ES) 2022/2557 III ir IV skyriuose nustatytos pareigos neturėtų būti taikomos finansų sektoriaus subjektams, kurie patenka į tos direktyvos taikymo sritį;

(20) debesijos paslaugų teikėjai yra viena iš skaitmeninių infrastruktūrų kategorijų, kuriai taikoma Direktyva (ES) 2022/2555. Šiuo reglamentu nustatoma Sąjungos priežiūros sistema (priežiūros sistema) taikoma visoms ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, įskaitant debesijos paslaugų teikėjus, teikiančius IRT paslaugas finansų sektoriaus subjektams, ir laikytina papildančia pagal Direktyvą (ES) 2022/2555 vykdomą priežiūrą. Be to, kai nėra Sąjungos horizontaliosios sistemos, pagal kurią būtų įkurta skaitmeninės priežiūros institucija, šiuo reglamentu nustatoma priežiūros sistema turėtų būti taikoma debesijos paslaugų teikėjams;

(21) siekiant ir toliau visiškai kontroliuoti IRT riziką, finansų sektoriaus subjektai turi turėti visapusiškų pajėgumų, kurie jiems leistų vykdyti griežtą ir veiksmingą IRT rizikos valdymą, taip pat specialius mechanizmus ir politiką visiems su IRT susijusiems incidentams tvarkyti ir pranešimams apie didelius su IRT susijusius incidentus teikti. Analogiškai, finansų sektoriaus subjektai turėtų turėti IRT sistemų testavimo, kontrolės priemonių ir procesų, taip pat trečiosios šalies keliamos IRT rizikos valdymo politiką. Reikėtų didinti pradinį finansų sektoriaus subjektų skaitmeninės veiklos atsparumo lygį, kartu taip pat sudarant sąlygas proporcingai taikyti reikalavimus tam tikriems finansų sektoriaus subjektams, visų pirma labai mažoms įmonėms, taip pat finansų sektoriaus subjektams, kuriems taikoma supaprastinta IRT rizikos valdymo sistema. Siekiant sudaryti palankesnes sąlygas veiksmingai profesinių pensijų įstaigų priežiūrai, kuri būtų proporcinga ir atitiktų poreikį mažinti kompetentingoms institucijoms tenkančią administracinę naštą, nustatant tokiems finansų sektoriaus subjektams taikomą atitinkamą nacionalinę priežiūros tvarką turėtų būti atsižvelgiama į jų dydį ir bendrą rizikos profilį, taip pat į jų paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą, net kai viršijamos atitinkamos Europos Parlamento ir Tarybos direktyvos (ES) 2016/2341 ([10]) 5 straipsnyje nustatytos ribos. Visų pirma vykdant priežiūros veiklą daugiausia dėmesio turėtų būti skiriama poreikiui šalinti didelę riziką, susijusią su konkretaus subjekto IRT rizikos valdymu.

([9]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2557 dėl ypatingos svarbos subjektų atsparumo, kuria panaikinama Tarybos direktyva 2008/114/EB (žr. šio Oficialiojo leidinio p. 164).

([10]) 2016 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/2341 dėl profesinių pensijų įstaigų (PPĮ) veiklos ir priežiūros (OL L 354, 2016 12 23, p. 37).

Kompetentingos institucijos taip pat turėtų laikytis atsargaus, bet proporcingo požiūrio prižiūrėdamos profesinių pensijų įstaigas, kurios pagal Direktyvos (ES) 2016/2341 31 straipsnį didelę savo pagrindinės veiklos dalį, pavyzdžiui, turto valdymą, aktuarinius skaičiavimus, apskaitą ir duomenų valdymą, perduoda paslaugų teikėjams;

(22) nacionalinio lygmens pranešimų apie su IRT susijusius incidentus teikimo ribos ir taksonomijos gerokai skiriasi. Nors bendrus principus galima nustatyti Europos Sąjungos kibernetinio saugumo agentūrai (ENISA), įsteigtai Europos Parlamento ir Tarybos reglamentu (ES) 2019/881 ([11]), ir bendradarbiavimo grupei, įsteigtai pagal Direktyvą (ES) 2022/2555, atliekant atitinkamą darbą finansų sektoriaus subjektų atžvilgiu, likusiems finansų sektoriaus subjektams vis dar taikomi arba gali atsirasti skirtingi ribų nustatymo ir taksonomijų naudojimo metodai. Dėl tų skirtumų finansų sektoriaus subjektams taikoma daugybė reikalavimų, kurių jie turi laikytis, ypač tais atvejais, kai jie vykdo veiklą keliose valstybėse narėse ir yra finansų grupės dalis. Be to, tokie skirtumai gali trukdyti kurti papildomus vienodus arba centralizuotus Sąjungos mechanizmus, kuriais būtų paspartintas pranešimų teikimo procesas ir padedama kompetentingoms institucijoms greitai ir sklandžiai keistis informacija – tai yra itin svarbu mažinant IRT riziką didelio masto išpuolių, galinčių turėti sisteminių padarinių, atveju;

(23) siekiant sumažinti tam tikriems finansų sektoriaus subjektams tenkančią administracinę naštą ir galbūt besidubliuojančias pareigas pranešti, reikalavimas pranešti apie incidentus pagal Europos Parlamento ir Tarybos direktyvą (ES) 2015/2366 ([12]) turėtų būti nebetaikomas mokėjimo paslaugų teikėjams, kurie patenka į šio reglamento taikymo sritį. Todėl kredito įstaigos, elektroninių pinigų įstaigos, mokėjimo įstaigos ir informavimo apie sąskaitas paslaugų teikėjai, kaip nurodyta tos direktyvos 33 straipsnio 1 dalyje, nuo šio reglamento taikymo dienos apie visus su mokėjimu susijusius operacinius ar saugumo incidentus, apie kuriuos anksčiau buvo pranešama pagal tą direktyvą, turėtų pranešti pagal šį reglamentą, nepriklausomai nuo to, ar tokie incidentai yra susiję su IRT;

(24) tam, kad kompetentingos institucijos galėtų vykdyti priežiūros funkcijas susidarydamos visapusišką su IRT susijusių incidentų pobūdžio, dažnumo, dydžio ir poveikio vaizdą, ir tobulinti atitinkamų valdžios institucijų, įskaitant teisėsaugos institucijas ir pertvarkymo institucijas, keitimąsi informacija, šiuo reglamentu turėtų būti nustatyta patikima pranešimų apie su IRT susijusius incidentus teikimo tvarka, taip atitinkamais reikalavimais užpildant finansinių paslaugų teisės spragas, ir pašalinti dabar besidubliuojantys ir pasikartojantys reikalavimai, kad būtų sumažintos išlaidos. Labai svarbu suderinti pranešimų apie su IRT susijusius incidentus teikimo tvarką reikalaujant, kad visi finansų sektoriaus subjektai teiktų pranešimus savo kompetentingoms institucijoms naudodamiesi šiame reglamente nustatyta viena bendra racionalizuota sistema. Be to, EPI turėtų būti suteikti įgaliojimai patikslinti atitinkamus pranešimų apie su IRT susijusius incidentus teikimo sistemos elementus, pavyzdžiui, taksonomiją, terminus, duomenų rinkinius, šablonus ir taikomas ribas. Siekiant užtikrinti visišką nuoseklumą su Direktyva (ES) 2022/2555, finansų sektoriaus subjektams turėtų būti leidžiama savanoriškai pranešti atitinkamai kompetentingai institucijai apie dideles kibernetines grėsmes, kai jie mano, kad kibernetinė grėsmė yra aktuali finansų sistemai, paslaugų naudotojams ar klientams;

(25) tam tikruose finansų subsektoriuose buvo parengti skaitmeninės veiklos atsparumo testavimo reikalavimai, kuriuose nustatytos ne visada visiškai suderintos sistemos. Dėl to tarpvalstybiniai finansų sektoriaus subjektai gali patirti dvigubų išlaidų, o abipusis skaitmeninės veiklos atsparumo testavimo rezultatų pripažinimas tampa sudėtingas, o tai savo ruožtu gali skaidyti vidaus rinką;

([11]) 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).

([12]) 2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 dėl mokėjimo paslaugų vidaus rinkoje, kuria iš dalies keičiamos direktyvos 2002/65/EB, 2009/110/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 ir panaikinama Direktyva 2007/64/EB (OL L 337, 2015 12 23, p. 35).

(26) be to, tais atvejais, kai IRT testavimas neprivalomas, pažeidžiamumai neaptinkami, o finansų sektoriaus subjektas dėl to patiria IRT riziką ir galiausiai kyla didesnė rizika finansų sektoriaus stabilumui ir vientisumui. Be Sąjungos įsikišimo skaitmeninės veiklos atsparumo testavimas toliau būtų nenuoseklus ir trūktų IRT testavimo skirtinguose jurisdikciją turinčiuose subjektuose rezultatų tarpusavio pripažinimo sistemos. Be to, kadangi mažai tikėtina, kad kiti finansų subsektoriai galėtų priimti reikšmingo masto testavimo schemas, jie nepasinaudotų galima testavimo sistemų teikiama nauda, pavyzdžiui, nenustatytų IRT pažeidžiamumų ir rizikos ir netestuotų apsaugos pajėgumų bei veiklos tęstinumo, o visa tai padeda įgyti didesnį klientų, tiekėjų ir verslo partnerių pasitikėjimą. Siekiant pašalinti tą reikalavimų dubliavimąsi, skirtumus ir spragas, būtina nustatyti suderinto testavimo tvarkos taisykles, taip sudarant palankesnes sąlygas finansų sektoriaus subjektų, atitinkančių šiame reglamente nustatytus kriterijus, pažangaus testavimo rezultatų tarpusavio pripažinimui;

(27) finansų sektoriaus subjektų priklausomybę nuo IRT paslaugų iš dalies lemia jų poreikis prisitaikyti prie besiformuojančios konkurencinės skaitmeninės pasaulio ekonomikos, didinti savo veiklos efektyvumą ir tenkinti vartotojų paklausą. Pastaraisiais metais tokios priklausomybės pobūdis ir mastas nuolat kinta, todėl mažėja finansinio tarpininkavimo išlaidos, sudaromos sąlygos verslo plėtrai ir finansinės veiklos diegimo didinimui, kartu siūlant platų IRT priemonių spektrą sudėtingiems vidaus procesams valdyti;

(28) platų IRT paslaugų naudojimą liudija sudėtingi sutartimi įforminti susitarimai, kurių atveju finansų sektoriaus subjektai dažnai susiduria su sunkumais derybose dėl sutarties sąlygų, pritaikytų pagal prudencinius standartus ar kitus reguliavimo reikalavimus, kurie jiems taikomi, arba kitaip siekdami pasinaudoti konkrečiomis teisėmis, pavyzdžiui, prieigos arba audito teisėmis, net kai pastarosios yra įtvirtintos jų sutartimi įformintuose susitarimuose. Daugelyje tokių sutartimi įformintų susitarimų taip pat nenumatoma pakankamų apsaugos priemonių, sudarančių sąlygas vykdyti visapusišką subrangos procesų stebėseną, todėl finansų sektoriaus subjektas praranda galimybę įvertinti susijusią riziką. Be to, kadangi IRT paslaugas teikiančios trečiosios šalys dažnai teikia standartizuotas paslaugas skirtingų rūšių klientams, tokie sutartimi įforminti susitarimai ne visada yra tinkamai pritaikyti prie individualių ar konkrečių finansų sektoriaus dalyvių poreikių;

(29) nors Sąjungos finansinių paslaugų teisės aktai apima tam tikras bendras veiklos rangai taikomas taisykles, sutarties aspekto stebėsena nėra visiškai įtvirtinta Sąjungos teisės aktuose. Nesant aiškių ir specialiai sukurtų Sąjungos standartų, kurie būtų taikomi sutartimi įformintiems susitarimams, sudarytiems su IRT paslaugas teikiančiomis trečiosiomis šalimis, nėra visapusiškai sprendžiama išorinių IRT rizikos šaltinių problema. Todėl būtina nustatyti tam tikrus pagrindinius principus, kuriais finansų sektoriaus subjektai vadovautųsi valdydami trečiosios šalies keliamą IRT riziką; šie principai yra ypač svarbūs, kai finansų sektoriaus subjektai naudojasi IRT paslaugas teikiančių trečiųjų šalių paslaugomis palaikydami savo ypatingos svarbos arba svarbias funkcijas. Kartu su tais principais turėtų būti nustatytos pagrindinės sutartinės teisės, susijusios su keliais sutartimi įformintų susitarimų vykdymo ir nutraukimo elementais, siekiant nustatyti tam tikras minimalias apsaugos priemones, sustiprinančias finansų sektoriaus subjektų gebėjimą veiksmingai stebėti visą IRT riziką, kylančią paslaugas teikiančių trečiųjų šalių lygmeniu. Tie principai papildo veiklos rangai taikomus sektorinius teisės aktus;

(30) trečiosios šalies keliamos IRT rizikos ir priklausomybės nuo IRT paslaugas teikiančių trečiųjų šalių stebėsenos atžvilgiu šiandien akivaizdžiai trūksta tam tikro suderinimo ir konvergencijos. Nepaisant pastangų spręsti veiklos rangos klausimą, pavyzdžiui, 2019 m. EBI gairėse dėl veiklos rangos ir 2021 m. ESMA gairėse dėl užsakomųjų paslaugų perdavimo debesijos paslaugų teikėjams, platesnis kovos su sistemine rizika, kuri gali kilti dėl to, kad finansų sektorių aptarnauja ribotas ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių skaičius, klausimas Sąjungos teisėje nėra sprendžiamas pakankamu mastu. Sąjungos lygmens taisyklių trūkumą dar labiau apsunkina tai, kad nėra nacionalinių taisyklių dėl įgaliojimų ir priemonių, leidžiančių finansų priežiūros institucijoms gerai suprasti priklausomybę nuo IRT paslaugas teikiančių trečiųjų šalių ir tinkamai stebėti riziką, kylančią dėl priklausomybės nuo IRT paslaugas teikiančių trečiųjų šalių koncentracijos;

(31) atsižvelgiant į galimą sisteminę riziką, kylančią dėl populiarėjančios veiklos rangos ir IRT paslaugas teikiančių trečiųjų šalių koncentracijos, ir atkreipus dėmesį į tai, kad nepakanka nacionalinių mechanizmų, kurie finansų priežiūros institucijoms suteiktų tinkamų priemonių kiekybiškai ir kokybiškai įvertinti bei ištaisyti IRT rizikos, su kuria susiduria ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys, padarinius, būtina sukurti tinkamą priežiūros sistemą, sudarančią sąlygas nuolat stebėti IRT paslaugas teikiančių trečiųjų šalių, kurios yra ypatingos svarbos IRT paslaugas finansų sektoriaus subjektams teikiančios trečiosios šalys, veiklą, kartu užtikrinant, kad būtų išsaugotas kitų klientų, kurie nėra finansų sektoriaus subjektai, konfidencialumas ir saugumas. Nors IRT paslaugų teikimas grupės viduje yra susijęs su specifine rizika ir nauda, jis neturėtų būti automatiškai laikomas mažiau rizikingu nei finansų grupei nepriklausančių paslaugų teikėjų teikiamos IRT paslaugos, todėl jam turėtų būti taikoma ta pati reguliavimo sistema. Tačiau kai IRT paslaugos teikiamos toje pačioje finansų grupėje, finansų sektoriaus subjektai galėtų griežčiau kontroliuoti paslaugų grupės viduje teikėjus ir į tai reikėtų atsižvelgti atliekant bendrą rizikos vertinimą;

(32) kadangi IRT grėsmės tampa vis labiau painesnės ir sudėtingesnės, geros IRT rizikos aptikimo ir prevencijos priemonės labai priklauso nuo reguliaraus finansų sektoriaus subjektų keitimosi žvalgybos informacija apie grėsmes ir pažeidžiamumą. Dalijantis informacija padedama didinti informuotumą apie kibernetines grėsmes. Tai savo ruožtu stiprina finansų sektoriaus subjektų gebėjimą neleisti kibernetinėms grėsmėms virsti realiais su IRT susijusiais incidentais ir sudaro sąlygas finansų sektoriaus subjektams efektyviau suvaldyti su IRT susijusių incidentų poveikį ir greičiau atkurti veiklą. Nesant rekomendacijų Sąjungos lygmeniu, regis, keli veiksniai trukdo taip dalytis žvalgybos informacija, visų pirma neaiškumas dėl dalijimosi atitikties duomenų apsaugos, antimonopolinėms ir atsakomybės taisyklėms;

(33) be to, dėl abejonių, kuria informacija galima dalytis su kitais rinkos dalyviais arba ne priežiūros institucijomis (pavyzdžiui, analitiniais duomenimis su ENISA arba teisėsaugos tikslais su Europolu), naudinga informacija lieka nepateikta. Todėl dalijimosi informacija mastas ir kokybė šiuo metu tebėra riboti ir fragmentiški, o atitinkama informacija daugiausia keičiamasi vietos lygmeniu (vykdant nacionalines iniciatyvas) netaikant nuoseklių Sąjungos masto dalijimosi informacija schemų, pritaikytų integruotos finansų sistemos poreikiams. Todėl svarbu stiprinti tuos komunikacijos kanalus;

(34) finansų sektoriaus subjektai turėtų būti skatinami tarpusavyje keistis informacija ir žvalgybos informacija apie kibernetines grėsmes ir kolektyviai naudotis savo individualiomis žiniomis ir praktine patirtimi strateginiu, taktiniu ir veiklos lygmenimis, kad dalyvaudami dalijimosi informacija schemose sustiprintų savo gebėjimus tinkamai įvertinti, stebėti, reaguoti į kibernetines grėsmes ir apsisaugoti nuo jų. Todėl būtina sudaryti sąlygas, kad Sąjungos lygmeniu būtų rengiamos savanoriško dalijimosi informacija schemos, kurias taikant patikimoje aplinkoje finansų sektoriaus bendruomenei būtų padedama užkirsti kelią kibernetinėms grėsmėms ir kolektyviai į jas reaguoti, greitai apribojant IRT rizikos plitimą ir neleidžiant neigiamam poveikiui plisti finansiniais kanalais. Tie mechanizmai turėtų atitikti galiojančias Sąjungos konkurencijos teisės taisykles, nustatytas 2011 m. sausio 14 d. Komisijos komunikate „Sutarties dėl Europos Sąjungos veikimo 101 straipsnio taikymo horizontaliesiems bendradarbiavimo susitarimams gairės“, taip pat Sąjungos duomenų apsaugos taisykles, visų pirma Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 ([13]). Jie turėtų veikti remiantis vienu ar daugiau to reglamento 6 straipsnyje nustatytų teisinių pagrindų, pavyzdžiui, tvarkant asmens duomenis duomenų valdytojo arba trečiosios šalies teisėto intereso pagrindu, kaip nurodyta to reglamento 6 straipsnio 1 dalies f punkte, taip pat tvarkant asmens duomenis, būtinus duomenų valdytojui tenkančiai teisinei pareigai vykdyti, kai tai būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui, arba vykdant duomenų valdytojui pavestus oficialius įgaliojimus, kaip nurodyta atitinkamai to reglamento 6 straipsnio 1 dalies c ir e punktuose;

([13]) 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).

(35) siekiant išlaikyti viso finansų sektoriaus skaitmeninės veiklos aukšto lygio atsparumą ir kartu neatsilikti nuo technologijų raidos, šiuo reglamentu turėtų būti sprendžiama rizikos, kylančios dėl visų rūšių IRT paslaugų, problema. Tuo tikslu IRT paslaugų apibrėžtis šio reglamento tekste turėtų būti suprantama plačiai, įtraukiant skaitmenines ir duomenų paslaugas, nuolat teikiamas per IRT sistemas vienam ar keliems vidaus ar išorės naudotojams. Į tą apibrėžtį, pavyzdžiui, turėtų būti įtrauktos vadinamosios internetu teikiamos paslaugos, kurios patenka į elektroninių ryšių paslaugų kategoriją. Į ją neturėtų būti įtraukta tik ribota tradicinių analoginio telefono ryšio paslaugų, priskiriamų viešojo komutuojamo telefono tinklo paslaugoms, fiksuotojo ryšio paslaugoms, fiksuoto telefono ryšio tinklo paslaugoms arba fiksuotojo ryšio telefono paslaugoms, kategorija;

(36) nepaisant šiame reglamente numatytos plačios taikymo srities, skaitmeninės veiklos atsparumo taisyklės turėtų būti taikomos atsižvelgiant į didelius finansų sektoriaus subjektų dydžio ir bendro rizikos profilio skirtumus. Paprastai finansų sektoriaus subjektai, skirdami išteklius ir pajėgumus IRT rizikos valdymo sistemai įgyvendinti, turėtų tinkamai nustatyti su IRT susijusius poreikius atsižvelgdami į savo dydį ir bendrą rizikos profilį bei savo paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą, o kompetentingos institucijos turėtų toliau vertinti ir peržiūrėti tokio paskirstymo metodą;

(37) Direktyvos (ES) 2015/2366 33 straipsnio 1 dalyje nurodyti informavimo apie sąskaitas paslaugų teikėjai, atsižvelgiant į specifinį jų veiklos pobūdį ir dėl to kylančią riziką, yra aiškiai įtraukti į šio reglamento taikymo sritį. Be to, elektroninių pinigų įstaigos ir mokėjimo įstaigos, kurioms pagal Europos Parlamento ir Tarybos direktyvos 2009/110/EB ([14]) 9 straipsnio 1 dalį ir Direktyvos (ES) 2015/2366 32 straipsnio 1 dalį taikoma išimtis, patenka į šio reglamento taikymo sritį, net jei pagal Direktyvą 2009/110/EB joms nesuteiktas leidimas išleisti elektroninius pinigus arba jei pagal Direktyvą (ES) 2015/2366 joms nesuteiktas leidimas teikti ir vykdyti mokėjimo paslaugas. Tačiau į šio reglamento taikymo sritį nepatenka Europos Parlamento ir Tarybos direktyvos 2013/36/ES ([15]) 2 straipsnio 5 dalies 3 punkte nurodytos pašto žiro įstaigos. Mokėjimo įstaigų, kurioms taikoma išimtis pagal Direktyvą (ES) 2015/2366, elektroninių pinigų įstaigų, kurioms taikoma išimtis pagal Direktyvą 2009/110/EB, ir informavimo apie sąskaitas paslaugų teikėjų, nurodytų Direktyvos (ES) 2015/2366 33 straipsnio 1 dalyje, atveju kompetentinga institucija turėtų būti pagal Direktyvos (ES) 2015/2366 22 straipsnį paskirta kompetentinga institucija;

(38) kadangi didesni finansų sektoriaus subjektai gali turėti daugiau išteklių ir gali greitai panaudoti lėšas valdymo struktūroms kurti ir įvairioms įmonių strategijoms rengti, turėtų būti reikalaujama, kad sudėtingesnes valdymo priemones diegtų tik tie finansų sektoriaus subjektai, kurie nėra labai mažos įmonės, kaip tai suprantama šiame reglamente. Tokie subjektai yra geriau pasirengę visų pirma nustatyti specialius valdymo padalinius, skirtus susitarimams su IRT paslaugas teikiančiomis trečiosiomis šalimis prižiūrėti arba krizių valdymo klausimams spręsti, organizuoti IRT rizikos valdymą pagal trijų gynybos linijų modelį arba sukurti vidaus rizikos valdymo ir kontrolės modelį, ir pateikti savo IRT rizikos valdymo sistemą vidaus auditui;

(39) pagal atitinkamą konkretiems sektoriams taikomą Sąjungos teisę kai kurie finansų sektoriaus subjektai naudojasi išimtimis arba jiems taikoma labai negriežta reguliavimo sistema. Tokie finansų sektoriaus subjektai yra, be kita ko, alternatyvaus investavimo fondų valdytojai, nurodyti Europos Parlamento ir Tarybos direktyvos 2011/61/ES ([16]) 3 straipsnio 2 dalyje, draudimo ir perdraudimo įmonės, nurodytos Europos Parlamento ir Tarybos direktyvos 2009/138/EB ([17]) 4 straipsnyje, ir profesinių pensijų įstaigos, valdančios pensijų sistemas, kurios kartu turi ne

([14]) 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos direktyva 2009/110/EB dėl elektroninių pinigų įstaigų steigimosi, veiklos ir riziką ribojančios priežiūros, iš dalies keičianti Direktyvas 2005/60/EB ir 2006/48/EB ir panaikinanti Direktyvą 2000/46/EB (OL L 267, 2009 10 10, p. 7).

([15]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyva 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų priežiūros, kuria iš dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB (OL L 176, 2013 6 27, p. 338).

([16]) 2011 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2011/61/ES dėl alternatyvaus investavimo fondų valdytojų, kuria iš dalies keičiami direktyvos 2003/41/EB ir 2009/65/EB bei reglamentai (EB) Nr. 1060/2009 ir (ES) Nr. 1095/2010 (OL L 174, 2011 7 1, p. 1).

([17]) 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/138/EB dėl draudimo ir perdraudimo veiklos pradėjimo ir jos vykdymo (Mokumas II) (OL L 335, 2009 12 17, p. 1).

daugiau kaip 15 narių. Atsižvelgiant į tas išimtis, būtų neproporcinga įtraukti tokius finansų sektoriaus subjektus į šio reglamento taikymo sritį. Be to, šiame reglamente pripažįstami draudimo tarpininkavimo rinkos struktūros ypatumai, todėl draudimo tarpininkams, perdraudimo tarpininkams ir papildomos draudimo veiklos tarpininkams, atitinkantiems labai mažų įmonių arba mažųjų ar vidutinių įmonių kriterijus, šis reglamentas neturėtų būti taikomas;

(40) kadangi Direktyvos 2013/36/ES 2 straipsnio 5 dalies 4–23 punktuose nurodyti subjektai nepatenka į tos direktyvos taikymo sritį, valstybės narės turėtų turėti galimybę nuspręsti netaikyti šio reglamento tokiems subjektams, esantiems jų atitinkamose teritorijose;

(41) taip pat, siekiant suderinti šį reglamentą su Europos Parlamento ir Tarybos direktyvos 2014/65/ES ([18]) taikymo sritimi, taip pat tikslinga į šio reglamento taikymo sritį neįtraukti tos direktyvos 2 ir 3 straipsniuose nurodytų fizinių ir juridinių asmenų, kuriems leidžiama teikti investicines paslaugas netaikant reikalavimo gauti veiklos leidimą pagal Direktyvą 2014/65/ES. Tačiau pagal Direktyvos 2014/65/ES 2 straipsnį į tos direktyvos taikymo sritį taip pat nepatenka subjektai, kurie šio reglamento tikslais laikomi finansų sektoriaus subjektais, pavyzdžiui, centriniams vertybinių popierių depozitoriumams, kolektyvinio investavimo subjektams arba draudimo ir perdraudimo įmonėms. Tos direktyvos 2 ir 3 straipsniuose nurodytų asmenų ir subjektų neįtraukimas į šio reglamento taikymo sritį neturėtų apimti tų centrinių vertybinių popierių depozitoriumų, kolektyvinio investavimo subjektų arba draudimo ir perdraudimo įmonių;

(42) pagal konkretiems sektoriams taikomą Sąjungos teisę kai kuriems finansų sektoriaus subjektams dėl priežasčių, susijusių su jų dydžiu arba jų teikiamomis paslaugomis, taikomi mažiau griežti reikalavimai arba išimtys. Ta finansų sektoriaus subjektų kategorija apima mažas ir tarpusavio sąsajų neturinčias investicines įmones, mažas profesinių pensijų įstaigas, kurioms Direktyvos (ES) 2016/2341 5 straipsnyje nustatytomis sąlygomis atitinkama valstybė narė gali netaikyti tos direktyvos ir kurios valdo pensijų sistemas, kurios kartu turi ne daugiau kaip 100 narių, taip pat įstaigas, kurioms pagal Direktyvą 2013/36/ES taikoma išimtis. Todėl, laikantis proporcingumo principo ir siekiant išlaikyti konkretiems sektoriams taikomos Sąjungos teisės dvasią, taip pat tikslinga pagal šį reglamentą tiems finansų sektoriaus subjektams taikyti supaprastintą IRT rizikos valdymo sistemą. Techniniai reguliavimo standartai, kuriuos turi parengti EPI, neturėtų pakeisti tiems finansų sektoriaus subjektams taikomos IRT rizikos valdymo sistemos proporcingumo. Be to, laikantis proporcingumo principo, tikslinga Direktyvos (ES) 2015/2366 32 straipsnio 1 dalyje nurodytoms mokėjimo įstaigoms ir Direktyvos 2009/110/EB 9 straipsnyje nurodytoms elektroninių pinigų įstaigoms, kurioms taikoma išimtis pagal nacionalinės teisės aktus, kuriais perkelti tie Sąjungos teisės aktai, pagal šį reglamentą taip pat taikyti supaprastintą IRT rizikos valdymo sistemą, o mokėjimo įstaigos ir elektroninių pinigų įstaigos, kurioms netaikoma išimtis pagal atitinkamus nacionalinės teisės aktus, kuriais perkelti Sąjungos sektorinės teisės aktai, turėtų laikytis šiuo reglamentu nustatytos bendrosios sistemos;

(43) taip pat neturėtų būti reikalaujama, kad finansų sektoriaus subjektai, kurie laikomi labai mažomis įmonėmis arba kuriems pagal šį reglamentą taikoma supaprastinta IRT rizikos valdymo sistema, sukurtų pareigybę, skirtą susitarimų dėl IRT paslaugų naudojimo, sudarytų su IRT paslaugas teikiančiomis trečiosiomis šalimis, stebėsenai, arba paskirtų vyresniosios vadovybės narį atsakingu už kylančios susijusios rizikos priežiūrą ir atitinkamus dokumentus, priskirtų atsakomybę už IRT rizikos valdymą ir priežiūrą kontrolės padaliniui ir užtikrintų tinkamą to kontrolės padalinio nepriklausomumo lygį, kad būtų išvengta interesų konfliktų, bent kartą per metus dokumentais pagrįstų ir peržiūrėtų IRT rizikos valdymo sistemą, reguliariai pateiktų IRT rizikos valdymo sistemą vidaus auditui, atliktų išsamų vertinimą po svarbių jų tinklų ir informacinių sistemų infrastruktūrų bei procesų pakeitimų, reguliariai atliktų senųjų IRT sistemų rizikos analizę, IRT reagavimo ir veiklos atkūrimo planų įgyvendinimui taikytų nepriklausomas vidaus audito peržiūras, turėtų krizių valdymo padalinį, išplėstų veiklos tęstinumo ir reagavimo bei veiklos atkūrimo planų testavimą, kad galėtų nustatyti pirminės IRT infrastruktūros pakeitimo atsarginiais įrenginiais scenarijus, kompetentingų institucijų prašymu praneštų joms apie apskaičiuotas bendras metines išlaidas ir nuostolius, patirtus dėl didelių su IRT susijusių incidentų, turėtų atsarginius IRT pajėgumus, nacionalinėms kompetentingoms institucijoms praneštų apie įgyvendintus pakeitimus atlikus peržiūras po su IRT susijusių

([18]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/65/ES dėl finansinių priemonių rinkų, kuria iš dalies keičiamos Direktyva 2002/92/EB ir Direktyva 2011/61/ES (OL L 173, 2014 6 12, p. 349).

incidentų, nuolat stebėtų atitinkamus technologinius pokyčius, parengtų išsamią skaitmeninės veiklos atsparumo testavimo programą, kuri būtų neatsiejama šiame reglamente numatytos IRT rizikos valdymo sistemos dalis, arba priimtų ir reguliariai peržiūrėtų trečiosios šalies keliamos IRT rizikos strategiją. Be to, turėtų būti reikalaujama, kad labai mažos įmonės tik įvertintų poreikį turėti tokius atsarginius IRT pajėgumus pagal jų rizikos profilį. Labai mažoms įmonėms turėtų būti taikoma lankstesnė skaitmeninės veiklos atsparumo testavimo programų tvarka. Svarstydamos atliktinų bandymų rūšį ir dažnumą, jos turėtų tinkamai suderinti tikslą išlaikyti aukštą skaitmeninės veiklos atsparumą, turimus išteklius ir bendrą jų rizikos profilį. Labai mažoms įmonėms ir finansų sektoriaus subjektams, kuriems pagal šį reglamentą taikoma supaprastinta IRT rizikos valdymo sistema, neturėtų būti taikomas reikalavimas atlikti IRT priemonių, sistemų ir procesų pažangų testavimą taikant grėsmėmis grindžiamą skverbimosi testavimą (angl. TLPT), nes tokį testavimą atlikti turėtų būti reikalaujama tik finansų sektoriaus subjektų, atitinkančių šiame reglamente nustatytus kriterijus. Atsižvelgiant į ribotus labai mažų įmonių pajėgumus, jos turėtų galėti susitarti su IRT paslaugas teikiančia trečiąja šalimi dėl finansų sektoriaus subjekto prieigos, tikrinimo ir audito teisių perdavimo nepriklausomai trečiajai šaliai, kurią turi paskirti IRT paslaugas teikianti trečioji šalis, su sąlyga, kad finansų sektoriaus subjektas gali bet kuriuo metu prašyti atitinkamos nepriklausomos trečiosios šalies pateikti visą svarbią informaciją ir patikinimą apie IRT paslaugas teikiančios trečiosios šalies veiklos rezultatus;

(44) kadangi turėtų būti reikalaujama, kad grėsmėmis grindžiamą skverbimosi testavimą atliktų tik tie finansų sektoriaus subjektai, kurie atrinkti atlikti pažangų skaitmeninio atsparumo testavimą, tokiam testavimui atlikti reikalingi administraciniai procesai ir finansinės išlaidos turėtų tekti nedidelei finansų sektoriaus subjektų daliai;

(45) siekiant užtikrinti visišką finansų sektoriaus subjektų veiklos strategijų ir atliekamo IRT rizikos valdymo suderinimą ir bendrą nuoseklumą, turėtų būti reikalaujama, kad finansų sektoriaus subjektų valdymo organai išlaikytų pagrindinį ir aktyvų vaidmenį valdant ir pritaikant IRT rizikos valdymo sistemą ir bendrą skaitmeninės veiklos atsparumo strategiją. Požiūris, kurio turi laikytis valdymo organai, turėtų būti orientuotas ne tik į priemones, kuriomis užtikrinamas IRT sistemų atsparumas, bet apimti ir žmones bei procesus taikant politiką, kuria kiekviename įmonės lygmenyje būtų skatinamas geras visų darbuotojų informuotumas apie kibernetinę riziką ir puoselėjamas įsipareigojimas visais lygmenimis laikytis griežtos kibernetinės higienos. Bendrasis tokio visapusiško požiūrio principas turėtų būti visiška valdymo organo atsakomybė valdant finansų sektoriaus subjekto IRT riziką; be to, pagal šį principą valdymo organas turėtų įsipareigoti nuolat kontroliuoti IRT rizikos valdymo stebėseną;

(46) be to, visos ir visiškos valdymo organo atsakomybės už finansų sektoriaus subjekto IRT rizikos valdymą principas yra neatsiejamas nuo poreikio užtikrinti tokį finansų sektoriaus subjekto su IRT susijusių investicijų ir bendro biudžeto mastą, kuris sudarytų sąlygas tam finansų sektoriaus subjektui pasiekti aukštą skaitmeninės veiklos atsparumo lygį;

(47) šiuo reglamentu, paremtu atitinkama kibernetinės rizikos valdymo tarptautine, nacionaline ir sektoriaus geriausia praktika, gairėmis, rekomendacijomis ar metodais, skatinama vadovautis principų, padedančių sukurti bendrą IRT rizikos valdymo struktūrą, rinkiniu. Todėl, jei pagrindiniai pajėgumai, kuriuos įdiegia finansų sektoriaus subjektai, atitinka šiame reglamente nustatytų įvairių IRT rizikos valdymo funkcijų (nustatymo, apsaugos ir prevencijos, aptikimo, reagavimo ir veiklos atkūrimo, mokymosi ir tobulėjimo bei komunikacijos) poreikius, finansų sektoriaus subjektai turėtų išlaikyti galimybę naudoti kitokios struktūros ar kategorijos IRT rizikos valdymo modelius;

(48) kad neatsiliktų nuo kintančios kibernetinių grėsmių aplinkos, finansų sektoriaus subjektai turėtų turėti atnaujinamas IRT sistemas, kurios yra patikimos ir pajėgios ne tik užtikrinti jų paslaugoms reikalingų duomenų tvarkymą, bet ir užtikrinti pakankamą technologinį atsparumą, kad jie galėtų tinkamai tenkinti papildomus tvarkymo poreikius, atsirandančius nepalankiausiomis rinkos sąlygomis arba kitomis nepalankiomis aplinkybėmis;

(49) siekiant, kad finansų sektoriaus subjektai galėtų operatyviai ir greitai reaguoti į su IRT susijusius incidentus, ypač kibernetinius išpuolius, ribodami žalą ir teikdami pirmenybę veiklos atnaujinimui ir veiklos atkūrimo veiksmams laikydamiesi savo atsarginių kopijų politikos, būtina veiksminga veiklos tęstinumo politika ir veiklos atkūrimo planai. Tačiau toks veiklos atnaujinimas neturėtų kelti jokio pavojaus tinklų ir informacinių sistemų vientisumui ir saugumui arba duomenų prieinamumui, autentiškumui, vientisumui ar konfidencialumui;

(50) nors šiuo reglamentu finansų sektoriaus subjektams leidžiama lanksčiai nustatyti savo veiklos atkūrimo laiko ir veiklos atkūrimo taško tikslus ir tokiu būdu tokius tikslus nustatyti visapusiškai atsižvelgiant į atitinkamų funkcijų pobūdį ir ypatingą svarbą bei konkrečius veiklos poreikius, nustatant tokius tikslus juo taip pat turėtų būti reikalaujama atlikti galimo bendro poveikio rinkos efektyvumui vertinimą;

(51) kibernetinių išpuolių vykdytojai paprastai siekia gauti finansinės naudos tiesiogiai išpuolio vykdymo vietoje, todėl finansų sektoriaus subjektai gali patirti reikšmingų pasekmių. Siekiant neleisti, kad IRT sistemos prarastų vientisumą arba taptų neprieinamos ir taip išvengti duomenų saugumo pažeidimų ir žalos fizinei IRT infrastruktūrai, reikėtų gerokai patobulinti ir racionalizuoti finansų sektoriaus subjektų pranešimų apie didelius su IRT susijusius incidentus teikimo tvarką. Pranešimų apie su IRT susijusius incidentus teikimo tvarka turėtų būti suderinta nustatant reikalavimą visiems finansų sektoriaus subjektams teikti pranešimus tiesiogiai savo atitinkamoms kompetentingoms institucijoms. Kai finansų sektoriaus subjektą prižiūri daugiau nei viena nacionalinė kompetentinga institucija, valstybės narės turėtų paskirti vieną bendrą kompetentingą instituciją, kuriai būtų teikiami tokie pranešimai. Kredito įstaigos, klasifikuojamos kaip svarbios pagal Tarybos reglamento (ES) Nr. 1024/2013 ([19]) 6 straipsnio 4 dalį, turėtų teikti tokius pranešimus nacionalinėms kompetentingoms institucijoms, kurios vėliau turėtų perduoti tuos pranešimus Europos Centriniam Bankui (ECB);

(52) tiesioginis pranešimų teikimas suteiktų galimybę finansų priežiūros institucijoms nedelsiant susipažinti su informacija apie didelius su IRT susijusius incidentus. Finansų priežiūros institucijos savo ruožtu turėtų perduoti informaciją apie didelius su IRT susijusius incidentus ne finansų valdžios institucijoms (pavyzdžiui, kompetentingoms institucijoms ir bendriesiems informaciniams centrams, paskirtiems pagal Direktyvą (ES) 2022/2555, bendriesiems informaciniams centrams, nacionalinėms duomenų apsaugos institucijoms ir teisėsaugos institucijoms didelių su IRT susijusių nusikalstamo pobūdžio incidentų atveju), siekiant padidinti tokių institucijų informuotumą apie tokius incidentus, o CSIRT atveju – sudaryti palankesnes sąlygas skubiai teikti pagalbą, kuri prireikus gali būti teikiama finansų sektoriaus subjektams. Be to, valstybės narės turėtų galėti nuspręsti, kad finansų sektoriaus subjektai patys turėtų teikti tokią informaciją valdžios institucijoms, nepriklausančioms finansinių paslaugų sričiai. Tie informacijos srautai turėtų sudaryti sąlygas finansų sektoriaus subjektams greitai pasinaudoti bet kokia atitinkama technine informacija, konsultacijomis dėl taisomųjų priemonių ir tolesniais tokių institucijų veiksmais. Informacija apie didelius su IRT susijusius incidentus turėtų būti perduodama abipusiai: finansų priežiūros institucijos turėtų teikti visą būtiną grįžtamąją informaciją arba rekomendacijas finansų sektoriaus subjektui, o EPI turėtų dalytis su incidentu susijusiais anoniminiais duomenimis apie kibernetines grėsmes ir pažeidžiamumus, kad prisidėtų prie platesnio masto kolektyvinės apsaugos;

(53) nors turėtų būti reikalaujama, kad visi finansų sektoriaus subjektai teiktų pranešimus apie incidentus, nesitikima, kad tas reikalavimas jiems visiems turės tokį patį poveikį. Iš tiesų atitinkamos reikšmingumo ribos ir pranešimų teikimo terminai turėtų būti tinkamai pakoreguoti deleguotuosiuose aktuose, grindžiamuose techniniais reguliavimo standartais, kuriuos turi parengti EPI, kad jie būtų taikomi tik dideliems su IRT susijusiems incidentams. Be to, nustatant pareigos pranešti terminus reikėtų atsižvelgti į finansų sektoriaus subjektų ypatumus;

(54) šiuo reglamentu turėtų būti reikalaujama, kad kredito įstaigos, mokėjimo įstaigos, informavimo apie sąskaitas paslaugų teikėjai ir elektroninių pinigų įstaigos praneštų apie visus su mokėjimu susijusius operacinius ar saugumo incidentus, apie kuriuos anksčiau buvo pranešama pagal Direktyvą (ES) 2015/2366, nepriklausomai nuo incidento IRT pobūdžio;

([19]) 2013 m. spalio 15 d. Tarybos reglamentas (ES) Nr. 1024/2013, kuriuo Europos Centriniam Bankui pavedami specialūs uždaviniai, susiję su rizikos ribojimu pagrįstos kredito įstaigų priežiūros politika (OL L 287, 2013 10 29, p. 63).

(55) EPI turėtų būti pavesta įvertinti galimo pranešimų apie su IRT susijusius incidentus teikimo centralizavimo Sąjungos lygmeniu galimybę ir sąlygas. Tokį centralizavimą galėtų sudaryti vienas bendras pranešimų apie su IRT susijusius incidentus teikimo ES centras, kuris arba tiesiogiai gautų atitinkamus pranešimus ir automatiškai informuotų nacionalines kompetentingas institucijas, arba tiesiog centralizuotų nacionalinių kompetentingų institucijų perduodamus atitinkamus pranešimus ir taip atliktų koordinavimo vaidmenį. EPI turėtų būti pavesta, konsultuojantis su ECB ir ENISA, parengti bendrą ataskaitą, kurioje būtų nagrinėjama galimybė įsteigti vieną bendrą ES centrą;

(56) siekiant užtikrinti aukštą skaitmeninės veiklos atsparumo lygį ir laikantis tiek atitinkamų tarptautinių standartų (pvz., G7 pagrindinių grėsmėmis grindžiamo skverbimosi testavimo elementų), tiek Sąjungoje taikomų sistemų, pavyzdžiui TIBER-ES, finansų sektoriaus subjektai turėtų reguliariai testuoti savo IRT sistemų ir darbuotojų, turinčių su IRT susijusių pareigų, prevencinių, aptikimo, reagavimo ir veiklos atkūrimo pajėgumų veiksmingumą, kad atskleistų ir pašalintų galimus IRT pažeidžiamumus. Siekiant atsižvelgti į finansų sektoriaus subjektų kibernetinio saugumo parengties lygio skirtumus įvairiuose finansų subsektoriuose ir tarp jų, testavimas turėtų apimti įvairias priemones ir veiksmus, pradedant pagrindinių reikalavimų vertinimu (pvz., pažeidžiamumo vertinimu ir skenavimu, atvirojo kodo analize, tinklo saugumo vertinimu, spragų analize, fizinio saugumo peržiūromis, klausimynais ir skenavimo programinės įrangos sprendimais, kai įmanoma – pirminio kodo peržiūromis, scenarijais grindžiamais testais, suderinamumo testavimu, veiklos efektyvumo testavimu ar visapusiu testavimu) ir baigiant pažangesniu testavimu taikant TLPT. Tokio pažangesnio testavimo turėtų būti reikalaujama tik iš tų finansų sektoriaus subjektų, kurie IRT požiūriu yra pakankamai brandūs, kad galėtų juos tinkamai atlikti. Taigi finansų sektoriaus subjektams (pavyzdžiui, didelėms, sisteminės svarbos ir IRT požiūriu brandžioms kredito įstaigoms, vertybinių popierių biržoms, centriniams vertybinių popierių depozitoriumams ir pagrindinėms sandorio šalims), atitinkantiems šiame reglamente nustatytus kriterijus, šiuo reglamentu nustatyti skaitmeninės veiklos atsparumo testavimo reikalavimai turėtų būti griežtesni nei kitiems finansų sektoriaus subjektams. Kartu toks skaitmeninės veiklos atsparumo testavimas taikant TLPT turėtų būti aktualesnis pagrindinių finansinių paslaugų subsektoriuose veikiantiems ir sisteminį vaidmenį (pavyzdžiui, mokėjimų, bankininkystės ir tarpuskaitos bei atsiskaitymo) atliekantiems finansų sektoriaus subjektams, ir mažiau aktualus kitiems subsektoriams (pavyzdžiui, turto valdytojams ir kredito reitingų agentūroms).

(57) Finansų sektoriaus subjektai, dalyvaujantys tarpvalstybinėje veikloje ir besinaudojantys įsisteigimo laisve arba paslaugų teikimo laisve Sąjungoje, savo buveinės valstybėje narėje turėtų laikytis vieno pažangaus testavimo (t. y. TLPT testavimo) reikalavimų rinkinio, kuris turėtų apimti IRT infrastruktūras visuose jurisdikciją turinčiuose subjektuose, kuriuose tarpvalstybinė finansų grupė vykdo veiklą Sąjungoje, taip sudarant sąlygas tokioms tarpvalstybinėms finansų grupėms patirti susijusias IRT testavimo išlaidas tik viename jurisdikciją turinčiame subjekte;

(58) siekiant pasinaudoti tam tikrų kompetentingų institucijų jau įgyta patirtimi, visų pirma susijusia su TIBER-ES sistemos įgyvendinimu, šiuo reglamentu valstybėms narėms turėtų būti leidžiama nacionaliniu lygmeniu paskirti vieną bendrą valdžios instituciją, finansų sektoriuje atsakingą už visus TLPT klausimus, arba kompetentingas institucijas, kurios, jei tokios paskirtos institucijos nėra, perduotų su TLPT susijusias užduotis kitai nacionalinei finansų srities kompetentingai institucijai;

(59) kadangi pagal šį reglamentą nereikalaujama, kad finansų sektoriaus subjektai, atlikdami vieną grėsmėmis grindžiamą skverbimosi testą, aprėptų visas ypatingos svarbos arba svarbias funkcijas, finansų sektoriaus subjektai turėtų galėti laisvai nuspręsti, kurios ypatingos svarbos arba svarbios funkcijos ir kiek jų turėtų būti įtraukta į tokio testo aprėptį;

(60) bendras testavimas, kaip apibrėžta šiame reglamente, kai TLPT veikloje dalyvauja keli finansų sektoriaus subjektai ir dėl kurio IRT paslaugas teikianti trečioji šalis gali tiesiogiai sudaryti sutartimi įformintus susitarimus su išorės testuotoju, turėtų būti leidžiamas tik tuo atveju, jei pagrįstai manoma, kad IRT paslaugas teikiančios trečiosios šalies teikiamų paslaugų klientams, kurie yra subjektai, kuriems šis reglamentas netaikomas, kokybei ar saugumui arba su tokiomis paslaugomis susijusių duomenų konfidencialumui bus padarytas neigiamas poveikis. Bendram testavimui taip pat turėtų būti taikomos apsaugos priemonės (vieno paskirto finansų sektoriaus subjekto vadovavimas, dalyvaujančių finansų sektoriaus subjektų skaičiaus kalibravimas), siekiant užtikrinti griežtą testavimą dalyvaujantiems finansų sektoriaus subjektams, atitinkantį TLPT tikslus pagal šį reglamentą;

(61) siekiant pasinaudoti įmonės lygmeniu turimais vidaus ištekliais, šiuo reglamentu TLPT atlikti turėtų būti leidžiama pasitelkti vidaus testuotojus, jei gaunamas priežiūros institucijos patvirtinimas, nėra interesų konfliktų ir periodiškai vykdomas pasitelkiant vidaus ir išorės testuotojus (kas trečią testą), kartu taip pat reikalaujant, kad TLPT žvalgybos informacijos apie grėsmes teikėjas finansų sektoriaus subjekto atžvilgiu visada būtų išorės subjektas. Visa atsakomybė už TLPT vykdymą turėtų tekti finansų sektoriaus subjektui. Institucijų liudijimai turėtų būti teikiami tik abipusio pripažinimo tikslu ir neturėtų trukdyti imtis tolesnių veiksmų, kurių reikia siekiant mažinti finansų sektoriaus subjektui kylančią IRT riziką, taip pat jie neturėtų būti laikomi finansų sektoriaus subjekto IRT rizikos valdymo ir mažinimo pajėgumų priežiūros patvirtinimu;

(62) siekiant užtikrinti patikimą trečiosios šalies keliamos IRT rizikos stebėseną finansų sektoriuje, būtina nustatyti rinkinį principais grindžiamų taisyklių, kuriomis finansų sektoriaus subjektai galėtų vadovautis stebėdami riziką, kylančią dėl funkcijų, kurių vykdymas perduotas IRT paslaugas teikiančioms trečiosioms šalims, visų pirma ypatingos svarbos arba svarbias funkcijas palaikančių IRT paslaugų, atveju, taip pat apskritai dėl visos priklausomybės nuo IRT paslaugas teikiančių trečiųjų šalių;

(63) siekiant spręsti įvairių IRT rizikos šaltinių sudėtingumo klausimą, kartu atsižvelgiant į technologinių sprendimų, kuriais sudaromos sąlygos sklandžiai teikti finansines paslaugas, teikėjų gausą ir įvairovę, šis reglamentas turėtų būti taikomas įvairioms IRT paslaugas teikiančioms trečiosioms šalims, įskaitant debesijos paslaugų, programinės įrangos, duomenų analizės paslaugų teikėjus ir duomenų centrų paslaugų teikėjus. Be to, kadangi finansų sektoriaus subjektai turėtų veiksmingai ir nuosekliai nustatyti ir valdyti visų rūšių riziką, be kita ko, kai IRT paslaugos perkamos finansų grupėje, reikėtų paaiškinti, kad finansų grupei priklausančios įmonės, teikiančios IRT paslaugas daugiausia savo patronuojančiajai įmonei arba savo patronuojančiosios įmonės patronuojamosioms įmonėms ar filialams, taip pat finansų sektoriaus subjektai, teikiantys IRT paslaugas kitiems finansų sektoriaus subjektams, pagal šį reglamentą taip pat turėtų būti laikomi IRT paslaugas teikiančiomis trečiosiomis šalimis. Galiausiai, atsižvelgiant į besivystančią mokėjimo paslaugų rinką, kuri tampa vis labiau priklausoma nuo sudėtingų techninių sprendimų, ir atsižvelgiant į atsirandančias mokėjimo paslaugų ir su mokėjimais susijusių sprendimų rūšis, mokėjimo paslaugų ekosistemos dalyviai, užsiimantys mokėjimų vykdymo veikla arba valdantys mokėjimo infrastruktūras, pagal šį reglamentą taip pat turėtų būti laikomi IRT paslaugas teikiančiomis trečiosiomis šalimis, išskyrus centrinius bankus, kai jie valdo mokėjimų ar vertybinių popierių atsiskaitymų sistemas, ir valdžios institucijas, kai jos teikia su IRT susijusias paslaugas valstybės funkcijų atlikimo kontekste;

(64) finansų sektoriaus subjektas visada turėtų išlikti visiškai atsakingas už šiame reglamente nustatytų jo pareigų vykdymą. Finansų sektoriaus subjektai turėtų taikyti proporcingą požiūrį į rizikos, kylančios IRT paslaugas teikiančių trečiųjų šalių lygmeniu, stebėseną, tinkamai atsižvelgiant į jų su IRT susijusios priklausomybės pobūdį, mastą, sudėtingumą ir svarbumą, paslaugų, procesų ar funkcijų, kurioms taikomi sutartimi įforminti susitarimai, ypatingą svarbą ar svarbumą ir galiausiai atidžiai įvertinus bet kokį galimą poveikį finansinių paslaugų tęstinumui ir kokybei atitinkamai individualiu ir grupės lygmeniu;

(65) vykdant tokią stebėseną turėtų būti laikomasi strateginio požiūrio į trečiosios šalies keliamą IRT riziką, įformintą finansų sektoriaus subjekto valdymo organui priėmus specialią strategiją dėl trečiosios šalies keliamos IRT rizikos, grindžiamą nuolatine visos priklausomybės nuo IRT paslaugas teikiančių trečiųjų šalių patikra. Siekiant didinti priežiūros institucijų informuotumą apie priklausomybę nuo IRT paslaugas teikiančių trečiųjų šalių ir dar labiau prisidėti prie darbo šiuo reglamentu nustatytos priežiūros sistemos kontekste, turėtų būti reikalaujama, kad visi finansų sektoriaus subjektai tvarkytų informacijos apie visus sutartimi įformintus susitarimus dėl IRT paslaugas teikiančių trečiųjų šalių teikiamų IRT paslaugų naudojimo registrą. Finansų priežiūros institucijos turėtų galėti prašyti viso registro arba konkrečių jo dalių ir taip gauti esminės informacijos, kad galėtų geriau suprasti finansų sektoriaus subjektų priklausomybę nuo IRT;

(66) sutartimi įforminti susitarimai turėtų būti oficialiai sudaromi tik atlikus išsamią ikisutartinę analizę, visų pirma daugiausia dėmesio skiriant tokiems elementams, kaip numatoma IRT sutartimi palaikomų paslaugų ypatinga svarba ar svarbumas, būtini priežiūros institucijų patvirtinimai ar kitos sąlygos, galimai kylanti koncentracijos rizika, taip pat išsamaus patikrinimo taikymas atrenkant ir vertinant IRT paslaugas teikiančias trečiąsias šalis ir vertinant galimus interesų konfliktus. Su ypatingos svarbos arba svarbiomis funkcijomis susijusių sutartimi įformintų susitarimų atveju finansų sektoriaus subjektai turėtų atsižvelgti į tai, ar IRT paslaugas teikiančios trečiosios šalys taiko naujausius ir aukščiausius informacijos saugumo standartus. Sutartimi įformintų susitarimų nutraukimą galėtų lemti bent keletas aplinkybių, iš kurių būtų matyti trūkumai IRT paslaugas teikiančios trečiosios

šalies lygmeniu, visų pirma reikšmingi teisės aktų ar sutartinių sąlygų pažeidimai, aplinkybės, kurios atskleidžia galimą sutartimi įformintuose susitarimuose numatytų funkcijų vykdymo pasikeitimą, IRT paslaugas teikiančios trečiosios šalies trūkumų, susijusių su jos bendru IRT rizikos valdymu, įrodymai arba aplinkybės, rodančios, kad atitinkama kompetentinga institucija negali veiksmingai prižiūrėti finansų sektoriaus subjekto;

(67) siekiant spręsti IRT paslaugas teikiančių trečiųjų šalių koncentracijos rizikos sisteminio poveikio problemą, šiuo reglamentu skatinamas subalansuotas sprendimas, laikantis lankstaus ir laipsniško požiūrio į tokią koncentracijos riziką, nes bet kokių griežtų viršutinių ribų arba griežtų apribojimų nustatymas galėtų trukdyti vykdyti verslą ir varžyti laisvę sudaryti sutartis. Finansų sektoriaus subjektai turėtų nuodugniai įvertinti savo numatytus sutartimi įformintus susitarimus, kad nustatytų tokios rizikos atsiradimo tikimybę, be kita ko, atlikdami išsamią subrangos susitarimų analizę, visų pirma, kai jie sudaromi su trečiojoje valstybėje įsisteigusiomis IRT paslaugas teikiančiomis trečiosiomis šalimis. Šiame etape ir siekiant užtikrinti tinkamą pusiausvyrą tarp būtinybės išsaugoti laisvę sudaryti sutartis ir užtikrinti finansinį stabilumą, manoma, kad nustatyti taisykles dėl griežtų IRT paslaugas teikiančių trečiųjų šalių rizikos pozicijų viršutinių ribų ir apribojimų yra netikslinga. Priežiūros sistemos kontekste pagal šį reglamentą paskirta Atsakingoji priežiūros institucija ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių atžvilgiu turėtų skirti ypatingą dėmesį tam, kad visapusiškai perprastų tarpusavio priklausomybės mastą, nustatytų konkrečius atvejus, kai didelė ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių koncentracija Sąjungoje gali kelti grėsmę Sąjungos finansų sistemos stabilumui ir vientisumui ir palaikyti dialogą su ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis, kai tokia speciali rizika nustatoma;

(68) siekiant reguliariai vertinti ir stebėti IRT paslaugas teikiančios trečiosios šalies gebėjimą saugiai teikti paslaugas finansų sektoriaus subjektui nedarant neigiamo poveikio finansų sektoriaus subjekto skaitmeninės veiklos atsparumui, su IRT paslaugas teikiančiomis trečiosiomis šalimis reikėtų suderinti keletą pagrindinių sutartinių elementų. Toks derinimas turėtų apimti būtiniausias sritis, kurios yra ypač svarbios sudarant sąlygas finansų sektoriaus subjektui vykdyti visapusišką rizikos, kurią galėtų kelti IRT paslaugas teikianti trečioji šalis, stebėseną, atsižvelgiant į finansų sektoriaus subjekto poreikį užtikrinti savo skaitmeninį atsparumą, kadangi jis yra labai priklausomas nuo gautų IRT paslaugų stabilumo, funkcinių galimybių, prieinamumo ir saugumo;

(69) iš naujo derėdamiesi dėl sutartimi įformintų susitarimų, kad jie būtų suderinti su šio reglamento reikalavimais, finansų sektoriaus subjektai ir IRT paslaugas teikiančios trečiosios šalys turėtų užtikrinti, kad būtų taikomos šiame reglamente numatytos pagrindinės sutartinės nuostatos;

(70) šiame reglamente vartojamas terminas „ypatingos svarbos arba svarbi funkcija“ apima „ypatingos svarbos funkcijas“, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2014/59/ES ([20]) 2 straipsnio 1 dalies 35 punkte. Ypatingos svarbos funkcijų, kaip tai suprantama šiame reglamente, apibrėžtis atitinkamai apima funkcijas, kurios pagal Direktyvą 2014/59/ES laikomos esant ypatingos svarbos;

(71) nepaisant IRT paslaugomis palaikomos funkcijos ypatingos svarbos arba svarbumo, sutartimi įformintuose susitarimuose visų pirma turėtų būti nurodyti išsamūs funkcijų ir paslaugų, vietų, kuriose vykdomos tokios funkcijos ir kuriuose turi būti tvarkomi duomenys, aprašymai, taip pat nurodomi paslaugų lygio aprašymai. Kiti esminiai elementai, kuriais finansų sektoriaus subjektui sudaromos galimybės stebėti su IRT paslaugas teikiančia trečiąja šalimis susijusią riziką, yra: sutartinės nuostatos, kuriomis apibrėžiama, kaip IRT paslaugas teikianti trečioji šalis užtikrina asmens duomenų pasiekiamumą, prieinamumą, vientisumą, saugumą ir apsaugą; nuostatos, kuriose išdėstomos atitinkamos garantijos, kad būtų galima prieiti prie duomenų, juos atkurti ir grąžinti IRT paslaugas teikiančios trečiosios šalies nemokumo, pertvarkymo ar veiklos operacijų nutraukimo atveju; nuostatos, kuriomis reikalaujama, kad IRT incidentų, susijusių su suteiktomis paslaugomis, atveju IRT paslaugas teikianti trečioji šalis teiktų pagalbą be papildomo mokesčio arba už iš anksto nustatytą mokestį; nuostatos dėl IRT paslaugas teikiančios trečiosios šalies pareigos visapusiškai bendradarbiauti su finansų sektoriaus subjekto kompetentingomis

([20]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/59/ES, kuria nustatoma kredito įstaigų ir investicinių įmonių gaivinimo ir pertvarkymo sistema ir iš dalies keičiamos Tarybos direktyva 82/891/EEB, direktyvos 2001/24/EB, 2002/47/EB, 2004/25/EB, 2005/56/EB, 2007/36/EB, 2011/35/ES, 2012/30/ES bei 2013/36/ES ir Europos Parlamento ir Tarybos reglamentai (ES) Nr. 1093/2010 bei (ES) Nr. 648/2012 (OL L 173, 2014 6 12, p. 190).

institucijomis ir pertvarkymo institucijomis ir nuostatos dėl sutarties nutraukimo teisių ir susijusių minimalus įspėjimo apie sutartimi įformintų susitarimų nutraukimą terminų, atsižvelgiant į kompetentingų institucijų ir pertvarkymo institucijų lūkesčius;

(72) be tokių sutartinių nuostatų ir siekiant užtikrinti, kad finansų sektoriaus subjektai ir toliau visapusiškai kontroliuotų visus pokyčius, vykstančius trečiųjų šalių lygmeniu, kurie gali pakenkti jų IRT saugumui, sutartyse dėl IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, teikimo taip pat turėtų būti numatyta: išsamių paslaugų lygio aprašymų nurodymas, nurodant tikslius kiekybinius ir kokybinius veiklos rezultatų tikslinius rodiklius, kad būtų galima nepagrįstai nedelsiant imtis tinkamų taisomųjų veiksmų, kai sutarti paslaugų lygiai neužtikrinami; IRT paslaugas teikiančios trečiosios šalies atitinkami įspėjimo terminai ir pareigos pranešti, taikomi įvykus pokyčiams, kurie gali turėti reikšmingos įtakos IRT paslaugas teikiančios trečiosios šalies gebėjimui veiksmingai teikti savo atitinkamas IRT paslaugas; reikalavimas IRT paslaugas teikiančiai trečiajai šaliai įgyvendinti ir išbandyti nenumatytų veiklos atvejų planus ir taikyti IRT saugumo priemones ir politiką, sudarančias sąlygas saugiai teikti paslaugas, taip pat dalyvauti ir visapusiškai bendradarbiauti finansų sektoriaus subjektui atliekant TLPT;

(73) sutartyse dėl IRT paslaugų teikimo, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, taip pat turėtų būti nuostatos, kuriomis sudaromos sąlygos finansų sektoriaus subjekto arba paskirtos trečiosios šalies prieigos, patikrinimo ir audito teises, taip pat teisę daryti kopijas, laikyti ypač svarbiomis finansų sektoriaus subjektų nuolatinės IRT paslaugas teikiančios trečiosios šalies veiklos efektyvumo stebėsenos priemonėmis, kurios derinamos su visapusišku paslaugų teikėjo bendradarbiavimu atliekant patikrinimus. Analogiškai finansų sektoriaus subjekto kompetentinga institucija turėtų turėti teisę, pateikusi įspėjimą ir laikydamasi konfidencialios informacijos apsaugos principo, patikrinti ir audituoti IRT paslaugas teikiančią trečiąją šalį;

(74) tokiuose sutartimi įformintuose susitarimuose taip pat turėtų būti numatytos specialios pasitraukimo strategijos, pagal kurias visų pirma būtų galima nustatyti privalomus pereinamuosius laikotarpius, per kuriuos IRT paslaugas teikiančios trečiosios šalys turėtų toliau teikti atitinkamas paslaugas, kad sumažintų sutrikimų riziką finansų sektoriaus subjekto lygmeniu, ar leisti pastarajam veiksmingai pereiti prie kitų IRT paslaugas teikiančių trečiųjų šalių naudojimo arba pasinaudoti vietoje taikomais sprendimais, atitinkančiais teikiamos IRT paslaugos sudėtingumą. Be to, finansų sektoriaus subjektai, kuriems taikoma Direktyva 2014/59/ES, turėtų užtikrinti, kad atitinkamos sutartys dėl IRT paslaugų būtų patikimos ir visapusiškai užtikrinamas jų vykdymas tų finansų sektoriaus subjektų pertvarkymo atveju. Todėl, atsižvelgdami į pertvarkymo institucijų lūkesčius, tie finansų sektoriaus subjektai turėtų užtikrinti, kad atitinkamos sutartys dėl IRT paslaugų būtų atsparios pertvarkymui. Tol, kol tie finansų sektoriaus subjektai toliau vykdo savo mokėjimo prievoles, jie, be kitų reikalavimų, turėtų užtikrinti, kad atitinkamose sutartyse dėl IRT paslaugų būtų numatytos sąlygos nenutraukti, nesustabdyti ir nekeisti sutarties dėl restruktūrizavimo ar pertvarkymo priežasčių;

(75) be to, savanoriškas valdžios institucijų arba Sąjungos institucijų parengtų standartinių sutarčių sąlygų, visų pirma, Komisijos parengtų standartinių sutarčių sąlygų naudojimas debesijos paslaugoms gali suteikti daugiau pasitikėjimo finansų sektoriaus subjektams ir IRT paslaugas teikiančioms trečiosioms šalims, nes būtų suteikta daugiau teisinio tikrumo dėl finansų sektoriuje naudojamų debesijos paslaugų, visapusiškai atsižvelgiant į Sąjungos finansinių paslaugų teisės aktais nustatytus reikalavimus ir lūkesčius. Standartinių sutarčių sąlygų rengimas grindžiamas priemonėmis, jau numatytomis 2018 m. „Fintech“ srities veiksmų plane, kuriuo Komisija paskelbė apie ketinimą skatinti ir palengvinti standartinių sutarčių sąlygų dėl finansų sektoriaus subjektų debesijos paslaugų veiklos rangos parengimą, remiantis tarpsektorinių debesijos paslaugų suinteresuotųjų subjektų indėliu, kurį Komisija užtikrino bendradarbiaudama su finansų sektoriumi;

(76) siekiant skatinti priežiūros metodų, taikomų sprendžiant trečiosios šalies keliamos IRT rizikos finansų sektoriuje problemą, konvergenciją ir veiksmingumą, taip pat stiprinti finansų sektoriaus subjektų, kurie IRT paslaugoms, kuriomis remiamas paslaugų teikimas, teikti pasitelkia ypatingos svarbos IRT paslaugas teikiančias trečiąsias šalis, skaitmeninės veiklos atsparumą ir taip prisidėti prie Sąjungos finansų sistemos stabilumo ir bendrosios finansinių paslaugų rinkos vientisumo išsaugojimo, ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims turėtų būti taikoma Sąjungos priežiūros sistema. Nors priežiūros sistemos sukūrimas yra pagrįstas veiksmų Sąjungos

lygmeniu pridėtine verte ir atsižvelgiant į tai, kad teikiant finansines paslaugas naudojamos IRT paslaugos ir į pastarųjų ypatumus, kartu reikėtų priminti, kad šis sprendimas atrodo tinkamas tik šio reglamento, konkrečiai susijusio su skaitmeninės veiklos atsparumu finansų sektoriuje, kontekste. Tačiau tokia priežiūros sistema neturėtų būti laikoma nauju Sąjungos priežiūros modeliu finansinių paslaugų ir veiklos srityse;

(77) priežiūros sistema turėtų būti taikoma tik ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims. Todėl turėtų būti nustatytas pripažinimo mechanizmas, kurį taikant būtų atsižvelgiama į finansų sektoriaus priklausomybės nuo tokių IRT paslaugas teikiančių trečiųjų šalių mastą ir pobūdį. Tas mechanizmas turėtų apimti kiekybinius ir kokybinius kriterijus, pagal kuriuos būtų nustatomi ypatingos svarbos parametrai, kuriais remiantis būtų galima juos įtraukti į priežiūros sistemą. Siekiant užtikrinti to vertinimo tikslumą ir neatsižvelgiant į IRT paslaugas teikiančios trečiosios šalies organizacinę struktūrą, nustatant tokius kriterijus, kai IRT paslaugas teikianti trečioji šalis priklauso platesnei grupei, turėtų būti atsižvelgiama į visą IRT paslaugas teikiančios trečiosios šalies grupės struktūrą. Viena vertus, ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys, kurios nėra automatiškai pripažįstamos taikant pirmiau minėtus kriterijus, turėtų turėti galimybę savanoriškai dalyvauti priežiūros sistemoje, o, kita vertus, IRT paslaugas teikiančioms trečiosioms šalims, kurioms jau taikomos priežiūros mechanizmų sistemos, kuriomis siekiama padėti vykdyti SESV 127 straipsnio 2 dalyje nurodytus Europos centrinių bankų sistemos uždavinius, turėtų būti taikoma išimtis;

(78) analogiškai, finansų sektoriaus subjektams, teikiantiems IRT paslaugas kitiems finansų sektoriaus subjektams ir priklausantiems IRT paslaugas teikiančių trečiųjų šalių kategorijai pagal šį reglamentą, priežiūros sistema taip pat neturėtų būti taikoma, nes jiems jau taikomi priežiūros mechanizmai, nustatyti atitinkamuose Sąjungos finansinių paslaugų teisės aktuose. Kai taikytina, kompetentingos institucijos, vykdydamos priežiūros veiklą, turėtų atsižvelgti į IRT paslaugas teikiančių finansų sektoriaus subjektų keliamą IRT riziką finansų sektoriaus subjektams. Be to, atsižvelgiant į esamus rizikos stebėsenos mechanizmus grupės lygmeniu, ta pati išimtis turėtų būti nustatyta IRT paslaugas teikiančioms trečiosioms šalims, teikiančioms paslaugas daugiausia savo grupės subjektams. IRT paslaugas teikiančioms trečiosioms šalims, IRT paslaugas teikiančioms tik vienoje valstybėje narėje finansų sektoriaus subjektams, veikiantiems tik toje valstybėje narėje, pripažinimo mechanizmas taip pat neturėtų būti taikomas dėl jų ribotos veiklos ir tarpvalstybinio poveikio nedarymo;

(79) skaitmeninė transformacija finansinių paslaugų srityje lėmė precedento neturintį IRT paslaugų naudojimo ir priklausomybės nuo jų lygį. Kadangi tapo neįmanoma teikti finansinių paslaugų nenaudojant debesijos kompiuterijos paslaugų, programinės įrangos sprendimų ir su duomenimis susijusių paslaugų, Sąjungos finansų ekosistema tapo neatsiejamai priklausoma ir nuo tam tikrų IRT paslaugų teikėjų teikiamų IRT paslaugų. Kai kurie iš tų paslaugų teikėjų, novatorių kuriant ir taikant IRT grindžiamas technologijas, atlieka svarbų vaidmenį teikiant finansines paslaugas arba yra integruoti į finansinių paslaugų vertės grandinę. Todėl jie tapo ypatingos svarbos Sąjungos finansų sistemos stabilumui ir vientisumui užtikrinti. Tokia plačiai paplitusi priklausomybė nuo ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių teikiamų paslaugų ir įvairių rinkos dalyvių informacinių sistemų tarpusavio priklausomybė kelia tiesioginę ir potencialiai didelę riziką Sąjungos finansinių paslaugų sistemai ir finansinių paslaugų teikimo tęstinumui, jei ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys turėtų veiklos sutrikimų arba patirtų didelius kibernetinius incidentus. Kibernetiniai incidentai turi išskirtinį gebėjimą daugėti ir plisti visoje finansų sistemoje gerokai greičiau nei kitų rūšių rizika, stebima finansų sektoriuje, ir jie gali apimti ir kitus sektorius ir peržengti geografines ribas. Jie gali virsti sistemine krize, kai pasitikėjimas finansų sistema sumažėja dėl funkcijų, kuriomis palaikoma realioji ekonomika, sutrikdymo arba didelių finansinių nuostolių, kurie yra pasiekę tokį lygį, kurio finansų sistema negali atlaikyti, arba kai reikia diegti griežtas sukrėtimų absorbavimo priemones. Siekiant užkirsti kelią šiems scenarijams, kurie keltų pavojų Sąjungos finansiniam stabilumui ir vientisumui, labai svarbu užtikrinti priežiūros praktikos, susijusios su trečiosios šalies keliama IRT rizika finansų srityje, konvergenciją, visų pirma nustatant naujas taisykles, kuriomis būtų sudarytos sąlygos Sąjungai vykdyti ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūrą;

(80) priežiūros sistema iš esmės priklauso nuo Atsakingosios priežiūros institucijos ir ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies, teikiančios finansų sektoriaus subjektams paslaugas, darančias poveikį finansinių paslaugų teikimui, bendradarbiavimo. Sėkminga priežiūra grindžiama, *inter alia*, Atsakingosios priežiūros institucijos gebėjimu veiksmingai vykdyti stebėsenos misijas ir atlikti patikrinimus siekiant įvertinti ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių taikomas taisykles, kontrolės priemones ir procesus, taip pat įvertinti galimą bendrą jų veiklos poveikį finansiniam stabilumui ir finansų sistemos vientisumui. Taip pat labai svarbu, kad ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys vadovautųsi Atsakingosios priežiūros institucijos rekomendacijomis ir spręstų jai susirūpinimą keliančius klausimus. Nebendradarbiaujant ypatingos svarbos IRT paslaugas teikiančiajai trečiajai šaliai, teikiančiai paslaugas, darančias poveikį finansinių paslaugų teikimui, pavyzdžiui, atsisakant suteikti galimybę patekti į jos patalpas arba pateikti informaciją, Atsakingoji priežiūros institucija galiausiai netektų savo esminių priemonių vertinant trečiųjų šalių keliamą IRT riziką ir tai galėtų neigiamai paveikti finansų sistemos finansinį stabilumą ir vientisumą, taip pat būtina numatyti atitinkamą sankcijų taikymo tvarką;

(81) atsižvelgiant į tai, Atsakingosios priežiūros institucijos poreikiui skirti baudas, kad ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys būtų priverstos laikytis šiame reglamente nustatytų skaidrumo ir su prieiga susijusių pareigų, neturėtų būti keliamas pavojus dėl sunkumų, kylančių dėl tų baudų vykdymo užtikrinimo trečiosiose valstybėse įsisteigusių ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių atžvilgiu. Siekiant užtikrinti tokių sankcijų vykdymą ir sudaryti sąlygas greitai įdiegti procedūras, kuriomis užtikrinamos ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių teisės į gynybą pripažinimo mechanizmo ir rekomendacijų teikimo kontekste, turėtų būti reikalaujama, kad tos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys, teikiančios finansų sektoriaus subjektams paslaugas, darančias poveikį finansinių paslaugų teikimui, toliau vykdytų tinkamo masto veiklą Sąjungoje. Dėl priežiūros pobūdžio ir dėl to, kad kitose jurisdikcijose nėra panašių susitarimų, nėra tinkamų alternatyvių mechanizmų, kuriais būtų užtikrintas šis tikslas veiksmingai bendradarbiaujant su trečiųjų valstybių finansų priežiūros institucijomis, kiek tai susiję su sisteminių IRT paslaugas teikiančių trečiųjų šalių, kurios gali būti laikomos trečiosiose valstybėse įsisteigusiomis ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis, keliamos skaitmeninės veiklos rizikos poveikio stebėsena. Todėl trečiojoje valstybėje įsisteigusi IRT paslaugas teikianti trečioji šalis, kuri pagal šį reglamentą pripažinta esanti ypatingos svarbos, siekdama toliau teikti IRT paslaugas finansų srities subjektams Sąjungoje, per 12 mėnesių po tokio pripažinimo turėtų imtis visų reikiamų priemonių užtikrinti, kad ji įsisteigtų Sąjungoje, įsteigdama patronuojamąją įmonę, kaip apibrėžta įvairiuose Sąjungos teisės aktuose, visų pirma Europos Parlamento ir Tarybos direktyvoje 2013/34/ES ([21]);

(82) reikalavimas įsteigti patronuojamąją įmonę Sąjungoje neturėtų trukdyti ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai teikti IRT paslaugas ir susijusią techninę paramą pasitelkiant už Sąjungos ribų esančius įrenginius ir infrastruktūrą. Šiuo reglamentu nenustatoma duomenų vietos nustatymo pareiga, kadangi nereikalaujama, kad duomenys būtų saugomi ar tvarkomi Sąjungoje;

(83) ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys turėtų turėti galimybę teikti IRT paslaugas iš bet kurios pasaulio vietos, taigi nebūtinai ar ne tik Sąjungoje esančiose patalpose. Priežiūros veikla pirmiausia turėtų būti vykdoma Sąjungoje esančiose patalpose ir bendraujant su Sąjungoje esančiais subjektais, įskaitant patronuojamąsias įmones, kurias pagal šį reglamentą įsteigė ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys. Tačiau tokių veiksmų Sąjungoje gali nepakakti, kad Atsakingoji priežiūros institucija galėtų visapusiškai ir veiksmingai vykdyti savo pareigas pagal šį reglamentą. Todėl Atsakingoji priežiūros institucija taip pat turėtų galėti vykdyti savo atitinkamus priežiūros įgaliojimus trečiosiose valstybėse. Naudodamasi tais įgaliojimais trečiosiose valstybėse Atsakingoji priežiūros institucija turėtų galėti patikrinti įrenginius, pasitelkiant kuriuos IRT paslaugas arba techninės paramos paslaugas faktiškai teikia arba valdo ypatingos svarbos IRT paslaugas teikianti trečioji šalis, ir turėtų galėti susidaryti išsamų vaizdą, kaip valdoma ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies IRT rizika. Atsakingosios priežiūros institucijos, kaip Sąjungos agentūros, galimybė naudotis įgaliojimais už Sąjungos teritorijos ribų turėtų būti tinkamai apibrėžta nustatant atitinkamas sąlygas, visų pirma atitinkamos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies sutikimą. Be to, atitinkamos trečiosios valstybės institucijos turėtų būti informuotos apie Atsakingosios priežiūros institucijos veiklą jų teritorijoje ir jai neprieštarauti. Tačiau siekiant užtikrinti veiksmingą įgyvendinimą ir nedarant poveikio atitinkamai Sąjungos institucijų ir valstybių narių kompetencijai, tokie įgaliojimai taip pat turi būti visapusiškai įtvirtinti sudarant administracinio bendradarbiavimo

([21]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyva 2013/34/ES dėl tam tikrų rūšių įmonių metinių finansinių ataskaitų, konsoliduotųjų finansinių ataskaitų ir susijusių pranešimų, kuria iš dalies keičiama Europos Parlamento ir Tarybos direktyva 2006/43/EB ir panaikinamos Tarybos direktyvos 78/660/EEB ir 83/349/EEB (OL L 182, 2013 6 29, p. 19).

susitarimus su atitinkamomis atitinkamos trečiosios valstybės institucijomis. Todėl šiuo reglamentu EPI turėtų būti suteikta galimybė sudaryti administracinio bendradarbiavimo susitarimus su atitinkamomis trečiųjų valstybių institucijomis, kurie neturėtų sukurti kitų teisinių pareigų Sąjungai ir jos valstybėms narėms;

(84) siekdamos palengvinti komunikaciją su Atsakingąja priežiūros institucija ir užtikrinti tinkamą atstovavimą, grupei priklausančios ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys savo koordinavimo punktu turėtų paskirti vieną juridinį asmenį;

(85) priežiūros sistema neturėtų būti daromas poveikis valstybių narių kompetencijai vykdyti nacionalinę IRT paslaugas teikiančių trečiųjų šalių, kurios nėra pripažintos esančios ypatingos svarbos pagal šį reglamentą, tačiau kurios galėtų būti laikomos svarbiomis nacionaliniu lygmeniu, priežiūrą arba stebėseną;

(86) siekiant pasinaudoti daugiasluoksne institucine struktūra finansinių paslaugų srityje, EPI jungtinis komitetas pagal savo užduotis kibernetinio saugumo srityje turėtų toliau užtikrinti bendrą tarpsektorinį koordinavimą visais su IRT rizika susijusiais klausimais. Jam turėtų padėti naujas pakomitetis (toliau – Priežiūros forumas), atliksiantis parengiamąjį darbą, susijusį tiek su atskirais sprendimais, skirtais ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, tiek su kolektyvinių rekomendacijų teikimu, visų pirma dėl ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūros programų lyginamosios analizės, ir nustatysiantis geriausią praktiką sprendžiant IRT koncentracijos rizikos klausimus;

(87) siekiant užtikrinti, kad ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys būtų tinkamai ir veiksmingai prižiūrimos Sąjungos lygmeniu, šiame reglamente nustatoma, kad bet kuri iš trijų EPI galėtų būti paskirta Atsakingąja priežiūros institucija. Ypatingos svarbos IRT paslaugas teikianti trečioji šalis vienai iš trijų EPI turėtų būti priskiriama įvertinus finansų sektoriaus subjektų, veikiančių finansų sektoriuose, už kuriuos ta EPI atsakinga, dominavimą. Toks požiūris turėtų padėti subalansuotai paskirstyti užduotis ir atsakomybę tarp trijų EPI priežiūros funkcijų vykdymo kontekste ir jį taikant turėtų būti kuo geriau pasinaudojama kiekvienos iš trijų EPI turimais žmogiškaisiais ištekliais ir techninėmis ekspertinėmis žiniomis;

(88) Atsakingosioms priežiūros institucijoms turėtų būti suteikti reikiami įgaliojimai atlikti ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių tyrimus, patikrinimus vietoje ir ne vietoje, patekti į tų trečiųjų šalių patalpas ir vietas bei gauti išsamią ir atnaujintą informaciją. Tie įgaliojimai turėtų sudaryti sąlygas Atsakingajai priežiūros institucijai realiai įvertinti finansų sektoriaus subjektams ir galiausiai Sąjungos finansų sistemai trečiosios šalies keliamos IRT rizikos rūšį, mastą ir poveikį. Pagrindinės priežiūros vaidmens pavedimas EPI yra būtina sąlyga norint suprasti ir mažinti sisteminę IRT riziką finansų sektoriuje. Dėl ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių poveikio Sąjungos finansiniam sektoriui ir galimų problemų, kurias kelia susijusi IRT koncentracijos rizika, reikia taikyti kolektyvinį požiūrį Sąjungos lygmeniu. Jeigu daug kompetentingų institucijų vienu metu atliktų daug atskirų auditų ir naudotųsi prieigos teisėmis, menkai koordinuodamos arba visai nekoordinuodamos savo darbo, finansų priežiūros institucijos negalėtų susidaryti išsamaus ir visa apimančio trečiosios šalies keliamos IRT rizikos Sąjungoje vaizdo, o ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, jei jos gautų daug stebėsenos ir patikrinimo prašymų, taip pat tektų perteklinis darbas, našta ir kiltų painiava;

(89) atsižvelgiant į didelį pripažinimo esant ypatingos svarbos IRT paslaugas teikiančia trečiąja šalimi poveikį, šiuo reglamentu turėtų būti užtikrinta, kad įgyvendinant priežiūros sistemą būtų laikomasi tokių paslaugų teikėjų teisių. Prieš paslaugų teikėjus pripažįstant esant ypatingos svarbos, tokie teikėjai turėtų, pavyzdžiui, turėti teisę Atsakingajai priežiūros institucijai pateikti pagrįstą pareiškimą, kuriame būtų pateikta visa svarbi informacija, reikalinga su jų pripažinimu susijusiam vertinimui atlikti. Kadangi Atsakingoji priežiūros institucija turėtų turėti įgaliojimus teikti rekomendacijas IRT rizikos ir tinkamų taisomųjų priemonių klausimais, kurie, be kita ko, apimą teisę pareikšti prieštaravimą tam tikriems sutartimi įformintiems susitarimams, kurie galiausiai daro poveikį finansų sektoriaus subjekto arba finansų sistemos stabilumui, ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims turėtų būti suteikta galimybė prieš patvirtinant galutinę tų rekomendacijų redakciją pateikti paaiškinimus dėl rekomendacijoje numatytų sprendimų tikėtino poveikio klientams, kurie yra subjektai, nepatenkantys į šio

reglamento taikymo sritį, ir suformuluoti rizikos mažinimo sprendimus. Ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, kurios nesutinka su rekomendacijomis, taip pat turėtų būti suteikta galimybė pateikti pagrįstą paaiškinimą, kodėl jos ketina nepritarti rekomendacijai. Jei toks pagrįstas paaiškinimas nepateikiamas arba jei jis laikomas nepakankamu, Atsakingoji priežiūros institucija turėtų paskelbti viešą pranešimą, kuriame trumpai apibūdinamas rekomendacijos nesilaikymo klausimas;

(90) kompetentingos institucijos, vykdydamos savo funkcijas, susijusias su finansų sektoriaus subjektų prudencine priežiūra, turėtų tinkamai įtraukti užduotį patikrinti, ar iš esmės laikomasi Atsakingosios priežiūros institucijos pateiktų rekomendacijų. Kompetentingos institucijos turėtų turėti galimybę reikalauti, kad finansų sektoriaus subjektai imtųsi papildomų priemonių, kad pašalintų riziką, nustatytą Atsakingosios priežiūros institucijos rekomendacijose, ir turėtų tinkamu laiku pateikti atitinkamus pranešimus. Kai Atsakingoji priežiūros institucija teikia rekomendacijas ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, kurios prižiūrimos pagal Direktyvą (ES) 2022/2555, kompetentingos institucijos, prieš priimdamos papildomas priemones, turėtų galėti savanoriškai konsultuotis su kompetentingomis institucijomis pagal tą direktyvą, kad būtų skatinamas koordinuotas požiūris tvarkant reikalus su atitinkamomis ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis;

(91) vykdant priežiūrą turėtų būti vadovaujamasi trimis veiklos principais, kuriais siekiama užtikrinti: a) glaudų EPI, vykdančių Atsakingosios priežiūros institucijos funkcijas, veiklos koordinavimą pasitelkiant jungtinį priežiūros tinklą (JPT), b) suderinamumą su Direktyva (ES) 2022/2555 nustatyta sistema (savanoriškai konsultuojantis su institucijomis pagal tą direktyvą, kad būtų išvengta priemonių, skirtų ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, dubliavimo) ir c) tikrinimą, kad būtų kuo labiau sumažinta galima ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių klientams, kurie yra subjektai, nepatenkantys į šio reglamento taikymo sritį, teikiamų paslaugų sutrikimo rizika;

(92) priežiūros sistema neturėtų būti pakeičiamas arba jokiu būdu ar jokia dalimi keičiamas finansų sektoriaus subjektams taikomas reikalavimas patiems valdyti riziką, kylančią naudojantis IRT paslaugas teikiančiomis trečiosiomis šalimis, įskaitant jų pareigą užtikrinti sutartimi įformintų susitarimų, sudarytų su ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis, nuolatinę stebėseną. Priežiūros sistema taip pat neturėtų būti daromas poveikis visai finansų sektoriaus subjektų atsakomybei laikytis visų šiame reglamente ir atitinkamuose finansinių paslaugų teisės aktuose nustatytų pareigų ir jas vykdyti;

(93) siekiant išvengti pasikartojančio ir besidubliuojančio darbo, kompetentingos institucijos neturėtų savarankiškai taikyti jokių priemonių, skirtų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių rizikai stebėti ir tuo atžvilgiu turėti pasikliauti atitinkamos Atsakingosios priežiūros institucijos vertinimu. Visas priemones bet kuriuo atveju reikėtų iš anksto koordinuoti ir suderinti su Atsakingąja priežiūros institucija vykdant užduotis pagal priežiūros sistemą;

(94) siekiant tarptautiniu lygmeniu skatinti konvergenciją, susijusią su geriausios praktikos naudojimu tikrinant ir stebint IRT paslaugas teikiančių trečiųjų šalių skaitmeninį rizikos valdymą, EPI turėtų būti skatinamos sudaryti bendradarbiavimo susitarimus su atitinkamomis trečiųjų valstybių priežiūros ir reguliavimo institucijomis;

(95) siekiant pasinaudoti kompetentingų institucijų, visų trijų EPA ir, savanoriškumo pagrindu, kompetentingų institucijų pagal Direktyvą ES 2022/2555 darbuotojų, besispecializuojančių operacinės ir IRT rizikos valdymo srityje, specialia kompetencija, techniniais gebėjimais ir ekspertinėmis žiniomis, Atsakingoji priežiūros institucija turėtų remtis nacionaliniais priežiūros pajėgumais bei žiniomis ir sukurti specialias kiekvienai ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai skirtas tyrimo grupes, jose suburdama įvairių sričių specialistus, kurie padėtų rengti ir vykdyti priežiūros veiklą, įskaitant ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių bendruosius tyrimus ir patikrinimus, ir imtųsi reikiamų tolesnių veiksmų;

(96) nors išlaidos, susijusios su priežiūros užduotimis, būtų visiškai finansuojamos iš mokesčių, renkamų iš ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių, vis dėlto tikėtina, kad EPI, prieš pradėdamos taikyti priežiūros sistemą, patirs išlaidų, susijusių su specialių, būsimą priežiūrą palaikančių IRT sistemų diegimu, nes specialias IRT sistemas reikės sukurti ir įdiegti iš anksto. Todėl šiame reglamente numatytas mišraus finansavimo modelis, pagal kurį priežiūros sistema būtų visiškai finansuojama iš mokesčių, o EPI IRT sistemų kūrimas būtų finansuojamas iš Sąjungos ir nacionalinių kompetentingų institucijų įnašų;

(97) kompetentingos institucijos turėtų turėti visus reikiamus priežiūros, tyrimo ir sankcijų taikymo įgaliojimus, kad užtikrintų tinkamą savo pareigų pagal šį reglamentą vykdymą. Iš esmės jos turėtų skelbti pranešimus apie jų skiriamas administracines nuobaudas. Kadangi finansų sektoriaus subjektai ir IRT paslaugas teikiančios trečiosios šalys gali būti įsisteigę skirtingose valstybėse narėse ir prižiūrimi skirtingų kompetentingų institucijų, šio reglamento taikymą turėtų palengvinti, viena vertus, glaudus atitinkamų kompetentingų institucijų, įskaitant ECB (kai tai susiję su Tarybos reglamentu (ES) Nr. 1024/2013 jam pavestais specialiais uždaviniais), bendradarbiavimas ir, kita vertus, konsultavimasis su EPI, tarpusavyje keičiantis informacija ir teikiant pagalbą, susijusią su atitinkama priežiūros veikla;

(98) siekiant toliau kiekybiškai ir kokybiškai įvertinti IRT paslaugas teikiančių trečiųjų šalių pripažinimo esant ypatingos svarbos kriterijus ir suderinti priežiūros mokesčius, Komisijai pagal Sutarties dėl Europos Sąjungos veikimo 290 straipsnį turėtų būti suteikti įgaliojimai priimti aktus, kuriais patikslinamas sisteminis poveikis, kurį IRT paslaugas teikiančios trečiosios šalies žlugimas arba veiklos sutrikdymas galėtų turėti finansų sektoriaus subjektams, kuriems ji teikia IRT paslaugas, pasaulinės sisteminės svarbos įstaigų (G-SII) ar kitų sisteminės svarbos įstaigų (O-SII), kurios yra priklausomos nuo atitinkamos IRT paslaugas teikiančios trečiosios šalies, skaičius, konkrečioje rinkoje veiklą vykdančių IRT paslaugas teikiančių trečiųjų šalių skaičius, duomenų ir darbo krūvio perkėlimo kitoms IRT paslaugas teikiančioms trečiosioms šalims išlaidos, taip pat priežiūros mokesčių suma ir jų mokėjimo būdas. 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 ([22]) 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;

(99) techniniais reguliavimo standartais turėtų būti užtikrintas nuoseklus šiame reglamente nustatytų reikalavimų suderinimas. EPI, kaip itin specializuotos praktinės patirties turinčios įstaigos, turėtų būti įgaliotos parengti ir Komisijai pateikti techninių reguliavimo standartų, kurie nėra susiję su sprendimais dėl politikos, projektus. Techniniai reguliavimo standartai turėtų būti rengiami IRT rizikos valdymo, pranešimo apie didelius su IRT susijusius incidentus, testavimo, taip pat pagrindinių trečiosios šalies keliamos IRT rizikos patikimos stebėsenos reikalavimų srityse. Komisija ir EPI turėtų užtikrinti, kad tuos standartus ir reikalavimus visi finansų sektoriaus subjektai galėtų taikyti tokiu būdu, kuris būtų proporcingas jų dydžiui ir bendram rizikos profiliui, taip pat jų paslaugų, veiklos ir operacijų pobūdžiui, mastui ir sudėtingumui. Komisijai turėtų būti suteikti įgaliojimai priimti tuos techninius reguliavimo standartus įgyvendinimo aktais pagal SESV 290 straipsnį ir reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsniuose nustatyta tvarka;

(100) siekiant gerinti pranešimų apie didelius su IRT susijusius incidentus ir didelius su mokėjimu susijusius operacinius arba saugumo incidentus palyginamumą, taip pat užtikrinti sutartimi įformintų susitarimų dėl IRT paslaugas teikiančių trečiųjų šalių teikiamų IRT paslaugų naudojimo skaidrumą, EPI turėtų parengti techninių įgyvendinimo standartų, kuriais nustatomi standartiniai šablonai, formos ir procedūros, skirti naudoti finansų sektoriaus subjektams pranešant apie didelį su IRT susijusį incidentą ir didelį su mokėjimu susijusį operacinį arba saugumo incidentą, taip pat standartiniai informacijos registro šablonai, projektus. Rengdamos tuos standartus, EPI turėtų atsižvelgti į finansų sektoriaus subjekto dydį ir bendrą rizikos profilį, taip pat į jo paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą. Komisijai turėtų būti suteikti įgaliojimai priimti tuos techninius įgyvendinimo standartus įgyvendinimo aktais pagal SESV 291 straipsnį reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 15 straipsnyje nustatyta tvarka;

([22]) OL L 123, 2016 5 12, p. 1.

(101) kadangi papildomi reikalavimai jau yra nustatyti deleguotaisiais ir įgyvendinimo aktais, pagrįstais Europos Parlamento ir Tarybos reglamentuose (EB) Nr. 1060/2009 ([23]), (ES) Nr. 648/2012 ([24]), (ES) Nr. 600/2014 ([25]) ir (ES) Nr. 909/2014 ([26]) nustatytais techniniais reguliavimo ir įgyvendinimo standartais, tikslinga pavesti EPI atskirai arba kartu per Jungtinį komitetą pateikti Komisijai techninius reguliavimo ir įgyvendinimo standartus, kad būtų priimti deleguotieji ir įgyvendinimo aktai, į kuriuos perkeliamos ir kuriais atnaujinamos dabartinės IRT rizikos valdymo taisyklės;

(102) kadangi šiame reglamente ir Europos Parlamento ir Tarybos direktyvoje (ES) 2022/2556 ([27]) konsoliduojamos IRT rizikos valdymo nuostatos įvairiuose Sąjungos finansinių paslaugų *acquis* reglamentuose ir direktyvose, įskaitant Europos Parlamento ir Tarybos reglamentus (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014 ir (ES) Nr. 909/2014 bei Europos Parlamento ir Tarybos reglamentą (ES) 2016/1011 ([28]), siekiant užtikrinti visišką nuoseklumą, tie reglamentai turėtų būti iš dalies pakeisti paaiškinant, kad taikytinos su IRT rizika susijusios nuostatos yra išdėstytos šiame reglamente;

(103) todėl su operacine rizika susijusių straipsnių, kuriais Europos Parlamento ir Tarybos reglamentuose (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 numatyti įgaliojimai priimti deleguotuosius ir įgyvendinimo aktus, taikymo sritis turėtų būti susiaurinta siekiant į šį reglamentą perkelti visas šiandien tuose reglamentuose pateiktas nuostatas, apimančias skaitmeninės veiklos atsparumo aspektus;

(104) galimą sisteminę kibernetinę riziką, susijusios su IRT infrastruktūros, kuri sudaro sąlygas mokėjimo sistemų veikimui, naudojimu ir mokėjimų vykdymo veiklos vykdymu, klausimą reikėtų tinkamai spręsti Sąjungos lygmeniu taikant suderintas skaitmeninio atsparumo taisykles. Tuo tikslu Komisija turėtų skubiai įvertinti poreikį peržiūrėti šio reglamento taikymo sritį, kartu derindama tokią peržiūrą atsižvelgiant į visapusiškos peržiūros, numatytos pagal Direktyvą (ES) 2015/2366, rezultatus. Didelis didelio masto išpuolių skaičius per pastarąjį dešimtmetį rodo, kad mokėjimo sistemoms kilo kibernetinių grėsmių. Mokėjimo sistemos ir mokėjimų vykdymo veikla yra mokėjimų paslaugų grandinės pagrindas ir turi stiprias tarpusavio sąsajas su visa finansų sistema, todėl jos tapo itin svarbios Sąjungos finansų rinkų veikimui. Kibernetiniai išpuoliai prieš tokias sistemas gali sukelti didelių veiklos sutrikimų, turinčių tiesioginį poveikį pagrindinėms ekonominėms funkcijoms, pavyzdžiui, mokėjimų palengvinimui, ir netiesioginį poveikį susijusiems ekonominiams procesams. Kol Sąjungos lygmeniu bus nustatyta suderinta mokėjimo sistemų operatorių ir mokėjimų vykdymo paslaugą teikiančių subjektų tvarka ir priežiūra, valstybės narės, siekdamos taikyti panašią rinkos praktiką, gali remtis šiuo reglamentu nustatytais skaitmeninės veiklos atsparumo reikalavimais, taikydamos taisykles mokėjimo sistemų operatoriams ir mokėjimų vykdymo paslaugą teikiantiems subjektams, kurių priežiūra vykdoma jų jurisdikcijose;

([23]) 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1060/2009 dėl kredito reitingų agentūrų (OL L 302, 2009 11 17, p. 1).

([24]) 2012 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų (OL L 201, 2012 7 27, p. 1).

([25]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 600/2014 dėl finansinių priemonių rinkų, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 (OL L 173, 2014 6 12, p. 84).

([26]) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 909/2014 dėl atsiskaitymo už vertybinius popierius gerinimo Europos Sąjungoje ir centrinių vertybinių popierių depozitoriumų, kuriuo iš dalies keičiamos direktyvos 98/26/EB ir 2014/65/ES bei Reglamentas (ES) Nr. 236/2012 (OL L 257, 2014 8 28, p. 1).

([27]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2556, kuria iš dalies keičiamos direktyvos 2009/65/EB, 2009/138/EB, 2011/61/ES, 2013/36/ES, 2014/59/ES, 2014/65/ES, (ES) 2015/2366 ir (ES) 2016/2341 dėl finansų sektoriaus skaitmeninės veiklos atsparumo (žr. šio Oficialiojo leidinio p. 153)

([28]) 2016 m. birželio 8 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/1011 dėl indeksų, kurie kaip lyginamieji indeksai naudojami finansinėse priemonėse ir finansinėse sutartyse arba siekiant įvertinti investicinių fondų veiklos rezultatus, kuriuo iš dalies keičiami direktyvos 2008/48/EB ir 2014/17/ES bei Reglamentas (ES) Nr. 596/2014 (OL L 171, 2016 6 29, p. 1).

(105) kadangi šio reglamento tikslo, t. y. užtikrinti reguliuojamų finansų sektoriaus subjektų aukšto lygio skaitmeninės veiklos atsparumą, valstybės narės negali deramai pasiekti, nes tam reikia suderinti įvairias skirtingas taisykles, esančias Sąjungos teisės aktuose arba nacionalinėje teisėje, o to tikslo dėl jo masto ir poveikio būtų geriau siekti Sąjungos lygmeniu, laikydamasi Europos Sąjungos sutarties 5 straipsnyje nustatyto subsidiarumo principo Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šiuo reglamentu neviršijama to, kas būtina nurodytam tikslui pasiekti;

(106) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([29]) 42 straipsnio 1 dalimi buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis pateikė nuomonę 2021 m. gegužės 10 d. ([30]),

PRIĖMĖ ŠĮ REGLAMENTĄ:

I SKYRIUS

Bendrosios nuostatos

1 straipsnis

Dalykas

1. Siekiant užtikrinti aukšto bendro lygio skaitmeninės veiklos atsparumą, šiuo reglamentu nustatomi šie vienodi reikalavimai dėl tinklų ir informacinių sistemų, kuriomis palaikomi finansų sektoriaus subjektų veiklos procesai, saugumo:

a) finansų sektoriaus subjektams taikomi reikalavimai, susiję su:

   i) informacinių ir ryšių technologijų (IRT) rizikos valdymu;

   ii) pranešimu kompetentingoms institucijoms apie didelius su IRT susijusius incidentus ir savanorišku pranešimu kompetentingoms institucijoms apie dideles kibernetines grėsmes;

   iii) finansinių subjektų, nurodytų 2 straipsnio 1 dalies a–d punktuose, pranešimu kompetentingoms institucijoms apie didelius su mokėjimais susijusius operacinius arba saugumo incidentus;

   iv) skaitmeninės veiklos atsparumo testavimu;

   v) keitimusi informacija ir žvalgybos informacija apie kibernetines grėsmes ir pažeidžiamumus;

   vi) priemonėmis, skirtomis tinkamai valdyti trečiosios šalies keliamą IRT riziką;

b) reikalavimai, susiję su IRT paslaugas teikiančių trečiųjų šalių ir finansų sektoriaus subjektų tarpusavyje sudarytais sutartimi įformintais susitarimais;

c) ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims skirtos priežiūros sistemos nustatymo ir veiklos taisyklės, kai pastarieji teikia paslaugas finansų sektoriaus subjektams;

d) kompetentingų institucijų bendradarbiavimo taisyklės ir kompetentingų institucijų vykdomos priežiūros ir vykdymo užtikrinimo taisyklės, susijusios su visais klausimais, kuriems taikomas šis reglamentas.

2. Finansų sektoriaus subjektų, kurie pagal nacionalines taisykles, kuriomis į nacionalinę teisę perkeliamas Direktyvos (ES) 2022/2555 3 straipsnis, laikomi esminiais ar svarbiais subjektais, atžvilgiu šis reglamentas laikomas konkrečiam sektoriui taikomu Sąjungos teisės aktu tos direktyvos 4 straipsnio tikslais.

3. Šiuo reglamentu nedaromas poveikis valstybių narių atsakomybei, susijusiai su esminėmis valstybinėmis funkcijomis, susijusiomis su visuomenės saugumu, gynyba ir nacionaliniu saugumu, pagal Sąjungos teisę.

([29]) 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).

([30]) OL C 229, 2021 6 15, p. 16.

2 straipsnis

Taikymo sritis

1. Nedarant poveikio 3 ir 4 dalims, šis reglamentas taikomas šiems subjektams:

a) kredito įstaigoms;

b) mokėjimo įstaigoms, įskaitant mokėjimo įstaigas, kurioms taikoma išimtis pagal Direktyvą (ES) 2015/2366,

c) informavimo apie sąskaitas paslaugų teikėjams;

d) elektroninių pinigų įstaigoms, įskaitant elektroninių pinigų įstaigas, kurioms taikoma išimtis pagal Direktyvą 2009/110/EB;

e) investicinėms įmonėms;

f) kriptoturto paslaugų teikėjams, turintiems veiklos leidimą pagal Europos Parlamento ir Tarybos reglamentą dėl kriptoturto rinkų, kuriuo iš dalies keičiami reglamentai (ES) Nr. 1093/2010 ir (ES) Nr. 1095/2010 ir direktyvos 2013/36/ES bei (ES) 2019/1937 (toliau – Reglamentas dėl kriptoturto rinkų), ir su turtu susietų žetonų emitentams;

g) centriniams vertybinių popierių depozitoriumams;

h) pagrindinėms sandorio šalims;

i) prekybos vietoms;

j) sandorių duomenų saugykloms;

k) alternatyvaus investavimo fondų valdytojams;

l) valdymo įmonėms;

m) duomenų teikimo paslaugų teikėjams;

n) draudimo ir perdraudimo įmonėms;

o) draudimo tarpininkams, perdraudimo tarpininkams ir papildomos draudimo veiklos tarpininkams;

p) profesinių pensijų įstaigoms;

q) kredito reitingų agentūroms;

r) ypatingos svarbos lyginamųjų indeksų administratoriams;

s) sutelktinio finansavimo paslaugų teikėjams;

t) pakeitimo vertybiniais popieriais duomenų saugykloms;

u) IRT paslaugas teikiančioms trečiosioms šalims.

2. Šiame reglamente 1 dalies a–t punktuose nurodyti subjektai kartu vadinami „finansų sektoriaus subjektais“.

3. Šis reglamentas netaikomas:

a) alternatyvaus investavimo fondų valdytojams, kaip nurodyta Direktyvos 2011/61/ES 3 straipsnio 2 dalyje;

b) draudimo ir perdraudimo įmonėms, kaip nurodyta Direktyvos 2009/138/EB 4 straipsnyje;

c) profesinių pensijų įstaigoms, valdančioms pensijų sistemas, kurios kartu turi ne daugiau kaip 15 narių;

d) fiziniams arba juridiniams asmenims, kuriems taikoma išimtis pagal Direktyvos 2014/65/ES 2 ir 3 straipsnius;

e) draudimo tarpininkams, perdraudimo tarpininkams ir papildomos draudimo veiklos tarpininkams, kurie yra labai mažos įmonės arba mažosios ar vidutinės įmonės;

f) pašto žiro įstaigoms, kaip nurodyta Direktyvos 2013/36/ES 2 straipsnio 5 dalies 3 punkte.

4. Valstybės narės gali šio reglamento netaikyti Direktyvos 2013/36/ES 2 straipsnio 5 dalies 4–23 punktuose nurodytais subjektais, esančiais jų atitinkamose teritorijose. Jei valstybė narė pasinaudoja tokia galimybe, ji apie tai ir visus vėlesnius jos pakeitimus praneša Komisijai. Komisija tą informaciją viešai paskelbia savo interneto svetainėje arba sudaro sąlygas visuomenei susipažinti su ja kitu lengvai prieinamu būdu.

3 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) skaitmeninės veiklos atsparumas – finansų sektoriaus subjekto gebėjimas sukurti, užtikrinti ir peržiūrėti savo veiklos vientisumą ir patikimumą, tiesiogiai ar netiesiogiai naudojantis IRT paslaugas teikiančių trečiųjų šalių suteiktomis paslaugomis, užtikrinant visus su IRT susijusius pajėgumus, reikalingus tinklų ir informacinių sistemų, kuriomis finansų sektoriaus subjektas naudojasi, saugumui užtikrinti, ir kuriais užtikrinamas nuolatinis finansinių paslaugų teikimas ir jų kokybė, be kita ko, esant sutrikimams;

2) tinklų ir informacinė sistema – tinklų ir informacinė sistema, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 1 punkte;

3) senoji IRT sistema – gyvavimo ciklo pabaigą (eksploatacijos pabaigą) pasiekusi IRT sistema, kuri dėl technologinių ar komercinių priežasčių nėra tinkama atnaujinti ar pataisyti arba kurios nebepalaiko jos tiekėjas ar IRT paslaugas teikianti trečioji šalis, tačiau kuri vis dar naudojama ir palaiko finansų sektoriaus subjekto funkcijas;

4) tinklų ir informacinių sistemų saugumas – tinklų ir informacinių sistemų saugumas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 2 punkte;

5) IRT rizika – bet kokia pagrįstai atpažįstama aplinkybė, susijusi su tinklų ir informacinių sistemų naudojimu, kuriai susiklosčius gali būti pakenkta tinklų ir informacinių sistemų, bet kurios nuo technologijų priklausomos priemonės ar proceso, operacijų ir procesų arba paslaugų teikimo saugumui, sukeliant neigiamą poveikį skaitmeninei arba fizinei aplinkai;

6) informacinis turtas – materialios arba nematerialios informacijos, kurią verta apsaugoti, rinkinys;

7) IRT turtas – programinė arba aparatinė įranga, finansų sektoriaus subjekto naudojama tinklų ir informacinėse sistemose;

8) su IRT susijęs incidentas – vienas įvykis arba keletas susijusių įvykių, kurių neplanavo finansų sektoriaus subjektas ir kurie kenkia tinklų ir informacinių sistemų saugumui ir daro neigiamą poveikį duomenų prieinamumui, autentiškumui, vientisumui ar konfidencialumui arba finansų sektoriaus subjekto teikiamoms paslaugoms;

9) su mokėjimu susijęs operacinis arba saugumo incidentas – 2 straipsnio 1 dalies a–d punktuose nurodytų finansų sektoriaus subjektų nesuplanuotas vienas arba keletas susijusių įvykių, kurie yra susiję arba nesusiję su IRT, darančių neigiamą poveikį su mokėjimu susijusių duomenų prieinamumui, autentiškumui, vientisumui ar konfidencialumui arba finansų sektoriaus subjekto teikiamoms su mokėjimu susijusioms paslaugoms;

10) didelis su IRT susijęs incidentas – su IRT susijęs incidentas, darantis didelį neigiamą poveikį tinklų ir informacinėms sistemoms, naudojamoms finansų sektoriaus subjekto ypatingos svarbos arba svarbioms funkcijoms palaikyti;

11) didelis su mokėjimu susijęs operacinis arba saugumo incidentas – su mokėjimu susijęs operacinis arba saugumo incidentas, darantis didelį neigiamą poveikį teikiamoms su mokėjimu susijusioms paslaugoms;

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

13) didelė kibernetinė grėsmė – kibernetinė grėsmė, kurios techninės savybės rodo, kad ji gali sukelti didelį su IRT susijusį incidentą arba didelį su mokėjimu susijusį operacinį arba saugumo incidentą;

14) kibernetinis išpuolis – su IRT susijęs piktavališkas incidentas, kuris yra sukeliamas, kai priešiškas subjektas bando sunaikinti, atskleisti, pakeisti, išjungti, pavogti ar įgyti neteisėtą prieigą prie bet kokio turto arba neteisėtai juo naudotis;

15) žvalgybos informacija apie grėsmes – informacija, kuri yra apibendrinama, pertvarkoma, analizuojama, aiškinama arba patikslinama siekiant pateikti būtiną kontekstą sprendimų priėmimui ir sudaryti sąlygas tinkamai ir pakankamai suprasti, kaip mažinti su IRT susijusio incidento arba kibernetinės grėsmės poveikį, įskaitant techninius kibernetinio išpuolio duomenis, už išpuolį atsakingus asmenis ir jų *modus operandi* bei motyvus;

16) pažeidžiamumas – turto, sistemos, proceso ar kontrolės priemonės silpnoji vieta, jautrumas ar trūkumas, kuriais gali būti pasinaudota;

17) grėsmėmis grindžiamas skverbimosi testavimas (TLPT) – sistema, kuria imituojama realių priešiškų subjektų, kurie laikomi keliančiais tikrą kibernetinę grėsmę, taktika, metodai ir procedūros ir pagal kurią atliekamas kontroliuojamas, specialiai pritaikytas, žvalgybos informacija grindžiamas (raudonosios komandos atliekamas) finansų sektoriaus subjekto ypatingos svarbos tikralaikių produkcijos sistemų testas;

18) trečiosios šalies keliama IRT rizika – IRT rizika, su kuria gali susidurti finansų sektoriaus subjektas, naudodamasis IRT paslaugas teikiančių trečiųjų šalių arba jų subrangovų teikiamomis IRT paslaugomis, be kita ko, pagal veiklos rangos susitarimus;

19) IRT paslaugas teikianti trečioji šalis – IRT paslaugas teikianti įmonė;

20) grupės vidaus IRT paslaugų teikėjas – įmonė, priklausanti finansų grupei ir teikianti daugiausia IRT paslaugas tos pačios grupės finansų sektoriaus subjektams arba tai pačiai institucinei užtikrinimo sistemai priklausantiems finansų sektoriaus subjektams, įskaitant jų patronuojančiąsias įmones, patronuojamąsias įmones, filialus ar kitus subjektus, kurie jiems bendrai priklauso arba yra jų kontroliuojami;

21) IRT paslaugos – skaitmeninės ir duomenų paslaugos, nuolat teikiamos naudojantis IRT sistemomis vienam ar keliems vidaus ar išorės naudotojams, įskaitant aparatinę įrangą kaip paslaugą ir aparatinės įrangos paslaugas, kurios apima techninės paramos teikimą, aparatinės įrangos teikėjui atliekant programinės įrangos arba programinės aparatinės įrangos atnaujinimus, išskyrus tradicines analoginio telefono ryšio paslaugas;

22) ypatingos svarbos arba svarbi funkcija – funkcija, kuriai sutrikus būtų reikšmingai pakenkta finansų sektoriaus subjekto finansinės veiklos rezultatams arba jo paslaugų ir veiklos patikimumui ar tęstinumui arba kurios nebevykdant, vykdant su trūkumais arba netinkamai būtų reikšmingai pakenkta finansų sektoriaus subjekto veiklos leidime nurodytų sąlygų ir pareigų arba kitų jo įsipareigojimų pagal taikytiną finansinių paslaugų teisę nenutrūkstamam vykdymui;

23) ypatingos svarbos IRT paslaugas teikianti trečioji šalis – IRT paslaugas teikianti trečioji šalis, pripažinta kaip ypatingos svarbos pagal 31 straipsnį;

24) trečiojoje valstybėje įsisteigusi IRT paslaugas teikianti trečioji šalis – IRT paslaugas teikianti trečioji šalis, kuri yra trečiojoje valstybėje įsisteigęs juridinis asmuo ir kuri yra sudariusi sutartimi įformintą susitarimą su finansų sektoriaus subjektu dėl IRT paslaugų teikimo;

25) patronuojamoji įmonė – patronuojamoji įmonė, kaip tai suprantama Direktyvos 2013/34/ES 2 straipsnio 10 punkte ir 22 straipsnyje;

26) grupė – grupė, kaip apibrėžta Direktyvos 2013/34/ES 2 straipsnio 11 punkte;

27) patronuojančioji įmonė – patronuojančioji įmonė, kaip tai suprantama Direktyvos 2013/34/ES 2 straipsnio 9 punkte ir 22 straipsnyje;

28) trečiojoje valstybėje įsisteigęs IRT subrangovas – IRT subrangovas, kuris yra trečiojoje valstybėje įsisteigęs juridinis asmuo ir kuris yra sudaręs sutartimi įformintą susitarimą su IRT paslaugas teikiančia trečiąja šalimi arba trečiojoje valstybėje įsisteigusia IRT paslaugas teikiančia trečiąja šalimi;

29) IRT koncentracijos rizika – dėl atskirų arba kelių susijusių ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių kylanti rizika, dėl kurios atsiranda tam tikra priklausomybė nuo tokių paslaugų teikėjų, kai dėl tokio paslaugų teikėjo neprieinamumo, žlugimo ar kitokio pobūdžio trūkumo gali kilti pavojus, kad finansų sektoriaus subjektas nebegalės vykdyti ypatingos svarbos arba svarbių funkcijų arba patirs kitokio pobūdžio neigiamą poveikį, įskaitant didelius nuostolius, arba gali kilti pavojus visos Sąjungos finansiniam stabilumui;

30) valdymo organas – valdymo organas, kaip apibrėžta Direktyvos 2014/65/ES 4 straipsnio 1 dalies 36 punkte, Direktyvos 2013/36/ES 3 straipsnio 1 dalies 7 punkte, Europos Parlamento ir Tarybos direktyvos 2009/65/EB ([31]) 2 straipsnio 1 dalies s punkte, Reglamento (ES) Nr. 909/2014 2 straipsnio 1 dalies 45 punkte, Reglamento (ES) 2016/1011 3 straipsnio 1 dalies 20 punkte, ir atitinkamose Reglamento dėl kriptoturto rinkų nuostatose, arba tokius pačius įgaliojimus turintys asmenys, kurie veiksmingai vadovauja subjektui arba vykdo pagrindines funkcijas pagal atitinkamus Sąjungos ar nacionalinės teisės aktus;

31) kredito įstaiga – kredito įstaiga, apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 575/2013 ([32]) 4 straipsnio 1 dalies 1 punkte;

32) įstaiga, kuriai taikoma išimtis pagal Direktyvą 2013/36/ES – subjektas, kaip nurodyta Direktyvos 2013/36/ES 2 straipsnio 5 dalies 4–23 punktuose;

33) investicinė įmonė – investicinė įmonė, kaip apibrėžta Direktyvos 2014/65/ES 4 straipsnio 1 dalies 1 punkte;

34) maža ir tarpusavio sąsajų neturinti investicinė įmonė – investicinė įmonė, atitinkanti Europos Parlamento ir Tarybos reglamento (ES) 2019/2033 ([33]) 12 straipsnio 1 dalyje nustatytas sąlygas;

35) mokėjimo įstaiga – mokėjimo įstaiga, kaip apibrėžta Direktyvos (ES) 2015/2366 4 straipsnio 4 punkte;

36) mokėjimo įstaiga, kuriai taikoma išimtis pagal Direktyvą (ES) 2015/2366 – mokėjimo įstaiga, kuriai taikoma išimtis pagal Direktyvos (ES) 2015/2366 32 straipsnio 1 dalį;

37) informavimo apie sąskaitas paslaugų teikėjas – informavimo apie sąskaitas paslaugų teikėjas, kaip nurodyta Direktyvos (ES) 2015/2366 33 straipsnio 1 dalyje;

38) elektroninių pinigų įstaiga – elektroninių pinigų įstaiga, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/110/EB 2 straipsnio 1 punkte;

39) elektroninių pinigų įstaiga, kuriai taikoma išimtis pagal Direktyvą 2009/110/EB – elektroninių pinigų įstaiga, kuri naudojasi netaikymo sąlyga, kaip nurodyta Direktyvos 2009/110/EB 9 straipsnio 1 dalyje;

40) pagrindinė sandorio šalis – pagrindinė sandorio šalis, kaip apibrėžta Reglamento (ES) Nr. 648/2012 2 straipsnio 1 punkte;

41) sandorių duomenų saugykla – sandorių duomenų saugykla, kaip apibrėžta Reglamento (ES) Nr. 648/2012 2 straipsnio 2 punkte;

42) centrinis vertybinių popierių depozitoriumas – centrinis vertybinių popierių depozitoriumas, kaip apibrėžta Reglamento (ES) Nr. 909/2014 2 straipsnio 1 dalies 1 punkte;

43) prekybos vieta – prekybos vieta, kaip apibrėžta Direktyvos 2014/65/ES 4 straipsnio 1 dalies 24 punkte;

44) alternatyvaus investavimo fondų valdytojas – alternatyvaus investavimo fondų valdytojas, kaip apibrėžta Direktyvos 2011/61/ES 4 straipsnio 1 dalies b punkte;

45) valdymo įmonė – valdymo įmonė, kaip apibrėžta Direktyvos 2009/65/EB 2 straipsnio 1 dalies b punkte;

46) duomenų teikimo paslaugų teikėjas – duomenų teikimo paslaugų teikėjas, kaip tai suprantama Reglamente (ES) Nr. 600/2014, kaip nurodyta jo 2 straipsnio 1 dalies 34–36 punktuose;

47) draudimo įmonė – draudimo įmonė, kaip apibrėžta Direktyvos 2009/138/EB 13 straipsnio 1 punkte;

48) perdraudimo įmonė – perdraudimo įmonė, kaip apibrėžta Direktyvos 2009/138/EB 13 straipsnio 4 punkte;

([31]) 2009 m. liepos 13 d. Europos Parlamento ir Tarybos direktyva 2009/65/EB dėl įstatymų ir kitų teisės aktų, susijusių su kolektyvinio investavimo į perleidžiamus vertybinius popierius subjektais (KIPVPS), derinimo (OL L 302, 2009 11 17, p. 32).

([32]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 575/2013 dėl prudencinių reikalavimų kredito įstaigoms ir investicinėms įmonėms ir kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 (OL L 176, 2013 6 27, p. 1).

([33]) 2019 m. lapkričio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/2033 dėl riziką ribojančių reikalavimų investicinėms įmonėms, kuriuo iš dalies keičiami reglamentai (ES) Nr. 1093/2010, (ES) Nr. 575/2013, (ES) Nr. 600/2014 ir (ES) Nr. 806/2014 (OL L 314, 2019 12 5, p. 1).

49) draudimo tarpininkas – draudimo tarpininkas, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2016/97 ([34]) 2 straipsnio 1 dalies 3 punkte;

50) papildomos draudimo veiklos tarpininkas – papildomos draudimo veiklos tarpininkas, kaip apibrėžta Direktyvos (ES) 2016/97 2 straipsnio 1 dalies 4 punkte;

51) perdraudimo tarpininkas – perdraudimo tarpininkas, kaip apibrėžta Direktyvos (ES) 2016/97 2 straipsnio 1 dalies 5 punkte;

52) profesinių pensijų įstaiga – profesinių pensijų įstaiga, kaip apibrėžta Direktyvos (ES) 2016/2341 6 straipsnio 1 punkte;

53) maža profesinių pensijų įstaiga – profesinių pensijų įstaiga, valdanti pensijų sistemas, kurios kartu turi ne daugiau kaip 100 narių;

54) kredito reitingų agentūra – kredito reitingų agentūra, kaip apibrėžta Reglamento (EB) Nr. 1060/2009 3 straipsnio 1 dalies b punkte;

55) kriptoturto paslaugų teikėjas – kriptoturto paslaugų teikėjas, kaip apibrėžta Reglamento dėl kriptoturto rinkų atitinkamoje nuostatoje;

56) su turtu susietų žetonų emitentas – su turtu susietų žetonų emitentas, kaip apibrėžta Reglamento dėl kriptoturto rinkų atitinkamoje nuostatoje;

57) ypatingos svarbos lyginamųjų indeksų administratorius – ypatingos svarbos lyginamųjų indeksų, kaip apibrėžta Reglamento (ES) 2016/1011 3 straipsnio 1 dalies 25 punkte, administratorius;

58) sutelktinio finansavimo paslaugų teikėjas – sutelktinio finansavimo paslaugų teikėjas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2020/1503 ([35]) 2 straipsnio 1 dalies e punkte;

59) pakeitimo vertybiniais popieriais duomenų saugykla – pakeitimo vertybiniais popieriais duomenų saugykla, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2017/2402 ([36]) 2 straipsnio 23 punkte;

60) labai maža įmonė – finansų sektoriaus subjektas, kuris nėra prekybos vieta, pagrindinė sandorio šalis, sandorių duomenų saugykla arba centrinis vertybinių popierių depozitoriumas, kuriame dirba mažiau nei 10 asmenų, o jo metinė apyvarta ir (arba) bendra metinio balanso suma neviršija 2 mln. EUR;

61) Atsakingoji priežiūros institucija – Europos priežiūros institucija, paskirta pagal šio reglamento 31 straipsnio 1 dalies b punktą;

62) Jungtinis komitetas – reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 54 straipsnyje nurodytas komitetas;

63) mažoji įmonė – finansų sektoriaus subjektas, kuriame dirba 10 ar daugiau, bet mažiau nei 50 asmenų, o jo metinė apyvarta ir (arba) bendra metinio balanso suma viršija 2 mln. EUR, bet yra ne didesnė nei 10 mln. EUR;

64) vidutinė įmonė – finansų sektoriaus subjektas, kuris nėra mažoji įmonė ir kuriame dirba mažiau kaip 250 darbuotojų, o jo metinė apyvarta neviršija 50 mln. EUR ir (arba) metinio balanso suma neviršija 43 mln. EUR;

65) valdžios institucija – Vyriausybinis arba kitas viešojo administravimo subjektas, įskaitant nacionalinius centrinius bankus.

([34]) 2016 m. sausio 20 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/97 dėl draudimo produktų platinimo (OL L 26, 2016 2 2, p. 19).

([35]) 2020 m. spalio 7 d. Europos Parlamento ir Tarybos reglamentas (ES) 2020/1503 dėl Europos sutelktinio finansavimo paslaugų verslui teikėjų, kuriuo iš dalies keičiamas Reglamentas (ES) 2017/1129 ir Direktyva (ES) 2019/1937 (OL L 347, 2020 10 20, p. 1).

([36]) 2017 m. gruodžio 12 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/2402, kuriuo nustatoma bendroji pakeitimo vertybiniais popieriais sistema ir sukuriama specialioji paprasto, skaidraus ir standartizuoto pakeitimo vertybiniais popieriais sistema, ir iš dalies keičiamos direktyvos 2009/65/EB, 2009/138/EB ir 2011/61/ES bei reglamentai (EB) Nr. 1060/2009 ir (ES) Nr. 648/2012 (OL L 347, 2017 12 28, p. 35).

4 straipsnis

Proporcingumo principas

1. Finansų sektoriaus subjektai įgyvendina II skyriuje nustatytas taisykles laikydamiesi proporcingumo principo, atsižvelgdami į savo įmonės dydį ir bendrą rizikos profilį, taip pat paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą.

2. Be to, III, IV skyrių ir V skyriaus I skirsnio taikymas finansų sektoriaus subjektams turi būti proporcingas jų įmonės dydžiui ir bendram rizikos profiliui, taip pat jų paslaugų, veiklos ir operacijų pobūdžiui, mastui ir sudėtingumui, kaip konkrečiai numatyta atitinkamose tuose skyriuose išdėstytose taisyklėse.

3. Kompetentingos institucijos, peržiūrėdamos IRT rizikos valdymo sistemos nuoseklumą, apsvarsto, kaip finansų sektoriaus subjektai taiko proporcingumo principą, remdamosi ataskaitomis, pateiktomis kompetentingų institucijų prašymu pagal 6 straipsnio 5 dalį ir 16 straipsnio 2 dalį.

II SKYRIUS

IRT rizikos valdymas

I skirsnis

5 straipsnis

Valdymas ir organizavimas

1. Finansų sektoriaus subjektai pagal 6 straipsnio 4 dalį įdiegia vidaus valdymo ir kontrolės sistemą, kuria užtikrinamas veiksmingas ir prudencinis IRT rizikos valdymas, kad būtų užtikrintas aukšto lygio skaitmeninės veiklos atsparumas.

2. Finansų sektoriaus subjekto valdymo organas nustato, tvirtina, prižiūri visų priemonių, susijusių su 6 straipsnio 1 dalyje nurodyta IRT rizikos valdymo sistema, įgyvendinimą ir už jį atsako.

Taikant pirmą pastraipą, valdymo organas:

a) prisiima galutinę atsakomybę už finansų sektoriaus subjekto IRT rizikos valdymą;

b) nustato politiką, kuria siekiama užtikrinti, kad būtų išlaikyti aukšti duomenų prieinamumo, autentiškumo, vientisumo ir konfidencialumo standartai;

c) nustato aiškius visų su IRT susijusių funkcijų vaidmenis ir atsakomybę ir nustato tinkamas valdymo priemones, kad būtų užtikrintas veiksmingas ir laiku vykdomas tų funkcijų tarpusavio komunikavimas, bendradarbiavimas ir koordinavimas;

d) prisiima bendrą atsakomybę už tai, kad būtų nustatyta ir patvirtinta 6 straipsnio 8 dalyje nurodyta skaitmeninės veiklos atsparumo strategija, įskaitant atitinkamo finansų sektoriaus subjektui priimtino IRT rizikos lygmens nustatymą, kaip nurodyta 6 straipsnio 8 dalies b punkte;

e) tvirtina, prižiūri ir periodiškai peržiūri finansų sektoriaus subjekto IRT veiklos tęstinumo politiką ir IRT reagavimo ir veiklos atkūrimo planus, kurie atitinkamai nurodyti 11 straipsnio 1 ir 3 dalyse, įgyvendinimą; ši politika ir planai gali būti priimti kaip speciali specifinė politika, sudaranti neatsiejamą finansų sektoriaus subjekto bendros veiklos tęstinumo politikos ir reagavimo bei veiklos atkūrimo plano dalį;

f) tvirtina ir periodiškai peržiūri finansų sektoriaus subjekto IRT vidaus audito planus, IRT auditus ir jų esminius pakeitimus;

g) paskirsto ir periodiškai peržiūri atitinkamą biudžetą, kad būtų tenkinami finansų sektoriaus subjekto skaitmeninės veiklos atsparumo poreikiai, susiję su visų rūšių ištekliais, įskaitant atitinkamas informuotumo apie IRT saugumą programas ir skaitmeninės veiklos atsparumo mokymą, nurodytus 13 straipsnio 6 dalyje, taip pat visų darbuotojų IRT įgūdžius;

h) tvirtina ir periodiškai peržiūri finansų sektoriaus subjekto politiką dėl susitarimų, susijusių su IRT paslaugas teikiančių trečiųjų šalių teikiamų IRT paslaugų naudojimu;

i) įdiegia įmonės lygmeniu pranešimų teikimo kanalus, kad galėtų būti tinkamai informuojamas apie:

i) susitarimus, sudarytus su IRT paslaugas teikiančiomis trečiosiomis šalimis dėl IRT paslaugų naudojimo,

ii) visus atitinkamus planuojamus esminius pokyčius, susijusius su IRT paslaugas teikiančiomis trečiosiomis šalimis,

iii) galimą tokių pokyčių poveikį ypatingos svarbos arba svarbioms funkcijoms, dėl kurių sudaryti tokie susitarimai, įskaitant rizikos analizės santrauką, kad būtų galima įvertinti tų pokyčių poveikį, taip pat bent apie didelius su IRT susijusius incidentus bei jų poveikį ir apie reagavimo, veiklos atkūrimo ir taisomąsias priemones.

3. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, sukuria pareigybę, skirtą susitarimų, sudarytų su IRT paslaugas teikiančiomis trečiosiomis šalimis dėl IRT paslaugų naudojimo, stebėsenai, arba paskiria vyresniosios vadovybės narį, atsakingą už gresiančios susijusios rizikos ir atitinkamų dokumentų priežiūrą.

4. Finansų sektoriaus subjekto valdymo organo nariai aktyviai siekia turėti naujausių pakankamų žinių ir įgūdžių IRT rizikai ir jos poveikiui finansų sektoriaus subjekto operacijoms suprasti ir įvertinti, be kita ko, reguliariai dalyvaudami specialiuose mokymuose, parengtuose atsižvelgiant į valdomą IRT riziką.

II skirsnis

6 straipsnis

IRT rizikos valdymo sistema

1. Finansų sektoriaus subjektai kaip savo bendros rizikos valdymo sistemos dalį turi turėti patikimą, išsamią ir gerai dokumentais pagrįstą IRT rizikos valdymo sistemą, kuri jiems leistų greitai, veiksmingai ir išsamiai mažinti IRT riziką ir užtikrinti aukšto lygio skaitmeninės veiklos atsparumą.

2. IRT rizikos valdymo sistema apima bent strategijas, politiką, procedūras, IRT protokolus ir priemones, kurie yra būtini siekiant deramai ir tinkamai apsaugoti visą informacinį turtą ir IRT turtą, įskaitant kompiuterių programinę įrangą, aparatinę įrangą, serverius, taip pat apsaugoti visus atitinkamus fizinius komponentus ir infrastruktūras, tokius kaip patalpos, duomenų centrai ir jautrios specialios zonos, kad būtų užtikrinta, kad visas informacinis turtas ir IRT turtas būtų tinkamai apsaugotas nuo rizikos, įskaitant žalą ir neteisėtą prieigą ar naudojimą.

3. Pagal savo IRT rizikos valdymo sistemą finansų sektoriaus subjektai kuo labiau sumažina IRT rizikos poveikį įgyvendindami atitinkamas strategijas, politiką, procedūras, IRT protokolus ir priemones. Jie kompetentingoms institucijoms jų prašymu pateikia išsamią ir atnaujintą informaciją apie IRT riziką ir apie savo IRT rizikos valdymo sistemą.

4. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, priskiria atsakomybę už IRT rizikos valdymą ir priežiūrą kontrolės funkcijai ir užtikrina tinkamą tokios kontrolės funkcijos nepriklausomumo lygį, kad būtų išvengta interesų konfliktų. Finansų sektoriaus subjektai užtikrina tinkamą IRT rizikos valdymo funkcijų, kontrolės funkcijų ir vidaus audito funkcijų atskyrimą ir nepriklausomumą pagal trijų gynybos linijų modelį arba vidaus rizikos valdymo ir kontrolės modelį.

5. IRT rizikos valdymo sistema pagrindžiama dokumentais ir peržiūrima bent kartą per metus arba – labai mažų įmonių atveju – periodiškai, taip pat įvykus dideliems su IRT susijusiems incidentams ir laikantis priežiūros nurodymų ar išvadų, padarytų atlikus atitinkamus skaitmeninės veiklos atsparumo testavimo arba audito procesus. Ji nuolat tobulinama remiantis įgyvendinimo ir stebėsenos patirtimi. Kompetentingai institucijai paprašius, jai pateikiama IRT rizikos valdymo sistemos peržiūros ataskaita.

6. Finansų sektoriaus subjektų, išskyrus labai mažas įmones, IRT rizikos valdymo sistemai taikomas vidaus auditas, kurį reguliariai atlieka auditoriai pagal finansų sektoriaus subjektų audito planą. Tie auditoriai turi turėti pakankamai žinių, įgūdžių ir patirties IRT rizikos srityje, taip pat jų nepriklausomumas turi būti tinkamo lygio. IRT auditų dažnumas ir tikrinami aspektai turi atitikti finansų sektoriaus subjekto IRT riziką.

7. Remdamiesi vidaus audito peržiūros išvadomis, finansų sektoriaus subjektai nustato oficialų tolesnių veiksmų procesą, įskaitant taisykles, pagal kurias laiku patikrinami ir ištaisomi svarbiausi IRT audito nustatyti trūkumai.

8. Į IRT rizikos valdymo sistemą įtraukiama skaitmeninės veiklos atsparumo strategija, kurioje nustatoma, kaip sistema turi būti įgyvendinama. Tuo tikslu skaitmeninės veiklos atsparumo strategija apima IRT rizikos mažinimo ir konkrečių IRT tikslų įgyvendinimo metodus:

a) paaiškinama, kaip IRT rizikos valdymo sistema prisidedama prie finansų sektoriaus subjekto veiklos strategijos ir tikslų;

b) nustatomas priimtinos IRT rizikos lygmuo, atsižvelgiant į finansų sektoriaus subjekto norimą prisiimti riziką, ir analizuojamas priimtinas IRT sutrikdymo poveikis;

c) nustatomi aiškūs informacijos saugumo tikslai, įskaitant pagrindinius veiklos rezultatų rodiklius ir pagrindinius rizikos parametrus;

d) paaiškinama IRT bazinė architektūra ir visi pakeitimai, reikalingi konkretiems veiklos tikslams pasiekti;

e) nurodomi įvairūs mechanizmai, įdiegti siekiant aptikti su IRT susijusius incidentus, užkirsti kelią jų poveikiui ir nuo jo apsisaugoti;

f) nurodoma esama skaitmeninės veiklos atsparumo padėtis remiantis didelių su IRT susijusių incidentų, apie kuriuos pranešta, skaičiumi ir prevencinių priemonių veiksmingumas;

g) įgyvendinamas skaitmeninės veiklos atsparumo testavimas pagal šio reglamento IV skyrių;

h) nurodoma komunikacijos strategija su IRT susijusių incidentų, kuriuos atskleisti reikalaujama pagal 14 straipsnį, atveju.

9. Finansų sektoriaus subjektai gali skaitmeninės veiklos atsparumo strategijos, nurodytos 8 dalyje, kontekste apibrėžti holistinę IRT kelių pardavėjų strategiją grupės ar subjekto lygmeniu, parodant pagrindinę priklausomybę nuo IRT paslaugas teikiančių trečiųjų šalių ir pateikiant pirkimo iš įvairių IRT paslaugas teikiančių trečiųjų šalių loginį pagrindimą.

10. Finansų sektoriaus subjektai gali, laikydamiesi Sąjungos ir nacionalinės sektorių teisės, perduoti grupės vidaus arba išorės įmonėms užduotis tikrinti atitiktį IRT rizikos valdymo reikalavimams. Tokio užduočių perdavimo atveju finansų sektoriaus subjektas išlieka visiškai atsakingas už atitikties IRT rizikos valdymo reikalavimams tikrinimą.

7 straipsnis

IRT sistemos, protokolai ir priemonės

Siekdami mažinti ir valdyti IRT riziką, finansų sektoriaus subjektai naudoja ir nuolat atnaujina IRT sistemas, protokolus ir priemones, kurie:

a) turi atitikti operacijų, kuriomis palaikomas jų veiklos vykdymas, mastą, laikantis 4 straipsnyje nurodyto proporcingumo principo;

b) yra patikimi;

c) yra aprūpinti pakankamais pajėgumais tiksliai tvarkyti duomenis, būtinus veiklai vykdyti ir laiku teikti paslaugas, ir prireikus susidoroti su didžiausiais pavedimų, pranešimų ar sandorių kiekiais, įskaitant atvejus, kai diegiamos naujos technologijos;

d) yra technologiškai atsparūs, kad galėtų tinkamai tenkinti papildomus informacijos tvarkymo poreikius, jei prireiktų nepalankiausiomis rinkos sąlygomis arba kitomis nepalankiomis aplinkybėmis.

8 straipsnis

Nustatymas

1. Pagal 6 straipsnio 1 dalyje nurodytą IRT rizikos valdymo sistemą finansų sektoriaus subjektai nustato, klasifikuoja ir tinkamai pagrindžia dokumentais visas IRT palaikomas veiklos funkcijas, vaidmenis ir pareigas, informacinį turtą ir IRT turtą, kuriais palaikomos šios funkcijos, taip pat jų vaidmenis ir priklausomybę, kiek tai susiję su IRT rizika. Prireikus ir bent kartą per metus finansų sektoriaus subjektai peržiūri šio klasifikavimo ir atitinkamų dokumentų tinkamumą.

2. Finansų sektoriaus subjektai nuolat nustato visus IRT rizikos, visų pirma rizikos kitų finansų sektoriaus subjektų atžvilgiu ir pastarųjų keliamos rizikos, šaltinius ir vertina kibernetines grėsmes ir IRT pažeidžiamumus, susijusius su jų IRT palaikomomis veiklos funkcijomis, informaciniu turtu ir IRT turtu. Finansų sektoriaus subjektai reguliariai ir bent kartą per metus peržiūri jiems poveikį darančius rizikos scenarijus.

3. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, atlieka rizikos vertinimą po kiekvieno svarbaus tinklų ir informacinių sistemų infrastruktūros, procesų ar procedūrų, turinčių įtakos jų IRT palaikomoms veiklos funkcijoms, informaciniam turtui ar IRT turtui, pakeitimo.

4. Finansų sektoriaus subjektai įvardija visą informacinį turtą ir IRT turtą, įskaitant esantį nutolusiose vietose, tinklo išteklius ir aparatinę įrangą ir pažymi tuos, kurie laikomi esančiais ypatingos svarbos. Jie pažymi informacinio turto ir IRT turto konfigūraciją ir skirtingo informacinio turto ir IRT turto sąsajas ir tarpusavio priklausomybę.

5. Finansų sektoriaus subjektai nustato ir dokumentais pagrindžia visus procesus, kurie priklauso nuo IRT paslaugas teikiančių trečiųjų šalių, ir nustato tarpusavio sąsajas su IRT paslaugas teikiančiomis trečiosiomis šalimis, kurios teikia paslaugas, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos.

6. 1, 4 ir 5 dalių tikslais finansų sektoriaus subjektai tvarko atitinkamus aprašus ir juos atnaujina reguliariai ir kiekvieną kartą, kai padaromas esminis pakeitimas, kaip nurodyta 3 dalyje.

7. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, reguliariai ir bent kartą per metus atlieka specialų visų senųjų IRT sistemų IRT rizikos vertinimą; bet kuriuo atveju jis atliekamas prieš technologijų, programų ar sistemų sujungimą ir po jo.

9 straipsnis

Apsauga ir prevencija

1. Siekdami tinkamai apsaugoti IRT sistemas ir parengti reagavimo priemones, finansų sektoriaus subjektai nuolat stebi ir kontroliuoja IRT sistemų ir priemonių saugumą ir veikimą ir kuo labiau mažina IRT rizikos poveikį IRT sistemoms, diegdami tinkamas IRT saugumo priemones, politikos priemones ir procedūras.

2. Finansų sektoriaus subjektai rengia, įsigyja ir įgyvendina IRT saugumo politiką, procedūras, protokolus ir priemones, kuriais siekiama užtikrinti IRT sistemų, visų pirma palaikančių ypatingos svarbos arba svarbias funkcijas, atsparumą, tęstinumą ir prieinamumą, taip pat išlaikyti aukštus saugomų, naudojamų ar perduodamų duomenų prieinamumo, autentiškumo, vientisumo ir konfidencialumo standartus.

3. Kad pasiektų 2 dalyje nurodytus tikslus, finansų sektoriaus subjektai naudoja IRT sprendimus ir procesus, kurie yra tinkami pagal 4 straipsnį. Tais IRT sprendimais ir procesais:

a) užtikrinamas duomenų perdavimo priemonių saugumas;

b) kuo labiau sumažinama duomenų sugadinimo ar praradimo, neteisėtos prieigos ir techninių trūkumų rizika, galinti trukdyti verslo veiklai;

c) užkertamas kelias duomenų nepakankamam prieinamumui, autentiškumo ir vientisumo pakenkimui, jų konfidencialumo pažeidimams, ir praradimui;

d) užtikrinama, kad duomenys būtų apsaugoti nuo tvarkant duomenis kylančios rizikos, be kita ko, dėl netinkamo administravimo, su duomenų apdorojimu susijusios rizikos ir žmogaus klaidos.

4. Pagal 6 straipsnio 1 dalyje nurodytą IRT rizikos valdymo sistemą finansų sektoriaus subjektai:

a) parengia ir dokumentais pagrindžia informacijos saugumo politiką, kurioje apibrėžiamos taisyklės, kaip apsaugoti duomenų, informacinio turto ir IRT turto, įskaitant, kai taikytina, jų klientų duomenų, informacinio turto ir IRT turto prieinamumą, autentiškumą, vientisumą ir konfidencialumą;

b) taikydami rizika grindžiamą požiūrį, nustato patikimą tinklų ir infrastruktūros valdymo struktūrą, naudodamiesi tinkamais būdais, metodais ir protokolais; tai gali apimti automatizuotų mechanizmų paveiktam informaciniam turtui izoliuoti kibernetinių išpuolių atveju įgyvendinimą;

c) įgyvendina politikos priemones, kuriomis fizinė ar loginė prieiga prie informacinio turto ir IRT turto apribojama tuo, kas reikalinga tik teisėtoms ir patvirtintoms funkcijoms ir veiklai, ir tuo tikslu parengia politikos priemonių, procedūrų ir kontrolės priemonių rinkinį dėl prieigos teisių ir patikimo jų administravimo;

d) įgyvendina griežtų tapatumo nustatymo mechanizmų politikos priemones ir protokolus, pagrįstus atitinkamais standartais, specialiomis kontrolės sistemomis ir apsaugos priemonėmis dėl kriptografinių raktų, kuriais duomenys užšifruojami remiantis patvirtintų duomenų klasifikavimo ir IRT rizikos vertinimo procesų rezultatais;

e) įgyvendina dokumentais pagrįstą IRT pakeitimų, įskaitant programinės įrangos, aparatinės įrangos, aparatinės programinės įrangos komponentų, sistemos ar saugumo nustatymus, valdymo politiką, procedūras ir kontrolės priemones, grindžiamas rizikos vertinimo požiūriu ir sudarančias neatsiejamą finansų sektoriaus subjekto bendro pakeitimų valdymo proceso dalį, siekiant užtikrinti, kad visi IRT sistemų pakeitimai būtų registruojami, testuojami, vertinami, tvirtinami, įgyvendinami ir tikrinami kontroliuojamu būdu;

f) turi turėti tinkamą ir išsamią dokumentais pagrįstą pataisų ir atnaujinimų politiką.

Pirmos pastraipos b punkto tikslais finansų sektoriaus subjektai tinklų ryšio infrastruktūrą kuria taip, kad būtų galimybė ją skubiai atjungti ar segmentuoti, siekiant kuo labiau sumažinti plintantį neigiamą poveikį ir užkirsti jam kelią, ypač tarpusavyje susijusių finansinių procesų atveju.

Pirmos pastraipos e punkto tikslais IRT pakeitimų valdymo procesas tvirtinamas atitinkamų tiesioginių vadovų ir nustatomi konkretūs protokolai.

10 straipsnis

Aptikimas

1. Pagal 17 straipsnį finansų sektoriaus subjektai turi būti įdiegę mechanizmus, skirtus neįprastai veiklai, įskaitant IRT tinklo veikimo problemas ir su IRT susijusius incidentus, skubiai aptikti ir galimiems reikšmingiems bendriems gedimo taškams nustatyti.

Visi pirmoje pastraipoje nurodyti aptikimo mechanizmai reguliariai testuojami pagal 25 straipsnį.

2. 1 dalyje nurodytais aptikimo mechanizmais sudaromos sąlygos keliems kontrolės lygmenims, nustatomos įspėjimo ribos ir kriterijai, pagal kuriuos būtų galima pradėti ir inicijuoti reagavimo į su IRT susijusius incidentus procesus, įskaitant automatinius įspėjimo mechanizmus atitinkamiems darbuotojams, atsakingiems už reagavimą į su IRT susijusius incidentus.

3. Finansų sektoriaus subjektai skiria pakankamai išteklių ir pajėgumų stebėti naudotojų veiklą, neįprastą IRT veiklą ir su IRT susijusius incidentus, visų pirma kibernetinius išpuolius.

4. Be to, duomenų paslaugų teikėjai turi būti įdiegę sistemas, kuriomis galima veiksmingai patikrinti prekybos pranešimų išsamumą, nustatyti praleidimus bei akivaizdžias klaidas ir kuriose reikalaujama tuos pranešimus pateikti iš naujo.

11 straipsnis

Reagavimas ir veiklos atkūrimas

1. Pagal 6 straipsnio 1 dalyje nurodytą IRT rizikos valdymo sistemą, remdamiesi 8 straipsnyje nurodytais nustatymo reikalavimais, finansų sektoriaus subjektai įdiegia išsamią IRT veiklos tęstinumo politiką, kuri gali būti priimta kaip speciali specifinė politika, sudaranti neatsiejamą finansų sektoriaus subjekto bendros veiklos tęstinumo politikos dalį.

2. Finansų sektoriaus subjektai įgyvendina IRT veiklos tęstinumo politiką taikydami specialius, tinkamus ir dokumentais pagrįstus susitarimus, planus, procedūras ir mechanizmus, kuriais siekiama:

a) užtikrinti finansų sektoriaus subjekto ypatingos svarbos arba svarbių funkcijų tęstinumą;

b) greitai, tinkamai ir veiksmingai reaguoti į visus su IRT susijusius incidentus ir juos spręsti taip, kad būtų padaryta kuo mažesnė žala, o pirmenybė būtų teikiama veiklos atnaujinimo ir atkūrimo veiksmams;

c) nedelsiant pradėti įgyvendinti specialius planus, kuriais sudaromos sąlygos taikyti izoliavimo priemones, procesus ir technologijas, kurie yra pritaikyti atsižvelgiant į kiekvieną su IRT susijusių incidentų rūšį, ir užkirsti kelią tolesnei žalai, taip pat pagal 12 straipsnį nustatytas pritaikytas reagavimo ir veiklos atkūrimo procedūras;

d) įvertinti preliminarų poveikį, žalą ir nuostolius;

e) nustatyti komunikacijos ir krizių valdymo veiksmus, kuriais užtikrinama, kad atnaujinta informacija būtų perduodama visiems atitinkamiems vidaus darbuotojams ir išorės suinteresuotiesiems subjektams pagal 14 straipsnį, ir teikti pranešimus kompetentingoms institucijoms pagal 19 straipsnį.

3. Pagal 6 straipsnio 1 dalyje nurodytą IRT rizikos valdymo sistemą finansų sektoriaus subjektai įgyvendina susijusius IRT reagavimo ir veiklos atkūrimo planus, kuriems finansų sektoriaus subjektų, išskyrus labai mažas įmones, atveju taikomos nepriklausomo vidaus audito peržiūros.

4. Finansų sektoriaus subjektai nustato, taiko ir periodiškai testuoja atitinkamus IRT veiklos tęstinumo planus, visų pirma susijusius su ypatingos svarbos arba svarbiomis funkcijomis, kurių vykdymas perduotas arba pagal susitarimus patikėtas vykdyti IRT paslaugas teikiančioms trečiosioms šalims.

5. Pagal bendrą veiklos tęstinumo politiką finansų sektoriaus subjektai atlieka didelių verslo sutrikdymų rizikos poveikio verslui analizę. Vykdydami poveikio verslui analizę finansų sektoriaus subjektai įvertina galimą didelių verslo sutrikdymų poveikį taikydami kiekybinius ir kokybinius kriterijus, atitinkamai naudodami vidaus ir išorės duomenis ir scenarijų analizę. Poveikio verslui analizėje atsižvelgiama į nustatytų ir pažymėtų veiklos funkcijų ypatingą svarbą, palaikymo procesus, priklausomybę nuo trečiųjų šalių ir informacinį turtą ir jų tarpusavio priklausomybę. Finansų sektoriaus subjektai užtikrina, kad IRT turtas ir IRT paslaugos būtų kuriamos ir naudojamos visapusiškai atsižvelgiant į poveikio verslui analizę, visų pirma siekiant tinkamai užtikrinti visų ypatingos svarbos komponentų atsarginius pajėgumus.

6. Vykdydami visapusišką IRT rizikos valdymą, finansų sektoriaus subjektai:

a) testuoja IRT veiklos tęstinumo planus ir IRT reagavimo ir veiklos atkūrimo planus, susijusius su visas funkcijas palaikančiomis IRT sistemomis, bent kartą per metus, taip pat padarius bet kokius esminius pakeitimus ypatingos svarbos arba svarbias funkcijas palaikančiose IRT sistemose;

b) testuoja pagal 14 straipsnį parengtus krizės komunikacijos planus.

Pirmos pastraipos a punkto tikslais finansų sektoriaus subjektai, išskyrus labai mažas įmones, į testavimo planus įtraukia kibernetinių išpuolių ir pirminės IRT infrastruktūros pakeitimo atsarginiais pajėgumais, atsarginėmis kopijomis ir atsarginiais įrenginiais, būtinais 12 straipsnyje nustatytoms pareigoms įvykdyti, scenarijus.

Finansų sektoriaus subjektai reguliariai peržiūri savo IRT veiklos tęstinumo politiką ir IRT reagavimo ir veiklos atkūrimo planus, atsižvelgdami į pagal pirmą pastraipą atliktų testų rezultatus ir rekomendacijas, pateiktas atlikus audito patikras arba priežiūrinį tikrinimą.

7. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, įdiegia krizių valdymo funkciją, kuri, pradėjus įgyvendinti IRT veiklos tęstinumo planus arba IRT reagavimo ir veiklos atkūrimo planus, nustato, *inter alia*, aiškias vidaus ir išorės pranešimų krizės atveju valdymo procedūras pagal 14 straipsnį.

8. Kai pradedami įgyvendinti IRT veiklos tęstinumo planai arba IRT reagavimo ir veiklos atkūrimo planai, finansų sektoriaus subjektai saugo įrašus apie veiklą iki sutrikdymo įvykių ir jų metu ir šie įrašai turi būti prieinami bet kuriuo metu.

9. Centriniai vertybinių popierių depozitoriumai pateikia kompetentingoms institucijoms IRT veiklos tęstinumo testų ar panašių tikrinimų rezultatų kopijas.

10. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, kompetentingoms institucijoms jų prašymu praneša apie preliminariai apskaičiuotas bendras metines išlaidas ir nuostolius, patirtus dėl didelių su IRT susijusių incidentų.

11. Vadovaujantis reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 16 straipsniu, EPI Jungtiniame komitete ne vėliau kaip 2024 m. liepos 17 d. parengia bendras 10 dalyje nurodytų preliminaraus bendrų metinių išlaidų ir nuostolių apskaičiavimo gaires.

12 straipsnis

Atsarginių kopijų politika ir procedūros, atstatymo ir atkūrimo procedūros ir metodai

1. Siekdami užtikrinti, kad IRT sistemos ir duomenys būtų atstatyti kuo greičiau, kuo mažiau sutrikdant ir patiriant kuo mažiau nuostolių, finansų sektoriaus subjektai, įgyvendindami savo IRT rizikos valdymo sistemą, parengia ir dokumentais pagrindžia:

a) atsarginių kopijų politiką ir procedūras, kuriose nurodoma duomenų, kurių atsarginės kopijos daromos, apimtis ir minimalus atsarginių kopijų darymo dažnumas, remiantis ypatinga informacijos svarba arba duomenų konfidencialumo lygiu;

b) atstatymo ir atkūrimo procedūras ir metodus.

2. Finansų sektoriaus subjektai sukuria atsargines sistemas, kurios gali būti aktyvuotos pagal atsarginių kopijų politiką ir procedūras, taip pat atstatymo ir atkūrimo procedūras ir metodus. Atsarginių sistemų aktyvavimas turi nekelti pavojaus tinklų ir informacinių sistemų saugumui arba duomenų prieinamumui, autentiškumui, vientisumui ir konfidencialumui. Periodiškai atliekamas atsarginių kopijų procedūrų ir atstatymo bei atkūrimo procedūrų ir metodų testavimas.

3. Tais atvejais, kai atstato atsarginius duomenis naudodamiesi savo pačių sistemomis, finansų sektoriaus subjektai naudoja IRT sistemas, kurios yra fiziškai ir loginiu būdu atskirtos nuo šaltinio IRT sistemos. IRT sistemos turi būti patikimai apsaugotos nuo bet kokios neteisėtos prieigos ar IRT sugadinimo ir turi leisti laiku atkurti paslaugas, prireikus panaudojant duomenų ir sistemų atsargines kopijas.

Pagrindinių sandorio šalių atveju veiklos atkūrimo planais suteikiama galimybė atkurti visus sandorius sutrikimo momentu, kad pagrindinė sandorio šalis galėtų patikimai tęsti savo veiklą ir numatytą dieną užbaigti atsiskaitymą.

Be to, duomenų paslaugų teikėjai turi turėti pakankamai išteklių ir atsarginių kopijų ir atkūrimo įrenginius, kad galėtų visada siūlyti ir teikti savo paslaugas.

4. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, turi turėti atsarginius IRT pajėgumus, kurių ištekliai, galimybės ir funkcijos būtų tinkami veiklos poreikiams užtikrinti. Labai mažos įmonės įvertina poreikį turėti tokius atsarginius IRT pajėgumus remdamosi savo rizikos profiliu.

5. Centriniai vertybinių popierių depozitoriumai turi turėti bent vieną antrinę duomenų tvarkymo vietą, kuriai būtų skirti tinkami ištekliai, pajėgumai, funkcijos ir numatytas personalas veiklos poreikiams užtikrinti.

Antrinė duomenų tvarkymo vieta turi:

a) būti geografiškai nutolusi nuo pirminės duomenų tvarkymo vietos, siekiant užtikrinti, kad jos rizikos profilis būtų kitoks ir jai nedarytų poveikio įvykis, paveikęs pirminę vietą;

b) galėti užtikrinti ypatingos svarbos arba svarbių funkcijų tęstinumą taip pat kaip ir pirminė vieta arba užtikrinti tokį paslaugų lygį, kuris būtinas, kad finansų sektoriaus subjektas galėtų atlikti savo ypatingos svarbos operacijas pagal savo veiklos atkūrimo tikslus;

c) būti iš karto prieinama finansų sektoriaus subjekto darbuotojams, kad būtų užtikrintas ypatingos svarbos arba svarbių funkcijų tęstinumas tuo atveju, jei pirminė duomenų tvarkymo vieta taptų neprieinama.

6. Nustatydami kiekvienos funkcijos atkūrimo laiko ir taško tikslus, finansų sektoriaus subjektai atsižvelgia į tai, ar tai yra ypatingos svarbos arba svarbi funkcija, ir į galimą bendrą poveikį rinkos veiksmingumui. Tokiais atkūrimo laiko tikslais užtikrinama, kad ekstremaliais atvejais būtų užtikrinti sutarti paslaugų lygiai.

7. Atkurdami veiklą po su IRT susijusio incidento finansų sektoriaus subjektai atlieka reikiamas patikras, įskaitant daugkartines patikras ir sutikrinimus, siekdami užtikrinti, kad būtų išlaikytas aukščiausias duomenų vientisumo lygis. Šios patikros taip pat atliekamos atkuriant išorės suinteresuotųjų šalių duomenis, siekiant užtikrinti, kad visi duomenys sistemose atitiktų.

13 straipsnis

Mokymasis ir tobulėjimas

1. Finansų sektoriaus subjektai turi turėti pajėgumų ir darbuotojų, kurie renka informaciją apie pažeidžiamumus ir kibernetines grėsmes, su IRT susijusius incidentus, visų pirma kibernetinius išpuolius, ir analizuoja jų galimą poveikį jų skaitmeninės veiklos atsparumui.

2. Finansų sektoriaus subjektai taiko peržiūras po su IRT susijusių incidentų, kurie vykdomi po to, kai sutrikdoma jų pagrindinė veikla dėl didelio su IRT susijusio incidento, ir kurių metu analizuojamos sutrikdymo priežastys ir nustatomi reikiami IRT operacijų ar 11 straipsnyje nurodytos IRT veiklos tęstinumo politikos patobulinimai.

Finansų sektoriaus subjektai, išskyrus labai mažas įmones, kompetentingų institucijų prašymu praneša joms apie pakeitimus, kurie buvo įgyvendinti atlikus peržiūras po su IRT susijusių incidentų, kaip nurodyta pirmoje pastraipoje.

Atliekant pirmoje pastraipoje nurodytas peržiūras po su IRT susijusių incidentų nustatoma, ar buvo laikomasi nustatytų procedūrų ir ar veiksmai, kurių imtasi, buvo veiksmingi, kiek tai susiję, be kita ko, su:

a) tuo, kaip greitai sureaguota į saugumo įspėjimus ir nustatytas su IRT susijusių incidentų poveikis ir jų rimtumas;

b) analitinės ekspertizės, kai ji buvo laikoma tikslinga, atlikimo kokybe ir greičiu;

c) incidento sprendimo finansų sektoriaus subjekto viduje veiksmingumu;

d) vidaus ir išorės komunikacijos veiksmingumu.

3. Į IRT rizikos vertinimo procesą nuolat tinkamai įtraukiama patirtis, įgyta vykdant skaitmeninės veiklos atsparumo testavimą pagal 26 ir 27 straipsnius ir reaguojant į realius su IRT susijusius incidentus, visų pirma kibernetinius išpuolius, taip pat į iššūkius, kilusius pradedant įgyvendinti IRT veiklos tęstinumo planus ir IRT reagavimo ir veiklos atkūrimo planus, ir atitinkama informacija, kuria keistasi su partneriais ir kuri įvertinta priežiūrinio tikrinimo metu. Tų nustatytų pastebėjimų pagrindu tinkamai peržiūrimi atitinkami 6 straipsnio 1 dalyje nurodytos IRT rizikos valdymo sistemos komponentai.

4. Finansų sektoriaus subjektai stebi savo skaitmeninės veiklos atsparumo strategijos, nurodytos 6 straipsnio 8 dalyje, įgyvendinimo veiksmingumą. Jie pažymi chronologinius IRT rizikos pokyčius, analizuoja su IRT susijusių incidentų, visų pirma kibernetinių išpuolių ir jų modelių, dažnumą, rūšis, mastą ir pokyčius, kad suprastų gresiančios IRT rizikos mastą, visų pirma kiek tai susiję su ypatingos svarbos arba svarbiomis funkcijomis, ir sustiprintų finansų sektoriaus subjekto kibernetinę brandą ir parengtį.

5. Vyresniosios grandies IRT darbuotojai bent kartą per metus valdymo organui praneša apie 3 dalyje nurodytus nustatytus pastebėjimus ir teikia rekomendacijas.

6. Finansų sektoriaus subjektai parengia ir į savo darbuotojų mokymo programas įtraukia privalomus informuotumo apie IRT saugumą programų ir skaitmeninės veiklos atsparumo mokymų modulius. Tos programos ir mokymai taikomi visiems darbuotojams ir vyresniosios vadovybės darbuotojams, o jų sudėtingumas turi būti proporcingas jų pareigas atitinkantiems įgaliojimams. Kai tinkama, finansų sektoriaus subjektai į savo atitinkamas mokymo programas taip pat įtraukia IRT paslaugas teikiančias trečiąsias šalis pagal 30 straipsnio 2 dalies i punktą.

7. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, nuolat stebi atitinkamus technologinius pokyčius, taip pat siekdami suprasti galimą tokių naujų technologijų diegimo poveikį IRT saugumo reikalavimams ir skaitmeninės veiklos atsparumui. Jie nuolat atnaujina savo žinias apie naujausius IRT rizikos valdymo procesus, kad galėtų veiksmingai kovoti su esamų ar naujų formų kibernetiniais išpuoliais.

14 straipsnis

Komunikacija

1. Finansų sektoriaus subjektai, įgyvendindami 6 straipsnio 1 dalyje nurodytą IRT rizikos valdymo sistemą, nustato krizių komunikacijos planus, pagal kuriuos būtų galima atsakingai atskleisti informaciją apie bent didelius su IRT susijusius incidentus arba pažeidžiamumus atitinkamai klientams ir partneriams, taip pat visuomenei.

2. Kaip IRT rizikos valdymo sistemos dalį, finansų sektoriaus subjektai įgyvendina komunikacijos politiką, skirtą vidaus darbuotojams ir išorės suinteresuotiesiems subjektams. Darbuotojams skirtoje komunikacijos politikoje atsižvelgiama į poreikį atskirti IRT rizikos valdymo srities darbuotojus, visų pirma, atsakingus už reagavimą ir veiklos atkūrimą, ir darbuotojus, kurie turi būti informuoti.

3. Bent vienam finansų sektoriaus subjekto darbuotojui pavedama įgyvendinti su IRT susijusių incidentų komunikacijos strategiją ir tuo tikslu vykdyti atstovo ryšiams su visuomene ir žiniasklaida funkciją.

15 straipsnis

Tolesnis IRT rizikos valdymo priemonių, metodų, procesų ir politikos derinimas

EPI Jungtiniame komitete, konsultuodamosi su Europos Sąjungos kibernetinio saugumo agentūra (ENISA), parengia bendrų techninių reguliavimo standartų projektus, kuriais siekiama:

a) išsamiau nurodyti elementus, kurie turi būti įtraukti į 9 straipsnio 2 dalyje nurodytą IRT saugumo politiką, procedūras, protokolus ir priemones, siekiant užtikrinti tinklų saugumą, sudaryti sąlygas taikyti tinkamas apsaugos nuo įsibrovimo ir netinkamo duomenų naudojimo priemones, išsaugoti duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą, įskaitant kriptografinius metodus, ir užtikrinti tikslų ir greitą duomenų perdavimą be didelių sutrikimų ir nepagrįsto vėlavimo;

b) plėtoti papildomus 9 straipsnio 4 dalies c punkte nurodytų prieigos valdymo teisių kontrolės priemonių komponentus ir susijusią žmogiškųjų išteklių politiką, nurodant prieigos teises, teisių suteikimo ir atšaukimo procedūras, neįprasto elgesio, susijusio su IRT rizika, stebėseną pagal atitinkamus rodiklius, įskaitant tinklo naudojimo modelius, valandas, IT veiklą ir nežinomus įrenginius;

c) toliau plėtoti 10 straipsnio 1 dalyje nurodytus mechanizmus, kuriuos naudojant galima greitai aptikti neįprastą veiklą, ir 10 straipsnio 2 dalyje nurodytus kriterijus, kuriuos įvykdžius pradedami su IRT susijusių incidentų aptikimo ir reagavimo į juos procesai;

d) patikslinti 11 straipsnio 1 dalyje nurodytos IRT veiklos tęstinumo politikos komponentus;

e) patikslinti 11 straipsnio 6 dalyje nurodytų IRT veiklos tęstinumo planų testavimą siekiant užtikrinti, kad atliekant tokį testavimą būtų tinkamai atsižvelgiama į scenarijus, pagal kuriuos ypatingos svarbos arba svarbios funkcijos vykdymo kokybė suprastėja iki nepriimtino lygio arba yra nepatenkinama, ir tinkamai atsižvelgiama į galimą bet kurios atitinkamos IRT paslaugas teikiančios trečiosios šalies nemokumo ar kitokio įsipareigojimų nevykdymo poveikį ir, kai aktualu, politinę riziką atitinkamų paslaugų teikėjų jurisdikcijose;

f) patikslinti 11 straipsnio 3 dalyje nurodytų IRT reagavimo ir veiklos atkūrimo planų komponentus;

g) patikslinti 6 straipsnio 5 dalyje nurodytos IRT rizikos valdymo sistemos peržiūros ataskaitos turinį ir formą.

Rengdamos tuos techninių reguliavimo standartų projektus, EPI atsižvelgia į finansų sektoriaus subjekto dydį ir bendrą rizikos profilį, taip pat į jo paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą, kartu deramai atsižvelgdamos į visas konkrečias ypatybes, atsirandančias dėl individualaus veiklos pobūdžio skirtinguose finansinių paslaugų sektoriuose.

EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai ne vėliau kaip 2024 m. sausio 17 d.

Komisijai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsnius suteikiami įgaliojimai papildyti šį reglamentą priimant pirmoje pastraipoje nurodytus techninius reguliavimo standartus.

16 straipsnis

Supaprastinta IRT rizikos valdymo sistema

1. Šio reglamento 5–15 straipsniai netaikomi mažoms ir tarpusavio sąsajų neturinčioms investicinėms įmonėms, mokėjimo įstaigoms, kurioms taikoma išimtis pagal Direktyvą (ES) 2015/2366, įstaigoms, kurioms taikoma išimtis pagal Direktyvą 2013/36/ES ir kurioms valstybės narės nusprendė netaikyti šio reglamento 2 straipsnio 4 dalyje nurodytos galimybės, elektroninių pinigų įstaigoms, kurioms taikoma išimtis pagal Direktyvą 2009/110/EB ir mažoms profesinių pensijų įstaigoms.

Nedarant poveikio pirmai pastraipai subjektai, nurodyti pirmoje pastraipoje:

a) nustato ir taiko patikimą ir dokumentais pagrįstą IRT rizikos valdymo sistemą, kurioje išsamiai apibūdinami mechanizmai ir priemonės, skirtos greitam, veiksmingam ir visapusiškam IRT rizikos valdymui, be kita ko, siekiant apsaugoti atitinkamus fizinius komponentus ir infrastruktūrą;

b) vykdo nuolatinę visų IRT sistemų saugumo ir veikimo stebėseną;

c) kuo labiau sumažina IRT rizikos poveikį naudodami patikimas, atsparias ir atnaujinamas IRT sistemas, protokolus ir priemones, kurie yra tinkami jų veiklos vykdymui ir paslaugų teikimui palaikyti ir tinkamai apsaugo tinklų ir informacinių sistemų duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą;

d) sudaro sąlygas tinklų ir informacinėse sistemose greitai nustatyti ir aptikti IRT rizikos šaltinius ir anomalijas ir skubiai pašalinti su IRT susijusius incidentus;

e) nustato pagrindinę priklausomybę nuo IRT paslaugas teikiančių trečiųjų šalių;

f) užtikrina ypatingos svarbos arba svarbių funkcijų tęstinumą, vykdydami veiklos tęstinumo planus ir reagavimo ir veiklos atkūrimo priemones, kurios apima bent su atsarginėmis kopijomis susijusias ir atstatymo priemones;

g) reguliariai testuoja f punkte nurodytus planus ir priemones, taip pat pagal a ir c punktus taikomos kontrolės veiksmingumą;

h) atitinkamai įgyvendina atitinkamas su veikla susijusias išvadas, parengtas atlikus g punkte nurodytą testavimą ir analizę po incidento, plėtodami IRT rizikos vertinimo procesą ir, atsižvelgdami į poreikius ir IRT rizikos profilį, parengia IRT saugumo informavimo programas ir skaitmeninės veiklos atsparumo mokymus darbuotojams ir vadovybei.

2. 1 dalies antros pastraipos a punkte nurodyta IRT rizikos valdymo sistema pagrindžiama dokumentais ir peržiūrima periodiškai ir įvykus dideliems su IRT susijusiems incidentams, laikantis priežiūros nurodymų. Ji nuolat tobulinama remiantis įgyvendinimo ir stebėsenos patirtimi. Kompetentingai institucijai paprašius, jai pateikiama IRT rizikos valdymo sistemos peržiūros ataskaita.

3. EPI Jungtiniame komitete, konsultuodamosi su ENISA, parengia bendrų techninių reguliavimo standartų projektus, kuriais siekiama:

a) patikslinti elementus, kurie turi būti įtraukti į 1 dalies antros pastraipos a punkte nurodytą IRT rizikos valdymo sistemą;

b) patikslinti elementus, susijusius su sistemomis, protokolais ir priemonėmis, skirtais kuo labiau sumažinti IRT rizikos poveikį, kaip nurodyta 1 dalies antros pastraipos c punkte, siekiant užtikrinti tinklų saugumą, sudaryti sąlygas taikyti tinkamas apsaugos nuo įsibrovimo ir netinkamo duomenų naudojimo priemones ir išsaugoti duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą;

c) patikslinti 1 dalies antros pastraipos f punkte nurodytų IRT veiklos tęstinumo planų komponentus;

d) patikslinti veiklos tęstinumo planų testavimo taisykles ir užtikrinti 1 dalies antros pastraipos g punkte nurodytų kontrolės priemonių veiksmingumą, bei užtikrinti, kad atliekant tokį testavimą būtų tinkamai atsižvelgiama į scenarijus, pagal kuriuos ypatingos svarbos arba svarbios funkcijos vykdymo kokybė suprastėja iki nepriimtino lygio arba yra nepatenkinama;

e) patikslinti 2 dalyje nurodytos IRT rizikos valdymo sistemos peržiūros ataskaitos turinį ir formą.

Rengdamos tų techninių reguliavimo standartų projektus, EPI atsižvelgia į finansų sektoriaus subjekto dydį ir bendrą rizikos profilį, taip pat į jo paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą.

EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai ne vėliau kaip 2024 m. sausio 17 d.

Komisijai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsnius suteikiami įgaliojimai papildyti šį reglamentą priimant pirmoje pastraipoje nurodytus techninius reguliavimo standartus.

III SKYRIUS

Su IRT susijusių incidentų valdymas, klasifikavimas ir pranešimų apie juos teikimas

17 straipsnis

Su IRT susijusių incidentų valdymo procesas

1. Finansų sektoriaus subjektai apibrėžia, nustato ir įgyvendina su IRT susijusių incidentų valdymo procesą, skirtą su IRT susijusiems incidentams aptikti, valdyti ir apie juos pranešti.

2. Finansų sektoriaus subjektai registruoja visus su IRT susijusius incidentus ir dideles kibernetines grėsmes. Finansų sektoriaus subjektai nustato tinkamas procedūras ir procesus, kad užtikrintų nuoseklią ir integruotą su IRT susijusių incidentų stebėseną, jų šalinimą ir tolesnius susijusius veiksmus ir tokiu būdu užtikrintų, kad būtų nustatytos, dokumentuotos ir pašalintos pagrindinės priežastys, siekiant užkirsti kelią tokiems incidentams.

3. 1 dalyje nurodytu su IRT susijusių incidentų valdymo procesu:

a) nustatomi ankstyvojo perspėjimo rodikliai;

b) nustatomos procedūros dėl su IRT susijusių incidentų nustatymo, atsekimo, registravimo, kategorizavimo ir klasifikavimo pagal jų prioritetą ir rimtumą, taip pat paslaugų, kurioms daromas poveikis, ypatingą svarbą, remiantis 18 straipsnio 1 dalyje nurodytais kriterijais;

c) priskiriamos pareigos ir atsakomybė, kurios turi būti pradėtos taikyti skirtingų rūšių su IRT susijusių incidentų ir scenarijų atvejais;

d) atitinkamai nustatomi komunikacijos su darbuotojais, išorės suinteresuotaisiais subjektais ir žiniasklaida planai pagal 14 straipsnį ir pranešimo klientams planai, planai dėl sprendimo finansų sektoriaus subjekto viduje procedūrų, įskaitant su IRT susijusių klientų skundų nagrinėjimą, taip pat planai dėl informacijos teikimo finansų sektoriaus subjektams, kurie veikia kaip partneriai;

e) užtikrinama, kad bent apie didelius su IRT susijusius incidentus būtų pranešama atitinkamai vyresniajai vadovybei, o valdymo organui būtų teikiama informacija bent apie didelius su IRT susijusius incidentus, paaiškinant poveikį, reagavimo veiksmus ir papildomas kontrolės priemones, kurios turi būti nustatytos dėl tokių su IRT susijusių incidentų;

f) nustatomos reagavimo į su IRT susijusius incidentus procedūros, kad būtų sumažintas poveikis ir užtikrinta, kad laiku būtų atkurtas saugus paslaugų teikimas.

18 straipsnis

Su IRT susijusių incidentų ir kibernetinių grėsmių klasifikavimas

1. Finansų sektoriaus subjektai su IRT susijusius incidentus klasifikuoja ir jų poveikį nustato remdamiesi šiais kriterijais:

a) klientų arba finansų partnerių, kurių veikla buvo sutrikdyta dėl su IRT susijusio incidento, skaičius ir (arba) svarbumas, taip pat, kai taikytina, sandorių, kuriuos sutrikdė su IRT susijęs incidentas, kiekis ar skaičius ir tai, ar su IRT susijęs incidentas turėjo poveikį reputacijai;

b) su IRT susijusio incidento trukmė, įskaitant laiką, kurį nebuvo teikiamos paslaugos;

c) geografinis pasiskirstymas su IRT susijusio incidento paveiktose vietovėse, ypač jei poveikis padarytas daugiau nei dviem valstybėms narėms;

d) duomenų praradimas dėl su IRT susijusio incidento, kiek tai susiję su duomenų prieinamumu, autentiškumu, vientisumu ir konfidencialumu;

e) paveiktų paslaugų, įskaitant finansų sektoriaus subjekto sandorius ir operacijas, ypatinga svarba;

f) su IRT susijusio incidento ekonominis poveikis, visų pirma tiesioginės ir netiesioginės sąnaudos ir nuostoliai, tiek absoliučiąja, tiek santykine verte.

2. Finansų sektoriaus subjektai kibernetines grėsmes klasifikuoja kaip dideles atsižvelgdami į paslaugų, kurioms kyla rizika, įskaitant finansų sektoriaus subjekto sandorius ir operacijas, ypatingą svarbą, klientų arba finansų partnerių, kuriems gresia rizika, skaičių ir (arba) svarbumą ir geografinį vietovių, kurioms kyla rizika, pasiskirstymą.

3. EPI Jungtiniame komitete, konsultuodamosi su ECB ir ENISA, parengia bendrų techninių reguliavimo standartų projektus, kuriuose patikslinami:

a) 1 dalyje nustatyti kriterijai, įskaitant reikšmingumo ribas, pagal kurias nustatomi dideli su IRT susiję incidentai arba, jei taikytina, dideli su mokėjimais susiję operaciniai arba saugumo incidentai, kuriems taikoma 19 straipsnio 1 dalyje nustatyta pareiga pranešti;

b) kriterijai, kuriuos turi taikyti kompetentingos institucijos vertindamos didelių su IRT susijusių incidentų arba, jei taikytina, didelių su mokėjimais susijusių operacinių arba saugumo incidentų svarbą kompetentingoms institucijoms kitose valstybėse narėse, ir pranešimų apie didelius su IRT susijusius incidentus arba, jei taikytina, didelius su mokėjimais susijusius operacinius arba saugumo incidentus duomenys, kuriais turi būti dalijamasi su kitomis kompetentingomis institucijomis pagal 19 straipsnio 6 ir 7 dalis.

c) šio straipsnio 2 dalyje nustatyti kriterijai, įskaitant didelio reikšmingumo ribas, pagal kurias nustatomos didelės kibernetinės grėsmės.

4. Rengdamos šio straipsnio 3 dalyje nurodytus bendrų techninių reguliavimo standartų projektus, EPI atsižvelgia į 4 straipsnio 2 dalyje nustatytus kriterijus, taip pat į tarptautinius standartus, taip pat ENISA parengtas ir paskelbtas gaires ir specifikacijas, įskaitant, kai tinkama, kitiems ekonomikos sektoriams skirtas specifikacijas. Taikydamos 4 straipsnio 2 dalyje nustatytus kriterijus, EPI deramai atsižvelgia į labai mažų įmonių ir mažųjų bei vidutinių įmonių poreikį sutelkti pakankamai išteklių ir pajėgumų, kad būtų užtikrintas spartus su IRT susijusių incidentų valdymas.

EPI tuos bendrus techninių reguliavimo standartų projektus pateikia Komisijai ne vėliau kaip 2024 m. sausio 17 d.

Komisijai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsnius suteikiami įgaliojimai papildyti šį reglamentą priimant 3 dalyje nurodytus techninius reguliavimo standartus.

19 straipsnis

Pranešimų apie didelius su IRT susijusius incidentus teikimas ir savanoriškas pranešimas apie dideles kibernetines grėsmes

1. Pagal šio straipsnio 4 dalį finansų sektoriaus subjektai praneša apie didelius su IRT susijusius incidentus atitinkamai kompetentingai institucijai, kaip nurodyta 46 straipsnyje.

Kai finansų sektoriaus subjektą prižiūri daugiau nei viena nacionalinė kompetentinga institucija, nurodyta 46 straipsnyje, valstybės narės paskiria vieną bendrą kompetentingą instituciją atitinkama kompetentinga institucija, atsakinga už šiame straipsnyje numatytų funkcijų ir pareigų vykdymą.

Kredito įstaigos, pagal Reglamento (ES) Nr. 1024/2013 6 straipsnio 4 dalį klasifikuojamos kaip svarbios, apie didelius su IRT susijusius incidentus praneša atitinkamai nacionalinei kompetentingai institucijai, paskirtai pagal Direktyvos 2013/36/ES 4 straipsnį, o pastaroji nedelsdama perduoda tą pranešimą ECB.

Taikant pirmą pastraipą, finansų sektoriaus subjektai, surinkę ir išanalizavę visą susijusią informaciją, parengia pradinį pranešimą ir pranešimus, nurodytus šio straipsnio 4 dalyje, naudodami 20 straipsnyje nurodytus šablonus ir pateikia juos kompetentingai institucijai. Tuo atveju, kai dėl techninių priežasčių negalima pateikti pradinio pranešimo naudojant šabloną, finansų sektoriaus subjektai pateikia pranešimą kompetentingai institucijai alternatyviomis priemonėmis.

Pradiniame pranešime ir pranešimuose, nurodytuose 4 dalyje, pateikiama visa informacija, būtina kompetentingai institucijai, kad ji galėtų nustatyti didelio su IRT susijusio incidento reikšmingumą ir įvertinti galimą tarpvalstybinį poveikį.

Nedarant poveikio finansų sektoriaus subjekto vykdomam pranešimų atitinkamai kompetentingai institucijai teikimui pagal pirmą pastraipą, valstybės narės gali papildomai nustatyti, kad kai kurie ar visi finansų sektoriaus subjektai taip pat teikia pradinį pranešimą ir kiekvieną šio straipsnio 4 dalyje nurodytą pranešimą naudodami 20 straipsnyje nurodytus šablonus, nacionalinėms kompetentingoms institucijoms arba reagavimo į kompiuterių saugumo incidentus tarnyboms (CSIRT), paskirtoms arba įsteigtoms pagal Direktyvą (ES) 2022/2555.

2. Finansų sektoriaus subjektai gali savanoriškai pranešti atitinkamai kompetentingai institucijai apie dideles kibernetines grėsmes, jeigu jie mano, kad grėsmė yra svarbi finansų sistemai, paslaugų naudotojams ar klientams. Atitinkama kompetentinga institucija gali pateikti tokią informaciją kitoms atitinkamoms institucijoms, nurodytoms 6 dalyje.

Kredito įstaigos, pagal Reglamento (ES) Nr. 1024/2013 6 straipsnio 4 dalį klasifikuojamos kaip svarbios, gali savanoriškai pranešti apie dideles kibernetines grėsmes atitinkamai nacionalinei kompetentingai institucijai, paskirtai pagal Direktyvos 2013/36/ES 4 straipsnį, o pastaroji nedelsdama perduoda tą pranešimą ECB.

Valstybės narės gali nustatyti, kad tie finansų sektoriaus subjektai, kurie savanoriškai pateikia pranešimą pagal pirmą pastraipą, taip pat gali perduoti tą pranešimą CSIRT, paskirtoms arba įsteigtoms pagal Direktyvą (ES) 2022/2555.

3. Kai įvyksta didelis su IRT susijęs incidentas ir jis daro poveikį klientų finansiniams interesams, finansų sektoriaus subjektai nepagrįstai nedelsdami, iš karto, kai sužino apie šį incidentą, informuoja savo klientus apie didelį su IRT susijusį incidentą ir apie priemones, kurių imtasi tokio incidento neigiamam poveikiui sumažinti.

Didelės kibernetinės grėsmės atveju finansų sektoriaus subjektai, kai taikytina, informuoja savo klientus, kuriems gali būti padarytas poveikis, apie visas tinkamas apsaugos priemones, kurių pastarieji, apsvarstę, galėtų imtis.

4. Finansų sektoriaus subjektai, laikydamiesi laiko terminų, kurie turi būti nustatyti pagal 20 straipsnio pirmos pastraipos a punkto ii papunktį, atitinkamai kompetentingai institucijai pateikia:

a) pradinį pranešimą;

b) tarpinį pranešimą, pateikiamą po a punkte nurodyto pradinio pranešimo, kai tik pirminio incidento padėtis reikšmingai pasikeičia arba, remiantis nauja turima informacija, pasikeičia didelio su IRT susijusio incidento šalinimo būdai, vėliau atitinkamai teikiant atnaujintus pranešimus kiekvieną kartą, kai esama naujos informacijos apie padėtį, taip pat gavus konkretų kompetentingos institucijos prašymą;

c) galutinį pranešimą, kai užbaigiama pagrindinės priežasties analizė, neatsižvelgiant į tai, ar poveikio mažinimo priemonės jau įgyvendintos, ir kai esama faktinių poveikio duomenų, kuriais galima pakeisti įverčius.

5. Finansų sektoriaus subjektai gali, laikydamiesi Sąjungos ir nacionalinės sektorių teisės, paslaugas teikiančiai trečiajai šaliai perduoti pareigas pranešti pagal šį straipsnį. Tokio perdavimo atveju finansų sektoriaus subjektas išlieka visiškai atsakingas už reikalavimų pranešti apie incidentus vykdymą.

6. Gavusi pradinį pranešimą ir kiekvieną 4 dalyje nurodytą pranešimą, kompetentinga institucija laiku pateikia duomenis apie didelį su IRT susijusį incidentą šiems gavėjams, remdamasi, kai taikytina, jų atitinkama kompetencija:

a) EBI, ESMA arba EIOPA;

b) ECB, 2 straipsnio 1 dalies a, b ir d punktuose nurodytų finansų sektoriaus subjektų atveju;

c) kompetentingoms institucijoms, bendriesiems informaciniams centrams arba CSIRT, paskirtiems arba įsteigtiems pagal Direktyvą (ES) 2022/2555;

d) pertvarkymo institucijoms, kaip nurodyta Direktyvos 2014/59/ES 3 straipsnyje, ir Bendrai pertvarkymo valdybai (BPV), kiek tai susiję su Europos Parlamento ir Tarybos reglamento (ES) Nr. 806/2014 ([37]) 7 straipsnio 2 dalyje nurodytais subjektais ir kiek tai susiję su Reglamento (ES) Nr. 806/2014 7 straipsnio 4 dalies b punkte ir 5 dalyje nurodytais subjektais ir grupėmis, jei tokie duomenys susiję su incidentais, kurie kelia riziką ypatingos svarbos funkcijų, kaip tai suprantama Direktyvos 2014/59/ES 2 straipsnio 1 dalies 35 punkte, užtikrinimui, ir

e) kitoms atitinkamoms valdžios institucijoms pagal nacionalinę teisę.

7. Gavę informaciją pagal 6 dalį, EBI, ESMA arba EIOPA ir ECB, pasikonsultavę su ENISA ir bendradarbiaudami su atitinkama kompetentinga institucija, įvertina, ar didelis su IRT susijęs incidentas yra svarbus kompetentingoms institucijoms kitose valstybėse narėse. Atlikusios tą vertinimą, EBI, ESMA arba EIOPA kuo greičiau pateikia atitinkamą pranešimą atitinkamoms kompetentingoms institucijoms kitose valstybėse narėse. ECB informuoja Europos centrinių bankų sistemos narius apie su mokėjimo sistema susijusias problemas. Remdamosi tuo pranešimu, kompetentingos institucijos, kai tinkama, imasi visų būtinų priemonių, kad nebūtų sutrikdytas tiesioginis finansų sistemos stabilumas.

([37]) 2014 m. liepos 15 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 806/2014, kuriuo nustatomos kredito įstaigų ir tam tikrų investicinių įmonių pertvarkymo vienodos taisyklės ir vienoda procedūra, kiek tai susiję su bendru pertvarkymo mechanizmu ir Bendru pertvarkymo fondu, ir iš dalies keičiamas Reglamentas (ES) Nr. 1093/2010 (OL L 225, 2014 7 30, p. 1).

8. Pranešimas, kurį ESMA turi pateikti pagal šio straipsnio 7 dalį, nedaro poveikio kompetentingos institucijos pareigai skubiai perduoti duomenis apie didelį su IRT susijusį incidentą atitinkamai priimančiosios valstybės narės institucijai, kai centrinis vertybinių popierių depozitoriumas priimančiojoje valstybėje narėje vykdo reikšmingą tarpvalstybinę veiklą, didelis su IRT susijęs incidentas gali turėti rimtų pasekmių priimančiosios valstybės narės finansų rinkoms ir jei kompetentingos institucijos, susijusios su finansų sektoriaus subjektų priežiūra, yra sudariusios bendradarbiavimo susitarimus.

20 straipsnis

Pranešimų turinio ir šablonų derinimas

EPI Jungtiniame komitete, konsultuodamosi su ENISA ir ECB, parengia:

a) bendrų techninių reguliavimo standartų projektus, kuriais siekiama:

   i) nustatyti pranešimų apie didelius su IRT susijusius incidentus turinį, siekiant atspindėti 18 straipsnio 1 dalyje nustatytus kriterijus ir įtraukti kitus elementus, pavyzdžiui, duomenis, pagal kuriuos nustatoma pranešimo kitoms valstybėms narėms svarba ir tai, ar incidentas yra didelis su mokėjimu susijęs operacinis arba saugumo incidentas;

   ii) nustatyti pradinio pranešimo ir kiekvieno 19 straipsnio 4 dalyje nurodyto pranešimo pateikimo laiko terminus;

   iii) nustatyti pranešimo apie dideles kibernetines grėsmes turinį.

   Rengdamos tuos techninių reguliavimo standartų projektus, EPI atsižvelgia į finansų sektoriaus subjekto dydį ir bendrą rizikos profilį, taip pat į jo paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą, visų pirma siekdamos užtikrinti, kad šios pastraipos a punkto ii papunkčio tikslais skirtingi laiko terminai galėtų atitinkamai atspindėti finansų sektorių ypatumus, nedarant poveikio nuoseklaus požiūrio į pranešimų apie su IRT susijusius incidentus teikimą pagal šį reglamentą ir pagal Direktyvą (ES) 2022/2555 išlaikymui. EPI, kai taikytina, pateikia pagrindimą, kai nukrypstama nuo požiūrių, kurių laikomasi tos direktyvos kontekste;

b) bendrų techninių įgyvendinimo standartų projektus, kad būtų nustatytos standartinės formos, šablonai ir procedūros, skirti finansų sektoriaus subjektams siekiant pranešti apie didelį su IRT susijusį incidentą ir pranešti apie didelę kibernetinę grėsmę.

EPI pateikia pirmos pastraipos a punkte nurodytus bendrų techninių reguliavimo standartų projektus ir pirmos pastraipos b punkte nurodytus bendrų techninių įgyvendinimo standartų projektus Komisijai ne vėliau kaip 2024 m. liepos 17 d.

Komisijai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsnius suteikiami įgaliojimai papildyti šį reglamentą priimant pirmos pastraipos a punkte nurodytus bendrus techninius reguliavimo standartus.

Komisijai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 15 straipsnį suteikiami įgaliojimai priimti pirmos pastraipos b punkte nurodytus bendrus techninius įgyvendinimo standartus.

21 straipsnis

Pranešimų apie didelius su IRT susijusius incidentus teikimo centralizavimas

1. EPI Jungtiniame komitete, konsultuodamosi su ECB ir ENISA, parengia bendrą ataskaitą, kurioje įvertinama galimybė toliau centralizuoti pranešimų apie incidentus teikimą, įsteigiant vieną bendrą ES centrą, kuriam finansų sektoriaus subjektai teiktų pranešimus apie didelius su IRT susijusius incidentus. Bendroje ataskaitoje nagrinėjami būdai, kaip palengvinti pranešimų apie su IRT susijusius incidentus srautą, sumažinti susijusias išlaidas ir prisidėti prie teminių analizių, siekiant didinti priežiūros konvergenciją.

2. 1 dalyje nurodytą bendrą ataskaitą sudaro bent šie elementai:

a) išankstinės vieno bendro ES centro įsteigimo sąlygos;

b) nauda, apribojimai ir rizika, įskaitant riziką, susijusią su didele neskelbtinos informacijos koncentracija;

c) būtini pajėgumai siekiant užtikrinti sąveikumą, kiek tai susiję su kitomis atitinkamomis pranešimų teikimo sistemomis;

d) operacinio valdymo elementai;

e) narystės sąlygos;

f) techninė tvarka, reglamentuojanti finansų sektoriaus subjektų ir nacionalinių kompetentingų institucijų prieigą prie vieno bendro ES centro;

g) preliminarus finansinių išlaidų, susijusių su vieno bendro ES centro veiklos platformos sukūrimu, įskaitant būtinas ekspertines žinias, įvertinimas.

3. EPI pateikia 1 dalyje nurodytą ataskaitą Europos Parlamentui, Tarybai ir Komisijai ne vėliau kaip 2025 m. sausio 17 d.

22 straipsnis

Priežiūros grįžtamoji informacija

1. Nedarant poveikio techniniam indėliui, rekomendacijoms ar taisomosioms priemonėms ir tolesnei informacijai, kuriuos gali pateikti, kai taikytina, laikantis nacionalinės teisės, CSIRT, įsteigtos pagal Direktyvą (ES) 2022/2555, kompetentinga institucija, gavusi pradinį pranešimą ir kiekvieną pranešimą, nurodytą 19 straipsnio 4 dalyje, patvirtina, kad pranešimą gavo, ir gali, kai įmanoma, finansų sektoriaus subjektui laiku pateikti aktualią ir proporcingą grįžtamąją informaciją arba aukšto lygio gairių, visų pirma pasidalyti visa aktualia anonimizuota informacija ir panašia žvalgybos informacija apie grėsmes, ir gali aptarti finansų sektoriaus subjekto lygmeniu taikomas taisomąsias priemones ir būdus kuo labiau sumažinti ir sušvelninti neigiamą poveikį visame finansų sektoriuje. Nedarant poveikio gautai priežiūros grįžtamajai informacijai, finansų sektoriaus subjektai išlieka visiškai atsakingi už su IRT susijusių incidentų, apie kuriuos pranešta pagal 19 straipsnio 1 dalį, šalinimą ir pasekmes.

2. EPI Jungtiniame komitete, remdamosi anonimizuota ir apibendrinta informacija, kasmet parengia ataskaitą apie didelius su IRT susijusius incidentus; duomenis apie šiuos incidentus pateikia kompetentingos institucijos pagal 19 straipsnio 6 dalį; ataskaitoje bent nurodoma didelių su IRT susijusių incidentų skaičius, jų pobūdis ir poveikis finansų sektoriaus subjektų ar klientų veiklai, taisomieji veiksmai, kurių buvo imtasi, ir patirtos išlaidos.

EPI skelbia įspėjimus ir rengia aukšto lygio statistinius duomenis, kuriais remiamasi vertinant IRT grėsmes ir pažeidžiamumus.

23 straipsnis

Su mokėjimais susiję operaciniai arba saugumo incidentai, susiję su kredito įstaigomis, mokėjimo įstaigomis, informavimo apie sąskaitas paslaugų teikėjais ir elektroninių pinigų įstaigomis

Šiame skyriuje nustatyti reikalavimai taip pat taikomi su mokėjimais susijusių operacinių arba saugumo incidentų ir didelių su mokėjimais susijusių operacinių arba saugumo incidentų atveju, kai šie incidentai yra susiję su kredito įstaigomis, mokėjimo įstaigomis, informavimo apie sąskaitas paslaugų teikėjais ir elektroninių pinigų įstaigomis.

IV SKYRIUS

Skaitmeninės veiklos atsparumo testavimas

24 straipsnis

Bendrieji skaitmeninės veiklos atsparumo testavimo reikalavimai

1. Siekdami įvertinti pasirengimą spręsti su IRT susijusius incidentus, nustatyti skaitmeninės veiklos atsparumo silpnąsias vietas, trūkumus ir spragas ir skubiai įgyvendinti taisomąsias priemones, finansų sektoriaus subjektai, išskyrus labai mažas įmones, atsižvelgdami į 4 straipsnio 2 dalyje pateiktus kriterijus, parengia, taiko ir peržiūri patikimą ir išsamią skaitmeninės veiklos atsparumo testavimo programą, kaip neatsiejamą 6 straipsnyje nurodytos IRT rizikos valdymo sistemos dalį.

2. Į skaitmeninės veiklos atsparumo testavimo programą įtraukiami įvairūs vertinimai, testai, metodikos, praktika ir priemonės, kurie turi būti taikomi pagal 25 ir 26 straipsnius.

3. Vykdydami šio straipsnio 1 dalyje nurodytą skaitmeninės veiklos atsparumo testavimo programą, finansų sektoriaus subjektai, išskyrus labai mažas įmones, vadovaujasi rizika grindžiamu požiūriu, atsižvelgdami į 4 straipsnio 2 dalyje pateiktus kriterijus, tinkamai atsižvelgdami į besikeičiančią IRT rizikos panoramą, bet kokią konkrečią riziką, gresiančią ar galinčią grėsti atitinkamam finansų sektoriaus subjektui, informacinio turto ir teikiamų paslaugų ypatingą svarbą, taip pat į visus kitus veiksnius, į kuriuos atsižvelgti finansų sektoriaus subjektas laiko tinkama.

4. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, užtikrina, kad testus atliktų nepriklausomos vidaus ar išorės šalys. Kai testus atlieka vidaus testuotojas, finansų sektoriaus subjektai skiria pakankamai išteklių ir užtikrina, kad per visą testo rengimo ir vykdymo etapų laikotarpį būtų išvengta interesų konfliktų.

5. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, nustato procedūras ir politiką, pagal kuriuos visos problemos, nustatytos atliekant testus, suskirstomos pagal prioritetą, klasifikuojamos ir sprendžiamos, taip pat parengia vidaus patvirtinimo metodikas, pagal kurias užtikrinama, kad nustatytos silpnosios vietos, trūkumai ar spragos būtų visiškai pašalinti.

6. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, užtikrina, kad bent kartą per metus būtų atliekami tinkami visų IRT sistemų ir programų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, testai.

25 straipsnis

IRT priemonių ir sistemų testavimas

1. 24 straipsnyje nurodytoje skaitmeninės veiklos atsparumo testavimo programoje numatoma, laikantis 4 straipsnio 2 dalyje pateiktų kriterijų, atlikti tinkamus testus, tokius kaip pažeidžiamumo vertinimą ir skenavimą, atvirojo kodo analizę, tinklo saugumo vertinimus, spragų analizavimą, fizinio saugumo peržiūras, klausimynus ir skenavimo programinės įrangos sprendimus, jei įmanoma – pirminio kodo peržiūras, scenarijais grindžiamus testus, suderinamumo testavimą, veiklos efektyvumo testavimą, visapusį testavimą ir skverbimosi testavimą.

2. Centriniai vertybinių popierių depozitoriumai ir pagrindinės sandorio šalys atlieka pažeidžiamumo vertinimus prieš įdiegdami ar pakartotinai įdiegdami naujas ar esamas programas ir infrastruktūros komponentus ir IRT paslaugas, kuriais palaikomos finansų sektoriaus subjekto ypatingos svarbos arba svarbios funkcijos.

3. Labai mažos įmonės 1 dalyje nurodytus testus atlieka derindamos rizika grindžiamą požiūrį su strateginiu IRT testavimo planavimu, tinkamai atsižvelgdamos į poreikį išlaikyti požiūrį, pagal kurį nustatoma pusiausvyra tarp, viena vertus, išteklių ir laiko, kurie turi būti skiriami šiame straipsnyje numatytam IRT testavimui, masto ir, kita vertus, skubos, rizikos rūšies, informacinio turto ir teikiamų paslaugų ypatingos svarbos, taip pat visų kitų svarbių veiksnių, įskaitant finansų sektoriaus subjekto gebėjimą prisiimti apskaičiuotą riziką.

26 straipsnis

IRT priemonių, sistemų ir procesų pažangus testavimas taikant TLPT

1. Finansų sektoriaus subjektai, išskyrus subjektus, nurodytus 16 straipsnio 1 dalies pirmoje pastraipoje, ir išskyrus labai mažas įmones, nustatyti pagal šio straipsnio 8 dalies trečią pastraipą, bent kas trejus metus atlieka pažangų testavimą taikant TLPT. Remdamasi finansų sektoriaus subjekto rizikos profiliu ir atsižvelgdama į su veikla susijusias aplinkybes, kompetentinga institucija prireikus gali paprašyti finansų sektoriaus subjekto šį testavimą atlikti rečiau ar dažniau.

2. Kiekvienas grėsmėmis grindžiamas skverbimosi testas apima kelias ar visas finansų sektoriaus subjekto ypatingos svarbos arba svarbias funkcijas ir yra atliekamas tokias funkcijas palaikančių tikralaikių produkcijos sistemų atžvilgiu.

Finansų sektoriaus subjektai nustato visas atitinkamas pagrindines IRT sistemas, procesus ir technologijas, kuriais palaikomos ypatingos svarbos arba svarbios funkcijos ir IRT paslaugos, įskaitant tas, kuriomis palaikomos ypatingos svarbos ar svarbios funkcijos, kurių vykdymas perduotas arba pagal sutartis patikėtas vykdyti IRT paslaugas teikiančioms trečiosioms šalims.

Finansų sektoriaus subjektai įvertina, kurioms ypatingos svarbos arba svarbioms funkcijoms turi būti taikomas TLPT. Pagal šį vertinimo rezultatą nustatoma tiksli TLPT aprėptis ir šį rezultatą turi patvirtinti kompetentingos institucijos.

3. Kai IRT paslaugas teikiančios trečiosios šalys yra įtrauktos į TLPT aprėptį, finansų sektoriaus subjektas imasi būtinų priemonių ir apsaugos priemonių, kad užtikrintų tokių IRT paslaugas teikiančių trečiųjų šalių dalyvavimą TLPT, ir visada išlaiko visą atsakomybę už šio reglamento laikymosi užtikrinimą.

4. Nedarant poveikio 2 dalies pirmai ir antrai pastraipoms, tais atvejais, kai pagrįstai manoma, kad IRT paslaugas teikiančios trečiosios šalies dalyvavimas TLPT, kaip nurodyta 3 dalyje, darys neigiamą poveikį IRT paslaugas teikiančios trečiosios šalies teikiamų paslaugų klientams, kurie yra subjektai, kuriems šis reglamentas netaikomas, kokybei ar saugumui arba su tokiomis paslaugomis susijusių duomenų konfidencialumui, finansų sektoriaus subjektas ir IRT paslaugas teikianti trečioji šalis gali raštu susitarti, kad IRT paslaugas teikianti trečioji šalis tiesiogiai sudarys sutartimi įformintą susitarimą su išorės testuotoju dėl bendro TLPT, kuriame dalyvautų keli finansų sektoriaus subjektai (toliau – bendras testavimas), kuriems IRT paslaugas teikianti trečioji šalis teikia IRT paslaugas, vykdymo vadovaujant vienam paskirtam finansų sektoriaus subjektui.

Tas bendras testavimas apima atitinkamas įvairias IRT paslaugas, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, kurias finansų sektoriaus subjektai pagal sutartis patikėjo vykdyti atitinkamai IRT paslaugas teikiančiai trečiajai šaliai. Bendras testavimas laikomas TLPT, jei jį atlieka bendrame testavime dalyvaujantys finansų sektoriaus subjektai.

Bendrame testavime dalyvaujančių finansų sektoriaus subjektų skaičius tinkamai kalibruojamas atsižvelgiant į susijusių paslaugų sudėtingumą ir rūšis.

5. Finansų sektoriaus subjektai, bendradarbiaudami su IRT paslaugas teikiančiomis trečiosiomis šalimis ir kitomis susijusiomis šalimis, įskaitant testuotojus, bet išskyrus kompetentingas institucijas, taiko veiksmingas rizikos valdymo kontrolės priemones, kad sumažintų riziką, susijusią su galimu poveikiu duomenims, žala turtui ir ypatingos svarbos arba svarbių funkcijų, paslaugų ar operacijų sutrikdymu pačiame finansų sektoriaus subjekte, jo partneriuose arba finansų sektoriuje.

6. Testavimo pabaigoje, susitarus dėl ataskaitų ir koregavimo planų, finansų sektoriaus subjektas ir, kai taikoma, išorės testuotojai pateikia pagal 9 ar 10 dalį paskirtai institucijai atitinkamų rezultatų santrauką, koregavimo planus ir dokumentus, įrodančius, kad TLPT buvo atliktas laikantis reikalavimų.

7. Institucijos finansų sektoriaus subjektams išduoda pažymą, kuria patvirtinama, kad tas testas buvo atliktas laikantis dokumentuose pateiktų reikalavimų, kad kompetentingos institucijos galėtų abipusiai pripažinti grėsmėmis grindžiamus skverbimosi testus. Finansų sektoriaus subjektas apie pažymą, atitinkamų rezultatų santrauką ir koregavimo planus praneša atitinkamai kompetentingai institucijai.

Nedarant poveikio tokiai pažymai, finansų sektoriaus subjektai visada išlieka visiškai atsakingi už 4 dalyje nurodytų testų poveikį.

8. Finansų sektoriaus subjektai pagal 27 straipsnį sudaro sutartis su testuotojais dėl TLPT atlikimo. Kai finansų sektoriaus subjektai TLPT atlikti naudojasi vidaus testuotojų paslaugomis, kas trečiam testui atlikti jie sudaro sutartis su išorės testuotojais.

Kredito įstaigos, kurios yra klasifikuojamos kaip svarbios pagal Reglamento (ES) Nr. 1024/2013 6 straipsnio 4 dalį, naudojasi tik išorės testuotojų paslaugomis pagal 27 straipsnio 1 dalies a–e punktus.

Kompetentingos institucijos nustato finansų sektoriaus subjektus, kuriems būtina atlikti TLPT, atsižvelgdamos į 4 straipsnio 2 dalyje nustatytus kriterijus ir įvertinusios:

a) su poveikiu susijusius veiksnius, visų pirma koks yra finansų sektoriaus subjekto teikiamų paslaugų ir vykdomos veiklos poveikio mastas;

b) galimas finansinio stabilumo problemas, įskaitant finansų sektoriaus subjekto sisteminį pobūdį atitinkamai Sąjungos ar nacionaliniu lygmeniu;

c) finansų sektoriaus subjekto specifinį IRT rizikos profilį ir IRT brandą arba susijusias technologijų ypatybes.

9. Valstybės narės gali paskirti po vieną bendrą valdžios instituciją finansų sektoriuje, kuri nacionaliniu lygmeniu būtų atsakinga už su TLPT susijusius klausimus finansų sektoriuje, ir tuo tikslu jai patiki visą kompetenciją ir užduotis.

10. Jei tokia valdžios institucija pagal šio straipsnio 9 dalį nepaskiriama, nedarant poveikio įgaliojimams nustatyti finansų sektoriaus subjektus, kuriems būtina atlikti TLPT, kompetentinga institucija gali perduoti kai kurių arba visų šiame straipsnyje ir 27 straipsnyje nurodytų užduočių vykdymą kitai nacionalinei finansų sektoriaus institucijai.

11. EPI, susitarusios su ECB, pagal TIBER–ES sistemą parengia bendrus techninių reguliavimo standartų projektus, kuriuose patikslinama:

a) kriterijai, naudojami 8 dalies antros pastraipos taikymo tikslu;

b) reikalavimai ir standartai, reglamentuojantys naudojimąsi vidaus testuotojų paslaugomis;

c) reikalavimai, susiję su:

   i) 2 dalyje nurodyta TLPT aprėptimi;

   ii) testavimo metodika ir požiūriu, kurio reikia laikytis kiekvienu konkrečiu testavimo proceso etapu;

   iii) testavimo rezultatais, užbaigimu ir koregavimo etapais;

d) kokios rūšies bendradarbiavimas priežiūros srityje ir kokios rūšies kitoks atitinkamas bendradarbiavimas yra reikalingas atliekant finansų sektoriaus subjektų, kurie vykdo veiklą daugiau nei vienoje valstybėje narėje, TLPT ir palengvinant tokio testavimo rezultatų abipusį pripažinimą, kad būtų sudarytos sąlygos tinkamo lygio priežiūros institucijų dalyvavimui ir lanksčiam įgyvendinimui, siekiant atsižvelgti į finansų subsektorių arba vietos finansų rinkų specifiką.

Rengdamos tuos techninių reguliavimo standartų projektus, EPI deramai atsižvelgia į visas konkrečias ypatybes, atsirandančias dėl skirtingo veiklos skirtinguose finansinių paslaugų sektoriuose pobūdžio.

EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai ne vėliau kaip 2024 m. liepos 17 d.

Komisijai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsnius suteikiami įgaliojimai papildyti šį reglamentą priimant pirmoje pastraipoje nurodytus techninius reguliavimo standartus.

27 straipsnis

Reikalavimai testuotojams dėl TLPT atlikimo

1. Finansų sektoriaus subjektai TLPT atlikti pasitelkia tik tuos testuotojus, kurie:

a) yra patys tinkamiausi ir geriausios reputacijos;

b) turi techninių ir organizacinių pajėgumų ir įrodo turintys specialių ekspertinių žinių žvalgybos informacijos apie grėsmes, skverbimosi testavimo ir raudonosios komandos testavimo srityse;

c) yra sertifikuoti valstybėje narėje akreditavimo įstaigos arba laikosi oficialių elgesio kodeksų ar etikos sistemų;

d) pateikia nepriklausomą patikinimą arba audito ataskaitą dėl patikimo rizikos, susijusios su TLPT atlikimu, valdymo, įskaitant tinkamą finansų sektoriaus subjekto konfidencialios informacijos apsaugą ir finansų sektoriaus subjekto verslo rizikos kompensavimą;

e) yra tinkamai ir visiškai apdrausti atitinkamu profesinės civilinės atsakomybės draudimu, įskaitant draudimą nuo netinkamo elgesio ir aplaidumo rizikos;

2. Jeigu pasitelkiami vidaus testuotojai, finansų sektoriaus subjektai užtikrina, kad be 1 dalyje nurodytų reikalavimų dar tenkinamos visos toliau išdėstytos sąlygos:

a) naudojimąsi jų paslaugomis yra patvirtinusi atitinkama kompetentinga institucija arba viena bendra valdžios institucija, paskirta pagal 26 straipsnio 9 ir 10 dalis;

b) atitinkama kompetentinga institucija yra patikrinusi, ar finansų sektoriaus subjektas turi pakankamai specialių išteklių, ir yra užtikrinusi, kad visais testo rengimo ir atlikimo etapais būtų išvengta interesų konfliktų, ir

c) žvalgybos informacijos apie grėsmes teikėjas yra išorės subjektas finansų sektoriaus subjekto atžvilgiu.

3. Finansų sektoriaus subjektai užtikrina, kad su išorės testuotojais sudarytose sutartyse būtų reikalaujama patikimai valdyti TLPT rezultatus ir kad dėl jokio jų duomenų tvarkymo, įskaitant bet kokį sukūrimą, saugojimą, apibendrinimą, rengimą, pranešimą, perdavimą ar sunaikinimą, nekiltų rizikos finansų sektoriaus subjektui.

V SKYRIUS

Trečiosios šalies keliamos IRT rizikos valdymas

I skirsnis

Pagrindiniai trečiosios šalies keliamos IRT rizikos patikimo valdymo principai

28 straipsnis

Bendrieji principai

1. Finansų sektoriaus subjektai valdo trečiosios šalies keliamą IRT riziką kaip neatsiejamą IRT rizikos komponentą pagal savo IRT rizikos valdymo sistemą, kaip nurodyta 6 straipsnio 1 dalyje, laikydamiesi šių principų:

a) finansų sektoriaus subjektai, kurie yra sudarę sutartimi įformintus susitarimus dėl IRT paslaugų naudojimo savo veiklos operacijoms vykdyti, visada išlieka visiškai atsakingi už visų šiame reglamente ir taikytinoje finansinių paslaugų teisėje nustatytų pareigų laikymąsi ir vykdymą;

b) finansų sektoriaus subjektai, valdydami trečiosios šalies keliamą IRT riziką, vadovaujasi proporcingumo principu, atsižvelgdami į:

i) su IRT susijusios priklausomybės pobūdį, mastą, sudėtingumą ir svarbą,

ii) riziką, kylančią dėl sutartimi įformintų susitarimų dėl IRT paslaugų naudojimo, sudarytų su IRT paslaugas teikiančiomis trečiosiomis šalimis, atsižvelgiant į atitinkamos paslaugos, proceso ar funkcijos ypatingą svarbą arba svarbumą, taip pat į galimą poveikį finansinių paslaugų ir veiklos tęstinumui ir prieinamumui individualiu ir grupės lygmenimis.

2. Taikydami IRT rizikos valdymo sistemą, finansų sektoriaus subjektai, išskyrus subjektus, nurodytus 16 straipsnio 1 dalies pirmoje pastraipoje, ir išskyrus labai mažas įmones, priima ir reguliariai peržiūri trečiosios šalies keliamos IRT rizikos strategiją, atsižvelgdami į 6 straipsnio 9 dalyje nurodytą kelių pardavėjų strategiją, jei taikytina. Trečiosios šalies keliamos IRT rizikos strategija apima IRT paslaugas teikiančių trečiųjų šalių teikiamų IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, naudojimo politiką ir yra taikoma individualiu ir, kai aktualu, iš dalies konsoliduotu ir konsoliduotu pagrindu. Valdymo organas, remdamasis finansų sektoriaus subjekto bendro rizikos profilio ir verslo paslaugų masto ir sudėtingumo vertinimu, reguliariai peržiūri nustatytą riziką, susijusią su sutartimi įformintais susitarimais dėl IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, naudojimo.

3. Taikydami IRT rizikos valdymo sistemą, finansų sektoriaus subjektai tvarko ir atnaujina subjektų lygmeniu ir iš dalies konsoliduotu bei konsoliduotu lygmenimis informacijos apie visus sutartimi įformintus susitarimus dėl IRT paslaugas teikiančių trečiųjų šalių teikiamų IRT paslaugų naudojimo registrą.

Pirmoje pastraipoje nurodyti sutartimi įforminti susitarimai tinkamai pagrindžiami dokumentais, atskiriant tuos, kurie taikomi IRT paslaugoms, susijusioms su ypatingos svarbos arba svarbioms funkcijomis, ir susitarimus, kurie joms netaikomi.

Finansų sektoriaus subjektai ne rečiau kaip kartą per metus kompetentingoms institucijoms praneša naujų susitarimų dėl IRT paslaugų naudojimo skaičių, taip pat apie IRT paslaugas teikiančių trečiųjų šalių kategorijas, sutartimi įformintų susitarimų rūšį ir teikiamas paslaugas bei funkcijas.

Kompetentingai institucijai paprašius, finansų sektoriaus subjektai pateikia jai visą informacijos registrą arba prašyme nurodytas jo dalis kartu su visa informacija, laikoma būtina veiksmingai finansų sektoriaus subjekto priežiūrai užtikrinti.

Finansų sektoriaus subjektai laiku informuoja kompetentingą instituciją apie bet kokį planuojamą sudaryti sutartimi įformintą susitarimą dėl IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, ir apie tai, kada funkcija tampa ypatingos svarbos ar svarbi.

4. Prieš sudarydami sutartimi įformintą susitarimą dėl IRT paslaugų naudojimo, finansų sektoriaus subjektai:

a) įvertina, ar sutartimi įformintas susitarimas taikomas IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, naudojimui;

b) įvertina, ar įvykdytos sutarčių sudarymo priežiūros sąlygos;

c) nustato ir įvertina visą atitinkamą riziką, susijusią su sutartimi įformintais susitarimais, įskaitant galimybę, kad tokiais sutartimi įformintais susitarimais gali būti prisidedama prie IRT koncentracijos rizikos, kaip nurodyta 29 straipsnyje, padidinimo;

d) atlieka numatomų IRT paslaugas teikiančių trečiųjų šalių išsamų patikrinimą ir, taikydami atrankos ir vertinimo procesus, užtikrina, kad IRT paslaugas teikianti trečioji šalis būtų tinkama;

e) nustato ir įvertina interesų konfliktus, galinčius atsirasti dėl sutartimi įforminto susitarimo.

5. Finansų sektoriaus subjektai gali sudaryti sutartimi įformintus susitarimus tik su tomis IRT paslaugas teikiančiomis trečiosiomis šalimis, kurios laikosi tinkamų informacijos saugumo standartų. Kai tie sutartimi įforminti susitarimai yra susiję su ypatingos svarbos arba svarbiomis funkcijomis, finansų sektoriaus subjektai, prieš sudarydami susitarimus, deramai atsižvelgia į tai, ar IRT paslaugas teikiančios trečiosios šalys taiko naujausius ir aukščiausios kokybės informacijos saugumo standartus.

6. Naudodamiesi prieigos, patikrinimo ir audito teisėmis IRT paslaugas teikiančios trečiosios šalies atžvilgiu, finansų sektoriaus subjektai, laikydamiesi rizika grindžiamo požiūrio, iš anksto nustato auditų ir patikrinimų dažnumą bei adituotinas sritis pagal visuotinai pripažintus audito standartus, atitinkančius priežiūros institucijų nurodymus dėl tokių audito standartų naudojimo ir integravimo.

Jei sutartimi įforminti susitarimai, sudaryti su IRT paslaugas teikiančiomis trečiosiomis šalimis dėl IRT paslaugų naudojimo, reiškia didelį techninį sudėtingumą, finansų sektoriaus subjektas patikrina, ar auditoriai (ar tai būtų vidaus ar išorės auditoriai, ar auditorių grupė) turi tinkamų įgūdžių ir žinių, kad galėtų veiksmingai atlikti atitinkamą auditą ir vertinimą.

7. Finansų sektoriaus subjektai užtikrina, kad sutartimi įforminti susitarimai dėl IRT paslaugų naudojimo galėtų būti nutraukti esant bet kuriai iš toliau nurodytų aplinkybių:

a) jei IRT paslaugas teikianti trečioji šalis reikšmingai pažeidė taikytinus įstatymus, kitus teisės aktus ar sutarties sąlygas;

b) aplinkybėmis, nustatytomis stebint trečiosios šalies keliamą IRT riziką, kurios laikomos galinčiomis pakeisti pagal sutartimi įformintą susitarimą teikiamų funkcijų atlikimą, įskaitant esminius pakeitimus, kurie daro poveikį susitarimui ar IRT paslaugas teikiančios trečiosios šalies padėčiai;

c) jei įrodoma, kad IRT paslaugas teikiančios trečiosios šalies veikla turi trūkumų, susijusių su jos atliekamu bendros IRT rizikos valdymu, visų pirma su tuo, kaip ji užtikrina duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą, ar tai būtų asmens duomenys ar kiti neskelbtini duomenys, ar ne asmens duomenys;

d) atvejais, kai kompetentinga institucija nebegali veiksmingai prižiūrėti finansų sektoriaus subjekto dėl atitinkamo sutartimi įforminto susitarimo sąlygų ar su juo susijusių aplinkybių.

8. IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, atveju finansų sektoriaus subjektai nustato pasitraukimo strategijas. Pasitraukimo strategijomis atsižvelgiama į riziką, kuri gali kilti IRT paslaugas teikiančios trečiosios šalies lygmeniu, visų pirma į galimą jos žlugimą, teikiamų IRT paslaugų kokybės pablogėjimą, bet kokį verslo sutrikdymą dėl netinkamo paslaugų teikimo ar jų neteikimo arba bet kokios reikšmingos rizikos, kylančios tinkamo ir nuolatinio atitinkamos IRT paslaugos diegimo atžvilgiu, arba nutraukus sutartimi įformintą susitarimą su IRT paslaugas teikiančiomis trečiosiomis šalimis susiklosčius bet kuriai iš 7 dalyje išvardytų aplinkybių.

Finansų sektoriaus subjektai užtikrina, kad jie galėtų pasitraukti iš sutartimi įformintų susitarimų:

a) nesutrikdydami savo verslo veiklos,

b) nesuvaržydami teisės aktų reikalavimų laikymosi,

c) nepakenkdami klientams teikiamų paslaugų tęstinumui ir kokybei.

Pasitraukimo planai turi būti išsamūs, pagrįsti dokumentais ir, remiantis 4 straipsnio 2 dalyje išdėstytais kriterijais, pakankamai išbandyti bei periodiškai peržiūrimi.

Finansų sektoriaus subjektai nustato alternatyvius sprendimus ir parengia pertvarkos planus, kad galėtų perimti pagal sutartis patikėtas IRT paslaugas ir atitinkamus duomenis iš IRT paslaugas teikiančios trečiosios šalies ir saugiai bei visa apimtimi juos perduoti alternatyviems paslaugų teikėjams arba juos vėl įtraukti į savo vidaus sistemas.

Finansų sektoriaus subjektai turi būti įdiegę tinkamas nenumatytų atvejų priemones, kad užtikrintų veiklos tęstinumą susiklosčius pirmoje pastraipoje nurodytomis aplinkybėmis.

9. EPI Jungtiniame komitete parengia techninių įgyvendinimo standartų projektus, pagal kuriuos nustatomi standartiniai šablonai, skirti 3 dalyje nurodytam informacijos registrui, įskaitant informaciją, kuri yra bendra visiems sutartimi įformintiems susitarimams dėl IRT paslaugų naudojimo. EPI tuos techninių įgyvendinimo standartų projektus pateikia Komisijai ne vėliau kaip 2024 m. sausio 17 d.

Komisijai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 15 straipsnį suteikiami įgaliojimai priimti pirmoje pastraipoje nurodytus techninius įgyvendinimo standartus.

10. EPI per Jungtinį komitetą parengia techninių reguliavimo standartų projektus, kuriuose patikslinamas 2 dalyje nurodytos politikos, taikomos sutartimi įformintiems susitarimams dėl IRT paslaugas teikiančių trečiųjų šalių teikiamų IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, naudojimo, išsamus turinys.

Rengdamos tuos techninių reguliavimo standartų projektus, EPI atsižvelgia į finansų sektoriaus subjekto dydį ir bendrą rizikos profilį, taip pat į jo paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą. EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai ne vėliau kaip 2024 m. sausio 17 d.

Komisijai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsnius suteikiami įgaliojimai papildyti šį reglamentą priimant pirmoje pastraipoje nurodytus techninius reguliavimo standartus.

29 straipsnis

Išankstinis IRT koncentracijos rizikos vertinimas subjektų lygmeniu

1. Nustatydami ir vertindami riziką, nurodytą 28 straipsnio 4 dalies c punkte, finansų sektoriaus subjektai atsižvelgia ir į tai, ar sudarius numatomą sutartimi įformintą susitarimą dėl IRT paslaugų, kuriomis palaikomos ypatingos svarbos ir svarbios funkcijos, susidarytų bent viena iš šių aplinkybių:

a) būtų sudaryta sutartis su IRT paslaugas teikiančia trečiąja šalimi, kuri nėra lengvai pakeičiama, arba

b) atsirastų keli sutartimi įforminti susitarimai dėl IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, teikimo su ta pačia IRT paslaugas teikiančia trečiąja šalimi arba su glaudžiai susijusiomis IRT paslaugas teikiančiomis trečiosiomis šalimis.

Finansų sektoriaus subjektai įvertina alternatyvių sprendimų, pavyzdžiui, skirtingų IRT paslaugas teikiančių trečiųjų šalių paslaugų naudojimo, naudą ir išlaidas, atsižvelgdami į tai, ar ir kaip numatyti sprendimai atitinka jų skaitmeninio atsparumo strategijoje nustatytus veiklos poreikius ir tikslus.

2. Jei sutartimi įformintame susitarime dėl IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, naudojimo yra numatyta galimybė IRT paslaugas teikiančiai trečiajai šaliai papildomai sudaryti subrangos sutartis dėl IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, su kitomis IRT paslaugas teikiančiomis trečiosiomis šalimis, finansų sektoriaus subjektai įvertina naudą ir riziką, galinčias atsirasti dėl tokių subrangos sutarčių, visų pirma tuo atveju, kai IRT subrangovas yra įsisteigęs trečiojoje valstybėje.

Kai sutartimi įforminti susitarimai susiję su IRT paslaugomis, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, finansų sektoriaus subjektai deramai apsvarsto nemokumo teisės nuostatas, kurios būtų taikomos IRT paslaugas teikiančios trečiosios šalies bankroto atveju, taip pat visus apribojimus, kurių galėtų atsirasti skubaus finansų sektoriaus subjekto duomenų atkūrimo atžvilgiu.

Jei sutartimi įforminti susitarimai dėl IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, naudojimo sudaromi su IRT paslaugas teikiančia trečiąja šalimi, įsisteigusia trečiojoje valstybėje, finansų sektoriaus subjektai, be antroje pastraipoje nurodytų aspektų, taip pat atsižvelgia į tai, ar laikomasi Sąjungos duomenų apsaugos taisyklių ir ar veiksmingai užtikrinamas teisės aktų vykdymas toje trečiojoje valstybėje.

Jei sutartimi įforminti susitarimai dėl IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, naudojimo numato galimybę sudaryti subrangos susitarimus, finansų sektoriaus subjektai įvertina, ar ir kaip galimai ilgos ar sudėtingos subrangos grandinės gali daryti poveikį jų galimybėms visapusiškai stebėti pagal sutartį perduotas funkcijas ir kompetentingos institucijos galimybėms šiuo atžvilgiu veiksmingai prižiūrėti finansų sektoriaus subjektą.

30 straipsnis

Pagrindinės sutartinės nuostatos

1. Finansų sektoriaus subjekto ir IRT paslaugas teikiančios trečiosios šalies teisės ir pareigos aiškiai paskirstomos ir išdėstomos raštu. Visa sutartis turi apimti paslaugų lygio susitarimus ir yra išdėstoma viename rašytiniame dokumente, kuris šalims yra prieinamas popierine forma, arba dokumente, kurį galima gauti kita atsisiunčiama, patvaria ir prieinama forma.

2. Sutartimi įformintuose susitarimuose dėl IRT paslaugų naudojimo turi būti nurodyti bent šie elementai:

a) aiškus ir išsamus visų funkcijų ir IRT paslaugų, kurias turi teikti IRT paslaugas teikianti trečioji šalis, aprašymas, nurodant, ar leidžiama sudaryti subrangos sutartis IRT paslaugoms, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, ar jos esminių dalių ir, jeigu taip, tokiai subrangos sutarčiai taikomos sąlygos;

b) vietos, t. y. regionai ar šalys, kuriuose turi būti teikiamos pagal sutartį arba subrangos sutartį atliekamos funkcijos ir IRT paslaugos ir kuriuose turi būti tvarkomi duomenys, nurodant saugojimo vietą, ir reikalavimas, kad IRT paslaugas teikianti trečioji šalis iš anksto praneštų finansų sektoriaus subjektui, jeigu ji ketina keisti tokias vietas;

c) nuostatos dėl duomenų prieinamumo, autentiškumo, vientisumo ir konfidencialumo, kiek tai susiję su duomenų, įskaitant asmens duomenis, apsauga;

d) nuostatos dėl prieigos prie asmens ir ne asmens duomenų, kuriuos tvarko finansų sektoriaus subjektas, jų atkūrimo ir grąžinimo lengvai prieinama forma užtikrinimo IRT paslaugas teikiančios trečiosios šalies nemokumo, pertvarkymo ar veiklos operacijų nutraukimo atveju arba sutartimi įforminto susitarimo nutraukimo atveju;

e) paslaugų lygio aprašymai, įskaitant jų atnaujinimus ir pataisymus;

f) IRT paslaugas teikiančios trečiosios šalies pareiga teikti pagalbą finansų sektoriaus subjektui be papildomo mokesčio arba už iš anksto nustatytą mokestį, kai įvyksta IRT incidentas, susijęs su finansų sektoriaus subjektui teikiama IRT paslauga;

g) IRT paslaugas teikiančios trečiosios šalies pareiga visapusiškai bendradarbiauti su kompetentingomis institucijomis ir finansų sektoriaus subjekto pertvarkymo institucijomis, įskaitant su jų paskirtais asmenimis;

h) sutarties nutraukimo teisės ir susiję minimalūs įspėjimo apie sutartimi įformintų susitarimų nutraukimą terminai, atsižvelgiant į kompetentingų institucijų ir pertvarkymo institucijų lūkesčius;

i) IRT paslaugas teikiančių trečiųjų šalių dalyvavimo finansų sektoriaus subjektų informuotumo apie IRT saugumą programose ir skaitmeninės veiklos atsparumo mokymuose pagal 13 straipsnio 6 dalį sąlygos.

3. Į sutartimi įformintus susitarimus dėl IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, naudojimo, be 2 dalyje nurodytų elementų, įtraukiami bent šie elementai:

a) išsamūs paslaugų lygio aprašymai, įskaitant jų atnaujinimus ir pataisymus, ir tikslūs kiekybiniai ir kokybiniai sutarto paslaugų lygio tiksliniai veiklos rezultatų rodikliai, kad finansų sektoriaus subjektas galėtų vykdyti veiksmingą IRT paslaugų stebėseną ir nepagrįstai nedelsdamas imtis tinkamų taisomųjų veiksmų, kai sutarti paslaugų lygiai neužtikrinami;

b) IRT paslaugas teikiančiai trečiajai šaliai taikomi įspėjimo terminai ir pareigos teikti pranešimus finansų sektoriaus subjektui, įskaitant pranešimą apie bet kokius pokyčius, kurie gali daryti reikšmingą poveikį IRT paslaugas teikiančios trečiosios šalies galimybėms veiksmingai teikti IRT paslaugas, kurios palaiko ypatingos svarbos arba svarbias funkcijas pagal sutartus paslaugų lygius;

c) reikalavimai IRT paslaugas teikiančiai trečiajai šaliai įgyvendinti ir testuoti nenumatytų veiklos atvejų planus ir taikyti IRT saugumo priemones ir politiką, kuriomis užtikrinamas tinkamas finansų sektoriaus subjekto teikiamų paslaugų saugumo lygis laikantis jo taikomos reguliavimo sistemos;

d) IRT paslaugas teikiančios trečiosios šalies pareiga dalyvauti ir visapusiškai bendradarbiauti finansų sektoriaus subjekto TLPT, kaip nurodyta 26 ir 27 straipsniuose;

e) teisė nuolat stebėti IRT paslaugas teikiančios trečiosios šalies veiklos rezultatus; ši teisė apima:

i) finansų sektoriaus subjekto arba paskirtos trečiosios šalies ir kompetentingos institucijos neribotas teises turėti prieigą, atlikti patikrinimą bei auditą ir teisę daryti atitinkamų dokumentų kopijas vietoje, jeigu jie turi ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies operacijoms; veiksmingai naudotis šiomis teisėmis netrukdo ir jų nevaržo kiti sutartimi įforminti susitarimai arba įgyvendinimo politika;

ii) teisę susitarti dėl alternatyvių saugumo užtikrinimo lygių, jei tai turi įtakos kitų klientų teisėms;

iii) IRT paslaugas teikiančios trečiosios šalies pareigą visapusiškai bendradarbiauti kompetentingoms institucijoms, atsakingajai priežiūros institucijai, finansų sektoriaus subjektui arba paskirtai trečiajai šaliai atliekant patikrinimus ir auditus ir

iv) pareigą pateikti išsamią informaciją apie tokių patikrinimų ir auditų apimtį, procedūras, kurių turi būti laikomasi jų metu, ir jų dažnumą;

f) pasitraukimo strategijos, visų pirma privalomo pakankamos trukmės pereinamojo laikotarpio nustatymas:

i) per kurį IRT paslaugas teikianti trečioji šalis toliau vykdys atitinkamas funkcijas ar teiks IRT paslaugas, kad būtų sumažinta finansų sektoriaus subjekto veiklos sutrikdymo rizika arba užtikrintas veiksmingas jo pertvarkymas ir restruktūrizavimas;

ii) per kurį finansų sektoriaus subjektas gali pereiti prie kitos IRT paslaugas teikiančios trečiosios šalies arba pasirinkti viduje taikomus sprendimus, atitinkančius teikiamos paslaugos sudėtingumą.

Nukrypstant nuo e punkto, IRT paslaugas teikianti trečioji šalis ir finansų sektoriaus subjektas, kuris yra labai maža įmonė, gali susitarti, kad prieigos, patikrinimo ir audito teisės gali būti perduotos IRT paslaugas teikiančios trečiosios šalies paskirtai nepriklausomai trečiajai šaliai ir kad finansų sektoriaus subjektas bet kuriuo metu gali prašyti tos trečiosios šalies pateikti informaciją ir patikinimą apie IRT paslaugas teikiančios trečiosios šalies veiklos rezultatus.

4. Derėdamiesi dėl sutartimi įformintų susitarimų, finansų sektoriaus subjektai ir IRT paslaugas teikiančios trečiosios šalys apsvarsto galimybę taikyti standartines sutarčių sąlygas, valdžios institucijų parengtas konkrečioms paslaugoms.

5. EPI Jungtiniame komitete parengia techninių reguliavimo standartų projektus, kuriuose patikslinami 2 dalies a punkte nurodyti elementai, kuriuos turi nustatyti ir įvertinti finansų sektoriaus subjektas, sudarydamas subrangos sutartis dėl IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos.

Rengdamos tų techninių reguliavimo standartų projektus, EPI atsižvelgia į finansų sektoriaus subjekto dydį ir bendrą rizikos profilį, taip pat į jo paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą.

EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai ne vėliau kaip 2024 m. liepos 17 d.

Komisijai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsnius suteikiami įgaliojimai papildyti šį reglamentą priimant pirmoje pastraipoje nurodytus techninius reguliavimo standartus.

II SKIRSNIS

Ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūros sistema

31 straipsnis

IRT paslaugas teikiančių trečiųjų šalių pripažinimas esančiomis ypatingos svarbos

1. EPI per Jungtinį komitetą ir remdamosi Priežiūros forumo, įsteigto pagal 32 straipsnio 1 dalį, rekomendacija:

a) IRT paslaugas teikiančias trečiąsias šalis pripažįsta esančiomis ypatingai svarbiomis finansų sektoriaus subjektams, atlikus įvertinimą, kuriuo atsižvelgiama į 2 dalyje nurodytus kriterijus;

b) kiekvienai ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai Atsakingąja priežiūros institucija paskiria EPI, kuri pagal reglamentus (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ar (ES) Nr. 1095/2010 yra atsakinga už finansų sektoriaus subjektus, kurie visi kartu valdo didžiausią bendro turto dalį, vertinant visų finansų sektoriaus subjektų, kurie naudojasi atitinkamos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies, paslaugomis, bendro turto verte, kurią įrodo tų finansų sektoriaus subjektų atskirų balansų suma.

2. 1 dalies a punkte nurodytas pripažinimas grindžiamas visais toliau nurodytais kriterijais, susijusiais su IRT paslaugas teikiančios trečiosios šalies teikiamomis IRT paslaugomis:

a) sisteminiu poveikiu finansinių paslaugų teikimo stabilumui, tęstinumui ar kokybei tuo atveju, jei atitinkama IRT paslaugas teikianti trečioji šalis patirtų didelį veiklos sutrikimą, trukdantį teikti paslaugas, atsižvelgiant į finansų sektoriaus subjektų skaičių ir į finansų sektoriaus subjektų, kuriems atitinkama IRT paslaugas teikianti trečioji šalis teikia paslaugas, bendrą turto vertę;

b) finansų sektoriaus subjektų, kurie yra priklausomi nuo atitinkamos IRT paslaugas teikiančios trečiosios šalies, sisteminiu pobūdžiu arba svarba, vertinant pagal šiuos parametrus:

   i) pasaulinės sisteminės svarbos įstaigų (G-SII) ar kitų sisteminės svarbos įstaigų (O-SII), kurios yra priklausomos nuo atitinkamos IRT paslaugas teikiančios trečiosios šalies, skaičių;

   ii) i punkte nurodytų G-SII arba O-SII ir kitų finansų sektoriaus subjektų tarpusavio priklausomybę, įskaitant atvejus, kai G-SII arba O-SII teikia finansinės infrastruktūros paslaugas kitiems finansų sektoriaus subjektams;

c) finansų sektoriaus subjektų priklausomybe nuo atitinkamos IRT paslaugas teikiančios trečiosios šalies teikiamų paslaugų, susijusių su finansų sektoriaus subjektų ypatingos svarbos arba svarbiomis funkcijomis, kurios galiausiai yra siejamos su ta pačia IRT paslaugas teikiančią trečiąja šalimi, neatsižvelgiant į tai, ar finansų sektoriaus subjektai yra priklausomi nuo tokių paslaugų tiesiogiai ar netiesiogiai pagal subrangos susitarimus;

d) IRT paslaugas teikiančios trečiosios šalies pakeičiamumu, atsižvelgiant į šiuos parametrus:

   i) realių alternatyvų, net ir dalinių, trūkumą dėl nedidelio konkrečioje rinkoje veiklą vykdančių IRT paslaugas teikiančių trečiųjų šalių skaičiaus, atitinkamos IRT paslaugas teikiančios trečiosios šalies rinkos dalies, susijusio techninio sudėtingumo ar pažangumo, be kita ko, dėl bet kokios nuosavybinės technologijos, arba IRT paslaugas teikiančios trečiosios šalies organizacinių ar veiklos ypatumų;

   ii) sunkumus iš dalies arba visiškai perkelti atitinkamus duomenis ir darbo krūvį iš atitinkamos IRT paslaugas teikiančios trečiosios šalies į kitą IRT paslaugas teikiančią trečiąją šalį arba dėl didelių finansinių išlaidų, laiko ar kitų išteklių, kurių gali prireikti perkėlimo procesui, arba dėl padidėjusios IRT rizikos ar kitos operacinės rizikos, su kuria finansų sektoriaus subjektas gali susidurti tokio perkėlimo metu.

3. Jei IRT paslaugas teikianti trečioji šalis priklauso grupei, 2 dalyje nurodyti kriterijai vertinami visos grupės teikiamų paslaugų atžvilgiu.

4. Ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys, priklausančios grupei, paskiria vieną juridinį asmenį koordinavimo punktu, kad būtų užtikrintas tinkamas atstovavimas ir komunikacija su Atsakingąja priežiūros institucija.

5. Atsakingoji priežiūros institucija praneša IRT paslaugas teikiančiai trečiajai šaliai apie vertinimo, kurio rezultatas būtų 1 dalies a punkte nurodytas pripažinimas, išvadas. Per 6 savaites nuo pranešimo dienos IRT paslaugas teikianti trečioji šalis gali pateikti Atsakingajai priežiūros institucijai pagrįstą pareiškimą su visa vertinimui reikalinga informacija. Atsakingoji priežiūros institucija apsvarsto pagrįstą pareiškimą ir gali paprašyti per 30 kalendorinių dienų pateikti papildomos informacijos nuo tokio pareiškimo gavimo dienos.

Pripažinusios IRT paslaugas teikiančią trečiąją šalį esančia ypatingos svarbos, EPI per Jungtinį komitetą praneša IRT paslaugas teikiančiai trečiajai šaliai apie tokį pripažinimą ir datą, nuo kurios ji faktiškai bus prižiūrima. Ta pradžios data turi būti ne vėlesnė kaip vienas mėnuo nuo pranešimo. IRT paslaugas teikianti trečioji šalis praneša finansų sektoriaus subjektams, kuriems ji teikia paslaugas, apie jos pripažinimą esančia ypatingos svarbos.

6. Komisijai pagal 57 straipsnį suteikiami įgaliojimai priimti deleguotąjį aktą, kuriuo šis reglamentas būtų papildytas patikslinant šio straipsnio 2 dalyje nurodytus kriterijus, ne vėliau kaip 2024 m. liepos 17 d.

7. 1 dalies a punkte nurodytas pripažinimas taikomas tik tada, kai Komisija priima deleguotąjį aktą pagal 6 dalį.

8. 1 dalies a punkte nurodytas pripažinimas netaikomas:

i) finansų sektoriaus subjektams, teikiantiems IRT paslaugas kitiems finansų sektoriaus subjektams;

ii) IRT paslaugas teikiančioms trečiosioms šalims, kurioms taikomos priežiūros sistemos, nustatytos siekiant padėti atlikti užduotis, nurodytas Sutarties dėl Europos Sąjungos veikimo 127 straipsnio 2 dalyje;

iii) grupės vidaus IRT paslaugų teikėjams;

iv) IRT paslaugas teikiančioms trečiosioms šalims, teikiančioms IRT paslaugas tik vienoje valstybėje narėje finansų sektoriaus subjektams, kurie vykdo veiklą tik toje valstybėje narėje.

9. EPI per Jungtinį komitetą sudaro, skelbia ir kasmet atnaujina Sąjungos lygmens ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių sąrašą.

10. 1 dalies a punkto tikslais kompetentingos institucijos kasmet apibendrina ir perduoda 28 straipsnio 3 dalies trečioje pastraipoje nurodytus pranešimus Priežiūros forumui, įsteigtam pagal 32 straipsnį. Priežiūros forumas įvertina finansų sektoriaus subjektų priklausomybę nuo IRT paslaugas teikiančių trečiųjų šalių, remdamasis iš kompetentingų institucijų gauta informacija.

11. IRT paslaugas teikiančios trečiosios šalys, neįtrauktos į 9 dalyje nurodytą sąrašą, gali prašyti, kad jas pripažintų esančiomis ypatingos svarbos pagal 1 dalies a punktą.

Pirmos pastraipos tikslais IRT paslaugas teikianti trečioji šalis pateikia pagrįstą prašymą EBI, ESMA arba EIOPA, kurios Jungtiniame komitete nusprendžia, ar pripažinti tą IRT paslaugas teikiančią trečiąją šalį esančia ypatingos svarbos pagal 1 dalies a punktą.

Antroje pastraipoje nurodytas sprendimas priimamas ir apie jį IRT paslaugas teikiančiai trečiajai šaliai pranešama per 6 mėnesius nuo prašymo gavimo dienos.

12. Finansų sektoriaus subjektai naudojasi trečiojoje valstybėje įsteigtos IRT paslaugas teikiančios trečiosios šalies, pripažintos esančia ypatingos svarbos pagal 1 dalies a punktą, paslaugomis tik tuo atveju, jei pastaroji per 12 mėnesių nuo pripažinimo įsteigė patronuojamąją įmonę Sąjungoje.

13. 12 dalyje nurodyta ypatingos svarbos IRT paslaugas teikianti trečioji šalis praneša Atsakingajai priežiūros institucijai apie visus Sąjungoje įsteigtos patronuojamosios įmonės valdymo struktūros pasikeitimus.

32 straipsnis

Priežiūros sistemos struktūra

1. Pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 57 straipsnio 1 dalį Jungtinis komitetas įsteigia Priežiūros forumą, kuris veikia kaip pakomitetis, padedantis Jungtiniam komitetui ir 31 straipsnio 1 dalies b punkte nurodytai Atsakingajai priežiūros institucijai dirbti trečiųjų šalių keliamos IRT rizikos finansų sektoriuose srityje. Priežiūros forumas rengia Jungtinio komiteto bendrų pozicijų ir bendrų aktų toje srityje projektus.

Priežiūros forumas reguliariai aptaria atitinkamus pokyčius, susijusius su IRT rizika ir pažeidžiamumais, ir skatina nuoseklų požiūrį į trečiųjų šalių keliamos IRT rizikos stebėseną Sąjungos lygmeniu.

2. Priežiūros forumas kasmet atlieka kolektyvinį visų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūros veiklos rezultatų ir nustatytų faktų vertinimą ir skatina taikyti koordinavimo priemones, kuriomis siekiama padidinti finansų sektoriaus subjektų skaitmeninės veiklos atsparumą, puoselėja geriausią IRT koncentracijos rizikos mažinimo praktiką ir tiria tarpsektorinio rizikos perleidimo mažinimo priemones.

3. Priežiūros forumas pateikia išsamius ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių lyginamuosius standartus, kuriuos pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 56 straipsnio 1 dalį Jungtinis komitetas turi priimti kaip bendras EPI pozicijas.

4. Priežiūros forumą sudaro:

a) EPI pirmininkai;

b) po vieną aukšto lygio atstovą iš 46 straipsnyje nurodytos atitinkamos kompetentingos institucijos dabartinių darbuotojų iš kiekvienos valstybės narės;

c) visų EPI vykdomieji direktoriai ir po vieną Komisijos, ESRV, ECB ir ENISA atstovą dalyvauti stebėtojų teisėmis;

d) kai tikslinga, po dar vieną 46 straipsnyje nurodytos kompetentingos institucijos atstovą iš kiekvienos valstybės narės dalyvauti stebėtojo teisėmis;

e) kai taikytina, pagal Direktyvą (ES) 2022/2555 paskirtų ar įsteigtų kompetentingų institucijų, atsakingų už esminio ar svarbaus subjekto, kuriam taikoma ta direktyva, kuris buvo pripažintas ypatingos svarbos IRT paslaugas teikiančia trečiąja šalimi, priežiūrą, atstovą dalyvauti stebėtojo teisėmis.

Priežiūros forumas, kai tikslinga, gali konsultuotis su nepriklausomais ekspertais, paskirtais pagal 6 dalį.

5. Kiekviena valstybė narė paskiria atitinkamą kompetentingą instituciją, kurios darbuotojas laikomas 4 dalies pirmos pastraipos b punkte nurodytu aukšto lygio atstovu, ir apie tai informuoja Atsakingąją priežiūros instituciją.

EPI savo svetainėje skelbia valstybių narių paskirtų aukšto lygio atstovų, skiriamų iš esamų atitinkamos kompetentingos institucijos darbuotojų, sąrašą.

6. 4 dalies antroje pastraipoje nurodytus nepriklausomus ekspertus skiria Priežiūros forumas iš ekspertų, atrinktų taikant viešą ir skaidrią paraiškų teikimo procesą, grupės.

Nepriklausomi ekspertai skiriami atsižvelgiant į jų ekspertines žinias finansinio stabilumo, skaitmeninės veiklos atsparumo ir IRT saugumo klausimais. Jie veikia nepriklausomai ir nešališkai, vadovaudamiesi tik visos Sąjungos interesais, ir nesiekia gauti Sąjungos institucijų ar įstaigų, valstybės narės Vyriausybės ar kitos viešosios ar privačiosios įstaigos nurodymų ir jais nesivadovauja.

7. Vadovaujantis reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 16 straipsniu, EPI ne vėliau kaip 2024 m. liepos 17 d. paskelbia šio skirsnio tikslais EPI ir kompetentingų institucijų bendradarbiavimo gaires, dėl išsamių procedūrų ir sąlygų, taikomų kompetentingų institucijų ir EPI užduočių pasidalinimui ir vykdymui, ir dėl išsamios informacijos apie keitimąsi informacija, kuri yra reikalinga, kad kompetentingos institucijos galėtų užtikrinti, kad būtų imtasi tolesnių veiksmų dėl rekomendacijų, teikiamų pagal 35 straipsnio 1 dalies d punktą, skirtų ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims.

8. Šiame skirsnyje nustatytais reikalavimais nedaromas poveikis Direktyvos (ES) 2022/2555 ir kitų Sąjungos priežiūros taisyklių, taikomų debesijos paslaugų teikėjams, taikymui.

9. EPI per Jungtinį komitetą ir remdamosi Priežiūros forumo atliktu parengiamuoju darbu kasmet pateikia Europos Parlamentui, Tarybai ir Komisijai šio skirsnio taikymo ataskaitą.

33 straipsnis

Atsakingosios priežiūros institucijos užduotys

1. Pagal 31 straipsnio 1 dalies b punktą paskirta Atsakingoji priežiūros institucija vykdo jai priskirtų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūrą ir visais su priežiūra susijusiais klausimais yra pagrindinis tų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių kontaktinis punktas.

2. 1 dalies tikslais Atsakingoji priežiūros institucija įvertina, ar kiekviena ypatingos svarbos IRT paslaugas teikianti trečioji šalis yra įdiegusi išsamias, patikimas ir veiksmingas taisykles, procedūras, mechanizmus ir tvarką, skirtus IRT rizikai, kurią ji gali kelti finansų sektoriaus subjektams, valdyti.

Atliekant pirmoje pastraipoje nurodytą vertinimą daugiausia dėmesio skiriama IRT paslaugoms, kurias teikia ypatingos svarbos IRT paslaugas teikianti trečioji šalis ir kuriomis palaikomos finansų sektoriaus subjektų ypatingos svarbos arba svarbios funkcijos. Kai būtina siekiant atsižvelgti į visą atitinkamą riziką, tas vertinimas turi apimti ir IRT paslaugas, kuriomis palaikomos kitos nei ypatingos svarbos arba svarbios funkcijos.

3. 2 dalyje nurodytas vertinimas apima:

a) IRT reikalavimus, kuriais visų pirma užtikrinamas paslaugų, kurias ypatingos svarbos IRT paslaugas teikianti trečioji šalis teikia finansų sektoriaus subjektams, saugumas, prieinamumas, tęstinumas, išplečiamumas ir kokybė, taip pat galimybės visada laikytis aukštų duomenų prieinamumo, autentiškumo, vientisumo ir konfidencialumo standartų;

b) fizinį saugumą, kuriuo prisidedama prie IRT saugumo užtikrinimo, įskaitant patalpų, įrenginių ir duomenų centrų saugumą;

c) rizikos valdymo procesus, įskaitant IRT rizikos valdymo politikos priemones, IRT veiklos tęstinumo politiką ir IRT reagavimo ir veiklos atkūrimo planus;

d) valdymo priemones, įskaitant organizacinę struktūrą su aiškiomis, skaidriomis ir nuosekliomis atsakomybės ir atskaitomybės taisyklėmis, leidžiančiomis veiksmingai valdyti IRT riziką;

e) reikšmingų su IRT susijusių incidentų identifikavimą, stebėseną ir skubų pranešimą apie juos finansų sektoriaus subjektams, tų incidentų, visų pirma kibernetinių išpuolių, valdymą ir sprendimą;

f) duomenų perkeliamumo, taikomųjų programų perkeliamumo ir sąveikumo mechanizmus, kuriais užtikrinama, kad finansų sektoriaus subjektai galėtų veiksmingai naudotis sutarties nutraukimo teisėmis;

g) IRT sistemų, infrastruktūros ir kontrolės priemonių testavimą;

h) IRT auditus;

i) atitinkamų nacionalinių ir tarptautinių standartų, taikomų teikiant IRT paslaugas finansų sektoriaus subjektams, laikymąsi.

4. Remdamasi 2 dalyje nurodytu vertinimu ir derindama veiksmus su 34 straipsnio 1 dalyje nurodytu Jungtiniu priežiūros tinklu (JPT), Atsakingoji priežiūros institucija patvirtina aiškų, išsamų ir pagrįstą individualų priežiūros planą, kuriame apibūdinami metiniai priežiūros tikslai ir pagrindiniai priežiūros veiksmai, numatyti kiekvienai ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai. Tas planas kiekvienais metais pateikiamas ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai.

Prieš patvirtindama priežiūros planą, Atsakingoji priežiūros institucija pateikia priežiūros plano projektą ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai.

Gavusi priežiūros plano projektą, ypatingos svarbos IRT paslaugas teikianti trečioji šalis gali per 15 kalendorinių dienų pateikti pagrįstą pareiškimą, kuriame būtų nurodytas tikėtinas poveikis klientams, kurie yra subjektai, nepatenkantys į šio reglamento taikymo sritį, ir, kai tikslinga, kuriame būtų suformuluoti rizikos mažinimo sprendimai.

5. Kai 4 dalyje nurodyti metiniai priežiūros planai patvirtinami ir jie pateikiami ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, kompetentingos institucijos gali imtis priemonių dėl ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių tik gavusios Atsakingosios priežiūros institucijos pritarimą.

34 straipsnis

Atsakingųjų priežiūros institucijų veiklos koordinavimas

1. Siekiant užtikrinti nuoseklų požiūrį į priežiūros veiklą ir siekiant sudaryti sąlygas suderintoms bendroms priežiūros strategijoms ir darniems veiklos metodams bei darbo metodikoms, trys pagal 31 straipsnio 1 dalies b punktą paskirtos Atsakingosios priežiūros institucijos įsteigia JPT siekdamos tarpusavyje koordinuoti veiksmus parengiamuosiuose etapuose ir koordinuoti priežiūros veiklą jų atitinkamų prižiūrimų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių atžvilgiu, taip pat imantis bet kurių veiksmų, kurių gali prireikti pagal 42 straipsnį.

2. 1 dalies tikslais Atsakingosios priežiūros institucijos parengia bendrą priežiūros protokolą, kuriame nustatomos išsamios procedūros, kurių reikia laikytis vykdant kasdienį koordinavimą ir užtikrinant greitą keitimąsi informacija ir reagavimą. Protokolas periodiškai peržiūrimas siekiant atsižvelgti į veiklos poreikius, visų pirma į praktinės priežiūros tvarkos raidą.

3. Atsakingosios priežiūros institucijos gali *ad hoc* pagrindu paprašyti ECB ir ENISA teikti technines konsultacijas, dalytis praktine patirtimi arba dalyvauti specialiuose JPT koordinavimo posėdžiuose.

35 straipsnis

Atsakingosios priežiūros institucijos įgaliojimai

1. Vykdydama šiame skirsnyje nustatytas pareigas Atsakingoji priežiūros institucija turi šiuos įgaliojimus ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių atžvilgiu:

a) prašyti visos atitinkamos informacijos ir dokumentų pagal 37 straipsnį;

b) atlikti bendruosius tyrimus ir patikrinimus atitinkamai pagal 38 ir 39 straipsnius;

c) užbaigus priežiūros veiklą prašyti pateikti ataskaitas, kuriose būtų nurodyti veiksmai, kurių ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys ėmėsi, arba taisomosios priemonės, kurias jos įgyvendino atsižvelgdamos į šios dalies d punkte nurodytas rekomendacijas;

d) teikti rekomendacijas dėl 33 straipsnio 3 dalyje nurodytų sričių, visų pirma dėl:

   i) konkrečių IRT saugumo ir kokybės reikalavimų ar procesų, visų pirma susijusių su pataisų, atnaujinimų, šifravimo ir kitų saugumo priemonių, kuriuos Atsakingoji priežiūros institucija laiko svarbiais finansų sektoriaus subjektams teikiamų paslaugų IRT saugumui užtikrinti, diegimu, taikymo;

   ii) sąlygų, įskaitant jų techninį įgyvendinimą, kuriomis ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys finansų sektoriaus subjektams teikia paslaugas ir kurias Atsakingoji priežiūros institucija laiko svarbiomis užkertant kelią pavienių gedimo taškų atsiradimui ar jų plitimui arba siekiant kuo labiau sumažinti galimą sisteminį poveikį visame Sąjungos finansų sektoriuje IRT koncentracijos rizikos atveju;

   iii) bet kokių planuojamų subrangos sutarčių, kai Atsakingoji priežiūros institucija mano, kad papildomos subrangos sutartys, įskaitant subrangos susitarimus, kuriuos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys ketina sudaryti su IRT paslaugas teikiančiomis trečiosiomis šalimis arba IRT subrangovais, įsisteigusiais trečiojoje valstybėje, gali kelti riziką finansų sektoriaus subjekto teikiamoms paslaugoms arba riziką finansiniam stabilumui, remdamasi pagal 37 ir 38 straipsnius surinktos informacijos analize;

   iv) papildomo subrangos susitarimo nesudarymo, jei tenkinamos visos toliau nurodytos sąlygos:

      — numatomas subrangovas yra IRT paslaugas teikianti trečioji šalis arba trečiojoje valstybėje įsisteigęs IRT subrangovas;

      — subrangos sutartis sudaroma dėl ypatingos svarbos arba svarbios finansų sektoriaus subjekto funkcijos ir

— Atsakingoji priežiūros institucija mano, kad tokios subrangos naudojimas kelia aiškią ir didelę riziką Sąjungos finansiniam stabilumui arba finansų sektoriaus subjektams, įskaitant finansų sektoriaus subjektų galimybes laikytis priežiūros reikalavimų.

Taikant šio punkto iv papunktį, IRT paslaugas teikiančios trečiosios šalys, naudodamos 41 straipsnio 1 dalies b punkte nurodytą šabloną, perduoda informaciją apie subrangos sutartis Atsakingajai priežiūros institucijai.

2. Naudodamasi šiame straipsnyje nurodytais įgaliojimais, Atsakingoji priežiūros institucija:

a) užtikrina reguliarų koordinavimą Jungtiniame priežiūros tinkle ir visų pirma atitinkamai siekia nuoseklių požiūrių į ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūrą;

b) deramai atsižvelgia į Direktyva (ES) 2022/2555 nustatytą sistemą ir prireikus konsultuojasi su atitinkamomis kompetentingomis institucijomis, paskirtomis ar įsteigtomis remiantis ta direktyva, kad būtų išvengta techninių ir organizacinių priemonių, kurios pagal tą direktyvą galėtų būti taikomos ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, dubliavimo;

c) siekia kuo labiau sumažinti riziką, kad bus sutrikdytos ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių teikiamos paslaugos klientams, kurie yra subjektai, nepatenkantys į šio reglamento taikymo sritį.

3. Prieš naudodamasi 1 dalyje nurodytais įgaliojimais Atsakingoji priežiūros institucija konsultuojasi su Priežiūros forumu.

Prieš pateikdama rekomendacijas pagal 1 dalies d punktą, Atsakingoji priežiūros institucija suteikia IRT paslaugas teikiančiai trečiajai šaliai galimybę per 30 kalendorinių dienų pateikti atitinkamą informaciją, įrodančią tikėtiną poveikį klientams, kurie yra subjektai, nepatenkantys į šio reglamento taikymo sritį, ir, kai tikslinga, suformuluoti rizikos mažinimo sprendimus.

4. Atsakingoji priežiūros institucija informuoja JPT apie naudojimosi 1 dalies a ir b punktuose nurodytais įgaliojimais rezultatus. Atsakingoji priežiūros institucija nepagrįstai nedelsdama perduoda 1 dalies c punkte nurodytas ataskaitas JPT ir finansų sektoriaus subjektų, kurie naudojasi tos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies IRT paslaugomis, kompetentingoms institucijoms.

5. Ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys sąžiningai bendradarbiauja su Atsakingąja priežiūros institucija ir jai padeda atlikti užduotis.

6. Tuo atveju, kai visiškai arba iš dalies nesilaikoma priemonių, kurių reikalaujama imtis naudojantis įgaliojimais pagal 1 dalies a, b ir c punktus, ir pasibaigus ne mažiau kaip 30 kalendorinių dienų laikotarpiui nuo tos dienos, kurią ypatingos svarbos IRT paslaugas teikianti trečioji šalis gavo pranešimą apie atitinkamas priemones, Atsakingoji priežiūros institucija priima sprendimą skirti periodinę baudą, kad priverstų ypatingos svarbos IRT paslaugas teikiančią trečiąją šalį laikytis tų priemonių.

7. 6 dalyje nurodyta periodinė bauda skiriama kasdien, kol bus pradėta laikytis priemonių, ir ne ilgiau kaip šešis mėnesius nuo pranešimo apie sprendimą dėl periodinės baudos skyrimo ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai dienos.

8. Periodinės baudos dydis, apskaičiuojamas nuo sprendime dėl periodinės baudos skyrimo nustatytos dienos, sudaro iki 1 % ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies vidutinės dienos pasaulinės apyvartos ankstesniais finansiniais metais. Nustatydama baudos dydį, Atsakingoji priežiūros institucija atsižvelgia į šiuos kriterijus, susijusius su 6 dalyje nurodytų priemonių nesilaikymu:

a) priemonių nesilaikymo sunkumą ir trukmę;

b) tai, ar priemonių nesilaikoma tyčia ar dėl aplaidumo;

c) IRT paslaugas teikiančios trečiosios šalies bendradarbiavimo su Atsakingąja priežiūros institucija lygį.

Pirmos pastraipos tikslais, siekdama užtikrinti nuoseklų požiūrį, Atsakingoji priežiūros institucija konsultuojasi JPT.

9. Baudos yra administracinio pobūdžio ir jų sumokėjimas yra užtikrinamas. Sumokėjimo užtikrinimui taikomos civilinio proceso taisyklės, galiojančios valstybėje narėje, kurios teritorijoje atliekami patikrinimai ir teikiama prieiga. Atitinkamos valstybės narės teismai turi jurisdikciją nagrinėti skundus, susijusius su neteisėtu baudų sumokėjimo užtikrinimu. Baudų sumos skiriamos į Europos Sąjungos bendrąjį biudžetą.

10. Atsakingoji priežiūros institucija viešai paskelbia apie kiekvieną skirtą periodinę baudą, išskyrus atvejus, kai toks paskelbimas sukeltų rimtą pavojų finansų rinkoms arba pernelyg pakenktų susijusioms šalims.

11. Prieš skirdama periodinę baudą pagal 6 dalį, Atsakingoji priežiūros institucija ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies, kurios atžvilgiu vyksta procesas, atstovams suteikia galimybę būti išklausytiems dėl nustatytų faktų ir savo sprendimus grindžia tik nustatytais faktais, dėl kurių ypatingos svarbos IRT paslaugas teikianti trečioji šalis, kurios atžvilgiu vyksta procesas, turėjo galimybę pateikti pastabas.

Proceso metu visapusiškai laikomasi asmenų, kurių atžvilgiu vyksta procesas, teisių į gynybą. Ypatingos svarbos IRT paslaugas teikianti trečioji šalis, kurios atžvilgiu vyksta procesas, turi teisę susipažinti su byla, nepažeidžiant kitų asmenų teisėto intereso apsaugoti savo verslo paslaptis. Teisė susipažinti su byla netaikoma konfidencialiai informacijai ar Atsakingosios priežiūros institucijos vidaus darbiniams dokumentams.

36 straipsnis

Naudojimasis Atsakingosios priežiūros institucijos įgaliojimais už Sąjungos ribų

1. Kai priežiūros tikslų neįmanoma pasiekti bendradarbiaujant su patronuojamąja įmone, įsteigta 31 straipsnio 12 dalies tikslais, arba vykdant priežiūros veiklą Sąjungoje esančiose patalpose, Atsakingoji priežiūros institucija gali naudotis įgaliojimais, nurodytais toliau pateiktose nuostatose, bet kuriose trečiojoje valstybėje esančiose patalpose, kurios priklauso ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai arba kurios kokiu nors būdu naudojamos paslaugoms Sąjungos finansų sektoriaus subjektams teikti, kai tai susiję su jos verslo operacijomis, funkcijomis ar paslaugomis, įskaitant administracinius, verslo ar veiklos biurus, patalpas, teritoriją, pastatus ar kitą nuosavybę:

a) 35 straipsnio 1 dalies a punkte ir

b) 35 straipsnio 1 dalies b punkte pagal 38 straipsnio 2 dalies a, b ir d punktus, ir pagal 39 straipsnio 1 dalį ir 2 dalies a punktą.

Pirmoje pastraipoje nurodytais įgaliojimais gali būti naudojamasi laikantis visų šių sąlygų:

i) patikrinimas trečiojoje valstybėje, Atsakingosios priežiūros institucijos nuomone, yra būtinas, kad pastaroji galėtų visapusiškai ir veiksmingai vykdyti savo pareigas pagal šį reglamentą;

ii) patikrinimas trečiojoje valstybėje yra tiesiogiai susijęs su IRT paslaugų teikimu finansų sektoriaus subjektams Sąjungoje;

iii) atitinkama ypatingos svarbos IRT paslaugas teikianti trečioji šalis sutinka, kad būtų atliktas patikrinimas trečiojoje valstybėje, ir

iv) Atsakingoji priežiūros institucija apie patikrinimą oficialiai pranešė atitinkamai trečiosios valstybės institucijai ir pastaroji tam neprieštaravo.

2. Nedarant poveikio atitinkamai Sąjungos institucijų ir valstybių narių kompetencijai, 1 dalies tikslais EBI, ESMA arba EIOPA sudaro administracinio bendradarbiavimo susitarimus su atitinkama trečiosios valstybės institucija, kad Atsakingajai priežiūros institucijai ir į tą trečiąją valstybę jos komandiruotai paskirtajai grupei būtų sudarytos sąlygos sklandžiai atlikti patikrinimus toje trečiojoje valstybėje. Tais bendradarbiavimo susitarimais Sąjungai ir jos valstybėms narėms nesukuriamos teisinės pareigos, taip pat jie nekliudo valstybėms narėms ir jų kompetentingoms institucijoms sudaryti dvišalius ar daugiašalius susitarimus su tomis trečiosiomis valstybėmis ir jų atitinkamomis institucijomis.

Tuose bendradarbiavimo susitarimuose nurodomi bent šie elementai:

a) pagal šį reglamentą vykdomos priežiūros veiklos ir konkrečios trečiosios valstybės atitinkamos institucijos vykdomos trečiosios šalies keliamos IRT rizikos finansų sektoriuje analogiškos stebėsenos koordinavimo procedūros, įskaitant išsamią informaciją dėl minėtos institucijos sutikimo leisti Atsakingajai priežiūros institucijai ir jos paskirtajai grupei vykdyti bendruosius tyrimus ir patikrinimus vietoje, kaip nurodyta 1 dalies pirmoje pastraipoje, jos jurisdikcijai priklausančioje teritorijoje perdavimo;

b) mechanizmas dėl bet kokios svarbios informacijos perdavimo tarp EBI, ESMA arba EIOPA ir konkrečios trečiosios valstybės atitinkamos institucijos, visų pirma kiek tai susiję su informacija, kurios Atsakingoji priežiūros institucija gali prašyti pagal 37 straipsnį;

c) mechanizmas, pagal kurį konkrečios trečiosios valstybės atitinkama institucija skubiai praneša EBI, ESMA arba EIOPA apie atvejus, kai manoma, kad trečiojoje valstybėje įsisteigusi IRT paslaugas teikianti trečioji šalis, pagal 31 straipsnio 1 dalies a punktą pripažinta esanti ypatingos svarbos, pažeidė reikalavimus, kurių ji pagal atitinkamos trečiosios valstybės taikytiną teisę privalo laikytis toje trečiojoje valstybėje teikdama paslaugas finansų įstaigoms, taip pat taikytos taisomosios priemonės ir nuobaudos;

d) naujausios informacijos apie reguliavimo ar priežiūros pokyčius, susijusius su finansų įstaigų trečiosios šalies keliama IRT rizika atitinkamoje trečiojoje valstybėje stebėsena, reguliarus perdavimas;

e) išsami informacija apie tai, kokiomis sąlygomis vienam atitinkamos trečiosios valstybės institucijos atstovui prireikus būtų leidžiama dalyvauti Atsakingosios priežiūros institucijos ir paskirtosios grupės vykdomuose patikrinimuose.

3. Kai Atsakingoji priežiūros institucija negali vykdyti priežiūros veiklos už Sąjungos ribų, kaip nurodyta 1 ir 2 dalyse, Atsakingoji priežiūros institucija:

a) naudojasi savo įgaliojimais pagal 35 straipsnį remdamasi visais savo turimais faktais ir dokumentais;

b) dokumentuoja ir paaiškina visus jos negalėjimo vykdyti šiame straipsnyje nurodytą numatytą priežiūros veiklą padarinius.

Į šios dalies b punkte nurodytus galimus padarinius atsižvelgiama Atsakingosios priežiūros institucijos rekomendacijose, teikiamose pagal 35 straipsnio 1 dalies d punktą.

37 straipsnis

Prašymas pateikti informaciją

1. Atsakingoji priežiūros institucija paprastu prašymu arba sprendimu gali pareikalauti, kad ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys pateiktų visą informaciją, būtiną Atsakingajai priežiūros institucijai, kad ji galėtų vykdyti šiame reglamente nustatytas pareigas, įskaitant visus atitinkamus verslo ar veiklos dokumentus, sutartis, politikos priemones, dokumentaciją, IRT saugumo audito ataskaitas, su IRT susijusių incidentų ataskaitas, taip pat bet kurią informaciją, susijusią su šalimis, kurioms ypatingos svarbos IRT paslaugas teikianti trečioji šalis yra perdavusi operacinių funkcijų ar veiklos vykdymą.

2. Siųsdama paprastą prašymą pateikti informaciją pagal 1 dalį, Atsakingoji priežiūros institucija:

a) nurodo šį straipsnį kaip prašymo teisinį pagrindą;

b) nurodo prašymo tikslą;

c) nurodo, kokios informacijos reikia;

d) nustato informacijos pateikimo terminą;

e) informuoja ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies, kurios prašoma pateikti informaciją, atstovą apie tai, kad jis informacijos pateikti neprivalo, tačiau tuo atveju jeigu jis į gautą prašymą savanoriškai atsakys, pateikta informacija privalo būti teisinga arba neklaidinanti.

3. Jei informaciją pagal 1 dalį pateikti reikalaujama sprendimu, Atsakingoji priežiūros institucija:

a) nurodo šį straipsnį kaip prašymo teisinį pagrindą;

b) nurodo prašymo tikslą;

c) nurodo, kokios informacijos reikia;

d) nustato informacijos pateikimo terminą;

e) nurodo 35 straipsnio 6 dalyje numatytas periodines baudas, jei pateikiama ne visa reikalaujama informacija arba tokia informacija nepateikiama iki šios dalies d punkte nurodyto termino;

f) nurodo teisę apskųsti sprendimą EPI apeliacinei tarybai ir prašyti, kad sprendimas būtų peržiūrėtas Europos Sąjungos Teisingumo Teisme (toliau – Teisingumo Teismas) pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 60 ir 61 straipsnius.

4. Ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių atstovai pateikia prašomą informaciją. Informaciją savo klientų vardu gali pateikti tinkamai įgalioti teisininkai. Visa atsakomybė už pateiktos informacijos išsamumą, teisingumą ir neklaidingumą tenka ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai.

5. Atsakingoji priežiūros institucija nedelsdama perduoda sprendimo pateikti informaciją kopiją finansų sektoriaus subjektų, kurie naudojasi atitinkamų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių paslaugomis, kompetentingoms institucijoms ir JPT.

38 straipsnis

Bendrieji tyrimai

1. Kad įvykdytų šiame reglamente nustatytas pareigas, Atsakingoji priežiūros institucija, padedama 40 straipsnio 1 dalyje nurodytos jungtinės tyrimo grupės, prireikus gali atlikti ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių tyrimus.

2. Atsakingoji priežiūros institucija turi įgaliojimus:

a) nagrinėti įrašus, duomenis, procedūras ir bet kurią kitą medžiagą, susijusią su jos užduočių vykdymu, neatsižvelgiant į tai, kokiose laikmenose jie saugomi;

b) daryti ar gauti tokių įrašų, duomenų, dokumentuojamų procedūrų ir bet kurios kitos medžiagos patvirtintas kopijas ar išrašus;

c) pakviesti ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies atstovus, kad jie žodžiu arba raštu pateiktų paaiškinimus dėl faktų ar dokumentų, susijusių su tyrimo dalyku ir tikslu, ir užfiksuoti atsakymus;

d) apklausti visus kitus fizinius ar juridinius asmenis, kurie sutinka būti apklausti, siekiant surinkti su tyrimo dalyku susijusios informacijos;

e) prašyti pateikti telefono pokalbių ir duomenų srauto išklotines.

3. Pareigūnai ir kiti asmenys, kuriems Atsakingoji priežiūros institucija yra suteikusi įgaliojimus 1 dalyje nurodyto tyrimo tikslais, savo įgaliojimais naudojasi pateikę raštišką įgaliojimą, kuriame nurodomas tyrimo dalykas ir tikslas.

Tame įgaliojime taip pat nurodomos 35 straipsnio 6 dalyje numatytos periodinės baudos, taikomos tais atvejais, jei reikalaujami įrašai, duomenys, dokumentuojamos procedūros ar bet kuri kita medžiaga, arba atsakymai į klausimus, užduotus IRT paslaugas teikiančios trečiosios šalies atstovams, nepateikti arba pateikti ne visi.

4. Ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies atstovai turi leisti atlikti tyrimus, reikalaujamus remiantis Atsakingosios priežiūros institucijos sprendimu. Sprendime nurodomas tyrimo dalykas ir tikslas, 35 straipsnio 6 dalyje numatytos periodinės baudos, pagal reglamentus (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 taikomos teisių gynimo priemonės bei teisė prašyti, kad sprendimas būtų peržiūrėtas Teisingumo Teisme.

5. Likus pakankamai laiko iki tyrimo pradžios, Atsakingoji priežiūros institucija praneša finansų sektoriaus subjektų, kurie naudojasi tos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies IRT paslaugomis, kompetentingoms institucijoms apie numatomą tyrimą ir nurodo įgaliotų asmenų tapatybę.

Atsakingoji priežiūros institucija perduoda JPT visą pagal pirmą pastraipą perduotą informaciją.

39 straipsnis

Patikrinimai

1. Kad įvykdytų šiame reglamente nustatytas pareigas, Atsakingoji priežiūros institucija, padedama 40 straipsnio 1 dalyje nurodytų jungtinių tyrimo grupių, gali patekti į IRT paslaugas teikiančių trečiųjų šalių verslo patalpas, teritoriją arba valdą, pavyzdžiui, pagrindines buveines, operacijų centrus, pagalbines patalpas, ir atlikti visus būtinus patikrinimus vietoje, taip pat atlikti patikrinimus ne vietoje.

Naudodamasi pirmoje pastraipoje nurodytais įgaliojimais Atsakingoji priežiūros institucija konsultuojasi su JPT.

2. Pareigūnai ir kiti asmenys, Atsakingosios priežiūros institucijos įgalioti atlikti patikrinimą vietoje, turi įgaliojimus:

a) patekti į tokias verslo patalpas, teritoriją arba valdą ir

b) užplombuoti bet kurias tokias verslo patalpas, buhalterines knygas ar įrašus tokiam laikotarpiui ir tokiu mastu, koks būtinas patikrinimui atlikti.

Atsakingosios priežiūros institucijos įgalioti pareigūnai ir kiti asmenys naudojasi savo įgaliojimais pateikę raštišką įgaliojimą, kuriame nurodomas patikrinimo dalykas bei tikslas ir 35 straipsnio 6 dalyje numatytos periodinės baudos, kurios yra taikomos, jei atitinkamų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių atstovai neleidžia atlikti patikrinimo.

3. Likus pakankamai laiko iki patikrinimo pradžios Atsakingoji priežiūros institucija informuoja finansų sektoriaus subjektų, kurie naudojasi tos IRT paslaugas teikiančios trečiosios šalies paslaugomis, kompetentingas institucijas.

4. Patikrinimai apima visas susijusias IRT sistemas, tinklus, įrenginius, informaciją ir duomenis, naudojamus IRT paslaugoms finansų sektoriaus subjektams teikti arba padedančius jas teikti.

5. Likus pakankamai laiko iki bet kurio planuojamo patikrinimo vietoje Atsakingoji priežiūros institucija apie tai įspėja ypatingos svarbos IRT paslaugas teikiančias trečiąsias šalis, išskyrus atvejus, kai tai neįmanoma dėl susidariusios ekstremalios padėties ar krizės arba jeigu dėl tokio įspėjimo patikrinimas ar auditas nebebūtų veiksmingas.

6. Ypatingos svarbos IRT paslaugas teikianti trečioji šalis leidžia atlikti Atsakingosios priežiūros institucijos sprendimu paskirtus patikrinimus vietoje. Sprendime nurodomas patikrinimo dalykas ir tikslas, nustatoma data, kada patikrinimas turi prasidėti, ir nurodomos 35 straipsnio 6 dalyje numatytos periodinės baudos, pagal reglamentus (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 taikomos teisių gynimo priemonės bei teisė prašyti, kad sprendimas būtų peržiūrėtas Teisingumo Teisme.

7. Jei Atsakingosios priežiūros institucijos įgalioti pareigūnai ir kiti asmenys nustato, kad ypatingos svarbos IRT paslaugas teikianti trečioji šalis nesutinka, jog būtų atliktas pagal šį straipsnį paskirtas patikrinimas, Atsakingoji priežiūros institucija informuoja ypatingos svarbos IRT paslaugas teikiančią trečiąją šalį apie tokio nesutikimo padarinius, įskaitant galimybę atitinkamų finansų sektoriaus subjektų kompetentingoms institucijoms reikalauti, kad finansų sektoriaus subjektai nutrauktų su ta ypatingos svarbos IRT paslaugas teikiančia trečiąja šalimi sudarytus sutartimi įformintus susitarimus.

40 straipsnis

Nuolatinė priežiūra

1. Vykdant priežiūros veiklą, visų pirma bendruosius tyrimus arba patikrinimus, Atsakingajai priežiūros institucijai padeda jungtinė tyrimo grupė, suburta kiekvienai ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai.

2. 1 dalyje nurodytą jungtinę tyrimo grupę sudaro darbuotojai iš:

a) EPI;

b) atitinkamų kompetentingų institucijų, prižiūrinčių finansų sektoriaus subjektus, kuriems ypatingos svarbos IRT paslaugas teikianti trečioji šalis teikia IRT paslaugas;

c) 32 straipsnio 4 dalies e punkte nurodytos nacionalinės kompetentingos institucijos (dalyvauja savanoriškai);

d) viena valstybės narės, kurioje yra įsisteigusi ypatingos svarbos IRT paslaugas teikianti trečioji šalis, nacionalinė kompetentinga institucija (dalyvauja savanoriškai).

Jungtinės tyrimo grupės nariai turi turėti ekspertinių žinių IRT klausimais ir operacinės rizikos srityje. Jungtinės tyrimo grupės darbą koordinuoja paskirtas Atsakingosios priežiūros institucijos darbuotojas (toliau – Atsakingosios priežiūros institucijos koordinatorius).

3. Per tris mėnesius nuo tyrimo arba patikrinimo pabaigos Atsakingoji priežiūros institucija, pasikonsultavusi su Priežiūros forumu, naudodamasi 35 straipsnyje nurodytais įgaliojimais priima rekomendacijas, skirtas ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai.

4. 3 dalyje nurodytos rekomendacijos nedelsiant perduodamos ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai ir finansų sektoriaus subjektų, kuriems ji teikia IRT paslaugas, kompetentingoms institucijoms.

Vykdydama priežiūros veiklą Atsakingoji priežiūros institucija gali atsižvelgti į visus atitinkamus trečiųjų šalių sertifikatus ir IRT paslaugas teikiančių trečiųjų šalių vidaus ar išorės audito ataskaitas, pateikiamus ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies.

41 straipsnis

Sąlygų, kuriomis galima vykdyti priežiūros veiklą, suderinimas

1. EPI Jungtiniame komitete parengia techninių reguliavimo standartų projektus, kuriuose nurodoma:

a) informacija, kurią IRT paslaugas teikianti trečioji šalis turi pateikti savanoriškame prašyme būti pripažinta esančia ypatingos svarbos pagal 31 straipsnio 11 dalį;

b) informacijos, kurią IRT paslaugas teikiančios trečiosios šalys turi pateikti, atskleisti arba pranešti pagal 35 straipsnio 1 dalį, turinys, struktūra ir formatas, įskaitant informacijos apie subrangos susitarimus pateikimo šabloną;

c) kriterijai, pagal kuriuos nustatoma jungtinės tyrimo grupės sudėtis, užtikrinant subalansuotą EPI ir atitinkamų kompetentingų institucijų darbuotojų dalyvavimą, jų skyrimą, užduotis ir darbo tvarką.

d) išsami informacija apie kompetentingų institucijų atliekamą ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priemonių, taikytų remiantis Atsakingosios priežiūros institucijos rekomendacijomis pagal 42 straipsnio 3 dalį, vertinimą.

2. EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai ne vėliau kaip 2024 m. liepos 17 d.

Komisijai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsnius suteikiami įgaliojimai papildyti šį reglamentą priimant 1 dalyje nurodytus techninius reguliavimo standartus.

42 straipsnis

Kompetentingų institucijų tolesni veiksmai

1. Per 60 kalendorinių dienų nuo Atsakingosios priežiūros institucijos pagal 35 straipsnio 1 dalies d punktą pateiktų rekomendacijų gavimo ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys Atsakingajai priežiūros institucijai praneša apie savo ketinimą laikytis rekomendacijų arba pateikia pagrįstą paaiškinimą, kodėl jos tokių rekomendacijų nesilaikys. Atsakingoji priežiūros institucija nedelsdama perduoda šią informaciją atitinkamų finansų sektoriaus subjektų kompetentingoms institucijoms.

2. Atsakingoji priežiūros institucija viešai atskleidžia atvejus, kai ypatingos svarbos IRT paslaugas teikianti trečioji šalis neinformuoja Atsakingosios priežiūros institucijos pagal 1 dalį arba kai ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies pateiktas paaiškinimas laikomas nepakankamu. Paskelbtoje informacijoje atskleidžiama ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies tapatybė, taip pat informacija apie reikalavimų nesilaikymo rūšį ir pobūdį. Tokia informacija apima tik tai, kas yra aktualu ir proporcinga norint užtikrinti visuomenės informuotumą, išskyrus atvejus, kai toks paskelbimas darytų neproporcingą žalą susijusioms šalims arba galėtų rimtai pakenkti finansų rinkų tvarkingam veikimui ir vientisumui arba visos Sąjungos finansų sistemos ar jos dalies stabilumui.

Atsakingoji priežiūros institucija praneša ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai apie tą viešą atskleidimą.

3. Kompetentingos institucijos informuoja atitinkamus finansų sektoriaus subjektus apie riziką, nustatytą ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims skirtose rekomendacijose, pateiktose pagal 35 straipsnio 1 dalies d punktą.

Valdydami trečiosios šalies keliamą IRT riziką, finansų sektoriaus subjektai atsižvelgia į pirmoje pastraipoje nurodytą riziką.

4. Jeigu kompetentinga institucija mano, kad finansų sektoriaus subjektas, valdydamas trečiosios šalies keliamą IRT riziką, neatsižvelgia arba nepakankamai atsižvelgia į konkrečią rekomendacijose nustatytą riziką, ji praneša finansų sektoriaus subjektui apie galimybę per 60 kalendorinių dienų nuo tokio pranešimo gavimo dienos pagal 6 dalį priimti sprendimą, jei nebus atitinkamų sutartimi įformintų susitarimų, kuriais būtų siekiama pašalinti tokią riziką.

5. Gavusios 35 straipsnio 1 dalies c punkte nurodytas ataskaitas ir prieš priimdamos šio straipsnio 6 dalyje nurodytą sprendimą kompetentingos institucijos gali savanoriškai pasikonsultuoti su pagal Direktyvą (ES) 2022/2555 paskirtomis ar įsteigtomis kompetentingomis institucijomis, atsakingomis už esminio ar svarbaus subjekto, kuriam taikoma ta direktyva ir kuris buvo pripažintas ypatingos svarbos IRT paslaugas teikiančia trečiąja šalimi, priežiūrą.

6. Kompetentingos institucijos gali kaip kraštutinę priemonę po to, kai pateikiamas pranešimas ir, jei tinkama, po konsultacijų, kaip nustatyta šio straipsnio 4 ir 5 dalyse, pagal 50 straipsnį priimti sprendimą, kuriuo reikalaujama, kad finansų sektoriaus subjektai laikinai iš dalies arba visiškai sustabdytų ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies teikiamos paslaugos naudojimą ar diegimą, kol bus imtasi veiksmų dėl rizikos, nustatytos ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims skirtose rekomendacijose. Prireikus jos gali reikalauti, kad finansų sektoriaus subjektai iš dalies arba visiškai nutrauktų atitinkamus sutartimi įformintus susitarimus, sudarytus su ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis.

7. Jeigu ypatingos svarbos IRT paslaugas teikianti trečioji šalis atsisako pritarti rekomendacijoms, remdamasi kitokiu požiūriu nei tas, kurį rekomendavo Atsakingoji priežiūros institucija, ir tas kitoks požiūris gali neigiamai paveikti daug finansų sektoriaus subjektų arba reikšmingą finansų sektoriaus dalį, o kompetentingų institucijų individualūs įspėjimai nedavė rezultatų, t. y. nuoseklių požiūrių, kuriais švelninama potenciali rizika finansų stabilumui, nebuvo nustatyta, Atsakingoji priežiūros institucija gali, pasikonsultavusi su Priežiūros forumu, pateikti kompetentingoms institucijoms neprivalomas ir neviešas nuomones, kad paskatintų, kai tinkama, imtis nuoseklių ir suderintų tolesnių priežiūros priemonių.

8. Gavusios 35 straipsnio 1 dalies c punkte nurodytas ataskaitas, kompetentingos institucijos, priimdamos šio straipsnio 6 dalyje nurodytą sprendimą atsižvelgia į rizikos, į kurią ypatingos svarbos IRT paslaugas teikianti trečioji šalis nereaguoja, rūšį ir mastą, taip pat į reikalavimų nesilaikymo rimtumą, pagal šiuos kriterijus:

a) reikalavimų nesilaikymo sunkumą ir trukmę;

b) tai, ar dėl reikalavimų nesilaikymo paaiškėjo rimtų ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies procedūrų, valdymo sistemų, rizikos valdymo ir vidaus kontrolės trūkumų;

c) tai, ar dėl reikalavimų nesilaikymo buvo lengviau įvykdyti finansinį nusikaltimą, reikalavimų nesilaikymas buvo finansinio nusikaltimo priežastis arba finansinis nusikaltimas yra kitaip sietinas su reikalavimų nesilaikymu;

d) tai, ar reikalavimų nesilaikoma tyčia ar dėl aplaidumo;

e) tai, ar dėl sutartimi įformintų susitarimų sustabdymo ar nutraukimo kyla rizika finansų sektoriaus subjekto veiklos operacijų tęstinumui, neatsižvelgiant į finansų sektoriaus subjekto pastangas išvengti jo paslaugų teikimo sutrikimo;

f) kai taikytina, pagal Direktyvą (ES) 2022/2555 paskirtų ar įsteigtų kompetentingų institucijų, atsakingų už esminio ar svarbaus subjekto, kuriam taikoma ta direktyva ir kuris buvo pripažintas ypatingos svarbos IRT paslaugas teikiančia trečiąja šalimi, priežiūrą, pateiktą nuomonę, kurios paprašyta savanoriškai pagal šio straipsnio 5 dalį.

Kompetentingos institucijos suteikia finansų sektoriaus subjektams būtiną laikotarpį, kad jie galėtų pakoreguoti sutartimi įformintus susitarimus su ypatingos svarbos IRT paslaugas teikiančia trečiąja šalimi siekiant išvengti neigiamo poveikio jų skaitmeninės veiklos atsparumui ir sudaryti jiems sąlygas įgyvendinti 28 straipsnyje nurodytas pasitraukimo strategijas ir pereinamojo laikotarpio planus.

9. Apie šio straipsnio 6 dalyje nurodytą sprendimą pranešama 32 straipsnio 4 dalies a, b ir c punktuose nurodytiems Priežiūros forumo nariams ir JPT.

Ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys, kurioms 6 dalyje numatyti sprendimai daro poveikį, turi visapusiškai bendradarbiauti su paveiktais finansų sektoriaus subjektais, visų pirma jų sutartimi įformintų susitarimų sustabdymo ar nutraukimo kontekste.

10. Kompetentingos institucijos reguliariai informuoja Atsakingąją priežiūros instituciją apie požiūrius, kurių jos laikėsi, ir priemones, kurias jos taikė vykdydamos priežiūros užduotis finansų sektoriaus subjektų atžvilgiu, taip pat apie finansų sektoriaus subjektų sudarytus sutartimi įformintus susitarimus, kai ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys iš dalies ar visiškai nepritarė joms skirtoms Atsakingosios priežiūros institucijos rekomendacijoms.

11. Atsakingoji priežiūros institucija gali gavusi prašymą papildomai paaiškinti pateiktas rekomendacijas, kuriomis kompetentingos institucijos galėtų vadovautis imdamosi tolesnių priemonių.

43 straipsnis

Priežiūros mokesčiai

1. Atsakingoji priežiūros institucija, laikydamasi šio straipsnio 2 dalyje nurodyto deleguotojo akto, ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims taiko mokesčius, kurie visiškai padengia būtinas Atsakingosios priežiūros institucijos išlaidas, susijusias su priežiūros užduočių vykdymu pagal šį reglamentą, be kita ko, kompensuoja visas išlaidas, kurios gali būti patiriamos dėl 40 straipsnyje nurodytos jungtinės tyrimo grupės atliekamo darbo, taip pat 32 straipsnio 4 dalies antroje pastraipoje nurodytų nepriklausomų ekspertų teikiamų konsultacijų išlaidas, susijusias su klausimais, patenkančiais į tiesioginės priežiūros veiklos sritį.

Ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai taikomo mokesčio dydis padengia visas išlaidas, susidarančias dėl šiame skirsnyje numatytų pareigų vykdymo, ir yra proporcingas jos apyvartai.

2. Komisijai pagal 57 straipsnį suteikiami įgaliojimai ne vėliau kaip 2024 m. liepos 17 d. priimti deleguotąjį aktą, kuriuo šis reglamentas būtų papildytas nustatant mokesčių dydį ir jų mokėjimo būdą.

44 straipsnis

Tarptautinis bendradarbiavimas

1. Nedarant poveikio 36 straipsniui, EBI, ESMA ir EIOPA, vadovaudamosi atitinkamai reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1095/2010 ir (ES) Nr. 1094/2010 33 straipsniu, gali su trečiųjų valstybių reguliavimo ir priežiūros institucijomis sudaryti administracinius susitarimus, kad būtų skatinamas tarptautinis bendradarbiavimas dėl trečiųjų šalių keliamos IRT rizikos įvairiuose finansų sektoriuose, visų pirma plėtojant geriausią praktiką, susijusią su IRT rizikos valdymo praktikos ir kontrolės priemonių, rizikos mažinimo priemonių ir reagavimo į incidentus peržiūra.

2. EPI per Jungtinį komitetą kas penkerius metus pateikia Europos Parlamentui, Tarybai ir Komisijai bendrą konfidencialią ataskaitą, kurioje apibendrinamos atitinkamų diskusijų su 1 dalyje nurodytomis trečiųjų valstybių institucijomis išvados, daugiausia dėmesio skiriant trečiųjų šalių keliamos IRT rizikos raidai ir jos poveikiui finansiniam stabilumui, rinkos vientisumui, investuotojų apsaugai ir vidaus rinkos veikimui.

VI SKYRIUS

Dalijimosi informacija schemos

45 straipsnis

Dalijimosi informacija ir žvalgybos informacija apie kibernetines grėsmes schemos

1. Finansų sektoriaus subjektai gali tarpusavyje keistis informacija ir žvalgybos informacija apie kibernetines grėsmes, įskaitant užvaldymo rodiklius, taktiką, metodus ir procedūras, kibernetinio saugumo įspėjimus ir konfigūravimo priemones, tiek, kiek toks dalijamasis informacija ir žvalgybos informacija:

a) yra skirtas finansų sektoriaus subjektų skaitmeninės veiklos atsparumui didinti, visų pirma didinant informuotumą apie kibernetines grėsmes, ribojant galimybes arba trukdant plisti kibernetinėms grėsmėms, remiant apsaugos pajėgumus, grėsmių aptikimo metodus, rizikos mažinimo strategijas arba reagavimo ir veiklos atkūrimo etapus;

b) vyksta patikimose finansų sektoriaus subjektų bendruomenėse;

c) yra įgyvendinamas pagal dalijimosi informacija schemas, kuriomis apsaugoma potencialiai neskelbtina informacija, kuria dalijamasi, ir kurioms taikomos elgesio taisyklės, visapusiškai atitinkančios verslo konfidencialumo reikalavimus, asmens duomenų apsaugos reikalavimus pagal Reglamentą (ES) 2016/679 ir konkurencijos politikos gaires.

2. 1 dalies c punkto tikslais dalijimosi informacija schemose apibrėžiamos dalyvavimo sąlygos ir, kai tinkama, išsamiai išdėstomos valdžios institucijų dalyvavimo sąlygos ir kompetencija, pagal kurią jos gali būti įtrauktos į dalijimosi informacija schemas, IRT paslaugas teikiančių trečiųjų šalių dalyvavimo sąlygos ir operaciniai elementai, įskaitant specialių IT platformų naudojimą.

3. Finansų sektoriaus subjektai praneša kompetentingoms institucijoms apie savo dalyvavimą 1 dalyje nurodytose dalijimosi informacija schemose, kai jų narystė patvirtinama arba, jei taikytina, nutraukiama, kai tas nutraukimas įsigalioja.

VII SKYRIUS

Kompetentingos institucijos

46 straipsnis

Kompetentingos institucijos

Nedarant poveikio šio reglamento V skyriaus II skirsnyje nurodytoms ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūros sistemos nuostatoms, šiame reglamente nustatytų pareigų vykdymą pagal atitinkamais teisės aktais suteiktus įgaliojimus užtikrina toliau nurodytos kompetentingos institucijos:

a) kredito įstaigų ir įstaigų, kurioms pagal Direktyvą 2013/36/ES taikoma išimtis, atveju – pagal tos direktyvos 4 straipsnį paskirta kompetentinga institucija, o kredito įstaigų, kurios klasifikuojamos kaip svarbios pagal Reglamento (ES) Nr. 1024/2013 6 straipsnio 4 dalį, atveju – ECB, vadovaujantis tuo reglamentu suteiktais įgaliojimais ir vykdant jame nustatytas užduotis;

b) mokėjimo įstaigų, įskaitant mokėjimo įstaigas, kurioms pagal Direktyvą (ES) 2015/2366 taikoma išimtis, elektroninių pinigų įstaigų, įskaitant tas, kurioms pagal Direktyvą 2009/110/EB taikoma išimtis, ir informavimo apie sąskaitas paslaugų teikėjų, nurodytų Direktyvos (ES) 2015/2366 33 straipsnio 1 dalyje, atveju – kompetentinga institucija, paskirta pagal Direktyvos (ES) 2015/2366 22 straipsnį;

c) investicinių įmonių atveju – kompetentinga institucija, paskirta pagal Europos Parlamento ir Tarybos direktyvos (ES) 2019/2034 ([38]) 4 straipsnį;

d) kriptoturto paslaugų teikėjų, turinčių veiklos leidimą pagal Reglamentą dėl kriptoturto rinkų, ir su turtu susietų žetonų emitentų atveju – kompetentinga institucija, paskirta pagal atitinkamą to reglamento nuostatą;

e) centrinių vertybinių popierių depozitoriumų atveju – kompetentinga institucija, paskirta pagal Reglamento (ES) Nr. 909/2014 11 straipsnį;

f) pagrindinių sandorio šalių atveju – kompetentinga institucija, paskirta pagal Reglamento (ES) Nr. 648/2012 22 straipsnį;

g) prekybos vietų ir duomenų teikimo paslaugų teikėjų atveju –kompetentinga institucija, paskirta pagal Direktyvos 2014/65/ES 67 straipsnį, ir kompetentinga institucija, kaip apibrėžta Reglamento (ES) Nr. 600/2014 2 straipsnio 1 dalies 18 punkte;

h) sandorių duomenų saugyklų atveju – kompetentinga institucija, paskirta pagal Reglamento (ES) Nr. 648/2012 22 straipsnį;

i) alternatyvaus investavimo fondų valdytojų atveju – kompetentinga institucija, paskirta pagal Direktyvos 2011/61/ES 44 straipsnį;

j) valdymo įmonių atveju – kompetentinga institucija, paskirta pagal Direktyvos 2009/65/EB 97 straipsnį;

k) draudimo ir perdraudimo įmonių atveju – kompetentinga institucija, paskirta pagal Direktyvos 2009/138/EB 30 straipsnį;

l) draudimo tarpininkų, perdraudimo tarpininkų ir papildomos draudimo veiklos tarpininkų atveju – kompetentinga institucija, paskirta pagal Direktyvos (ES) 2016/97 12 straipsnį;

m) profesinių pensijų išmokėjimo atveju – kompetentinga institucija, paskirta pagal Direktyvos (ES) 2016/2341 47 straipsnį;

n) kredito reitingų agentūrų atveju – kompetentinga institucija, paskirta pagal Reglamento (EB) Nr. 1060/2009 21 straipsnį;

o) ypatingos svarbos lyginamųjų indeksų administratorių atveju – kompetentinga institucija, paskirta pagal Reglamento (ES) 2016/1011 40 ir 41 straipsnius;

([38]) 2019 m. lapkričio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/2034 dėl investicinių įmonių riziką ribojančios priežiūros, kuria iš dalies keičiamos direktyvos 2002/87/EB, 2009/65/EB, 2011/61/ES, 2013/36/ES, 2014/59/ES ir 2014/65/ES (OL L 314, 2019 12 5, p. 64).

p) sutelktinio finansavimo paslaugų teikėjų atveju – kompetentinga institucija, paskirta pagal Reglamento (ES) 2020/1503 29 straipsnį;

q) pakeitimo vertybiniais popieriais duomenų saugyklų atveju – kompetentinga institucija, paskirta pagal Reglamento (ES) 2017/2402 10 straipsnį ir 14 straipsnio 1 dalį.

47 straipsnis

Bendradarbiavimas su struktūromis ir institucijomis, įsteigtomis Direktyva (ES) 2022/2555

1. Siekiant skatinti pagal šį reglamentą paskirtų kompetentingų institucijų ir pagal Direktyvos (ES) 2022/2555 14 straipsnį įsteigtos Bendradarbiavimo grupės bendradarbiavimą ir sudaryti sąlygas keistis priežiūros informacija, EPI ir kompetentingos institucijos gali dalyvauti Bendradarbiavimo grupės veikloje klausimais, aktualiais jų priežiūros veiklai, susijusiai su finansų sektoriaus subjektais. EPI ir kompetentingos institucijos gali prašyti būti pakviestos dalyvauti Bendradarbiavimo grupės darbe klausimais, susijusiais su esminiais ar svarbiais subjektais, kuriems taikoma Direktyva (ES) 2022/2555, kurie pagal šio reglamento 31 straipsnį taip pat buvo pripažinti ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis.

2. Kai tinkama, kompetentingos institucijos gali konsultuotis ir dalytis informacija su bendraisiais informaciniais centrais ir CSIRT, paskirtais ar įsteigtais pagal Direktyvą (ES) 2022/2555.

3. Kai tinkama, kompetentingos institucijos gali prašyti kompetentingų institucijų, paskirtų ar įsteigtų pagal Direktyvą (ES) 2022/2555 atitinkamų techninių konsultacijų bei pagalbos ir sudaryti bendradarbiavimo susitarimus, kuriais būtų sudarytos sąlygos sukurti veiksmingus ir greitą reagavimą užtikrinančius koordinavimo mechanizmus.

4. Šio straipsnio 3 dalyje nurodytuose susitarimuose, *inter alia*, nurodomos priežiūros ir priežiūros veiklos koordinavimo procedūros, susijusios su esminiais ar svarbiais subjektais, kuriems taikoma Direktyva (ES) 2022/2555, kurie pagal šio reglamento 31 straipsnį pripažinti ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis, be kita ko, siekiant pagal nacionalinę teisę vykdyti tyrimus ir patikrinimus vietoje, taip pat taikyti pagal šį reglamentą nustatytų kompetentingų institucijų ir pagal tą direktyvą paskirtų ar įsteigtų kompetentingų institucijų keitimosi informacija mechanizmus, apimančius prieigą prie pastarųjų institucijų prašomos informacijos.

48 straipsnis

Institucijų bendradarbiavimas

1. Kompetentingos institucijos glaudžiai bendradarbiauja tarpusavyje ir, kai taikytina, su Atsakingąja priežiūros institucija.

2. Kompetentingos institucijos ir Atsakingoji priežiūros institucija laiku tarpusavyje keičiasi visa atitinkama informacija, susijusia su ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis, kuri yra būtina tam, kad jos galėtų vykdyti savo atitinkamas pareigas pagal šį reglamentą, visų pirma susijusias su nustatyta rizika, požiūriais, kurių laikomasi, ir priemonėmis, kurių imamasi vykdant Atsakingosios priežiūros institucijos priežiūros užduotis.

49 straipsnis

Finansinės tarpsektorinės užduotys, komunikacija ir bendradarbiavimas

1. EPI per Jungtinį komitetą ir bendradarbiaudamos atitinkamai su kompetentingomis institucijomis, pertvarkymo institucijomis, nurodytomis Direktyvos 2014/59/ES 3 straipsnyje, ECB, Bendra pertvarkymo valdyba, jei informacija susijusi su subjektais, kuriems taikomas Reglamentas (ES) Nr. 806/2014, ESRV ir ENISA, gali nustatyti mechanizmus, kurie sudarytų sąlygas dalytis veiksminga praktika skirtinguose finansų sektoriuose, kad būtų didinamas informuotumas apie padėtį ir nustatomi bendri kibernetiniai pažeidžiamumo atvejai ir rizika įvairiuose sektoriuose.

Jos gali parengti krizių valdymo ir nenumatytų atvejų pratybas, apimančias kibernetinių išpuolių scenarijus, siekdamos plėtoti komunikacijos kanalus ir palaipsniui sudaryti sąlygas veiksmingam Sąjungos lygmens koordinuotam atsakui didelio tarpvalstybinio IRT incidento ar susijusios grėsmės, turinčios sisteminį poveikį visam Sąjungos finansų sektoriui, atveju.

Atitinkamais atvejais tos užduotys taip pat gali padėti patikrinti finansų sektoriaus priklausomybę nuo kitų ekonomikos sektorių.

2. Kompetentingos institucijos, EPI ir ECB glaudžiai bendradarbiauja tarpusavyje ir keičiasi informacija, kad galėtų vykdyti savo pareigas pagal 47–54 straipsnius. Jie glaudžiai koordinuoja jų vykdomą priežiūros veiklą, kad būtų nustatyti ir ištaisyti šio reglamento pažeidimai, plėtojama ir skatinama geriausia praktika, palengvinamas bendradarbiavimas, skatinamas nuoseklus aiškinimas ir teikiami įvairius jurisdikciją turinčius subjektus apimantys vertinimai nesutarimų atveju.

50 straipsnis

Administracinės nuobaudos ir taisomosios priemonės

1. Kompetentingos institucijos turi visus priežiūros, tyrimo ir sankcijų taikymo įgaliojimus, būtinus jų pareigoms pagal šį reglamentą vykdyti.

2. 1 dalyje nurodyti įgaliojimai apima bent šiuos įgaliojimus:

a) susipažinti su visais bet kokios formos dokumentais arba duomenimis, kurie, kompetentingos institucijos manymu, reikalingi jos pareigoms vykdyti, ir gauti arba pasidaryti jų kopiją;

b) atlikti patikrinimus vietoje arba tyrimus, kurie apima išvardytuosius toliau, bet jais neapsiriboja:

   i) pakviesti finansų sektoriaus subjektų atstovus, kad jie žodžiu arba raštu pateiktų paaiškinimus dėl faktų ar dokumentų, susijusių su tyrimo dalyku ir tikslu, ir užfiksuoti atsakymus;

   ii) apklausti visus kitus fizinius ar juridinius asmenis, kurie sutinka būti apklausti, siekiant surinkti su tyrimo dalyku susijusios informacijos;

c) reikalauti šio reglamento reikalavimų pažeidimų atvejais taikyti korekcines ir taisomąsias priemones.

3. Nedarant poveikio valstybių narių teisei taikyti baudžiamąsias sankcijas pagal 52 straipsnį, valstybės narės nustato taisykles, pagal kurias už šio reglamento pažeidimus skiriamos atitinkamos administracinės nuobaudos ir taisomosios priemonės, ir užtikrina veiksmingą jų įgyvendinimą.

Tos nuobaudos ir priemonės turi būti veiksmingos, proporcingos ir atgrasančios.

4. Valstybės narės suteikia kompetentingoms institucijoms įgaliojimus už šio reglamento reikalavimų pažeidimus taikyti bent šias administracines nuobaudas arba taisomąsias priemones:

a) paskelbti įsakymą fiziniam arba juridiniam asmeniui atsisakyti elgesio, kuriuo pažeidžiamas šis reglamentas, ir nebekartoti to elgesio;

b) reikalauti laikinai arba visam laikui nutraukti bet kokią praktiką ar elgesį, kurie, kompetentingos institucijos manymu, prieštarauja šio reglamento nuostatoms, ir užkirsti kelią tos praktikos ar elgesio pasikartojimui;

c) patvirtinti bet kurios rūšies priemonę, įskaitant piniginę, kurią taikant galima užtikrinti, kad finansų sektoriaus subjektai nuolat laikytųsi teisinių reikalavimų;

d) tiek, kiek leidžiama pagal nacionalinę teisę, reikalauti esamų duomenų srauto išklotinių, kurias turi telekomunikacijų operatorius, kai pagrįstai įtariama, kad padarytas šio reglamento pažeidimas, ir kai tokios išklotinės gali būti svarbios tiriant šio reglamento pažeidimus, ir

e) skelbti viešus įspėjimus, įskaitant viešus pareiškimus, kuriuose nurodoma fizinio arba juridinio asmens tapatybė ir pažeidimo pobūdis.

5. Kai 2 dalies c punktas ir 4 dalis taikomi juridiniams asmenims, valstybės narės suteikia kompetentingoms institucijoms įgaliojimus, laikantis nacionalinėje teisėje numatytų sąlygų, skirti administracines nuobaudas ir taisomąsias priemones valdymo organo nariams ir kitiems asmenims, kurie pagal nacionalinę teisę yra atsakingi už pažeidimą.

6. Valstybės narės užtikrina, kad visi sprendimai, kuriais skiriamos 2 dalies c punkte nustatytos administracinės nuobaudos ar taisomosios priemonės, būtų tinkamai motyvuoti ir galėtų būti apskųsti.

51 straipsnis

Naudojimasis įgaliojimu skirti administracines nuobaudas ir taisomąsias priemones

1. Kompetentingos institucijos savo įgaliojimais skirti 50 straipsnyje nurodytas administracines nuobaudas ir taisomąsias priemones naudojasi pagal savo nacionalines teisines sistemas, kai tinkama, tokiu būdu:

a) tiesiogiai;

b) bendradarbiaudamos su kitomis institucijomis;

c) savo atsakomybe perduodamos įgaliojimus kitoms institucijoms; arba

d) kreipdamosi į kompetentingas teismines institucijas.

2. Priimdamos sprendimą dėl administracinių nuobaudų ar taisomųjų priemonių, skiriamų pagal 50 straipsnį, rūšies ir dydžio, kompetentingos institucijos atsižvelgia į tai, kiek pažeidimas yra tyčinis ar padarytas dėl aplaidumo, ir į visas kitas atitinkamas aplinkybes, įskaitant, kai tinkama, šias:

a) pažeidimo reikšmingumą, sunkumą ir trukmę;

b) už pažeidimą atsakingo fizinio ar juridinio asmens atsakomybės laipsnį;

c) atsakingo fizinio ar juridinio asmens finansinį pajėgumą;

d) atsakingo fizinio ar juridinio asmens gauto pelno arba išvengtų nuostolių, jei juos galima nustatyti, dydį;

e) dėl pažeidimo patirtus trečiųjų šalių nuostolius, jei juos galima nustatyti;

f) atsakingo fizinio ar juridinio asmens bendradarbiavimo su kompetentinga institucija lygį, nedarant poveikio poreikiui užtikrinti, kad tas fizinis ar juridinis asmuo grąžintų neteisėtai gautą pelną ar išvengtus nuostolius;

g) atsakingo fizinio ar juridinio asmens anksčiau padarytus pažeidimus.

52 straipsnis

Baudžiamosios sankcijos

1. Valstybės narės gali priimti sprendimą nenustatyti taisyklių dėl administracinių nuobaudų ar taisomųjų priemonių už pažeidimus, už kuriuos pagal jų nacionalinę teisę skiriamos baudžiamosios sankcijos.

2. Jeigu valstybės narės yra nusprendusios nustatyti baudžiamąsias sankcijas už šio reglamento pažeidimus, jos užtikrina, kad būtų nustatytos tinkamos priemonės, kad kompetentingos institucijos turėtų visus būtinus įgaliojimus palaikyti ryšius su savo jurisdikcijos teisminėmis, baudžiamojo persekiojimo ar baudžiamosios justicijos institucijomis, kad galėtų gauti konkrečią informaciją, susijusią su nusikalstamų veikų tyrimais arba procesais, pradėtais dėl šio reglamento pažeidimų, ir tą pačią informaciją teikti kitoms kompetentingoms institucijoms ir EBI, ESMA ar EIOPA, ir taip galėtų įvykdyti pareigas bendradarbiauti šio reglamento tikslais.

53 straipsnis

Pareiga pranešti

Valstybės narės ne vėliau kaip 2025 m. sausio 17 d. praneša Komisijai, ESMA, EBI ir EIOPA apie įstatymus ir kitus teisės aktus, kuriais įgyvendinamas šis skyrius, įskaitant visas atitinkamas baudžiamosios teisės nuostatas. Valstybės narės nepagrįstai nedelsdamos praneša Komisijai, ESMA, EBI ir EIOPA apie visus vėlesnius jų pakeitimus.

54 straipsnis

Administracinių nuobaudų skelbimas

1. Kompetentingos institucijos nepagrįstai nedelsdamos savo oficialiose interneto svetainėse skelbia visus sprendimus dėl administracinės nuobaudos skyrimo, jeigu jie nėra apskųsti, po to, kai apie tokį sprendimą pranešama asmeniui, kuriam nuobauda taikoma.

2. Skelbiant 1 dalyje nurodytą informaciją nurodoma pažeidimo rūšis ir pobūdis, atsakingų asmenų tapatybė ir skirtos nuobaudos.

3. Jeigu kompetentinga institucija, kiekvienu konkrečiu atveju atlikusi vertinimą, mano, kad juridinių asmenų tapatybės arba fizinių asmenų tapatybės ir asmens duomenų paskelbimas būtų neproporcingas, įskaitant su asmens duomenų apsauga susijusią riziką, keltų grėsmę finansų rinkų stabilumui ar vykdomam baudžiamajam tyrimui arba padarytų neproporcingą žalą atitinkamam asmeniui, kiek ją galima nustatyti, ji sprendimo dėl administracinės nuobaudos skyrimo atžvilgiu priima vieną iš toliau nurodytų sprendimų:

a) atidėti jo paskelbimą tol, kol nebeliks jokių priežasčių jo neskelbti;

b) paskelbti nuasmenintą sprendimą pagal nacionalinę teisę arba

c) jo neskelbti, jeigu manoma, kad pasirinkus a ir b punktuose nurodytus variantus būtų nepakankamai užtikrinta, kad finansų rinkų stabilumui nekils pavojus, arba jeigu toks paskelbimas būtų neproporcingas skiriamos nuobaudos švelnumui.

4. Tuo atveju, kai pagal 3 dalies b punktą nusprendžiama paskelbti nuasmenintą sprendimą dėl administracinės nuobaudos, atitinkamų duomenų paskelbimas gali būti atidėtas.

5. Jeigu kompetentinga institucija paskelbia sprendimą dėl administracinės nuobaudos skyrimo, kuris atitinkamose teisminėse institucijose yra apskųstas, kompetentingos institucijos nedelsdamos savo oficialioje interneto svetainėje paskelbia tą informaciją, o vėliau paskelbia ir visą paskesnę susijusią informaciją apie tokio skundo nagrinėjimo rezultatus. Taip pat paskelbiami visi teisminės institucijos sprendimai, kuriais sprendimas dėl administracinės nuobaudos skyrimo panaikinamas.

6. Kompetentingos institucijos užtikrina, kad bet kokia pagal 1–4 dalis paskelbta informacija jų oficialioje interneto svetainėje būtų prieinama tik tokį laikotarpį, kuris yra būtinas šio straipsnio taikymo tikslais. Šis laikotarpis negali viršyti penkerių metų nuo informacijos paskelbimo.

55 straipsnis

Profesinė paslaptis

1. Bet kokiai konfidencialiai informacijai, kuri yra gauta, kuria keičiamasi ar kuri yra perduodama pagal šį reglamentą, taikomos 2 dalyje nustatytos profesinės paslapties sąlygos.

2. Pareiga saugoti profesinę paslaptį taikoma visiems asmenims, kurie dirba ar dirbo kompetentingose institucijose pagal šį reglamentą arba bet kokioje kitoje institucijoje ar rinkos subjekte, arba fiziniam arba juridiniam asmeniui, kuriems tos kompetentingos institucijos delegavo savo įgaliojimus, įskaitant jų samdomus auditorius ir ekspertus.

3. Informacija, kuriai taikomas profesinės paslapties reikalavimas, įskaitant pagal šį reglamentą nustatytų kompetentingų institucijų ir pagal Direktyvą (ES) 2022/2555 paskirtų ar įsteigtų kompetentingų institucijų keitimąsi informacija, negali būti atskleista jokiam kitam asmeniui ar institucijai, išskyrus Sąjungos arba nacionalinės teisės nuostatose nurodytais atvejais.

4. Visa su verslo ar veiklos sąlygomis ir kitais ekonominiais ar asmeniniais reikalais susijusi informacija, kuria pagal šį reglamentą tarpusavyje keičiasi kompetentingos institucijos, laikoma konfidencialia ir jai taikomi profesinės paslapties reikalavimai, išskyrus atvejus, kai perduodama tokią informaciją kompetentinga institucija pareiškia, kad ši informacija gali būti atskleidžiama, arba kai toks atskleidimas būtinas teismo procesui.

56 straipsnis

Duomenų apsauga

1. EPI ir kompetentingoms institucijoms leidžiama tvarkyti asmens duomenis tik tais atvejais, kai tai būtina jų atitinkamoms pareigoms, taip pat jų pareigoms pagal šį reglamentą vykdyti, visų pirma tyrimo, tikrinimo, prašymo pateikti informaciją, komunikacijos, skelbimo, įvertinimo, patikrinimo, vertinimo ir priežiūros planų rengimo tikslais. Asmens duomenys tvarkomi pagal Reglamentą (ES) 2016/679 arba Reglamentą (ES) 2018/1725, atsižvelgiant į tai, kuris taikomas.

2. Išskyrus atvejus, kai sektorių teisės aktuose numatyta kitaip, 1 dalyje nurodyti asmens duomenys saugomi iki taikomų priežiūros pareigų įvykdymo ir bet kuriuo atveju ne ilgiau kaip 15 metų, išskyrus atvejus, kai vyksta teismo procesas, kuriam tokius duomenis reikia saugoti ilgiau.

VIII SKYRIUS

Deleguotieji aktai

57 straipsnis

Įgaliojimų delegavimas

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

2. 31 straipsnio 6 dalyje ir 43 straipsnio 2 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo 2024 m. sausio 17 d. 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 31 straipsnio 6 dalyje ir 43 straipsnio 2 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 31 straipsnio 6 dalį ir 43 straipsnio 2 dalį priimtas deleguotasis aktas įsigalioja tik tuo atveju, jeigu per tris 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 trimis mėnesiais.

IX SKYRIUS

Pereinamojo laikotarpio ir baigiamosios nuostatos

I skirsnis

58 straipsnis

Nuostata dėl peržiūros

1. Komisija ne vėliau kaip 2028 m. sausio 17 d., atitinkamai pasikonsultavusi su EPI ir ESRV, atlieka peržiūrą ir Europos Parlamentui ir Tarybai pateikia ataskaitą, prie kurios prireikus prideda pasiūlymą dėl teisėkūros procedūra priimamo akto. Peržiūra turi apimti bent šiuos aspektus:

a) IRT paslaugas teikiančių trečiųjų šalių pripažinimą esant ypatingos svarbos pagal 31 straipsnio 2 dalį kriterijus;

b) 19 straipsnyje nurodyto pranešimo apie dideles kibernetines grėsmes savanorišką pobūdį;

c) 31 straipsnio 12 dalyje nurodytą tvarką ir 35 straipsnio 1 dalies d punkto iv papunkčio pirmoje įtraukoje numatytus Atsakingosios priežiūros institucijos įgaliojimus, siekiant įvertinti tų nuostatų veiksmingumą, susijusį su ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių, įsisteigusių trečiojoje valstybėje, veiksmingos priežiūros užtikrinimu, ir poreikį įsteigti patronuojamąją įmonę Sąjungoje.

   Atliekant peržiūrą šio punkto pirmos pastraipos tikslais įtraukiama 31 straipsnio 12 dalyje nurodytos tvarkos analizė, įskaitant kiek tai susiję su Sąjungos finansų sektoriaus subjektų prieigos prie paslaugų, teikiamų iš trečiųjų valstybių, sąlygomis ir tokių paslaugų prieinamumu Sąjungos rinkoje, ir atsižvelgiama į tolesnius pokyčius paslaugų, kurioms taikomas šis reglamentas, rinkose, su taikymu susijusią finansų sektoriaus subjektų ir finansų priežiūros institucijų praktinę patirtį ir atitinkamai tos tvarkos priežiūrą, taip pat visus aktualius tarptautiniu lygmeniu vykstančius reguliavimo ir priežiūros pokyčius;

d) tai, ar tikslinga į šio reglamento taikymo sritį įtraukti 2 straipsnio 3 dalies e punkte nurodytus finansų sektoriaus subjektus, kurie naudojasi automatinėmis prekybos sistemomis, atsižvelgiant į būsimą rinkos raidą, susijusią su tokių sistemų naudojimu;

e) JPT veikimą ir veiksmingumą padedant užtikrinti priežiūros nuoseklumą ir keitimosi informacija Priežiūros tinkle veiksmingumą.

2. Atlikdama Direktyvos (ES) 2015/2366 peržiūrą, Komisija įvertina didesnio mokėjimo sistemų ir mokėjimų vykdymo veiklos kibernetinio atsparumo poreikį, taip pat šio reglamento taikymo srities išplėtimo įtraukiant mokėjimo sistemų operatorius ir mokėjimų vykdymo veikloje dalyvaujančius subjektus tikslingumą. Atsižvelgdama į šį vertinimą, Komisija ne vėliau kaip 2023 m. liepos 17 d., atlikdama Direktyvos (ES) 2015/2366 peržiūrą, pateikia ataskaitą Europos Parlamentui ir Tarybai.

Remdamasi ta peržiūros ataskaita ir pasikonsultavusi su EPI, ECB ir ESRV, Komisija, jei tinkama ir kaip pasiūlymo dėl teisėkūros procedūra priimamo akto, kurį ji gali priimti pagal Direktyvos (ES) 2015/2366 108 straipsnio antrą pastraipą, dalį gali patekti pasiūlymą, kuriuo būtų užtikrinta, kad visi mokėjimo sistemų operatoriai ir mokėjimų vykdymo veikloje dalyvaujantys subjektai būtų tinkamai prižiūrimi, kartu atsižvelgiant į esamą centrinio banko vykdomą priežiūrą.

3. Ne vėliau kaip 2026 m. sausio 17 d. Komisija, pasikonsultavusi su EPI ir Europos audito priežiūros įstaigų komitetu, atlieka peržiūrą ir pateikia Europos Parlamentui ir Tarybai ataskaitą, prie kurios prireikus prideda pasiūlymą dėl teisėkūros procedūra priimamo akto dėl tikslingumo sugriežtinti teisės aktų nustatytą auditą atliekantiems auditoriams ir audito įmonėms taikomus reikalavimus, susijusius su skaitmeninės veiklos atsparumu, įtraukiant teisės aktų nustatytą auditą atliekančius auditorius ir audito įmones į šio reglamento taikymo sritį arba iš dalies pakeičiant Europos Parlamento ir Tarybos direktyvą 2006/43/EB ([39]).

II SKIRSNIS

Pakeitimai

59 straipsnis

Reglamento (EB) Nr. 1060/2009 daliniai pakeitimai

Reglamentas (EB) Nr. 1060/2009 iš dalies keičiamas taip:

1) I priedo A skirsnio 4 punkto pirma pastraipa pakeičiama taip:

„Kredito reitingų agentūra turi turėti patikimas administracines bei apskaitos procedūras, vidaus kontrolės mechanizmus, efektyvias rizikos vertinimo procedūras ir efektyvias IRT sistemų valdymo kontrolės ir apsaugos priemones, atitinkančias Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 (*).

_____

(*) 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).“;

2) III priedo 12 punktas pakeičiamas taip:

„12. Kredito reitingų agentūra pažeidžia 6 straipsnio 2 dalį, skaitomą kartu su I priedo A skirsnio 4 punktu, neturėdama patikimų administracinių ar apskaitos procedūrų, vidaus kontrolės mechanizmų, efektyvių rizikos vertinimo procedūrų arba efektyvių IRT sistemų valdymo kontrolės ir apsaugos priemonių, atitinkančių Reglamentą (ES) 2022/2554; ar neįgyvendindama ar neišlaikydama sprendimų priėmimo procedūrų ar organizacinių struktūrų, kaip reikalaujama pagal tą punktą.“

60 straipsnis

Reglamento (ES) Nr. 648/2012 daliniai pakeitimai

Reglamentas (ES) Nr. 648/2012 iš dalies keičiamas taip:

1) 26 straipsnis iš dalies keičiamas taip:

a) 3 dalis pakeičiama taip:

„3. Pagrindinė sandorio šalis išlaiko ir naudoja organizacinę struktūrą, kuria užtikrinamas tęstinumas ir sklandus veikimas teikiant paslaugas ir vykdant veiklą. Ji naudoja tinkamas ir proporcingas sistemas, išteklius ir procedūras, įskaitant IRT sistemas, valdomas vadovaujantis Europos Parlamento ir Tarybos reglamentu (ES) 2022/2554 (*).

_____

(*) 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).“;

([39]) 2006 m. gegužės 17 d. Europos Parlamento ir Tarybos direktyva 2006/43/EB dėl teisės aktų nustatyto metinės finansinės atskaitomybės ir konsoliduotos finansinės atskaitomybės audito, iš dalies keičianti Tarybos direktyvas 78/660/EEB ir 83/349/EEB bei panaikinanti Tarybos direktyvą 84/253/EEB (OL L 157, 2006 6 9, p. 87).

b) 6 dalis išbraukiama;

2) 34 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. Pagrindinė sandorio šalis nustato, įgyvendina ir palaiko tinkamą veiklos tęstinumo politiką ir veiklos atkūrimo po ekstremaliųjų įvykių planą, apimantį IRT veiklos tęstinumo politiką ir IRT reagavimo ir veiklos atkūrimo planus, parengtus ir įgyvendinamus vadovaujantis Reglamentu (ES) 2022/2554, kurių tikslas – užtikrinti, kad būtų išsaugotos pagrindinės sandorio šalies funkcijos, laiku atkurta veikla ir kad būtų vykdomi pagrindinės sandorio šalies įsipareigojimai.“;

b) 3 dalies pirma pastraipa pakeičiama taip:

„3. Siekiant užtikrinti nuoseklų šio straipsnio taikymą, EVPRI, pasikonsultavusi su ECBS nariais, parengia techninių reguliavimo standartų projektus, kuriuose nurodomas minimalus veiklos tęstinumo politikos ir veiklos atkūrimo po ekstremaliųjų įvykių plano, išskyrus IRT veiklos tęstinumo politikos ir veiklos atkūrimo po ekstremaliųjų įvykių planus, turinys ir reikalavimai.“;

3) 56 straipsnio 3 dalies pirma pastraipa pakeičiama taip:

„3. Siekiant užtikrinti nuoseklų šio straipsnio taikymą, EVPRI parengia techninių reguliavimo standartų, kuriuose išsamiai nustatomi 1 dalyje nurodytos registracijos paraiškos duomenys, išskyrus reikalavimus, susijusius su IRT rizikos valdymu, projektus.“;

4) 79 straipsnio 1 ir 2 dalys pakeičiamos taip:

„1. Sandorių duomenų saugykla nustato galimus veiklos rizikos šaltinius ir juos sumažina sukurdama tinkamas sistemas, kontrolės priemones ir procedūras, įskaitant IRT sistemas, valdomas vadovaujantis Reglamentu (ES) 2022/2554.

2. Sandorių duomenų saugykla nustato, įgyvendina ir palaiko tinkamą veiklos tęstinumo politiką ir veiklos atkūrimo po ekstremaliųjų įvykių planą, įskaitant IRT veiklos tęstinumo politiką ir IRT reagavimo ir veiklos atkūrimo planus, nustatytus vadovaujantis Reglamentu (ES) 2022/2554, kurių tikslas – užtikrinti, kad būtų palaikomos jos funkcijos, būtų laiku atkurta veikla ir kad būtų vykdomi sandorių duomenų saugyklos įsipareigojimai.“;

5) 80 straipsnio 1 dalis išbraukiama.

6) I priedo II skirsnis iš dalies keičiamas taip:

a) a ir b punktai pakeičiami taip:

„a) sandorių duomenų saugykla pažeidžia 79 straipsnio 1 dalį, jei nenustato galimų veiklos rizikos šaltinių arba nesumažina šios rizikos sukurdama tinkamas sistemas, kontrolės priemones ir procedūras, įskaitant IRT sistemas, valdomas vadovaujantis Reglamentu (ES) 2022/2554;

b) sandorių duomenų saugykla pažeidžia 79 straipsnio 2 dalį, jei nenustato, neįgyvendina arba nepalaiko tinkamos veiklos tęstinumo politikos ir veiklos atkūrimo po ekstremaliųjų įvykių plano, parengto vadovaujantis Reglamentu (ES) 2022/2554, kurio tikslas – užtikrinti, kad būtų palaikomos jos funkcijos, laiku atkurta veikla ir kad būtų vykdomi sandorių duomenų saugyklos įsipareigojimai.“;

b) c punktas išbraukiamas;

7) III priedas iš dalies keičiamas taip:

a) II skirsnis iš dalies keičiamas taip:

i) c punktas pakeičiamas taip:

„c) 2 lygio pagrindinė sandorio šalis pažeidžia 26 straipsnio 3 dalį, jei nepalaiko arba nenaudoja organizacinės struktūros, kuria užtikrinamas tęstinumas ir sklandus veikimas teikiant paslaugas ir vykdant veiklą, arba nenaudoja tinkamų ir proporcingų sistemų, išteklių ar procedūrų, įskaitant IRT sistemas, valdomas vadovaujantis Reglamentu (ES) 2022/2554;“;

ii) f punktas išbraukiamas;

b) III skirsnio a punktas pakeičiamas taip:

„a) 2 lygio pagrindinė sandorio šalis pažeidžia 34 straipsnio 1 dalį, jei nenustato, neįgyvendina ar nepalaiko tinkamos veiklos tęstinumo politikos ir reagavimo ir veiklos atkūrimo plano, parengto vadovaujantis Reglamentu (ES) 2022/2554, kurių tikslas – užtikrinti, kad būtų išsaugotos pagrindinės sandorio šalies funkcijos, laiku atkurta veikla ir kad būtų vykdomi pagrindinės sandorio šalies įsipareigojimai, kad esant sutrikimams bent būtų suteikta galimybė atkurti visus duomenis apie sandorius, kad pagrindinė sandorio šalis galėtų patikimai tęsti savo veiklą ir numatytą datą atlikti atsiskaitymus;“.

61 straipsnis

Reglamento (ES) Nr. 909/2014 daliniai pakeitimai

Reglamento (ES) Nr. 909/2014 45 straipsnis iš dalies keičiamas taip:

1) 1 dalis pakeičiama taip:

„1. CVPD nustato tiek vidinius, tiek išorinius operacinės rizikos šaltinius ir kuo labiau sumažina jų poveikį įdiegdamas tinkamas IRT priemones, procesus ir politiką, parengtus ir valdomus vadovaujantis Europos Parlamento ir Tarybos reglamentu (ES) 2022/2554 (*), taip pat bet kokias kitas atitinkamas priemones, vykdydamas kontrolę ir taikydamas procedūras kitų rūšių operacinei rizikai, be kita ko, visose jo valdomose vertybinių popierių atsiskaitymo sistemose.

_____

(*) 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).“;

2) 2 dalis išbraukiama;

3) 3 ir 4 dalys pakeičiamos taip:

„3. Jo teikiamų paslaugų ir kiekvienos jo valdomos vertybinių popierių atsiskaitymo sistemos atžvilgiu CVPD nustato, įgyvendina ir palaiko tinkamą veiklos tęstinumo politiką ir veiklos atkūrimo po ekstremaliųjų įvykių planą, įskaitant IRT veiklos tęstinumo politiką ir IRT reagavimo ir veiklos atkūrimo po ekstremaliųjų įvykių planus, nustatytus vadovaujantis Reglamentu (ES) 2022/2554, siekiant užtikrinti, kad įvykių, kurie kelia didelę veiklos sutrikdymo riziką, atveju būtų išsaugotos CVPD paslaugos, laiku atkurtos jo operacijos ir vykdomi jo įsipareigojimai.

4. 3 dalyje nurodytame plane numatoma atkurti visus sandorius bei dalyvių pozicijas sutrikdymo momentu, kad CVPD dalyviai galėtų patikimai tęsti savo veiklą ir numatytą dieną atlikti atsiskaitymus, be kita ko, užtikrinant, kad ypatingos svarbos IT sistemos galėtų nedelsiant atnaujinti operacijas nuo sutrikdymo momento, kaip numatyta Reglamento (ES) 2022/2554 12 straipsnio 5 ir 7 dalyse.“;

4) 6 dalis pakeičiama taip:

„6. CVPD nustato, stebi ir valdo riziką, kurią jo operacijoms galėtų kelti pagrindiniai jo valdomų vertybinių popierių atsiskaitymo sistemų dalyviai, taip pat paslaugų ir komunalinių paslaugų teikėjai ir kiti CVPD ar kitos rinkos infrastruktūros. Gavęs prašymą jis pateikia kompetentingoms ir atitinkamoms institucijoms informaciją apie bet kokią tokią nustatytą riziką. Jis taip pat nedelsdamas informuoja kompetentingą instituciją ir atitinkamas institucijas apie operacinius incidentus, įvykusius dėl tokios rizikos, išskyrus susijusius su IRT rizika.“;

5) 7 dalies pirma pastraipa pakeičiama taip:

„7. ESMA, glaudžiai bendradarbiaudama su ECBS nariais, parengia techninių reguliavimo standartų projektus, kuriuose patikslinama 1 ir 6 dalyse nurodyta operacinė rizika, išskyrus IRT riziką, bei tos rizikos testavimo, reagavimo į ją ar kuo didesnio sumažinimo metodai, įskaitant 3 ir 4 dalyse nurodytą veiklos tęstinumo politiką bei veiklos atkūrimo po ekstremaliųjų įvykių planus ir jų vertinimo metodus.“

62 straipsnis

Reglamento (ES) Nr. 600/2014 daliniai pakeitimai

Reglamentas (ES) Nr. 600/2014 iš dalies keičiamas taip:

1) 27g straipsnis iš dalies keičiamas taip:

a) 4 dalis pakeičiama taip:

„4. „PSS turi laikytis tinklų ir informacinių sistemų saugumo reikalavimų, išdėstytų Europos Parlamento ir Tarybos reglamente (ES) 2022/2554 (*).

_____

(*) 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).“;

b) 8 dalies c punktas pakeičiamas taip:

„c) 3 ir 5 dalyse nustatyti konkretūs organizaciniai reikalavimai.“;

2) 27h straipsnis iš dalies keičiamas taip:

a) 5 dalis pakeičiama taip:

„5. KIJT turi laikytis tinklų ir informacinių sistemų saugumo reikalavimų, išdėstytų Reglamente (ES) 2022/2554.“;

b) 8 dalies e punktas pakeičiamas taip:

„e) 4 dalyje nustatyti konkretūs organizaciniai reikalavimai.“;

3) 27i straipsnis iš dalies keičiamas taip:

a) 3 dalis pakeičiama taip:

„3. PPTS turi laikytis tinklų ir informacinių sistemų saugumo reikalavimų, išdėstytų Reglamente (ES) 2022/2554.“;

b) 5 dalies b punktas pakeičiamas taip:

„b) 2 ir 4 dalyse nustatyti konkretūs organizaciniai reikalavimai.“

63 straipsnis

Reglamento (ES) 2016/1011 dalinis pakeitimas

Reglamento (ES) 2016/1011 6 straipsnis papildomas šia dalimi:

„6. „Ypatingos svarbos lyginamiesiems indeksams administratorius turi turėti patikimas administracines bei apskaitos procedūras, vidaus kontrolės mechanizmus, veiksmingas rizikos vertinimo procedūras ir veiksmingas IRT sistemų valdymo kontrolės ir apsaugos priemones, atitinkančias Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 (*).

_____

(*) 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).“

64 straipsnis

Įsigaliojimas ir taikymas

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

Jis taikomas nuo 2025 m. sausio 17 d.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Strasbūre 2022 m. gruodžio 14 d.

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkė	*Pirmininkas*
R. METSOLA	M. BEK

DIREKTYVOS

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2022/2555

2022 m. gruodžio 14 d.

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)

(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 Centrinio Banko nuomonę ([1]),

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę ([2]),

pasikonsultavę su Regionų komitetu,

laikydamiesi įprastos teisėkūros procedūros ([3]),

kadangi:

(1) Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 ([4]) buvo siekiama sukurti kibernetinio saugumo pajėgumus visoje Sąjungoje, sumažinti grėsmes tinklų ir informacinėms sistemoms, kurios naudojamos teikiant esmines paslaugas pagrindiniuose sektoriuose, ir užtikrinti tokių paslaugų nuolatinį teikimą įvykus incidentams, taip prisidedant prie Sąjungos saugumo ir veiksmingo jos ekonomikos ir visuomenės veikimo;

(2) nuo Direktyvos (ES) 2016/1148 įsigaliojimo padaryta didelė pažanga didinant Sąjungos kibernetinio atsparumo lygį. Atlikus direktyvos peržiūrą, paaiškėjo, kad ji tapo institucinio ir reguliavimo požiūrio į kibernetinį saugumą Sąjungoje paskata ir sudarė sąlygas reikšmingam mąstysenos pokyčiui. Direktyva padėjo galutinai sukurti nacionalines tinklų ir informacinių sistemų saugumo sistemas parengiant nacionalines tinklų ir informacinių sistemų saugumo strategijas, nustatant nacionalinius pajėgumus ir įgyvendinant reguliavimo priemones, taikomas esminiams infrastruktūros objektams ir kiekvienos valstybės narės identifikuotiems subjektams. Direktyva (ES) 2016/1148 taip pat prisidėta prie bendradarbiavimo Sąjungos lygmeniu įsteigus Bendradarbiavimo grupę ir sukuriant nacionalinių reagavimo į kompiuterinius saugumo incidentus tarnybų tinklą. Nepaisant tų laimėjimų, atlikus Direktyvos (ES) 2016/1148 peržiūrą paaiškėjo jos trūkumai, trukdantys veiksmingai spręsti dabartines ir naujas kibernetinio saugumo problemas;

(3) tinklų ir informacinės sistemos dėl sparčios skaitmeninės transformacijos ir visuomenės tarpusavio junglumo, įskaitant tarpvalstybinius mainus, tapo pagrindiniu kasdienio gyvenimo aspektu. Dėl tokių pokyčių kibernetinių grėsmių padėtis tapo sudėtingesnė ir atsirado naujų problemų, kurioms spręsti reikia pritaikytų, koordinuotų ir novatoriškų atsakomųjų veiksmų visose valstybėse narėse. Incidentų skaičius, mastas, sudėtingumas, dažnumas ir poveikis didėja bei kelia didelę grėsmę tinklų ir informacinių sistemų veikimui. Todėl incidentai gali trukdyti vykdyti ekonominę veiklą vidaus rinkoje, sukelti finansinių nuostolių, pakirsti naudotojų pasitikėjimą ir padaryti didelę žalą

([1]) OL C 233, 2022 6 16, p. 22.
([2]) OL C 286, 2021 7 16, p. 170.
([3]) 2022 m. lapkričio 10 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2022 m. lapkričio 28 d. Tarybos sprendimas.
([4]) 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1).

Sąjungos ekonomikai ir visuomenei. Todėl kibernetinio saugumo parengtis ir veiksmingumas kaip niekad anksčiau yra labai svarbūs tinkamam vidaus rinkos veikimui. Be to, kibernetinis saugumas yra daugelio ypatingos svarbos sektorių pagrindinė įgalinanti priemonė siekiant sėkmingai vykdyti skaitmeninę transformaciją ir visapusiškai pasinaudoti skaitmeninimo teikiama ekonomine, socialine ir tvarumo nauda;

(4) Direktyvos (ES) 2016/1148 teisinis pagrindas buvo Sutarties dėl Europos Sąjungos veikimo (SESV) 114 straipsnis, kurio tikslas – tobulinant nacionalinių taisyklių suderinimo priemones sukurti vidaus rinką ir užtikrinti jos veikimą. Subjektams, teikiantiems ekonomiškai svarbias paslaugas arba vykdantiems ekonomiškai svarbią veiklą, nustatyti kibernetinio saugumo reikalavimai valstybėse narės gerokai skiriasi atsižvelgiant į reikalavimų rūšį, jų išsamumo lygį ir priežiūros metodą. Dėl tų skirtumų patiriama papildomų išlaidų, o prekes ar paslaugas tarpvalstybiniu mastu tiekiantiems ar tiekiantiems subjektams kyla sunkumų. Vienos valstybės narės nustatyti reikalavimai, kurie skiriasi nuo kitos valstybės narės nustatytų reikalavimų arba net jiems prieštarauja, gali daryti didelį poveikį tokiai tarpvalstybinei veiklai. Be to, tikėtina, kad dėl netinkamos kibernetinio saugumo reikalavimų struktūros arba įgyvendinimo vienoje valstybėje narėje kils pasekmių kitų valstybių narių kibernetinio saugumo lygiui, visų pirma atsižvelgiant į tarpvalstybinių mainų intensyvumą. Atlikus Direktyvos (ES) 2016/1148 peržiūrą, paaiškėjo, kad valstybėse narėse ji įgyvendinama labai įvairiai, be kita ko, kiek tai susiję su jos taikymo sritimi, nes jos ribų nustatymo klausimas iš esmės buvo paliktas valstybių narių diskrecijai. Direktyva (ES) 2016/1148 valstybėms narėms taip pat buvo suteikta labai plati diskrecija dėl joje nustatytų saugumo pareigų ir pranešimų apie incidentus teikimo pareigų įgyvendinimo. Todėl tos pareigos nacionaliniu lygmeniu buvo įgyvendintos labai skirtingai. Panašių skirtumų yra ir Direktyvos (ES) 2016/1148 nuostatų dėl priežiūros ir vykdymo užtikrinimo įgyvendinimo srityje;

(5) visi šie skirtumai lemia vidaus rinkos susiskaidymą ir gali daryti neigiamą poveikį vidaus rinkos veikimui, visų pirma tai pasakytina apie poveikį tarpvalstybiniam paslaugų teikimui ir kibernetinio atsparumo lygiui, kurį lemia taikomos įvairios priemonės. Galiausiai dėl tų skirtumų kai kurios valstybės narės galėtų tapti labiau pažeidžiamos kibernetinių grėsmių atžvilgiu, o tai gali daryti šalutinį poveikį visoje Sąjungoje. Šia direktyva siekiama pašalinti tokius didelius skirtumus tarp valstybių narių, visų pirma nustatant būtiniausias taisykles, susijusias su koordinuotos reguliavimo sistemos veikimu, sukuriant kiekvienos valstybės narės atsakingų institucijų veiksmingo bendradarbiavimo mechanizmus, atnaujinant sektorių ir veiklos, kuriems taikomos kibernetinio saugumo pareigos, sąrašą ir numatant veiksmingas taisomąsias ir vykdymo užtikrinimo priemones, kurios yra labai svarbios veiksmingam tų pareigų vykdymui užtikrinti. Todėl Direktyva (ES) 2016/1148 turėtų būti panaikinta ir pakeista šia direktyva;

(6) panaikinus Direktyvą (ES) 2016/1148, taikymo sritis sektoriams turėtų būti praplėsta, kad apimtų platesnį ekonomikos veiklų spektrą, kad apimtų visus sektorius ir paslaugas, kurie yra nepaprastai svarbūs pagrindinei visuomeninei ir ekonominei veiklai vidaus rinkoje. Visų pirma šia direktyva siekiama pašalinti trūkumus, susijusius su esminių paslaugų operatorių ir skaitmeninių paslaugų teikėjų diferencijacija, kuri yra pasenusi, nes neatspindi sektorių arba paslaugų svarbos visuomeninei ir ekonominei veiklai vidaus rinkoje;

(7) pagal Direktyvą (ES) 2016/1148 valstybės narės buvo atsakingos už subjektų, atitinkančių esminių paslaugų operatoriams taikomus kriterijus, identifikavimą. Siekiant tuo atžvilgiu pašalinti didelius valstybių narių skirtumus ir visiems atitinkamiems subjektams užtikrinti teisinį tikrumą kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti atžvilgiu, turėtų būti nustatytas vienas kriterijus, kuriuo remiantis nustatomi subjektai, kurie patenka į šios direktyvos taikymo sritį. Tas kriterijus turėtų būti grindžiamas dydžio ribos taisykle, pagal kurią į šios direktyvos taikymo sritį patenka visi subjektai, kurie laikomi vidutinėmis įmonėmis pagal Komisijos rekomendacijos 2003/361/EB ([5]) priedo 2 straipsnį arba kurie viršija to straipsnio 1 dalyje nustatytas viršutines ribas, ir veikiantys sektoriuose bei teikiantys atitinkamų rūšių paslaugas ar vykdantys veiklą, kuriems taikoma ši direktyva. Valstybės

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

narės taip pat turėtų numatyti, kad į šios direktyvos taikymo sritį patenka tam tikros mažosios įmonės ir labai mažos įmonės, kaip tai apibrėžta to priedo 2 straipsnio 2 ir 3 dalyse, kurios atitinka specifinius kriterijus, pagal kuriuos parodomas jų esminis vaidmuo visuomenei, ekonomikai arba konkretiems sektoriams ar paslaugų rūšims;

(8) ši direktyva neturėtų būti taikoma viešojo administravimo subjektams, kurių veikla daugiausia vykdoma nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas. Tačiau ši direktyva turėtų būti taikoma viešojo administravimo subjektams, kurių veikla su tomis sritimis susijusi tik nežymiai. Šios direktyvos tikslais reguliavimo kompetenciją turintys subjektai nelaikomi subjektais, vykdančiais veiklą teisėsaugos srityje, todėl ši direktyva nėra jiems netaikoma tuo pagrindu. Ši direktyva netaikoma viešojo administravimo subjektams, įsteigtiems kartu su trečiąja valstybe pagal tarptautinį susitarimą. Ši direktyva netaikoma valstybių narių diplomatinėms ir konsulinėms atstovybėms trečiosiose valstybėse arba jų tinklų ir informacinėms sistemoms, jeigu tokios sistemos yra atstovybės patalpose arba naudojamos naudotojų labui trečiojoje valstybėje;

(9) valstybės narės turėtų galėti imtis priemonių, būtinų esminiams nacionalinio saugumo interesams užtikrinti, viešajai tvarkai palaikyti bei visuomenės saugumui užtikrinti, ir priemonių, kurios leistų sudaryti sąlygas vykdyti nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas. Tuo tikslu valstybės narės turėtų turėti galimybę atleisti konkrečius subjektus, vykdančius veiklą nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas, nuo tam tikrų šioje direktyvoje nustatytų pareigų tos veiklos atžvilgiu. Kai subjektas teikia paslaugas išimtinai viešojo administravimo subjektui, kuriam ši direktyva netaikoma, valstybės narės turėtų turėti galimybę atleisti tą subjektą nuo tam tikrų šioje direktyvoje nustatytų pareigų tų paslaugų atžvilgiu. Be to, iš jokios valstybės narės neturi būti reikalaujama teikti informacijos, kurios atskleidimas, jos nuomone, prieštarautų esminiams jos nacionalinio saugumo, viešojo saugumo ar gynybos interesams. Tame kontekste turėtų būti atsižvelgiama į Sąjungos arba nacionalines taisykles dėl įslaptintos informacijos apsaugos, susitarimus dėl informacijos neatskleidimo ir neoficialius susitarimus dėl informacijos neatskleidimo, pavyzdžiui, Srauto kontrolės protokolą. Srauto kontrolės protokolas turi būti suprantamas kaip priemonė informacijai apie bet kokius apribojimus, taikomus tolesnei informacijos sklaidai, teikti. Jį naudoja beveik visos reagavimo į kompiuterinius saugumo incidentus tarnybos (toliau – CSIRT) ir kai kurie informacijos analizės ir dalijimosi informacija centrai;

(10) nors ši direktyva taikoma subjektams, vykdantiems elektros energijos gamybos atominėse elektrinėse veiklą, dalis šios veiklos gali būti susijusi su nacionaliniu saugumu. Tokiu atveju valstybė narė, laikydamasi Sutarčių, turėtų turėti galimybę vykdyti savo pareigą užtikrinti savo nacionalinį saugumą, kiek tai susiję su ta veikla, įskaitant veiklą branduolinio sektoriaus vertės grandinėje;

(11) kai kurie subjektai vykdo veiklą nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas, taip pat teikia patikimumo užtikrinimo paslaugas. Patikimumo užtikrinimo paslaugų teikėjai, kuriems taikomas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 ([6]), turėtų būti įtraukti į šios direktyvos taikymo sritį, kad būtų užtikrintas toks pat saugumo reikalavimų ir priežiūros lygis, koks anksčiau tame reglamente buvo nustatytas patikimumo užtikrinimo paslaugų teikėjų atžvilgiu. Atsižvelgiant į tai, kad Reglamentas (ES) Nr. 910/2014 netaikomas tam tikroms konkrečioms paslaugoms, ši direktyva neturėtų būti taikoma patikimumo užtikrinimo paslaugų, kuriomis naudojamasi tik uždarose sistemose, sukurtose pagal nacionalinę teisę arba apibrėžtos dalyvių grupės susitarimus, teikimui;

([6]) 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).

(12) pašto paslaugų teikėjams, kaip apibrėžta Europos Parlamento ir Tarybos direktyvoje 97/67/EB ([7]), įskaitant kurjerių paslaugų teikėjus, ši direktyva turėtų būti taikoma, jeigu jie teikia paslaugas bent viename pašto paslaugų teikimo grandinės etape, ypač pašto siuntų surinkimo, rūšiavimo, vežimo arba paskirstymo etape, įskaitant siuntų paėmimo paslaugas, atsižvelgiant į jų priklausomumo nuo tinklų ir informacinių sistemų laipsnį. Teikiamos vežimo paslaugos, kai jos nėra susijusios su vienu iš tų etapų, neturėtų patekti į pašto paslaugų apibrėžtį;

(13) dėl intensyvėjančių įkibernetinių grėsmių ir didėjančio sudėtingumo valstybės narės turėtų stengtis užtikrinti, kad subjektai, kuriems netaikoma ši direktyva, pasiektų aukštą kibernetinio saugumo lygį, ir remti lygiaverčių kibernetinio saugumo rizikos valdymo priemonių, atspindinčių jautrų tų subjektų pobūdį, įgyvendinimą;

(14) pagal šią direktyvą vykdomam asmens duomenų tvarkymui taikoma Sąjungos duomenų apsaugos teisė ir Sąjungos privatumo teisė. Visų pirma, šia direktyva nedaromas poveikis Europos Parlamento ir Tarybos reglamentui (ES) 2016/679 ([8]) ir Europos Parlamento ir Tarybos direktyvai 2002/58/EB ([9]). Todėl šia direktyva neturėtų būti daromas poveikis, *inter alia*, institucijų, kurios yra kompetentingos kontroliuoti, kaip laikomasi taikytinos Sąjungos duomenų apsaugos teisės ir Sąjungos privatumo teisės, užduotims ir įgaliojimams;

(15) atitikties kibernetinio saugumo rizikos valdymo priemonėms ir pranešimų teikimo tikslu subjektai, kurie patenka į šios direktyvos taikymo sritį, turėtų būti skirstomi į dvi kategorijas: esminiai subjektai ir svarbūs subjektai, atspindint jų svarbos mastą jų sektoriaus arba jų teikiamų paslaugų rūšies, taip pat jų dydžio požiūriais. Tuo atžvilgiu, kai taikytina, turėtų būti tinkamai atsižvelgiama į visus atitinkamus kompetentingų institucijų atliktus sektorių rizikos vertinimus ar pateiktas gaires. Abiejų kategorijų subjektams taikomi priežiūros ir vykdymo užtikrinimo režimai turėtų būti diferencijuojami siekiant užtikrinti tinkamą, viena vertus, rizika grindžiamų reikalavimų ir pareigų ir, kita vertus, administracinės naštos, atsirandančios dėl atitikties priežiūros, pusiausvyrą;

(16) siekiant kad subjektai, turintys įmonių partnerių arba kurie yra susijusios įmonės, nebūtų laikomi esminiais arba svarbiais subjektais, kai tai būtų neproporcinga, valstybės narės, taikydamos Rekomendacijos 2003/361/EB priedo 6 straipsnio 2 dalį, gali atsižvelgti į subjekto nepriklausomumo nuo savo įmonės partnerės ar susijusių įmonių lygį. Visų pirma valstybės narės gali atsižvelgti į tai, kad subjektas yra nepriklausomas nuo savo įmonės partnerės ar susijusių įmonių kalbant apie tinklų ir informacines sistemas, kuriomis tas subjektas naudojasi teikdamas savo paslaugas, ir kalbant apie subjekto teikiamas paslaugas. Tuo remdamosi, kai tinkama, valstybės narės gali laikyti, kad toks subjektas negali būti laikomas vidutine įmone pagal Komisijos rekomendacijos 2003/361/EB priedo 2 straipsnį arba kad jis neviršija to straipsnio 1 dalyje vidutinei įmonei nustatytų viršutinių ribų, jeigu, atsižvelgus į to subjekto nepriklausomumo lygį, tas subjektas nebūtų laikomas vidutine įmone arba jis neviršytų tų viršutinių ribų tuo atveju, jei būtų atsižvelgiama tik į jo paties duomenis. Tai nedaro poveikio šioje direktyvoje nustatytoms įmonių partnerių ir susijusių įmonių, kurioms taikoma ši direktyva, pareigoms;

(17) valstybės narės turėtų galėti nuspręsti, kad subjektai, kurie prieš šios direktyvos įsigaliojimą buvo identifikuoti kaip esminių paslaugų operatoriai pagal Direktyvą (ES) 2016/1148, būtų laikomi esminiais subjektais;

([7]) 1997 m. gruodžio 15 d. Europos Parlamento ir Tarybos direktyva 97/67/EB dėl Bendrijos pašto paslaugų vidaus rinkos plėtros bendrųjų taisyklių ir paslaugų kokybės gerinimo (OL L 15, 1998 1 21, p. 14).

([8]) 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).

([9]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).

(18) siekdamos užtikrinti aiškią subjektų, kuriems taikoma ši direktyva, apžvalgą, valstybės narės turėtų sudaryti esminių ir svarbių subjektų bei domenų vardų registravimo paslaugas teikiančių subjektų sąrašą. Tuo tikslu valstybės narės turėtų reikalauti, kad subjektai kompetentingoms institucijoms pateiktų bent šią informaciją: subjekto pavadinimą, adresą ir naujausius kontaktinius duomenis, įskaitant el. pašto adresus, IP adresus ir telefono numerius, ir, kai taikytina, atitinkamą sektorių ir subsektorių, nurodytus prieduose, taip pat, kai taikytina, valstybių narių, kuriose jie teikia paslaugas, kurioms taikoma ši direktyva, sąrašą. Tuo tikslu Komisija, padedant Europos Sąjungos kibernetinio saugumo agentūrai (toliau – ENISA), nepagrįstai nedelsdama turėtų pateikti gaires ir šablonus dėl pareigos teikti informaciją. Siekiant sudaryti palankesnes sąlygas sukurti ir atnaujinti esminių ir svarbių subjektų bei domenų vardų registravimo paslaugas teikiančių subjektų sąrašą, valstybės narės turėtų turėti galimybę nustatyti nacionalinius mechanizmus, kuriuos taikant subjektai galėtų užsiregistruoti patys. Tais atvejais, kai nacionaliniu lygmeniu registrai jau yra sukurti, valstybės narės gali nuspręsti dėl tinkamų mechanizmų, kuriais sudaroma galimybė identifikuoti subjektus, kuriems taikoma ši direktyva;

(19) valstybės narės turėtų būti atsakingos už tai, kad Komisijai būtų pateiktas bent kiekvieno prieduose nurodyto sektoriaus ir subsektoriaus esminių ir svarbių subjektų skaičius, taip pat atitinkama informacija apie identifikuotų subjektų skaičių ir šioje direktyvoje numatyta nuostata, pagal kurią jie buvo identifikuoti, ir jų teikiamos paslaugos rūšį. Valstybės narės raginamos keistis su Komisija informacija apie esminius ir svarbius subjektus, o didelio masto kibernetinio saugumo incidento atveju – atitinkama informacija, pavyzdžiui, apie atitinkamo subjekto pavadinimą;

(20) Komisija, bendradarbiaudama su Bendradarbiavimo grupe ir pasikonsultavusi su atitinkamais suinteresuotaisiais subjektais, turėtų pateikti labai mažoms ir mažosioms įmonėms taikomų kriterijų įgyvendinimo gaires įvertinimo, ar jos patenka į šios direktyvos taikymo sritį, tikslais. Komisija taip pat turėtų užtikrinti, kad atitinkamos gairės būtų pateiktos labai mažoms ir mažosioms įmonėms, kurioms taikoma ši direktyva. Komisija, padedant valstybėms narėms, turėtų pateikti labai mažoms ir mažosioms įmonėms informacijos tuo klausimu;

(21) Komisija galėtų pateikti gaires, skirtas padėti valstybėms narėms įgyvendinti šios direktyvos nuostatas dėl taikymo srities ir įvertinti priemonių, kurių turi būti imamasi pagal šią direktyvą, proporcingumą, visų pirma atsižvelgiant į subjektus, kurių verslo modeliai arba veiklos aplinka yra sudėtingi, kai subjektas vienu metu gali atitikti ir esminiams, ir svarbiems subjektams nustatytus kriterijus arba gali tuo pačiu metu vykdyti veiklą, kurios dalis patenka į šios direktyvos taikymo sritį, o dalis nepatenka;

(22) šioje direktyvoje nustatomi kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti, taikomų į jos taikymo sritį patenkančiuose sektoriuose, pagrindai. Siekiant išvengti Sąjungos teisės aktų nuostatų dėl kibernetinio saugumo susiskaidymo, kai manoma, kad, siekiant užtikrinti aukšto lygio kibernetinį saugumą visoje Sąjungoje, reikalingi tolesni konkretiems sektoriams taikomi Sąjungos teisės aktai, susiję su kibernetinio saugumo rizikos valdymo priemonėmis ir pareigomis pranešti, Komisija turėtų įvertinti, ar tokios tolesnės nuostatos galėtų būti nustatytos pagal šią direktyvą priimame įgyvendinimo akte. Jei toks įgyvendinimo aktas būtų netinkamas tam tikslui, konkretiems sektoriams taikomi Sąjungos teisės aktai galėtų padėti užtikrinti aukšto lygio kibernetinį saugumą visoje Sąjungoje, visapusiškai atsižvelgiant į atitinkamų sektorių specifiką ir sudėtingumą. Tuo tikslu šia direktyva nedraudžiama priimti tolesnių konkretiems sektoriams taikomų Sąjungos teisės aktų, kuriais reglamentuojamos kibernetinio saugumo rizikos valdymo priemonės ir pareigos pranešti ir kuriais tinkamai atsižvelgiama į poreikį sukurti visapusišką bei nuoseklią kibernetinio saugumo sistemą. Šia direktyva nedaromas poveikis dabartiniams įgyvendinimo įgaliojimams, kurie Komisijai suteikti įvairiuose sektoriuose, įskaitant transporto ir energetikos sektorius;

(23) jei konkrečiam sektoriui taikomame Sąjungos teisės akte yra nuostatos, pagal kurias reikalaujama, kad esminiai arba svarbūs subjektai priimtų kibernetinio saugumo rizikos valdymo priemones arba praneštų apie didelius incidentus, ir jei tų reikalavimų poveikis yra bent lygiavertis šioje direktyvoje nustatytų pareigų poveikiui, tos nuostatos,

įskaitant nuostatas dėl priežiūros ir vykdymo užtikrinimo, turėtų būti taikomos tokiems subjektams. Jei konkrečiam sektoriui taikomas Sąjungos teisės aktas taikomas ne visiems konkretaus sektoriaus, kuriam taikoma ši direktyva, subjektams, atitinkamos šios direktyvos nuostatos turėtų būti toliau taikomos subjektams, kuriems netaikomas tas aktas;

(24) jei pagal konkrečiam sektoriui taikomo Sąjungos teisės akto nuostatas reikalaujama, kad esminiai arba svarbūs subjektai laikytųsi pareigų pranešti, kurių poveikis yra bent lygiavertis šioje direktyvoje nustatytų pareigų pranešti poveikiui, turėtų būti užtikrintas pranešimų apie incidentus tvarkymo nuoseklumas ir veiksmingumas. Tuo tikslu konkrečiam sektoriui taikomo Sąjungos teisės akto nuostatomis dėl pranešimo apie incidentus turėtų būti suteikta galimybė CSIRT, kompetentingoms institucijoms arba bendriesiems kibernetinio saugumo kontaktiniams punktams (toliau – bendrieji kontaktiniai punktai) pagal šią direktyvą nedelsiant susipažinti su pranešimais apie incidentus, pateiktais pagal konkrečiam sektoriui taikomą Sąjungos teisės aktą. Visų pirma tokia neatidėliotina prieiga gali būti užtikrinta, jei pranešimai apie incidentus nepagrįstai nedelsiant persiunčiami CSIRT, kompetentingai institucijai arba bendrajam kontaktiniam punktui pagal šią direktyvą. Prireikus valstybės narės turėtų įdiegti automatinį tiesioginio pranešimo mechanizmą, kuriuo būtų užtikrinamas sistemingas ir neatidėliotinas keitimasis informacija su CSIRT, kompetentingomis institucijomis arba bendruoju kontaktiniu punktu dėl tokių pranešimų apie incidentus tvarkymo. Siekdamos supaprastinti pranešimų teikimą ir įgyvendinti automatinį tiesioginio pranešimo mechanizmą, valstybės narės, vadovaudamosi konkrečiam sektoriui taikomu Sąjungos teisės aktu, galėtų naudotis viena bendra prieiga;

(25) konkretiems sektoriams taikomuose Sąjungos teisės aktuose, pagal kuriuos numatytos kibernetinio saugumo rizikos valdymo priemonės arba pareigos pranešti, kurių poveikis yra bent lygiavertis šioje direktyvoje numatytų priemonių ar pareigų poveikiui, galėtų būti nustatyta, kad kompetentingos institucijos pagal tokius aktus savo priežiūros ir vykdymo užtikrinimo įgaliojimais, susijusiais su tokiomis priemonėmis arba pareigomis, naudojasi padedant kompetentingoms institucijoms pagal šią direktyvą. Atitinkamos kompetentingos institucijos tuo tikslu galėtų sudaryti bendradarbiavimo susitarimus. Tokiuose bendradarbiavimo susitarimuose, *inter alia*, galėtų būti nustatytos priežiūros veiklos koordinavimo procedūros, įskaitant tyrimų ir patikrinimų vietoje procedūras laikantis nacionalinės teisės, ir kompetentingų institucijų keitimosi atitinkama informacija apie priežiūrą ir vykdymo užtikrinimą mechanizmas, be kita ko, prieiga prie su kibernetine sritimi susijusios informacijos, kurios prašo tos kompetentingos institucijos pagal šią direktyvą;

(26) jei pagal konkretiems sektoriams taikomus Sąjungos teisės aktus reikalaujama, kad subjektai praneštų apie dideles kibernetines grėsmes arba skatinama, kad jie tai darytų, valstybės narės taip pat turėtų skatinti dalytis informacija apie dideles kibernetines grėsmes su CSIRT, kompetentingomis institucijomis arba bendraisiais kontaktiniais punktais pagal šią direktyvą, siekiant užtikrinti didesnį tų įstaigų informuotumą apie kibernetinių grėsmių padėtį ir sudaryti joms galimybę veiksmingai bei laiku reaguoti, jei didelės kibernetinės grėsmės pasireikštų;

(27) būsimuose konkretiems sektoriams taikomuose Sąjungos teisės aktuose turėtų būti tinkamai atsižvelgta į šioje direktyvoje nustatytas terminų apibrėžtis ir priežiūros bei vykdymo užtikrinimo sistemą;

(28) Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 ([10]) turėtų būti vertinamas kaip konkrečiam sektoriui taikomas Sąjungos teisės aktas šios direktyvos atžvilgiu, kiek tai susiję su finansų sektoriaus subjektais. Reglamento (ES) 2022/2554 nuostatos, susijusios su informacinių ir ryšių technologijų (IRT) rizikos valdymu, su IRT susijusių incidentų valdymu, ypač pranešimų apie didelius su IRT susijusius incidentus teikimu, taip pat su skaitmeninės veiklos atsparumo testavimu, dalijimosi informacija susitarimais ir trečiosios šalies IRT rizika, turėtų būti taikomos vietoj šioje direktyvoje įtvirtintų nuostatų. Todėl valstybės narės šios direktyvos nuostatų dėl kibernetinio saugumo rizikos valdymo ir pareigų pranešti bei priežiūros ir vykdymo užtikrinimo neturėtų taikyti finansų sektoriaus subjektams, kuriems taikomas Reglamentas (ES) 2022/2554. Kartu pagal šią direktyvą svarbu išlaikyti tvirtus ryšius su finansų sektoriumi ir užtikrinti, kad su juo būtų keičiamasi informacija. Tuo tikslu Reglamentu (ES) 2022/2554 Europos priežiūros institucijoms (EPI) ir kompetentingoms institucijoms pagal tą reglamentą leidžiama dalyvauti Bendradarbiavimo grupės veikloje ir keistis informacija bei bendradarbiauti su bendraisiais kontaktiniais punktais, taip pat CSIRT ir kompetentingomis institucijomis pagal šią direktyvą. Kompetentingos institucijos pagal Reglamentą (ES) 2022/2554 CSIRT, kompetentingoms institucijoms arba bendriesiems kontaktiniams punktams pagal šią direktyvą taip pat turėtų perduoti išsamius duomenis apie didelius su IRT susijusius incidentus ir, kai

([10]) 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 (žr. šio Oficialiojo leidinio p.1).

tinkama, dideles kibernetines grėsmes. Tai galima pasiekti suteikiant neatidėliotiną prieigą prie pranešimų apie incidentus ir juos perduodant, tiesiogiai arba per vieną bendrą prieigą. Be to, valstybės narės į savo kibernetinio saugumo strategijas turėtų toliau įtraukti finansų sektorių, o CSIRT savo veikloje gali aptarti finansų sektoriaus klausimus;

(29) siekiant išvengti kibernetinio saugumo pareigų, nustatytų aviacijos sektoriaus subjektams, spragų ar šių pareigų dubliavimosi, nacionalinės institucijos pagal Europos Parlamento ir Tarybos reglamentus (EB) Nr. 300/2008 ([11]) ir (ES) 2018/1139 ([12]) ir kompetentingos institucijos pagal šią direktyvą turėtų bendradarbiauti įgyvendindamos kibernetinio saugumo rizikos valdymo priemones ir vykdydamos atitikties toms priemonėms priežiūrą nacionaliniu lygmeniu. Kompetentingos institucijos pagal šią direktyvą galėtų laikyti, kad subjekto atitiktis saugumo reikalavimams, nustatytiems reglamentuose (EB) Nr. 300/2008 ir (ES) 2018/1139 bei atitinkamuose pagal tuos reglamentus priimtuose deleguotuosiuose ir įgyvendinimo aktuose, yra atitiktis atitinkamiems šioje direktyvoje nustatytiems reikalavimams;

(30) atsižvelgiant į kibernetinio saugumo ir subjektų fizinio saugumo tarpusavio ryšius, reikėtų užtikrinti nuoseklų požiūrį tarp Europos Parlamento ir Tarybos direktyvos (ES) 2022/2557 ([13]) ir šios direktyvos. Kad būtų pasiektas šis tikslas, subjektai, identifikuoti kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557, turėtų būti laikomi esminiais subjektais pagal šią direktyvą. Be to, kiekviena valstybė narė turėtų užtikrinti, kad jos nacionalinėje kibernetinio saugumo strategijoje būtų numatyta politikos sistema, pagal kurią toje valstybėje narėje būtų numatytas tvirtesnis jos kompetentingų institucijų pagal šią direktyvą ir kompetentingų institucijų pagal Direktyvą (ES) 2022/2557 veiklos koordinavimas keičiantis informacija apie riziką, kibernetines grėsmes, ir incidentus, taip pat nekibernetinę riziką, grėsmes bei incidentus, taip pat vykdant priežiūros užduotis. Kompetentingos institucijos pagal šią direktyvą ir pagal Direktyvą (ES) 2022/2557 turėtų bendradarbiauti ir keistis informacija nepagrįstai nedelsdamos, visų pirma kiek tai susiję su ypatingos svarbos subjektų identifikavimu, rizika, kibernetinėmis grėsmėmis, ir incidentais, taip pat su nekibernetine rizika, grėsmėmis ir incidentais, darančiais poveikį ypatingos svarbos subjektams, įskaitant kibernetinio saugumo ir fizines priemones, kurių ėmėsi ypatingos svarbos subjektai, taip pat tokių subjektų atžvilgiu vykdomos priežiūros veiklos rezultatais.

Be to, siekiant supaprastinti kompetentingų institucijų pagal šią direktyvą ir pagal Direktyvą (ES) 2022/2557 vykdomą tarpusavio priežiūros veiklą ir kuo labiau sumažinti atitinkamiems subjektams tenkančią administracinę naštą, tos kompetentingos institucijos turėtų stengtis suderinti pranešimo apie incidentus šablonus ir priežiūros procesus. Prireikus kompetentingos institucijos pagal Direktyvą (ES) 2022/2557 turėtų galėti prašyti kompetentingų institucijų pagal šią direktyvą naudotis savo priežiūros ir vykdymo užtikrinimo įgaliojimais subjekto, kuris identifikuotas kaip ypatingos svarbos subjektas pagal Direktyvą (ES) 2022/2557, atžvilgiu. Tuo tikslu kompetentingos institucijos pagal šią direktyvą ir pagal Direktyvą (ES) 2022/2557 turėtų bendradarbiauti ir keistis informacija, kai įmanoma – tikruoju laiku;

(31) skaitmeninės infrastruktūros sektoriaus subjektai iš esmės priklauso nuo tinklų ir informacinių sistemų, todėl pagal šią direktyvą tiems subjektams nustatytomis pareigomis turėtų būti visapusiškai atsižvelgiama į tokių sistemų fizinį saugumą, kaip jų kibernetinio saugumo rizikos valdymo priemonių ir pranešimų teikimo pareigų dalį. Kadangi tiems klausimams taikoma ši direktyva, Direktyvos (ES) 2022/2557 III, IV ir VI skyriuose nustatytos pareigos tokiems subjektams netaikomos;

([11]) 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių ir panaikinantis Reglamentą (EB) Nr. 2320/2002 (OL L 97, 2008 4 9, p. 72).

([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).

([13]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2557 dėl ypatingos svarbos subjektų atsparumo, kuria panaikinama Tarybos direktyva 2008/114/EB (žr. šio Oficialiojo leidinio p.164).

(32) patikimos, atsparios ir saugios domenų vardų sistemos (DNS) palaikymas ir išsaugojimas yra pagrindiniai veiksniai užtikrinant interneto vientisumą ir tai yra labai svarbu jos nuolatiniam ir stabiliam veikimui, nuo kurio priklauso skaitmeninė ekonomika ir visuomenė. Todėl ši direktyva turėtų būti taikoma aukščiausio lygio domenų vardų registrams ir DNS paslaugų teikėjams, kurie suprantami kaip subjektai, teikiantys viešai prieinamas rekursinio domenų vardų keitimo paslaugas galutinių interneto naudotojų reikmėms ar patikimo domenų vardų keitimo paslaugas trečiųjų šalių reikmėms. Ši direktyva neturėtų būti taikoma šakninio pavadinimo serveriams;

(33) debesijos kompiuterijos paslaugos turėtų apimti skaitmenines paslaugas, kurios pagal poreikį suteikia administravimo paslaugas ir plataus masto nuotolinę prieigą prie kintamo masto pritaikomos bendrų kompiuterijos išteklių bazės, įskaitant atvejus, kai tokie ištekliai yra paskirstyti per kelias vietas. Kompiuterijos ištekliai apima tokius išteklius, kaip tinklai, serveriai ar kita infrastruktūra, operacinės sistemos, programinė įranga, kaupikliai, taikomosios programos ir paslaugos. Debesijos kompiuterijos paslaugų modeliai, *inter alia*, apima paslauginę infrastruktūrą (IaaS), paslauginę platformą (PaaS), paslauginę programinę įrangą (SaaS) ir paslauginį tinklą (NaaS). Debesijos kompiuterijos diegimo modeliai turėtų apimti privačią, bendrą, viešą ir mišrią debesiją. Debesijos kompiuterijos paslaugos ir diegimo modeliai turi tokią pačią reikšmę kaip ir pagal ISO/IEC 17788:2014 standartą apibrėžti paslaugos sąlygų ir diegimo modeliai. Debesijos kompiuterijos naudotojo gebėjimas vienašališkai pasirūpinti kompiuterijos pajėgumais, pavyzdžiui, serverio laiku arba tinklo saugykla, be jokio žmogaus įsikišimo, atliekamo debesijos kompiuterijos paslaugų teikėjo, galėtų būti apibūdinamas kaip administravimas pagal poreikį.

Terminas „plataus masto nuotolinė prieiga“ naudojamas apibūdinant debesijos pajėgumus, kurie užtikrinami tinkle ir kuriais galima pasinaudoti per mechanizmus, kuriais skatinamas įvairių mažafunkcių arba daugiafunkcių kompiuterių platformų, įskaitant mobiliuosius telefonus, planšetinius kompiuterius, knyginius kompiuterius ir profesionaliuosius kompiuterius, naudojimas. Terminas „kintamo masto“ reiškia, kad atsižvelgdamas į paklausos svyravimus, debesijos paslaugų teikėjas lanksčiai paskirsto kompiuterijos išteklius nepriklausomai nuo geografinės išteklių vietos. Terminas „pritaikoma bazė“ reiškia, kad siekiant sparčiai padidinti ir sumažinti turimus kompiuterijos išteklius pagal darbo krūvį, tais ištekliais aprūpinama ir jie yra tiekiami atsižvelgiant į paklausą. Terminas „bendri“ reiškia, kad kompiuterijos ištekliai yra tiekiami keliems naudotojams, kurie dalijasi bendra prieiga prie paslaugos, tačiau tie ištekliai tvarkomi atskirai kiekvieno naudotojo atveju, nors paslauga yra teikiama naudojant tą pačią elektroninę įrangą. Terminas „paskirstyti“ reiškia kompiuterijos išteklius, kurie yra skirtinguose tinkliniuose kompiuteriuose ar prietaisuose ir kurie tarpusavyje bendrauja ir koordinuoja perduodami pranešimus;

(34) atsižvelgiant į novatoriškų technologijų ir naujų verslo modelių atsiradimą, tikimasi, kad vidaus rinkoje atsiras naujų debesijos kompiuterijos paslaugų ir diegimo modelių, atsižvelgiant į kintančius vartotojų poreikius. Šiomis aplinkybėmis debesijos kompiuterijos paslaugos gali būti teikiamos labai paskirstyta forma, dar arčiau duomenų generavimo ar rinkimo vietos, taip pereinant nuo tradicinio modelio prie labai paskirstyto modelio (tinklo paribio kompiuterija);

(35) duomenų centro paslaugų teikėjų siūlomos paslaugos ne visada gali būti teikiamos debesijos kompiuterijos paslaugos forma. Taigi, duomenų centrai ne visada gali priklausyti debesijos kompiuterijos infrastruktūrai. Siekiant valdyti visą riziką, kuri kyla tinklų ir informacinių sistemų saugumui, ši direktyva turėtų būti taikoma duomenų centrų paslaugų, kurios nėra debesijos kompiuterijos paslaugos, teikėjams. Taikant šią direktyvą, sąvoka „duomenų centro paslauga“ turėtų apimti paslaugos, kuri apima struktūras arba struktūrų grupes, skirtas informacinių technologijų (IT) ir tinklo įrangos centralizuotam pritaikymui, tarpusavio junglumui ir eksploatavimui, teikiant duomenų saugojimo, tvarkymo ir transportavimo paslaugas kartu su visa energijos paskirstymo ir aplinkos kontrolės įranga ir infrastruktūra, teikimą. Sąvoka „duomenų centro paslauga“ neturėtų būti taikoma vidaus korporatyviniams duomenų centrams, kurie priklauso atitinkamam subjektui ir yra jo eksploatuojami to subjekto reikmėms;

(36) vienas iš svarbiausių vaidmenų kuriant naujus produktus ir procesus tenka tyrimų veiklai. Didžiąją dalį tos veiklos vykdo subjektai, kurie dalijasi savo tyrimų rezultatais, juos platina arba naudoja komerciniais tikslais. Todėl tie subjektai gali būti svarbūs vertės grandinių dalyviai, o jų tinklų ir informacinių sistemų saugumas yra neatsiejama bendro vidaus rinkos kibernetinio saugumo dalis. Tyrimų organizacijos turėtų būti suprantamos kaip apimančios subjektus, kurie pagrindinę dalį savo veiklos skiria taikomųjų mokslinių tyrimų arba eksperimentinės plėtros

vykdymui, kaip tai suprantama 2015 m. Ekonominio bendradarbiavimo ir plėtros organizacijos Fraskačio vadove: mokslinių tyrimų ir eksperimentinės plėtros duomenų rinkimo ir teikimo gairėse (angl. „Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development“), siekdami panaudoti savo rezultatus komerciniais tikslais, pavyzdžiui, produkto ar proceso gamybos ar kūrimo arba paslaugos teikimo ir jų pateikimo rinkai tikslais;

(37) didėjančią tarpusavio priklausomybę lemia vis labiau tarptautinio pobūdžio ir tarpusavyje priklausomas paslaugų teikimo tinklas, kuriame naudojami pagrindiniai visoje Sąjungoje esantys tokių sektorių kaip energetika, transportas, skaitmeninė infrastruktūra, geriamasis vanduo ir nuotekos, sveikata, tam tikri viešojo administravimo aspektai, taip pat kosmosas, infrastruktūros objektai, kiek tai susiję su tam tikrų paslaugų teikimu, kuriam įtakos turi antžeminės infrastruktūros objektai, kurie priklauso valstybėms narėms arba privačioms šalims, yra jų valdomi arba eksploatuojami, todėl tai neapima infrastruktūros objektų, kurie priklauso Sąjungai, kai ji įgyvendina savo kosmoso programą, arba kurie yra valdomi ar eksploatuojami Sąjungos vardu šios programos įgyvendinimo metu. Ta tarpusavio priklausomybė reiškia, kad bet koks sutrikimas, kuris iš pradžių įvyksta tik viename subjekte arba sektoriuje, gali turėti platesnį grandininį poveikį ir sukelti platesnio masto ir ilgalaikes neigiamas pasekmes paslaugų teikimui visoje vidaus rinkoje. COVID-19 pandemijos metu padažnėję kibernetiniai išpuoliai parodė, kad vis labiau tarpusavyje priklausoma visuomenė yra pažeidžiama atsižvelgiant į mažai tikėtiną riziką;

(38) atsižvelgiant į nacionalinių valdymo struktūrų skirtumus ir siekiant išsaugoti jau veikiančias sektorių sistemas ar Sąjungos priežiūros ir reguliavimo įstaigas, valstybės narės turėtų turėti teisę paskirti ar įsteigti vieną ar daugiau kompetentingų institucijų, atsakingų už užduočių kibernetinio saugumo ir priežiūros srityse pagal šią direktyvą vykdymą;

(39) siekiant palengvinti tarpvalstybinį institucijų bendradarbiavimą ir ryšių palaikymą bei sudaryti sąlygas veiksmingai įgyvendinti šią direktyvą, būtina, kad kiekviena valstybė narė paskirtų bendrąjį kontaktinį punktą, atsakingą už klausimų, susijusių su tinklų ir informacinių sistemų saugumu, koordinavimą ir tarpvalstybinį bendradarbiavimą Sąjungos lygmeniu;

(40) bendrieji kontaktiniai punktai turėtų užtikrinti veiksmingą tarpvalstybinį bendradarbiavimą su atitinkamomis kitų valstybių narių institucijomis ir prireikus su Komisija ir ENISA. Todėl bendriesiems kontaktiniams punktams turėtų būti pavesta, CSIRT arba kompetentingai institucijai paprašius, persiųsti pranešimus apie didelius tarpvalstybinio poveikio incidentus kitų paveiktų valstybių narių bendriesiems kontaktiniams punktams. Nacionaliniu lygmeniu bendrieji kontaktiniai punktai turėtų sudaryti sąlygas sklandžiam tarpsektoriniam bendradarbiavimui su kitomis kompetentingomis institucijomis. Bendrieji kontaktiniai punktai taip pat galėtų gauti atitinkamą informaciją apie incidentus, susijusius su finansų sektoriaus subjektais, iš kompetentingų institucijų pagal Reglamentą (ES) 2022/2554, kurią jie turėtų turėti galimybę, kai tinkama, persiųsti CSIRT arba kompetentingoms institucijoms pagal šią direktyvą;

(41) valstybės narės turėtų būti tinkamai pasirengusios – turėti tiek techninių, tiek organizacinių pajėgumų, kad galėtų užkirsti kelią incidentams bei rizikai, juos atskleisti, į juos reaguoti ir sušvelninti jų poveikį. Todėl valstybės narės turėtų pagal šią direktyvą įsteigti ar paskirti vieną ar daugiau CSIRT ir užtikrinti, kad jos turėtų pakankamai išteklių bei techninių pajėgumų. CSIRT turėtų atitikti šioje direktyvoje nustatytus reikalavimus, kad būtų garantuoti veiksmingi bei suderinami incidentų bei rizikos valdymo pajėgumai ir užtikrintas veiksmingas bendradarbiavimas Sąjungos lygmeniu. Valstybės narės turėtų turėti galimybę CSIRT paskirti jau esamas kompiuterinių incidentų tyrimo tarnybas (CERT). Siekiant stiprinti pasitikėjimu grindžiamus santykius tarp subjektų ir CSIRT, tais atvejais, kai CSIRT veikia kompetentingoje institucijoje, valstybės narės turėtų galėti apsvarstyti galimybę funkciniu požiūriu atskirti CSIRT vykdomas operatyvines užduotis, ypač susijusias su dalijimusi informacija ir subjektams teikiama pagalba, ir kompetentingų institucijų priežiūros veiklą;

(42) CSIRT pavesta valdyti incidentus. Tai apima didelių kartais neskelbtinų duomenų kiekių tvarkymą. Valstybės narės turėtų užtikrinti, kad CSIRT turėtų dalijimosi informacija ir jos tvarkymo infrastruktūrą, taip pat gerai aprūpintą personalą, kuris užtikrintų jų operacijų konfidencialumą ir patikimumą. CSIRT taip pat galėtų priimti elgesio kodeksus šiuo klausimu;

(43) kalbant apie asmens duomenis pažymėtina, kad CSIRT turėtų turėti galimybę pagal Reglamentą (ES) 2016/679 subjekto, kuriam taikoma ši direktyva, prašymu imtis iniciatyvos patikrinti tinklų ir informacines sistemas, naudojamas esminio ar svarbaus subjekto paslaugoms teikti. Jei taikoma, valstybės narės turėtų siekti užtikrinti vienodą visų sektorių CSIRT techninių pajėgumų lygį. Valstybės narės turėtų turėti galimybę paprašyti ENISA padėti kurti jų CSIRT;

(44) CSIRT turėtų turėti galimybę esminio ar svarbaus subjekto prašymu stebėti subjekto su internetu susietus išteklius tiek patalpose, tiek už jų ribų, kad nustatytų, suprastų ir valdytų subjekto bendrą organizacinę riziką, susijusią su naujai nustatytomis tiekimo grandinės spragomis ar kritiniais pažeidžiamumais. Subjektas turėtų būti skatinamas pranešti CSIRT, ar jis naudoja privilegijuotojo valdymo sąsają, nes tai galėtų turėti įtakos rizikos mažinimo veiksmų įgyvendinimo spartai;

(45) atsižvelgiant į tarptautinio bendradarbiavimo kibernetinio saugumo srityje svarbą, CSIRT turėtų turėti galimybę dalyvauti ne tik šia direktyva sukurto CSIRT tinklo, bet ir tarptautinio bendradarbiavimo tinklų veikloje. Todėl siekdamos vykdyti savo užduotis, CSIRT ir kompetentingos institucijos turėtų turėti galimybę keistis informacija, įskaitant asmens duomenis, su trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis arba kompetentingomis institucijomis, jeigu laikomasi Sąjungos duomenų apsaugos teisės aktuose nustatytų asmens duomenų perdavimo trečiosioms valstybėms sąlygų, *inter alia*, Reglamento (ES) 2016/679 49 straipsnyje nustatytų sąlygų;

(46) norint pasiekti šios direktyvos tikslus ir sudaryti galimybę kompetentingoms institucijoms bei CSIRT vykdyti joje nustatytas užduotis, nepaprastai svarbu užtikrinti pakankamus išteklius. Valstybės narės nacionaliniu lygmeniu gali nustatyti finansavimo mechanizmą, pagal kurį būtų dengiamos būtinos išlaidos, susijusios su už kibernetinį saugumą valstybėje narėje atsakingų viešųjų subjektų užduočių vykdymu pagal šią direktyvą. Toks mechanizmas turėtų atitikti Sąjungos teisę, būti proporcingas ir nediskriminacinis, taip pat juo turėtų būti atsižvelgiama į skirtingus požiūrius į saugių paslaugų teikimą;

(47) CSIRT tinklas turėtų toliau padėti stiprinti valstybių narių tarpusavio pasitikėjimą bei patikimumą ir skatinti spartų ir efektyvų operatyvinį bendradarbiavimą. Siekdamas intensyvinti operatyvinį bendradarbiavimą Sąjungos lygmeniu, CSIRT tinklas turėtų apsvarstyti galimybę pakviesti savo darbe dalyvauti kibernetinio saugumo politikos srityje veikiančius Sąjungos organus ir agentūras, pavyzdžiui, Europolą;

(48) siekiant pasiekti ir išlaikyti aukštą kibernetinio saugumo lygį, nacionalines kibernetinio saugumo strategijas, kurių reikalaujama pagal šią direktyvą, turėtų sudaryti nuoseklios sistemos, kuriose būtų numatyti strateginiai tikslai bei prioritetai kibernetinio saugumo srityje ir jų įgyvendinimo valdymas. Tas strategijas gali sudaryti viena ar daugiau teisėkūros arba ne teisėkūros priemonių;

(49) kibernetinės higienos politikoje numatomi tinklų ir informacinių sistemų infrastruktūros, aparatinės įrangos, programinės įrangos ir internetinių programų saugumo, taip pat subjektų naudojamų verslo ir galutinių naudotojų duomenų apsaugos pagrindai. Kibernetinės higienos politika, apimanti bendrą praktikos pavyzdžių, be kita ko, susijusių su programinės ir aparatinės įrangos atnaujinimu, slaptažodžių keitimu, naujai įdiegtų programų valdymu, administratoriaus lygmens prieigos paskyrų ribojimu ir duomenų atsarginiu kopijavimu, rinkinį, sudaro sąlygas iniciatyviai pasirengimo ir bendros saugos bei saugumo incidentų ar kibernetinių grėsmių atveju sistemai. ENISA turėtų stebėti ir analizuoti valstybių narių kibernetinės higienos politiką;

(50) informuotumas apie kibernetinį saugumą ir kibernetinė higiena yra nepaprastai svarbūs siekiant padidinti kibernetinio saugumo lygį Sąjungoje, visų pirma atsižvelgiant į didėjantį prijungtųjų įrenginių, kurie vis dažniau naudojami kibernetinių išpuolių metu, skaičių. Reikėtų dėti pastangas siekiant didinti bendrą informuotumą apie riziką, susijusią su tokiais įrenginiais, o vertinimai Sąjungos lygmeniu galėtų padėti užtikrinti bendrą supratimą apie tokią riziką vidaus rinkoje;

(51) valstybės narės turėtų skatinti naudoti visas novatoriškas technologijas, įskaitant dirbtinį intelektą, kurias naudojant galėtų būti geriau atskleidžiami kibernetiniai išpuoliai ir geriau jų išvengiama, sudarant sąlygas veiksmingiau nukreipti išteklius kovai su kibernetiniais išpuoliais. Todėl valstybės narės savo nacionalinėje kibernetinio saugumo strategijoje turėtų skatinti tyrimų ir plėtros veiklą, kad būtų sudarytos palankesnės sąlygos naudoti tokias technologijas, visų pirma susijusias su automatizuotomis arba pusiau automatizuotomis kibernetinio saugumo priemonėmis, ir prireikus dalytis duomenimis, kurių reikia tokių technologijų naudotojams mokyti ir joms tobulinti. Bet kokių novatoriškų technologijų, įskaitant dirbtinį intelektą, naudojimas turėtų atitikti Sąjungos duomenų apsaugos teisės aktus, įskaitant tokius duomenų apsaugos principus, kaip duomenų tikslumo, duomenų kiekio mažinimo, sąžiningumo ir skaidrumo, taip pat duomenų saugumo, pavyzdžiui, pažangiausio šifravimo. Turėtų būti visapusiškai naudojamasi Reglamente (ES) 2016/679 nustatytais pritaikytosios ir standartizuotosios duomenų apsaugos reikalavimais;

(52) atvirojo kodo kibernetinio saugumo priemonėmis ir taikomosiomis programomis gali būti prisidedama prie didesnio atvirumo ir daromas teigiamas poveikis pramonės inovacijų veiksmingumui. Atviraisiais standartais sudaromos palankesnės sąlygos saugumo priemonių sąveikumui, o tai yra naudinga pramonės suinteresuotųjų subjektų saugumo požiūriu. Atvirojo kodo kibernetinio saugumo priemonėmis ir taikomosiomis programomis gali būti daromas sverto poveikis platesnei technologijų kūrėjų bendruomenei, sudarant galimybes tiekėjų diversifikacijai. Atvirasis kodas gali paskatinti skaidresnį su kibernetiniu saugumu susijusių priemonių tikrinimo procesą ir bendruomenės inicijuotą pažeidžiamumų nustatymo procesą. Todėl valstybės narės turėtų turėti galimybę skatinti atvirojo kodo programinės įrangos ir atvirųjų standartų naudojimą, vykdydamos politiką, susijusią su atvirųjų duomenų ir atvirojo kodo naudojimu, kad skaidrumu būtų prisidėta prie saugumo užtikrinimo. Atvirojo kodo kibernetinio saugumo priemonių diegimo ir tvaraus naudojimo skatinimo politika itin svarbi mažosioms ir vidutinėms įmonėms, patiriančioms dideles įgyvendinimo sąnaudas, kurias būtų galima minimizuoti sumažinant poreikį naudoti konkrečias taikomąsias programas ar priemones;

(53) komunalinės paslaugos miestuose vis dažniau prijungiamos prie skaitmeninių tinklų, siekiant patobulinti miesto transporto tinklus, modernizuoti vandens tiekimo ir atliekų šalinimo įrenginius ir padidinti apšvietimo bei pastatų šildymo efektyvumą. Toms suskaitmenintoms komunalinėms paslaugoms kyla kibernetinių išpuolių rizika ir sėkmingo kibernetinio išpuolio atveju kyla pavojus, kad dėl jų tarpusavio sąsajų bus padaryta didelė žala piliečiams. Valstybės narės turėtų parengti politiką, pagal kurią būtų sprendžiami tokių sujungtų ar pažangiųjų miestų plėtros ir galimo jų poveikio visuomenei klausimai, esančią jų nacionalinės kibernetinio saugumo strategijos dalimi;

(54) pastaraisiais metais Sąjungoje eksponentiškai padaugėjo išpuolių naudojant išpirkos reikalavimo programinę įrangą, per kuriuos kenkimo programinė įranga užšifruoja duomenis bei sistemas ir reikalauja išpirkos už iššifravimą. Vis dažnesnius ir rimtesnius išpuolius naudojant išpirkos reikalavimo programinę įrangą gali lemti keli veiksniai, pavyzdžiui, skirtingi išpuolių modeliai, nusikalstamo verslo modeliai, susiję su „paslaugine išpirkos reikalavimo programine įranga“ ir kriptovaliuta, išpirkos reikalavimai ir išaugę išpuoliai tiekimo grandinėje. Valstybės narės turėtų parengti kovos su dažnėjančiais išpuoliais naudojant išpirkos reikalavimo programinę įrangą politiką, esančią jų nacionalinės kibernetinio saugumo strategijos dalimi;

(55) viešojo ir privačiojo sektorių partnerystė kibernetinio saugumo srityje gali būti tinkama keitimosi žiniomis, dalijimosi geriausios praktikos pavyzdžiais ir bendro supratimo tarp suinteresuotųjų subjektų nustatymo sistema. Valstybės narės turėtų skatinti politiką, pagal kurią būtų kuriamos konkrečiai su kibernetiniu saugumu susijusios viešojo ir privačiojo sektorių partnerystės. Toje politikoje, *inter alia*, turėtų būti patikslinama taikymo sritis ir dalyvaujantys suinteresuotieji subjektai, valdymo modelis, turimos finansavimo galimybės ir dalyvaujančių suinteresuotųjų subjektų tarpusavio ryšys, kiek tai susiję su viešojo ir privačiojo sektorių partnerystėmis. Viešojo ir privačiojo sektorių partnerystės gali naudotis privačiojo sektoriaus subjektų ekspertinėmis žiniomis, kad padėtų kompetentingoms institucijoms kurti pažangiausias paslaugas ir procesus, įskaitant keitimąsi informacija, ankstyvuosius perspėjimus, kibernetinių grėsmių ir incidentų valdymo pratybas, krizių valdymą ir atsparumo planavimą;

(56) savo nacionalinėse kibernetinio saugumo strategijose valstybės narės turėtų atsižvelgti į konkrečius mažųjų ir vidutinių įmonių kibernetinio saugumo poreikius. Mažosios ir vidutinės įmonės Sąjungoje sudaro didelę pramoninės ir verslo rinkos procentinę dalį ir dažnai joms sunku prisitaikyti prie naujos verslo praktikos labiau susietame pasaulyje, ir prie skaitmeninės aplinkos, kai darbuotojai dirba iš namų, o verslas vis dažniau vykdomas internetu. Kai kurios mažosios ir vidutinės įmonės susiduria su konkrečiomis kibernetinio saugumo problemomis, pvz., mažu kibernetiniu sąmoningumu, nuotolinio IT saugumo trūkumu, didelėmis kibernetinio saugumo sprendimų sąnaudomis ir išaugusiu grėsmių lygiu, pvz., išpirkos reikalavimo programinės įrangos grėsme, kurių klausimu jos turėtų gauti gaires ir pagalbą. Mažosios ir vidutinės įmonės vis dažniau tampa išpuolių prieš tiekimo grandines taikiniu dėl ne tokių griežtų jų kibernetinio saugumo rizikos valdymo priemonių ir išpuolių valdymo ir dėl to, kad turi ribotus saugumo išteklius. Tokie išpuoliai prieš tiekimo grandines daro poveikį ne tik mažosioms ir vidutinėms įmonėms ir jų veiklai atskirai, bet ir gali daryti pakopinį poveikį didesniems išpuoliams prieš subjektus, kuriems jos tiekė prekes. Valstybės narės savo nacionalinėmis kibernetinio saugumo strategijomis turėtų padėti

mažosioms ir vidutinėms įmonėms spręsti problemas, su kuriomis jos susiduria savo tiekimo grandinėse. Valstybės narės turėtų turėti nacionalinį arba regioninį kontaktinį punktą, skirtą mažosioms ir vidutinėms įmonėms, kuris teiktų gaires ir pagalbą mažosioms ir vidutinėms įmonėms arba nukreiptų jas į atitinkamas įstaigas, teikiančias gaires ir pagalbą su kibernetiniu saugumu susijusiais klausimais. Valstybės narės taip pat skatinamos siūlyti tokias paslaugas, kaip interneto svetainių konfigūravimas ir registravimo galimybių suteikimas, tokių gebėjimų neturinčioms labai mažoms ir mažosioms įmonėms;

(57) valstybės narės turėtų priimti aktyvios kibernetinės apsaugos skatinimo politiką, kaip platesnės gynybos strategijos dalį, esančią jų nacionalinių kibernetinio saugumo strategijų dalimi. Vietoj reaguojamojo pobūdžio atsako aktyvi kibernetinė apsauga yra aktyvaus pobūdžio tinklo saugumo pažeidimų prevencija, nustatymas, stebėjimas, analizė ir poveikio švelninimas, sykiu naudojant nukentėjusiųjų tinkle ir už jo ribų įdiegtus pajėgumus. Tai galėtų apimti valstybių narių siūlomas nemokamas paslaugas ar priemones, įskaitant savarankiškus pasitikrinimus, atskleidimo priemones ir turinio pašalinimo paslaugas, tam tikriems subjektams. Gebėjimas greitai ir automatiškai dalytis informacija apie grėsmes ir analize, įspėjimais apie kibernetinę veiklą ir informacija apie reagavimo veiksmus ir juos suprasti yra nepaprastai svarbus siekiant užtikrinti, kad būtų imamasi vieningų pastangų sėkmingai užkirsti kelią išpuoliams prieš tinklų ir informacines sistemas, juos atskleisti, kovoti su jais ir juos blokuoti. Aktyvi kibernetinė apsauga grindžiama gynybos strategija, į kurią neįtraukiamos puolamosios priemonės;

(58) kadangi pasinaudojimas tinklų ir informacinių sistemų pažeidžiamumais gali sukelti rimtus sutrikimus ir žalą, greitas tokių pažeidžiamumų nustatymas ir jų ištaisymas yra svarbus veiksnys mažinant riziką. Todėl tinklų ir informacines sistemas kuriantys arba administruojantys subjektai turėtų nustatyti atitinkamas procedūras, kurias taikant būtų šalinami aptikti pažeidžiamumai. Kadangi pažeidžiamumus dažnai aptinka ir atskleidžia trečiosios šalys, IRT produktų ar IRT paslaugų gamintojas arba teikėjas taip pat turėtų nustatyti būtinas procedūras, pagal kurias iš trečiųjų šalių būtų gaunama informacija apie pažeidžiamumą. Šuo atžvilgiu tarptautiniuose standartuose ISO/IEC 30111 ir ISO/IEC 29147 pateikiamos gairės dėl pažeidžiamumų šalinimo ir atskleidimo. Siekiant sudaryti sąlygas savanoriškai pažeidžiamumų atskleidimo sistemai, ypač svarbu stiprinti koordinavimą tarp pranešimą teikiančių fizinių ir juridinių asmenų ir IRT produktų ar IRT paslaugų gamintojų arba teikėjų. Koordinuotas pažeidžiamumų atskleidimas yra struktūrinis procesas, per kurį potencialiai pažeidžiamų IRT produktų ar IRT paslaugų gamintojui arba teikėjui pranešama apie pažeidžiamumus taip, kad jam būtų sudarytos sąlygos pažeidžiamumą nustatyti ir ištaisyti prieš atskleidžiant išsamią informaciją apie pažeidžiamumus trečiosioms šalims arba visuomenei. Koordinuotas pažeidžiamumų atskleidimas taip pat turėtų apimti pranešimą teikiančio fizinio ar juridinio asmens ir potencialiai pažeidžiamų IRT produktų ar IRT paslaugų gamintojo arba teikėjo koordinavimą ištaisymo laiko ir paskelbimo apie pažeidžiamumus klausimais;

(59) Komisija, ENISA ir valstybės narės turėtų toliau skatinti derinimą su tarptautiniais standartais ir esama sektoriaus gerąją praktika kibernetinio saugumo rizikos valdymo srityje, pavyzdžiui, tiekimo grandinės saugumo vertinimų, dalijimosi informacija ir pažeidžiamumų atskleidimo srityse;

(60) valstybės narės, bendradarbiaudamos su ENISA, turėtų imtis priemonių, kad palengvintų koordinuotą pažeidžiamumų atskleidimą, nustatydamos atitinkamą nacionalinę politiką. Vykdydamos savo nacionalinę politiką, 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;

(61) valstybės narės turėtų paskirti vieną iš savo CSIRT koordinatore, kuri, prireikus, veiktų kaip patikima tarpininkė tarp pranešimus teikiančių fizinių ar juridinių subjektų ir IRT produktų ar IRT paslaugų gamintojų arba teikėjų, kuriems pažeidžiamumas gali daryti poveikį. Koordinatore paskirtos CSIRT užduotys turėtų apimti atitinkamų subjektų identifikavimą ir susisiekimą su jais, pranešimus apie pažeidžiamumą teikiančių fizinių ar juridinių subjektų rėmimą, derybas dėl informacijos atskleidimo terminų ir pažeidžiamumų, kurie daro poveikį keliems subjektams,

valdymą (kelių šalių koordinuotas pažeidžiamumų atskleidimas). Kai pažeidžiamumas, apie kurį pranešta, galėtų daryti didelį poveikį subjektams daugiau nei vienoje valstybėje narėje, kai tikslinga, koordinatorėmis paskirtos CSIRT turėtų bendradarbiauti CSIRT tinkle;

(62) prieiga prie teisingos ir laiku pateikiamos informacijos apie pažeidžiamumus, kurie daro poveikį IRT produktams ir IRT paslaugoms, padeda geriau valdyti kibernetinio saugumo riziką. Viešai prieinamos informacijos apie pažeidžiamumus šaltiniai yra svarbi priemonė ne tik subjektams ir jų paslaugų naudotojams, bet ir kompetentingoms institucijoms bei CSIRT. Dėl tos priežasties ENISA turėtų sukurti Europos pažeidžiamumų duomenų bazę, kurioje subjektai, nepriklausomai nuo to, ar jie patenka į šios direktyvos taikymo sritį, ir jų tinklų ir informacinių sistemų tiekėjai, taip pat kompetentingos institucijos ir CSIRT gali savanoriškai atskleisti ir registruoti viešai žinomus pažeidžiamumus, siekiant sudaryti sąlygas naudotojams imtis atitinkamų rizikos mažinimo priemonių. Tos duomenų bazės tikslas – atremti unikalius iššūkius, kurie iškyla dėl Sąjungos subjektams kylančios rizikos. Be to, ENISA turėtų nustatyti tinkamą procedūrą, susijusią su viešinimo procesu, kad subjektai turėtų laiko imtis rizikos mažinimo priemonių, susijusių su jų pažeidžiamumais, ir pradėtų taikyti pažangiąsias kibernetinio saugumo rizikos valdymo priemones, taip pat kompiuterio skaitomus duomenų rinkinius ir atitinkamas sąsajas. Siekiant skatinti pažeidžiamumų atskleidimo kultūrą, atskleidimas neturėtų pakenkti pranešančiajam fiziniam ar juridiniam asmeniui;

(63) nors panašūs pažeidžiamumų registrai arba duomenų bazės jau yra sukurti, jų prieglobą vykdo ir juos tvarko subjektai, kurie nėra įsisteigę Sąjungoje. ENISA tvarkoma Europos pažeidžiamumų duomenų bazė padėtų užtikrinti didesnį paskelbimo proceso iki viešo pažeidžiamumų atskleidimo skaidrumą ir atsparumą panašių paslaugų teikimo sutrikimo arba nutraukimo atveju. Siekdama kuo labiau išvengti veiksmų dubliavimo ir siekti papildomumo, ENISA turėtų išnagrinėti galimybę sudaryti struktūrinio bendradarbiavimo susitarimus su panašiais registrais arba duomenų bazėmis, kurie priklauso trečiųjų valstybių jurisdikcijoms. Visų pirma ENISA turėtų išnagrinėti galimybę glaudžiai bendradarbiauti su Bendros pažeidžiamumų ir rizikos (BPR) sistemos operatoriais;

(64) Bendradarbiavimo grupė turėtų remti ir palengvinti valstybių narių strateginį bendradarbiavimą ir keitimąsi informacija, taip pat didinti jų tarpusavio pasitikėjimą ir patikimumą. Bendradarbiavimo grupė turėtų kas dvejus metus patvirtinti darbo programą. Darbo programa turėtų apimti veiksmus, kurių Bendradarbiavimo grupė turi imtis, kad pasiektų savo tikslus ir įvykdytų užduotis. Pirmosios pagal šią direktyvą darbo programos patvirtinimo laikotarpis turėtų būti suderintas su paskutinės darbo programos, patvirtintos pagal Direktyvą (ES) 2016/1148, laikotarpiu, kad būtų išvengta galimų Bendradarbiavimo grupės darbo sutrikimų;

(65) rengdama gairių dokumentus, Bendradarbiavimo grupė turėtų nuosekliai išsiaiškinti nacionalinius sprendimus ir patirtį, įvertinti Bendradarbiavimo grupės rezultatų poveikį nacionaliniams požiūriams, aptarti įgyvendinimo problemas ir suformuluoti konkrečias rekomendacijas, visų pirma dėl šios direktyvos perkėlimo į nacionalinę teisę suderinimo tarp valstybių narių palengvinimo, į kurias turėtų būti atsižvelgiama geriau įgyvendinant dabartines taisykles. Bendradarbiavimo grupė taip pat galėtų apibendrinti nacionalinius sprendimus, kad būtų skatinamas kibernetinio saugumo sprendimų, taikomų kiekvienam konkrečiam sektoriui visoje Sąjungoje, suderinamumas. Tai ypač svarbu tarptautinio ar tarpvalstybinio pobūdžio sektoriams;

(66) Bendradarbiavimo grupė turėtų išlikti lanksčiu forumu ir sugebėti reaguoti į kintančius ir naujus politikos prioritetus bei problemas ir kartu atsižvelgti į prieinamus išteklius. Ji galėtų nuolat rengti bendrus susitikimus su atitinkamais privačiais suinteresuotaisiais subjektais iš visos Sąjungos, kad aptartų Bendradarbiavimo grupės vykdomą veiklą ir surinktų duomenų bei informacijos apie naujus politikos iššūkius. Be to, Bendradarbiavimo grupė turėtų reguliariai vertinti kibernetinių grėsmių ar incidentų, pavyzdžiui, susijusių su išpirkos reikalavimo programine įranga, padėtį. Siekdama didinti bendradarbiavimą Sąjungos lygmeniu, Bendradarbiavimo grupė turėtų apsvarstyti galimybę pakviesti savo veikloje dalyvauti atitinkamas kibernetinio saugumo politikos srityje veikiančias Sąjungos institucijas,

įstaigas, organus ir agentūras, pavyzdžiui, Europos Parlamentą, Europolą, Europos duomenų apsaugos valdybą, Europos Sąjungos aviacijos saugos agentūrą, įsteigtą Reglamentu (ES) 2018/1139, ir Europos Sąjungos kosmoso programos agentūrą, įsteigtą Europos Parlamento ir Tarybos reglamentu (ES) 2021/696 ([14]);

(67) kompetentingos institucijos ir CSIRT turėtų turėti galimybę dalyvauti pareigūnų iš kitų valstybių narių mainų programose specialioje sistemoje ir, kai taikytina, taikant reikiamą tokiose mainų programose dalyvaujančių pareigūnų patikimumo patikrinimą, siekiant pagerinti bendradarbiavimą ir didinti valstybių narių tarpusavio pasitikėjimą. Kompetentingos institucijos turėtų imtis būtinų priemonių, kad pareigūnai iš kitų valstybių narių galėtų veiksmingai dalyvauti priimančiosios kompetentingos institucijos arba priimančiosios CSIRT veikloje;

(68) valstybės narės turėtų prisidėti kuriant Komisijos rekomendacijoje (ES) 2017/1584 ([15]) numatytą ES reagavimo į kibernetinio saugumo krizes sistemą per esamus bendradarbiavimo tinklus, visų pirma per Europos ryšių palaikymo dėl kibernetinių krizių organizacinį tinklą (EU-CyCLONe), CSIRT tinklą ir Bendradarbiavimo grupę. EU-CyCLONe ir CSIRT tinklas turėtų bendradarbiauti remdamiesi procedūrinėmis taisyklėmis, kuriomis išsamiau apibrėžiamas tas bendradarbiavimas, ir vengti bet kokio užduočių dubliavimosi. EU-CyCLONe darbo tvarkos taisyklėse taip pat turėtų būti aptarta to tinklo veikimo tvarka, įskaitant tinklo vaidmenis, bendradarbiavimo būdus, sąveiką su kitais atitinkamais dalyviais ir dalijimosi informacija šablonus, taip pat ryšių palaikymo priemones. Siekdamos valdyti krizę Sąjungos lygmeniu, atitinkamos šalys turėtų kliautis ES integruoto politinio atsako į krizes mechanizmu, kaip nustatyta Tarybos įgyvendinimo sprendime (ES) 2018/1993 ([16]) (toliau – IPCR mechanizmas). Komisija tuo tikslu turėtų naudoti aukšto lygmens tarpsektorinį krizės koordinavimo procesą ARGUS. Jei krizė susijusi su svarbiais išorės arba bendros saugumo ir gynybos politikos aspektais, turėtų būti panaudotas Europos išorės veiksmų tarnybos reagavimo į krizę mechanizmas;

(69) pagal Rekomendacijos (ES) 2017/1584 priedą didelio masto kibernetinio saugumo incidentas turėtų reikšti incidentą, į kurio sukeltą sutrikimą viena valstybė narė nepajėgia reaguoti arba kuris turi didelį poveikį ne mažiau kaip dviem valstybėms narėms. Priklausomai nuo jų priežasties ir poveikio, didelio masto kibernetinio saugumo incidentai gali stiprėti ir virsti plataus masto krizėmis, dėl kurių vidaus rinka negali tinkamai veikti, arba kelti rimtą pavojų visuomenės saugumui ir subjektų ar piliečių saugai keliose valstybėse narėse arba visoje Sąjungoje. Atsižvelgiant į tai, kad tokie incidentai yra labai įvairaus masto ir dažniausiai tarpvalstybinio pobūdžio, valstybės narės ir atitinkamos Sąjungos institucijos, įstaigos, organai ir agentūros turėtų bendradarbiauti techniniu, operatyviniu ir politiniu lygmenimis, kad tinkamai koordinuotų atsaką visoje Sąjungoje;

(70) kilus didelio masto kibernetinio saugumo incidentams ir krizėms Sąjungos lygmeniu, dėl didelės sektorių ir valstybių narių tarpusavio priklausomybės reikia imtis koordinuotų veiksmų, kad būtų užtikrintas greitas ir veiksmingas reagavimas. Siekiant užtikrinti Sąjungos saugumą ir apsaugoti jos piliečius, įmones bei institucijas nuo incidentų ir kibernetinių grėsmių, taip pat didinti asmenų ir organizacijų pasitikėjimą Sąjungos gebėjimu propaguoti ir apsaugoti pasaulinę, atvirą, laisvą, stabilią ir saugią kibernetinę erdvę, grindžiamą žmogaus teisėmis, pagrindinėmis laisvėmis, demokratija ir teisine valstybe, nepaprastai svarbu turėti kibernetinėms grėsmėms atsparias tinklų ir informacines sistemas bei prieinamus, konfidencialius ir vientisus duomenis;

([14]) 2021 m. balandžio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/696, kuriuo sudaroma Sąjungos kosmoso programa, įsteigiama Europos Sąjungos kosmoso programos agentūra ir panaikinami reglamentai (ES) Nr. 912/2010, (ES) Nr. 1285/2013 bei (ES) Nr. 377/2014 ir Sprendimas Nr. 541/2014/ES (OL L 170, 2021 5 12, p. 69).

([15]) 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (OL L 239, 2017 9 19, p. 36).

([16]) 2018 m. gruodžio 11 d. Tarybos įgyvendinimo sprendimas (ES) 2018/1993 dėl ES integruoto politinio atsako į krizes mechanizmo (OL L 320, 2018 12 17, p. 28).

(71) didelio masto kibernetinio saugumo incidentų ir krizių metu EU-CyCLONe turėtų veikti kaip tarpininkas tarp techninio ir politinio lygmens ir turėtų stiprinti bendradarbiavimą operatyviniu lygmeniu bei remti sprendimų priėmimą politiniu lygmeniu. Bendradarbiaudamas su Komisija ir atsižvelgdamas į Komisijos kompetenciją krizių valdymo srityje, EU-CyCLONe turėtų remtis CSIRT tinklo nustatytais faktais ir naudotis savo pajėgumais, kad parengtų didelio masto kibernetinio saugumo incidentų ir krizių poveikio analizę;

(72) kibernetiniai išpuoliai yra tarpvalstybinio pobūdžio ir didelis incidentas gali sutrikdyti ypatingos svarbos informacinės infrastruktūros, nuo kurios priklauso sklandus vidaus rinkos veikimas, veiklą ir jai gali būti pakenkta. Rekomendacijoje (ES) 2017/1584 aptariamas visų susijusių veikėjų vaidmuo. Be to, pagal Sąjungos civilinės saugos mechanizmo, sukurto Europos Parlamento ir Tarybos sprendimu Nr. 1313/2013/ES ([17]), Komisija yra atsakinga už bendruosius pasirengimo veiksmus, įskaitant Reagavimo į nelaimes koordinavimo centro ir Bendros ekstremaliųjų situacijų ryšių ir informacijos sistemos valdymą, informuotumo apie padėtį ir jos analizės pajėgumų išlaikymą bei tolesnį plėtojimą, taip pat pajėgumų mobilizuoti ir siųsti ekspertų grupes valstybei narei arba trečiajai valstybei paprašius pagalbos sukūrimą ir valdymą. Komisija yra atsakinga ir už analitinių ataskaitų dėl IPCR mechanizmo pagal Įgyvendinimo sprendimą (ES) 2018/1993 teikimą, be kita ko, kiek tai susiję su informuotumu apie kibernetinio saugumo padėtį ir pasirengimu, taip pat dėl informuotumo apie padėtį ir reagavimo į krizes žemės ūkio, nepalankių oro sąlygų, konfliktų kartografavimo ir prognozių, ankstyvojo perspėjimo apie gaivalines nelaimes sistemų, ekstremaliųjų sveikatos situacijų, infekcinių ligų stebėjimo, augalų sveikatos, cheminių incidentų, maisto ir pašarų saugos, gyvūnų sveikatos, migracijos, muitinės, branduolinių ir radiologinių ekstremaliųjų situacijų bei energetikos srityse;

(73) pagal SESV 218 straipsnį Sąjunga, kai tinkama, gali sudaryti tarptautinius susitarimus su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis, pagal kuriuos joms būtų leidžiama dalyvauti tam tikroje Bendradarbiavimo grupės, CSIRT tinklo ir EU-CyCLONe veikloje ir toks dalyvavimas būtų organizuojamas. Tokiuose susitarimuose turėtų būti užtikrinami Sąjungos interesai ir tinkama duomenų apsauga. Tai neturėtų daryti poveikio valstybių narių teisei bendradarbiauti su trečiosiomis valstybėmis pažeidžiamumų valdymo ir kibernetinio saugumo rizikos valdymo klausimais, palengvinant pranešimų teikimą ir keitimąsi bendrąja informacija laikantis Sąjungos teisės;

(74) siekdamos palengvinti šios direktyvos veiksmingą įgyvendinimą dėl, *inter alia*, pažeidžiamumų valdymo, kibernetinio saugumo rizikos valdymo priemonių, pareigų pranešti ir dalijimosi kibernetinio saugumo informacija susitarimų, valstybės narės gali bendradarbiauti su trečiosiomis valstybėmis ir imtis veiklos, kuri laikoma tinkama tam tikslui, įskaitant keitimąsi informacija apie kibernetines grėsmes, incidentus, pažeidžiamumus, priemones ir metodus, taktiką, metodiką ir procedūras, kibernetinio saugumo krizių valdymo parengtį ir pratybas, mokymus, pasitikėjimo stiprinimą ir struktūrizuoto dalijimosi informacija susitarimus;

(75) turėtų būti įvesti tarpusavio vertinimai siekiant padėti pasimokyti iš bendros patirties, stiprinti tarpusavio pasitikėjimą ir pasiekti aukštą bendrą kibernetinio saugumo lygį. Tarpusavio vertinimai gali padėti gauti vertingų įžvalgų ir rekomendacijų, kuriomis būtų stiprinami bendri kibernetinio saugumo pajėgumai, sukuriant dar vieną funkcionalų būdą dalytis valstybių narių geriausios praktikos pavyzdžiais ir prisidedant prie valstybių narių brandos kibernetinio saugumo srityje lygio didinimo. Be to, atliekant tarpusavio vertinimus turėtų būti atsižvelgiama į panašių mechanizmų, pavyzdžiui, CSIRT tinklo tarpusavio vertinimo sistemos, rezultatus ir jais turėtų būti kuriama pridėtinė vertė bei vengiama dubliavimo. Tarpusavio vertinimų įgyvendinimas neturėtų daryti poveikio Sąjungos ar nacionalinei teisei dėl konfidencialios ar įslaptintos informacijos apsaugos;

(76) Bendradarbiavimo grupė turėtų nustatyti valstybėms narėms skirtą įsivertinimo metodiką, kuria būtų siekiama apimti tokius veiksnius kaip kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti įgyvendinimo lygis, pajėgumų lygis ir kompetentingų institucijų užduočių vykdymo veiksmingumas, CSIRT operaciniai pajėgumai, savitarpio pagalbos įgyvendinimo lygis, dalijimosi kibernetinio saugumo informacija susitarimų įgyvendinimo lygis arba konkretūs tarpvalstybinio ar tarpsektorinio pobūdžio klausimai. Valstybės narės turėtų būti skatinamos reguliariai atlikti įsivertinimus ir Bendradarbiavimo grupėje pristatyti bei aptarti savo įsivertinimo rezultatus;

([17]) 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (OL L 347, 2013 12 20, p. 924).

(77) atsakomybė už tinklų ir informacinių sistemų saugumo užtikrinimą didžiąja dalimi tenka esminiams ir svarbiems subjektams. Turėtų būti skatinama ir plėtojama rizikos valdymo kultūra, apimanti rizikos vertinimus ir rizikas, su kuriomis susiduriama, atitinkančių kibernetinio saugumo rizikos valdymo priemonių įgyvendinimą;

(78) kibernetinio saugumo rizikos valdymo priemonėse turėtų būti atsižvelgiama į esminio ar svarbaus subjekto priklausomybę nuo tinklų ir informacinių sistemų ir jos turėtų apimti priemones, skirtas incidentų rizikai nustatyti, incidentų prevencijos, atskleidimo, nustatymo, reagavimo į juos bei veiklos atstatymo po jų ir jų poveikio švelninimo priemones. Tinklų ir informacinių sistemų saugumas turėtų apimti saugomų, perduodamų ir tvarkomų duomenų saugumą. Kibernetinio saugumo rizikos valdymo priemonėse turėtų būti numatyta sisteminė analizė, atsižvelgiant į žmogiškąjį veiksnį, kad būtų galima susidaryti visapusišką tinklų ir informacinės sistemos saugumo vaizdą;

(79) kadangi grėsmė tinklų ir informacinių sistemų saugumui gali būti įvairios kilmės, kibernetinio saugumo rizikos valdymo priemonės turėtų būti grindžiamos visų rūšių pavojus apimančiu požiūriu, kuriuo siekiama apsaugoti tinklų ir informacines sistemas bei jų fizinę aplinką nuo tokių įvykių kaip vagystė, gaisras, potvynis, telekomunikacijų ar elektros energijos tiekimo triktys, arba nuo neleistinos fizinės prieigos prie esminio ar svarbaus subjekto informacijos ir informacijos tvarkymo objektų ir žalos jiems, ir jų trikdžių, kurie galėtų kelti pavojų saugomų, perduodamų ar tvarkomų duomenų arba per tinklų ir informacines sistemas teikiamų ar prieinamų paslaugų prieinamumui, autentiškumui, vientisumui arba konfidencialumui. Todėl kibernetinio saugumo rizikos valdymo priemonėmis taip pat turėtų būti sprendžiamas tinklų ir informacinių sistemų fizinis ir aplinkos saugumas, įtraukiant priemones, skirtas tokioms sistemoms apsaugoti nuo sistemos gedimų, žmogaus klaidų, piktavališkų veiksmų ar gamtos reiškinių laikantis Europos ir tarptautinių standartų, pavyzdžiui, įtrauktų į ISO/IEC 27000 seriją. Tuo atžvilgiu esminiai ir svarbūs subjektai savo kibernetinio saugumo rizikos valdymo priemonėmis turėtų taip pat užtikrinti žmogiškųjų išteklių saugumą ir įdiegti tinkamą prieigos kontrolės politiką. Tos priemonės turėtų būti suderinamos su Direktyva (ES) 2022/2557;

(80) siekdamos įrodyti atitiktį kibernetinio saugumo rizikos valdymo priemonėms ir nesant tinkamų Europos kibernetinio saugumo sertifikavimo schemų, priimtų pagal Europos Parlamento ir Tarybos reglamentą (ES) 2019/881 ([18]), valstybės narės, konsultuodamosi su Bendradarbiavimo grupe ir Europos kibernetinio saugumo sertifikavimo grupe, turėtų skatinti esminius ir svarbius subjektus naudoti atitinkamus Europos ir tarptautinius standartus arba gali reikalauti, kad subjektai naudotų sertifikuotus IRT produktus, IRT paslaugas ir IRT procesus;

(81) siekiant neužkrauti neproporcingos finansinės ir administracinės naštos esminiams ir svarbiems subjektams, kibernetinio saugumo rizikos valdymo priemonės turėtų būti proporcingos rizikai, kuri kyla atitinkamai tinklų ir informacinei sistemai, atsižvelgiant į tokių priemonių modernumą ir, kai taikytina, atitinkamus Europos bei tarptautinius standartus, taip pat jų įgyvendinimo išlaidas;

(82) kibernetinio saugumo rizikos valdymo priemonės turėtų būti proporcingos esminio ar svarbaus subjekto galimybės patirti riziką laipsniui ir visuomeniniam bei ekonominiam poveikiui, kurį sukeltų incidentas. Nustatant kibernetinio saugumo rizikos valdymo priemones, pritaikytas esminiams ir svarbiems subjektams, reikėtų tinkamai atsižvelgti į skirtingą esminiams ir svarbiems subjektams kylančią riziką, pavyzdžiui, subjekto svarbą, jo patiriamą riziką, įskaitant visuomenei kylančią riziką, subjekto dydį ir incidentų tikimybę bei jų sunkumą, be kita ko, jų socialinį ir ekonominį poveikį;

([18]) 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).

(83) esminiai ir svarbūs subjektai turėtų užtikrinti tinklų ir informacinių sistemų, kurias jie naudoja savo veikloje, saugumą. Tos sistemos visų pirma yra privačios tinklų ir informacinės sistemos, kurias administruoja esminių ir svarbių subjektų vidaus IT personalas arba kurių saugumą pavesta užtikrinti užsakomųjų paslaugų teikėjams. Šioje direktyvoje nustatytos kibernetinio saugumo rizikos valdymo priemonės ir pareigos pranešti turėtų būti taikomos atitinkamiems esminiams ir svarbiems subjektams, nepaisant to, ar tie subjektai savo tinklų ir informacines sistemas techniškai prižiūri patys, ar šias paslaugas užsako;

(84) atsižvelgiant į DNS paslaugų teikėjų, aukščiausio lygio domenų vardų registrų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo paslaugų teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, internetinių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų paslaugų teikėjų ir patikimumo užtikrinimo paslaugų teikėjų tarpvalstybinį pobūdį, jiems turėtų būti taikomas didesnio lygio suderinimas Sąjungos lygmeniu. Todėl kibernetinio saugumo rizikos valdymo priemonių įgyvendinimą tų subjektų atžvilgiu turėtų palengvinti įgyvendinimo aktas;

(85) rizikų, kylančių subjekto tiekimo grandinėje ir jo santykiuose su tiekėjais, pavyzdžiui, duomenų saugojimo ir tvarkymo paslaugų teikėjais arba valdomų saugumo paslaugų teikėjais ir programinės įrangos redaktoriais, mažinimas yra ypač svarbus atsižvelgiant į incidentų paplitimą tais atvejais, kai subjektai tapo kibernetinių išpuolių aukomis ir kai piktavališki nusikalstamos veikos vykdytojai galėjo kelti pavojų subjekto tinklų ir informacinių sistemų saugumui pasinaudodami pažeidžiamumais, darančiais poveikį trečiųjų šalių produktams ir paslaugoms. Todėl esminiai ir svarbūs subjektai turėtų įvertinti ir atsižvelgti į bendrą produktų ir paslaugų kokybę ir atsparumą, juose integruotas kibernetinio saugumo rizikos valdymo priemones bei savo tiekėjų ir paslaugų teikėjų kibernetinio saugumo praktiką, įskaitant jų saugaus kūrimo procedūras. Esminiai ir svarbūs subjektai visų pirma turėtų būti skatinami įtraukti kibernetinio saugumo rizikos valdymo priemones į susitarimus su savo tiesioginiais tiekėjais ir paslaugų teikėjais. Tie subjektai galėtų atsižvelgti į rizikas, kylančias dėl kitų lygmenų tiekėjų ir paslaugų teikėjų;

(86) kalbant apie paslaugų teikėjus, valdomų saugumo paslaugų teikėjai tokiose srityse kaip reagavimas į incidentus, skverbimosi testavimas, saugumo auditai ir konsultacijos atlieka itin svarbų vaidmenį padėdami subjektams užkirsti kelią incidentams, juos atskleisti, į juos reaguoti ar atstatyti po jų veiklą. Tačiau valdomų saugumo paslaugų teikėjai patys yra kibernetinių išpuolių taikiniai ir dėl jų glaudžios integracijos į subjektų veiklą kyla specifinė rizika. Todėl esminiai ir svarbūs subjektai, atrinkdami valdomų saugumo paslaugų teikėją, turėtų veikti atidžiau;

(87) kompetentingoms institucijoms vykdant jų priežiūros užduotis taip pat gali būti naudingos kibernetinio saugumo paslaugos, pavyzdžiui, saugumo auditai, skverbimosi testavimas arba reagavimas į incidentus;

(88) esminiai ir svarbūs subjektai taip pat turėtų mažinti riziką, kylančią dėl jų sąveikos ir santykių su kitais suinteresuotaisiais subjektais platesnėje ekosistemoje, be kita ko, atsižvelgiant į kovą su pramoniniu šnipinėjimu ir komercinių paslapčių apsaugą. Visų pirma tie subjektai turėtų imtis tinkamų priemonių siekdami užtikrinti, kad jų bendradarbiavimas su akademinėmis ir mokslinių tyrimų įstaigomis vyktų laikantis jų kibernetinio saugumo politikos ir būtų laikomasi gerosios praktikos, susijusios su saugia prieiga prie informacijos ir jos sklaida apskritai ir ypač su intelektinės nuosavybės apsauga. Be to, atsižvelgiant į duomenų svarbą ir vertę esminių ir svarbių subjektų veiklai, kai jie naudojasi duomenų transformavimo ir duomenų analizės paslaugomis, kurias teikia trečiosios šalys, subjektai turėtų imtis visų tinkamų kibernetinio saugumo rizikos valdymo priemonių;

(89) esminiai ir svarbūs subjektai turėtų naudoti platų pagrindinės kibernetinės higienos praktikos pavyzdžių spektrą, pavyzdžiui, nulinio pasitikėjimo principus, programinės įrangos atnaujinimus, prietaisų konfigūravimą, tinklo segmentavimą, tapatybės ir prieigos valdymą arba naudotojų informuotumą, rengti savo darbuotojams mokymus ir didinti informuotumą apie kibernetines grėsmes, duomenų viliojimą ar socialinės inžinerijos metodus. Be to, tie subjektai turėtų įvertinti savo kibernetinio saugumo pajėgumus ir prireikus siekti integruoti kibernetinio saugumo stiprinimo technologijas, pavyzdžiui, dirbtinį intelektą ar mašinų mokymosi sistemas, kad sustiprintų savo pajėgumus bei tinklų ir informacinių sistemų saugumą;

(90) siekiant toliau mažinti pagrindines tiekimo grandinės rizikas ir padėti esminiams ir svarbiems subjektams, vykdantiems veiklą sektoriuose, kuriems taikoma ši direktyva, tinkamai valdyti su tiekimo grandine ir tiekėjais susijusią riziką, Bendradarbiavimo grupė, bendradarbiaudama su Komisija ir ENISA ir prireikus, pasikonsultavusi su atitinkamais suinteresuotaisiais subjektais, įskaitant pramonės sektoriaus atstovus, turėtų atlikti koordinuotus ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimus, kaip jau padaryta 5G tinklų atveju pagal Komisijos rekomendaciją (ES) 2019/534 ([19]), siekiant nustatyti kiekvieno sektoriaus ypatingos svarbos IRT paslaugas, IRT sistemas ar IRT produktus, atitinkamas grėsmes ir pažeidžiamumus. Tokiuose koordinuotuose saugumo rizikos vertinimuose turėtų būti nustatytos priemonės, rizikos mažinimo planai ir geriausios praktikos pavyzdžiai šalinant kritines priklausomybes, galimus visuotinį neveikimą sukeliančius gedimo taškus, grėsmes, pažeidžiamumus ir kitus rizikos veiksnius, susijusius su tiekimo grandine, ir turėtų būti ieškoma būdų, kaip toliau skatinti esminius ir svarbius subjektus juos plačiau taikyti. Galimi netechniniai rizikos veiksniai, kaip antai nederamas trečiosios valstybės poveikis tiekėjams ir paslaugų teikėjams, visų pirma alternatyvių valdymo modelių atveju, apima paslėptus pažeidžiamumus arba užpakalines duris ir galimus sisteminius tiekimo sutrikimus, visų pirma technologinio susaistymo arba priklausomybės nuo tiekėjų atveju;

(91) atliekant koordinuotus ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimus, atsižvelgiant į atitinkamo sektoriaus ypatumus, turėtų būti atsižvelgiama tiek į techninius, tiek, kai tinkama, į netechninius veiksnius, įskaitant apibrėžtus Rekomendacijoje (ES) 2019/534, 5G tinklų kibernetinio saugumo ES koordinuotame rizikos vertinime ir ES 5G kibernetinio saugumo priemonių rinkinyje, dėl kurio susitarė Bendradarbiavimo grupė. Siekiant išsiaiškinti, kurioms tiekimo grandinėms turėtų būti taikomas koordinuotas saugumo rizikos vertinimas, turėtų būti atsižvelgta į šiuos kriterijus: i) kokiu mastu esminiai ir svarbūs subjektai naudojasi konkrečiomis ypatingos svarbos IRT paslaugomis, IRT sistemomis ar IRT produktais ir nuo jų priklauso; ii) konkrečių ypatingos svarbos IRT paslaugų, IRT sistemų ar IRT produktų svarba vykdant ypatingos svarbos arba jautrias funkcijas, įskaitant asmens duomenų tvarkymą; iii) alternatyvių IRT paslaugų, IRT sistemų ar IRT produktų prieinamumas; iv) visos IRT paslaugų, IRT sistemų ar IRT produktų tiekimo grandinės atsparumas sutrikimų atžvilgiu per jų gyvavimo ciklą ir v) atsirandančių IRT paslaugų, IRT sistemų ar IRT produktų atveju, jų galimą būsimą svarbą subjektų veiklai. Be to, ypatingas dėmesys turėtų būti skiriamas IRT paslaugoms, IRT sistemoms ar IRT produktams, kuriems taikomi konkretūs trečiųjų valstybių reikalavimai;

(92) siekiant supaprastinti viešųjų elektroninių ryšių tinklų ar viešai prieinamų elektroninių ryšių paslaugų teikėjams ir patikimumo užtikrinimo paslaugų teikėjams taikomas pareigas, susijusias su jų tinklų ir informacinių sistemų saugumu, taip pat sudaryti sąlygas tiems subjektams ir kompetentingoms institucijoms pagal atitinkamai Europos Parlamento ir Tarybos direktyvą (ES) 2018/1972 ([20]) ir Reglamentą (ES) Nr. 910/2014 pasinaudoti šioje direktyvoje nustatyta teisine sistema, įskaitant CSIRT, atsakingos už incidentų valdymą, paskyrimą, atitinkamų kompetentingų institucijų dalyvavimą Bendradarbiavimo grupės ir CSIRT tinklo veikloje, tie subjektai turėtų būti įtraukti į šios direktyvos taikymo sritį. Todėl atitinkamos Reglamento (ES) Nr. 910/2014 ir Direktyvos (ES) 2018/1972 nuostatos, susijusios su saugumo ir pranešimo reikalavimo nustatymu tų rūšių subjektams, turėtų būti panaikintos. Šioje direktyvoje nustatytos taisyklės dėl pranešimų teikimo pareigų neturėtų daryti poveikio Reglamentui (ES) 2016/679 ir Direktyvai 2002/58/EB;

(93) šioje direktyvoje nustatytos kibernetinio saugumo pareigos turėtų būti laikomos papildančiomis Reglamentu (ES) Nr. 910/2014 patikimumo užtikrinimo paslaugų teikėjams nustatytus reikalavimus. Turėtų būti reikalaujama, kad patikimumo užtikrinimo paslaugų teikėjai imtųsi visų tinkamų ir proporcingų jų paslaugoms kylančios rizikos valdymo priemonių, be kita ko, klientų ir pasikliaujančiųjų trečiųjų šalių atžvilgiu, ir pagal šią direktyvą praneštų apie incidentus. Tokios kibernetinio saugumo ir pranešimo pareigos turėtų būti taikomos ir teikiamų paslaugų fizinei apsaugai. Toliau taikomi Reglamento (ES) Nr. 910/2014 24 straipsnyje nustatyti reikalavimai kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams;

([19]) 2019 m. kovo 26 d. Komisijos rekomendacija (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo (OL L 88, 2019 3 29, p. 42).

([20]) 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (OL L 321, 2018 12 17, p. 36).

(94) valstybės narės atlikti patikimumo užtikrinimo paslaugų srities kompetentingų institucijų vaidmenį gali pavesti priežiūros įstaigoms pagal Reglamentą (ES) Nr. 910/2014, kad būtų užtikrintas dabartinės praktikos tęstinumas ir toliau plėtojamos taikant tą reglamentą įgytos žinios ir patirtis. Tokiu atveju kompetentingos institucijos pagal šią direktyvą turėtų glaudžiai ir laiku bendradarbiauti su tomis priežiūros įstaigomis, keisdamosi aktualia informacija, kad būtų užtikrinta veiksminga patikimumo užtikrinimo paslaugų teikėjų priežiūra ir užtikrinta, kad jie laikytųsi šioje direktyvoje bei Reglamente (ES) Nr. 910/2014 nustatytų reikalavimų. Kai taikytina, CSIRT ar kompetentinga institucija pagal šią direktyvą turėtų nedelsdama informuoti priežiūros įstaigą pagal Reglamentą (ES) Nr. 910/2014 apie visas dideles kibernetines grėsmes arba incidentus, darančius poveikį patikimumo užtikrinimo paslaugoms, apie kuriuos pranešta, taip pat apie visus atvejus, kai patikimumo užtikrinimo paslaugų teikėjas pažeidžia šią direktyvą. Pranešimų teikimo tikslais valstybės narės, kai taikytina, gali naudotis viena bendra prieiga, nustatyta siekiant užtikrinti bendrą automatinį pranešimą apie incidentus tiek priežiūros įstaigai pagal Reglamentą (ES) Nr. 910/2014, tiek CSIRT ar kompetentingai institucijai pagal šią direktyvą;

(95) kai tinkama ir siekiant išvengti nereikalingo trikdymo, perkeliant šią direktyvą į nacionalinę teisę turėtų būti atsižvelgiama į galiojančias nacionalines gaires, priimtas siekiant į nacionalinę teisę perkelti taisykles, susijusias su Direktyvos (ES) 2018/1972 40 ir 41 straipsniuose nustatytomis saugumo priemonėmis, taip plėtojant taikant Direktyvą (ES) 2018/1972 jau įgytas žinias ir patirtį, susijusias su saugumo priemonėmis ir pranešimais apie incidentus. ENISA taip pat gali parengti gaires dėl saugumo reikalavimų ir pareigų pranešti, skirtas viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjams, kad būtų sudarytos palankesnės sąlygos suderinimui bei pertvarkai ir kuo labiau sumažinti trikdžiai. Valstybės narės gali pagal Direktyvą (ES) 2018/1972 pavesti elektroninių ryšių srities kompetentingų institucijų vaidmenį atlikti nacionalinėms reguliavimo institucijoms, kad būtų užtikrintas dabartinės praktikos tęstinumas ir toliau plėtojamos įgyvendinant tą direktyvą įgytos žinios ir patirtis;

(96) atsižvelgiant į didėjančią su numeriu nesiejamo asmenų tarpusavio ryšio paslaugų, kaip apibrėžta Direktyvoje (ES) 2018/1972, svarbą, būtina užtikrinti, kad tokioms paslaugoms, atsižvelgiant į jų specifinį pobūdį ir ekonominę svarbą, taip pat būtų taikomi tinkami saugumo reikalavimai. Kadangi išpuolių perimetras vis didėja, su numeriu nesiejamo asmenų tarpusavio ryšio paslaugos, pavyzdžiui, pranešimų paslaugos, tampa plačiai paplitusiais išpuolių vektoriais. Piktavališki nusikalstamos veikos vykdytojai naudoja platformas, kad bendrautų su aukomis ir jas suviliotų atverti saugumui pavojų keliančius interneto puslapius, todėl padidėja incidentų, susijusių su asmens duomenų naudojimu ir atitinkamai – tinklų ir informacinių sistemų saugumu, tikimybė. Su numeriu nesiejamo asmenų tarpusavio ryšio paslaugų teikėjai turėtų užtikrinti tinklų ir informacinių sistemų saugumo lygį, atitinkantį keliamą riziką. Atsižvelgiant į tai, kad su numeriu nesiejamo asmenų tarpusavio ryšio paslaugų teikėjai paprastai neturi tikrų galimybių kontroliuoti tinklais siunčiamus perdavimo signalus, galima laikyti, kad tam tikrais atžvilgiais tokioms paslaugoms kyla mažesnio laipsnio rizika nei tradicinėms elektroninių ryšių paslaugoms. Tas pats pasakytina ir apie asmenų tarpusavio ryšio paslaugas, kaip apibrėžta Direktyvoje (ES) 2018/1972, kurias teikiant naudojami numeriai ir kurias teikiant faktiškai nekontroliuojamas signalų perdavimas;

(97) vidaus rinka labiau nei bet kada priklauso nuo interneto veikimo. Beveik visų esminių ir svarbių subjektų paslaugos priklauso nuo internetu teikiamų paslaugų. Siekiant užtikrinti sklandų esminių ir svarbių subjektų teikiamų paslaugų teikimą, svarbu, kad visi viešųjų elektroninių ryšių tinklų teikėjai įdiegtų tinkamas kibernetinio saugumo rizikos valdymo priemones ir praneštų apie su jomis susijusius didelius incidentus. Valstybės narės turėtų užtikrinti, kad būtų išlaikytas viešųjų elektroninių ryšių tinklų saugumas ir kad jų gyvybiškai svarbūs saugumo interesai būtų apsaugoti nuo sabotažo ir šnipinėjimo. Kadangi tarptautinis junglumas stiprina ir spartina konkurencingą Sąjungos ir jos ekonomikos skaitmeninimą, apie incidentus, darančius poveikį povandeniniams ryšių kabeliams, turėtų būti pranešama CSIRT arba, kai taikytina, kompetentingai institucijai. Nacionalinėje kibernetinio saugumo strategijoje, kai tinkama, turėtų būti atsižvelgiama į povandeninių ryšių kabelių kibernetinį saugumą ir į ją turėtų būti įtraukta galimos kibernetinio saugumo rizikos kartograma bei rizikos mažinimo priemonės, siekiant užtikrinti aukščiausią jų apsaugos lygį;

(98) siekiant užtikrinti viešųjų elektroninių ryšių tinklų ir viešai prieinamų elektroninių ryšių paslaugų saugumą, turėtų būti skatinama naudoti šifravimo technologijas, visų pirma ištisinį šifravimą, taip pat į duomenis orientuotas saugumo koncepcijas, pavyzdžiui, kartografiją, segmentavimą, žymėjimą, prieigos politiką ir prieigos valdymą bei automatinius sprendimus dėl prieigos. Kai būtina, šifravimo, visų pirma ištisinio šifravimo, naudojimas turėtų būti privalomas viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjams laikantis pritaikytojo ir standartizuotojo saugumo bei privatumo principų šios direktyvos tikslais. Ištisinio šifravimo naudojimas turėtų derėti su valstybių narių įgaliojimais užtikrinti savo esminių saugumo interesų apsaugą ir visuomenės saugumą ir leisti užkirsti kelią nusikalstamoms veikoms, jas tirti, nustatyti ir vykdyti baudžiamąjį persekiojimą už jas laikantis Sąjungos teisės. Tačiau dėl to neturėtų būti susilpnintas ištisinis šifravimas, kuris yra kritinė technologija siekiant veiksmingai apsaugoti duomenis ir privatumą bei ryšių saugumą;

(99) siekiant užtikrinti viešųjų elektroninių ryšių tinklų ir viešai prieinamų elektroninių ryšių paslaugų saugumą ir užkirsti kelią piktnaudžiavimui bei manipuliavimui jais, turėtų būti skatinama naudoti saugaus maršruto parinkimo standartus, kad būtų užtikrintas maršruto parinkimo funkcijų vientisumas ir patikimumas visoje prieigos prie interneto paslaugų tiekėjų ekosistemoje;

(100) siekiant apsaugoti interneto funkcionalumą ir vientisumą ir skatinti DNS saugumą bei atsparumą, atitinkami suinteresuotieji subjektai, įskaitant Sąjungos privačiojo sektoriaus subjektus, viešai prieinamų elektroninių ryšių paslaugų teikėjus, visų pirma prieigos prie interneto paslaugų teikėjus, ir interneto paieškos sistemų teikėjus, turėtų būti skatinami priimti DNS keitimo įvairinimo strategiją. Be to, valstybės narės turėtų skatinti kurti ir naudoti viešą ir saugų Europos DNS keitiklį;

(101) šia direktyva nustatomas kelių etapų pranešimų apie didelius incidentus teikimo metodas, siekiant užtikrinti tinkamą pusiausvyrą tarp, viena vertus, greito pranešimų teikimo, kuris padeda sumažinti galimą didelių incidentų plitimą ir suteikia galimybę esminiams ir svarbiems subjektams prašyti pagalbos, ir, kita vertus, išsamių pranešimų, kuriuose atsižvelgiama į vertingą su atskirais incidentais susijusią patirtį ir ilgainiui didinamas atskirų subjektų ir visų sektorių kibernetinis atsparumas. Tuo atžvilgiu šioje direktyvoje turėtų būti numatytas pranešimas apie incidentus, kurie, remiantis atitinkamo subjekto atliktu pradiniu vertinimu, galėtų sukelti didelį paslaugų teikimo sutrikdymą arba finansinių nuostolių tam subjektui arba paveiktų kitus fizinius ar juridinius asmenis sukeliant jiems didelės turtinės arba neturtinės žalos. Atliekant tokį pradinį vertinimą turėtų būti atsižvelgiama, *inter alia*, į paveiktas tinklų ir informacines sistemas, ypač į jų svarbą subjekto paslaugų teikimui, kibernetinės grėsmės rimtumą ir technines charakteristikas bei visus pagrindinius pažeidžiamumus, kuriais naudojamasi, taip pat į subjekto patirtį įvykus panašiems incidentams. Tokie rodikliai, kaip poveikio paslaugos veikimui mastas, incidento trukmė arba paveiktų paslaugų gavėjų skaičius, galėtų būti svarbūs nustatant, ar paslaugos teikimo sutrikdymas yra didelis;

(102) jei esminiai ar svarbūs subjektai sužino apie didelį incidentą, reikalaujama, kad jie nepagrįstai nedelsdami ir bet kuriuo atveju per 24 valandas pateiktų ankstyvąjį perspėjimą. Po to ankstyvojo perspėjimo turėtų būti pateikiamas pranešimas apie incidentą. Atitinkami subjektai turėtų nepagrįstai nedelsdami ir bet kuriuo atveju per 72 valandas nuo tada, kai sužinojo apie didelį incidentą, pateikti pranešimą apie incidentą, visų pirma siekdami atnaujinti ankstyvuoju perspėjimu pateiktą informaciją ir pateikti didelio incidento, įskaitant jo rimtumą ir poveikį, pradinį vertinimą, taip pat užvaldymo rodiklius, jei tokių yra. Galutinis pranešimas turėtų būti pateiktas ne vėliau kaip per vieną mėnesį nuo pranešimo apie incidentą. Ankstyvajame perspėjime turėtų būti pateikta tik ta informacija, kurios reikia, kad CSIRT arba, kai taikytina, kompetentinga institucija, būtų informuota apie didelį incidentą, o atitinkamas subjektas prireikus galėtų kreiptis pagalbos. Tokiame ankstyvajame perspėjime, jei taikytina, turėtų būti nurodyta, ar įtariama, kad didelį incidentą sukėlė neteisėti arba piktavališki veiksmai, ir ar tikėtina, kad jis turės tarpvalstybinį poveikį. Valstybės narės turėtų užtikrinti, kad dėl pareigos pateikti tą ankstyvąjį perspėjimą arba vėlesnį pranešimą apie incidentą pranešančio subjekto ištekliai nebūtų nukreipti nuo veiklos, susijusios su incidentų valdymu, kuriai turėtų būti teikiama pirmenybė, siekiant užkirsti kelią tam, kad dėl pranešimų apie incidentus teikimo pareigų nebūtų nukreipiami ištekliai nuo reagavimo į didelius incidentus valdymo arba kitaip nebūtų pakenkta subjekto

pastangoms šioje srityje. Tuo atveju, jei galutinio pranešimo pateikimo metu incidentas tebevyksta, valstybės narės turėtų užtikrinti, kad atitinkami subjektai tuo metu pateiktų pažangos ataskaitą, o galutinę ataskaitą – per vieną mėnesį nuo tada, kai suvaldė didelį incidentą;

(103) kai taikytina, esminiai ir svarbūs subjektai turėtų nedelsdami pranešti savo paslaugų gavėjams apie visas priemones ar taisomąsias priemones, kurių jie gali imtis, kad sumažintų dėl didelės kibernetinės grėsmės kylančią riziką. Kai tinkama ir ypač tais atvejais, kai tikėtina, kad didelė kibernetinė grėsmė pasireikš, tie subjektai taip pat turėtų informuoti savo paslaugų gavėjus apie pačią grėsmę. Reikalavimo informuoti tuos gavėjus apie dideles kibernetines grėsmes turėtų būti laikomasi dedant visas įmanomas pastangas, tačiau jis neturėtų atleisti tų subjektų nuo pareigos savo sąskaita imtis tinkamų ir neatidėliotinų priemonių, kad būtų užkirstas kelias tokioms grėsmėms arba jos būtų pašalintos ir atkurtas įprastas paslaugos saugumo lygis. Tokia informacija apie dideles kibernetines grėsmes paslaugų gavėjams turėtų būti teikiama nemokamai ir parengta lengvai suprantama kalba;

(104) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai turėtų įgyvendinti pritaikytojo ir standartizuotojo saugumo priemones ir informuoti savo paslaugų gavėjus apie dideles kibernetines grėsmes ir priemones, kurių jie gali imtis savo prietaisų ir ryšių saugumui užtikrinti, pavyzdžiui, naudodami konkrečių rūšių programinę įrangą arba šifravimo technologijas;

(105) iniciatyvus požiūris į kibernetines grėsmes yra nepaprastai svarbus kibernetinio saugumo rizikos valdymo priemonių elementas, kuris turėtų sudaryti sąlygas kompetentingoms institucijoms veiksmingai užkirsti kelią kibernetinių grėsmių tapimui incidentais, dėl kurių gali būti patiriama didelė turtinė ar neturtinė žala. Tuo tikslu labai svarbu, kad apie kibernetines grėsmes būtų pranešama. Todėl subjektai raginami savanoriškai pranešti apie kibernetines grėsmes;

(106) siekiant supaprastinti pagal šią direktyvą reikalaujamą informacijos pranešimą ir sumažinti subjektams tenkančią administracinę naštą, valstybės narės turėtų numatyti technines priemones, pavyzdžiui, vieną bendrą prieigą, automatizuotas sistemas, internetines formas, patogias naudoti sąsajas, šablonus, specialias platformas, skirtas subjektams naudoti, nepriklausomai nuo to, ar jie patenka į šios direktyvos taikymo sritį, kad būtų galima teikti atitinkamą su pranešimų teikimu susijusią informaciją. Sąjungos finansavimas, kuriuo remiamas šios direktyvos įgyvendinimas, visų pirma pagal Skaitmeninės Europos programą, nustatytą Europos Parlamento ir Tarybos reglamentu (ES) 2021/694 ([21]), galėtų apimti paramą vienai bendrai prieigai. Be to, subjektai dažnai atsiduria tokioje padėtyje, kai apie konkretų incidentą dėl jo ypatumų, atsižvelgiant į įvairiuose teisės aktuose nustatytas pareigas pranešti, reikia pranešti įvairioms institucijoms. Tokiais atvejais sukuriama papildoma administracinė našta ir gali kilti neaiškumų dėl tokių pranešimų formos ir procedūrų. Tais atvejais, kai įsteigiama viena bendra prieiga, valstybės narės taip pat raginamos tą vieną bendrą prieigą naudoti pranešimams apie saugumo incidentus, kurių reikalaujama pagal kitus Sąjungos teisės aktus, pavyzdžiui, Reglamentą (ES) 2016/679 ir Direktyvą 2002/58/EB, teikti. Tokios vienos bendros prieigos 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. ENISA, bendradarbiaudama su Bendradarbiavimo grupe, turėtų parengti bendrus pranešimo šablonus, pateikdama gaires, kuriomis supaprastinama ir racionalizuojama pagal Sąjungos teisę reikalaujama pranešimų teikimo informacija ir sumažinama pranešantiems subjektams tenkanti administracinė našta;

(107) kai įtariama, kad incidentas yra susijęs su sunkia nusikalstama veika pagal Sąjungos arba nacionalinę teisę, valstybės narės turėtų skatinti esminius ir svarbius subjektus, remiantis pagal Sąjungos teisę taikytinomis baudžiamojo proceso taisyklėmis, pranešti atitinkamoms teisėsaugos institucijoms apie įtariamus sunkius nusikalstamo pobūdžio incidentus. Atitinkamais atvejais, nedarant poveikio Europolui taikomų asmens duomenų apsaugos taisyklėms, pageidautina, kad skirtingų valstybių narių kompetentingų institucijų ir teisėsaugos institucijų veiklos koordinavimą palengvintų Europos kovos su elektroniniu nusikalstamumu centras (EC3) ir ENISA;

([21]) 2021 m. balandžio 29 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/694, kuriuo nustatoma Skaitmeninės Europos programa ir panaikinamas Sprendimas (ES) 2015/2240 (OL L 166, 2021 5 11, p. 1).

(108) daugeliu atvejų dėl incidentų kyla pavojus asmens duomenų saugumui. Tokiomis aplinkybėmis kompetentingos institucijos turėtų bendradarbiauti ir keistis informacija visais svarbiais klausimais su institucijomis, nurodytomis Reglamente (ES) 2016/679 ir Direktyvoje 2002/58/EB;

(109) siekiant užtikrinti DNS saugumą, stabilumą ir atsparumą, būtina turėti tikslias ir išsamias domenų vardų registracijos duomenų (WHOIS duomenų) bazes ir suteikti teisėtą prieigą prie tokių duomenų, o tai savo ruožtu prisideda prie aukšto bendro kibernetinio saugumo lygio visoje Sąjungoje. Tuo konkrečiu tikslu turėtų būti reikalaujama, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai tvarkytų tam tikrus duomenis, būtinus tam tikslui pasiekti. Toks tvarkymas turėtų būti laikomas teisine prievole, kaip tai suprantama Reglamento (ES) 2016/679 6 straipsnio 1 dalies c punkte. Ta prievole nedaromas poveikis galimybei domenų vardų registracijos duomenis rinkti kitais tikslais, pavyzdžiui, remiantis sutartimi arba teisiniais reikalavimais, nustatytais kitoje Sąjungos ar nacionalinėje teisėje. Tos prievolės tikslas – užtikrinti išsamų tikslių registracijos duomenų rinkinį ir dėl jos tie patys duomenys neturėtų būti renkami kelis kartus. Aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų bendradarbiauti tarpusavyje, kad būtų išvengta tos užduoties dubliavimosi;

(110) siekiant užkirsti kelią piktnaudžiavimui DNS ir kovoti su juo, taip pat užkirsti kelią incidentams ir juos atskleisti bei į juos reaguoti, labai svarbu teisėtiems prieigos prašantiems subjektams užtikrinti domenų vardų registracijos duomenų prieinamumą ir galimybę laiku su jais susipažinti. Teisėti prieigos prašantys subjektai turi būti suprantami kaip bet kuris fizinis ar juridinis asmuo, teikiantis prašymą pagal Sąjungos arba nacionalinę teisę. Jie gali apimti institucijas, kurios yra kompetentingos pagal šią direktyvą ir kurios yra kompetentingos pagal Sąjungos ar nacionalinę teisę nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas srityje, taip pat CERT arba CSIRT. Pagal Sąjungos ir nacionalinę teisę turėtų būti reikalaujama, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai suteiktų teisėtiems prieigos prašantiems subjektams teisėtą prieigą prie konkrečių domenų vardų registracijos duomenų, kurie yra būtini prieigos prašymo tikslais. Prie teisėtų prieigos prašančių subjektų prašymo turėtų būti pridėtas motyvų pareiškimas, kuriuo remiantis būtų galima įvertinti prieigos prie duomenų būtinumą;

(111) siekiant užtikrinti tikslių ir išsamių domenų vardų registracijos duomenų prieinamumą, aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų rinkti domenų vardų registracijos duomenis ir užtikrinti jų vientisumą ir prieinamumą. Visų pirma, aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų nustatyti politiką ir procedūras, skirtas tiksliems ir išsamiems domenų vardų registracijos duomenims rinkti ir saugoti, taip pat užkirsti kelią netiksliems registracijos duomenims ir juos ištaisyti laikantis Sąjungos duomenų apsaugos teisės. Toje politikoje ir procedūrose turėtų būti kuo labiau atsižvelgiama į standartus, kuriuos tarptautiniu lygmeniu parengė įvairių suinteresuotųjų subjektų valdymo struktūros. Aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų patvirtinti ir įgyvendinti proporcingas procedūras, kurios skirtos patikrinti domenų vardų registracijos duomenis. Tos procedūros turėtų atspindėti geriausią sektoriuje taikomą praktiką ir, kiek įmanoma, elektroninės atpažinties srityje padarytą pažangą. Tikrinimo procedūros, be kita ko, gali būti *ex ante* kontrolė, atliekama registracijos metu, ir *ex post* kontrolė, atliekama po registracijos. Aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų visų pirma patikrinti bent vieną iš susisiekimo su registruotoju būdų;

(112) turėtų būtų reikalaujama, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai viešai skelbtų domenų vardų registracijos duomenis, kuriems netaikoma Sąjungos duomenų apsaugos teisė, pavyzdžiui, duomenis, susijusius su juridiniais asmenimis, atsižvelgiant į Reglamento (ES) 2016/679 preambulę. Juridinių asmenų atveju aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų viešai skelbti bent registruotojo pavadinimą bei kontaktinį telefono numerį. Kontaktinis el. pašto adresas taip pat turėtų būti skelbiamas su sąlyga, kad jame nėra jokių asmens duomenų, kaip, pavyzdžiui, el. pašto slapyvardžių ar funkcinių paskyrų atveju. Pagal Sąjungos duomenų apsaugos teisę aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, taip pat turėtų suteikti teisėtiems prieigos prašantiems subjektams teisėtą prieigą prie konkrečių domenų vardų registracijos duomenų, susijusių su fiziniais asmenimis. Valstybės narės turėtų reikalauti, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai nepagrįstai nedelsdami atsakytų į teisėtų prieigos prašančių subjektų prašymus atskleisti domenų vardų registracijos duomenis. Aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, turėtų nustatyti registracijos duomenų skelbimo ir atskleidimo politiką ir procedūras, įskaitant susitarimus dėl paslaugų lygio, skirtus nagrinėti teisėtų prieigos prašančių subjektų prašymus suteikti prieigą. Toje politikoje ir procedūrose turėtų būti kuo labiau

atsižvelgiama į bet kokias gaires ir standartus, kuriuos tarptautiniu lygmeniu parengė įvairių suinteresuotųjų subjektų valdymo struktūros. Prieigos procedūra galėtų apimti sąsajos, portalo ar kitos techninės priemonės naudojimą, kad būtų sukurta veiksminga registracijos duomenų prašymų ir prieigos prie jų sistema. Siekdama skatinti suderintą praktiką visoje vidaus rinkoje, Komisija gali, nedarant poveikio Europos duomenų apsaugos valdybos kompetencijai, pateikti tokių procedūrų gaires, kuriose kuo labiau atsižvelgiama į įvairių suinteresuotųjų subjektų valdymo struktūrų tarptautiniu lygmeniu parengtus standartus. Valstybės narės turėtų užtikrinti, kad visų rūšių prieiga prie asmens ir ne asmens domenų vardų registracijos duomenų būtų nemokama;

(113) subjektai, kuriems taikoma ši direktyva, turėtų būti laikomi priklausančiais valstybės narės, kurioje jie įsisteigę, jurisdikcijai. Tačiau viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai turėtų būti laikomi priklausančiais valstybės narės, kurioje jie teikia savo paslaugas, jurisdikcijai. DNS paslaugų teikėjai, aukščiausio lygio domenų vardų registrai, domenų vardų registravimo paslaugas teikiantys subjektai, debesijos kompiuterijos paslaugų teikėjai, duomenų centrų paslaugų teikėjai, turinio teikimo tinklo paslaugų teikėjai, valdomų paslaugų teikėjai, valdomų saugumo paslaugų teikėjai, taip pat internetinių prekyviečių, interneto paieškos sistemų bei socialinio tinklo paslaugų platformų paslaugų teikėjai turėtų būti laikomi priklausančiais valstybės narės, kurioje yra jų pagrindinė buveinė Sąjungoje, jurisdikcijai. Viešojo administravimo subjektai turėtų priklausyti valstybės narės, kuri juos įsteigė, jurisdikcijai. Jeigu subjektas teikia paslaugas arba yra įsisteigęs daugiau nei vienoje valstybėje narėje, jis turėtų priklausyti atskirai ir konkuruojančiai kiekvienos iš tų valstybių narių jurisdikcijai. Tų valstybių narių kompetentingos institucijos turėtų bendradarbiauti, teikti viena kitai savitarpio pagalbą ir prireikus vykdyti bendrus priežiūros veiksmus. Tuo atveju, kai valstybės narės naudojasi jurisdikcija, jos neturėtų taikyti vykdymo užtikrinimo priemonių ar sankcijų daugiau kaip vieną kartą už tą patį elgesį, laikydamosi ne *bis in idem* principo;

(114) siekiant atsižvelgti į DNS paslaugų teikėjų, aukščiausio lygio domenų vardų registrų, domenų vardų registravimo paslaugas teikiančių subjektų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo paslaugų teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, taip pat internetinių prekyviečių, interneto paieškos sistemų bei socialinio tinklo paslaugų platformų paslaugų teikėjų tarpvalstybinį paslaugų ir veiklos pobūdį, jurisdikciją tų subjektų atžvilgiu turėtų turėti tik viena valstybė narė. Jurisdikcija turėtų būti priskirta valstybei narei, kurioje yra atitinkamo subjekto pagrindinė buveinė Sąjungoje. Šioje direktyvoje įsisteigimo kriterijus reiškia veiksmingą veiklos vykdymą per nuolatines struktūras. Tuo atžvilgiu teisinė tokių struktūrų forma, nepaisant to, ar tai filialas ar patronuojamoji įmonė, turinti juridinio asmens statusą, nėra lemiamas veiksnys. Tai, ar šio kriterijaus laikomasi, neturėtų priklausyti nuo to, ar tinklų ir informacinės sistemos fiziškai yra tam tikroje vietoje; tokių sistemų buvimas ir naudojimas pats savaime nereiškia tokios pagrindinės buveinės, todėl tai nėra lemiami kriterijai, kuriais remiantis nustatoma pagrindinė buveinė. Turėtų būti laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje Sąjungoje daugiausia priimami su kibernetinio saugumo rizikos valdymo priemonėmis susiję sprendimai. Paprastai ji sutampa su subjektų centrinės administracijos vieta Sąjungoje. Jei tokios valstybės narės neįmanoma nustatyti arba jei tokie sprendimai nepriimami Sąjungoje, turėtų būti laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje vykdomos kibernetinio saugumo operacijos. Jei tokios valstybės narės neįmanoma nustatyti, turėtų būti laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje subjektas turi padalinį, kuriame dirba daugiausia darbuotojų Sąjungoje. Jeigu paslaugas teikia įmonių grupė, pagrindinė kontroliuojančiosios įmonės buveinė turėtų būti laikoma pagrindine įmonių grupės buveine;

(115) kai viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjas teikia viešai prieinamą rekursinę DNS paslaugą tik kaip interneto prieigos paslaugos dalį, subjektas turėtų būti laikomas priklausančiu visų valstybių narių, kuriose teikiamos jo paslaugos, jurisdikcijai;

(116) kai paslaugas Sąjungoje siūlo DNS paslaugų teikėjas, aukščiausio lygio domenų vardų registras, domenų vardų registravimo paslaugas teikiantis subjektas, debesijos kompiuterijos paslaugų teikėjas, duomenų centrų paslaugų teikėjas, turinio teikimo tinklo paslaugų teikėjas, valdomų paslaugų teikėjas, valdomų saugumo paslaugų teikėjas arba internetinės prekyvietės, interneto paieškos sistemos ar socialinio tinklo paslaugų platformos paslaugų teikėjas, kuris nėra įsisteigęs Sąjungoje, jis turėtų paskirti atstovą Sąjungoje. Siekiant nustatyti, ar toks subjektas siūlo paslaugas Sąjungoje, reikėtų įvertinti, ar subjektas ketina siūlyti paslaugas asmenims vienoje ar daugiau valstybių narių. Turėtų būti laikoma, kad vien to, jog Sąjungoje prieinama subjekto ar tarpininko interneto svetainė arba el. pašto adresas ar kiti kontaktiniai duomenys arba kad vartojama kalba, kuri paprastai vartojama trečiojoje valstybėje, kurioje yra įsisteigęs subjektas, nepakanka siekiant įrodyti, kad esama tokio ketinimo. Tačiau dėl tokių veiksnių kaip kalba ar valiuta, paprastai vartojamų (naudojamų) vienoje ar daugiau valstybių narių, įskaitant galimybę užsakyti paslaugas ta kalba, arba nurodant Sąjungoje esančius vartotojus ar naudotojus, gali būti akivaizdu, kad subjektas ketina siūlyti paslaugas Sąjungoje. Atstovas turėtų veikti subjekto vardu, o kompetentingos institucijos arba CSIRT turėtų turėti galimybę kreiptis į atstovą. Atstovas turėtų būti aiškiai paskirtas rašytiniu subjekto įgaliojimu veikti pastarojo vardu vykdant šioje direktyvoje nustatytas jo pareigas, įskaitant pranešimą apie incidentus;

(117) siekiant užtikrinti aiškų DNS paslaugų teikėjų, aukščiausio lygio domenų vardų registrų, domenų vardų registravimo paslaugas teikiančių subjektų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo paslaugų teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, taip pat internetinių prekyviečių, interneto paieškos sistemų bei socialinio tinklo paslaugų platformų paslaugų teikėjų, kurie teikia paslaugas visoje Sąjungoje, patenkančias į šios direktyvos taikymo sritį, vaizdą, ENISA turėtų sukurti ir tvarkyti tokių subjektų registrą, remiantis iš valstybių narių gauta informacija, kai taikytina, naudojant nacionalinius mechanizmus, sukurtus subjektų saviregistracijai. Bendrieji kontaktiniai punktai turėtų perduoti ENISA informaciją ir visus jos pakeitimus. Kad būtų užtikrintas į tą registrą įtrauktinos informacijos tikslumas ir išsamumas, valstybės narės gali pateikti ENISA bet kokiuose nacionaliniuose registruose turimą informaciją apie tuos subjektus. ENISA ir valstybės narės turėtų imtis priemonių tokių registrų sąveikumui palengvinti, kartu užtikrindamos konfidencialios ar įslaptintos informacijos apsaugą. ENISA turėtų nustatyti tinkamus informacijos klasifikavimo ir valdymo protokolus, kad užtikrintų atskleistos informacijos saugumą ir konfidencialumą ir apribotų prieigą prie tokios informacijos, jos saugojimą ir perdavimą numatytiems naudotojams;

(118) jeigu pagal šią direktyvą keičiamasi informacija, kuri yra įslaptinta pagal Sąjungos arba nacionalinę teisę, apie ją pranešama arba ja kitaip dalijamasi, turėtų būti taikomos atitinkamos įslaptintos informacijos tvarkymo taisyklės. Be to, ENISA turėtų turėti infrastruktūrą, procedūras ir taisykles, kuriomis būtų tvarkoma neskelbtina ir įslaptinta informacija, laikantis ES įslaptintai informacijai apsaugoti taikomų saugumo taisyklių;

(119) kadangi kibernetinės grėsmės tampa vis sudėtingesnės ir painesnės, geros tokių grėsmių atskleidimo ir prevencijos priemonės labai priklauso nuo to, ar subjektai reguliariai keičiasi žvalgybos informacija apie grėsmes ir pažeidžiamumą. Dalijantis informacija padedama didinti informuotumą apie kibernetines grėsmes, o tai savo ruožtu didina subjektų gebėjimą užkirsti kelią tokioms grėsmėms virsti incidentais ir sudaro sąlygas subjektams geriau suvaldyti incidentų poveikį ir veiksmingiau atstatyti veiklą. Nesant gairių Sąjungos lygmeniu, atrodo, kad keli veiksniai trukdo dalytis tokia žvalgybos informacija, visų pirma netikrumas dėl suderinamumo su konkurencijos ir atsakomybės taisyklėmis;

(120) valstybės narės turėtų skatinti subjektus ir jiems padėti bendrai naudotis savo asmeninėmis žiniomis ir praktine praktika strateginiu, taktiniu ir operatyviniu lygmenimis, kad sustiprintų savo gebėjimus tinkamai užkirsti kelią incidentams, juos atskleisti, į juos reaguoti ar atstatyti po jų veiklą arba sumažinti jų poveikį. Todėl būtina sudaryti sąlygas Sąjungos lygmeniu, kad atsirastų savanoriško dalijimosi kibernetinio saugumo informacija susitarimai. Tuo tikslu valstybės narės turėtų aktyviai padėti subjektams, kaip antai tiems, kurie daugiausia dėmesio skiria kibernetinio saugumo paslaugoms ir moksliniams tyrimams, taip pat atitinkamiems subjektams, kuriems ši direktyva netaikoma, ir juos skatinti dalyvauti keičiantis kibernetinio saugumo informacija pagal tokius susitarimus. Tie susitarimai turėtų būti parengti pagal Sąjungos konkurencijos taisykles ir Sąjungos duomenų apsaugos teisės aktus;

(121) esminių ir svarbių subjektų vykdomas asmens duomenų tvarkymas tiek, kiek tai būtina ir proporcinga siekiant užtikrinti tinklų ir informacinių sistemų saugumą, galėtų būti laikomas teisėtu remiantis tuo, kad toks tvarkymas atitinka duomenų valdytojui taikomą teisinę prievolę pagal Reglamento (ES) 2016/679 6 straipsnio 1 dalies c punkto ir 6 straipsnio 3 dalies reikalavimus. Taip pat tvarkyti asmens duomenis gali reikėti siekiant teisėtų interesų, kurių siekia esminiai ir svarbūs subjektai, taip pat tų subjektų vardu veikiantys saugumo technologijų bei paslaugų tiekėjai ir teikėjai, laikantis Reglamento (ES) 2016/679 6 straipsnio 1 dalies f punkto, be kita ko, kai toks tvarkymas yra būtinas pagal dalijimosi kibernetinio saugumo informacija susitarimus arba savanoriškai pranešant atitinkamą informaciją pagal šią direktyvą. Taikant priemones, susijusias su incidentų prevencija, atskleidimu, nustatymu, apribojimu, analize ir reagavimu į juos, informuotumo apie konkrečias kibernetines grėsmes didinimo priemones, keitimąsi informacija ištaisant pažeidžiamumus ir koordinuotai juos atskleidžiant, taip pat savanorišką keitimąsi informacija apie tuos incidentus, kibernetines grėsmes ir pažeidžiamumus, užvaldymo rodiklius, taktiką, metodus ir procedūras, kibernetinio saugumo įspėjimus ir konfigūracijos priemones gali reikėti tvarkyti tam tikrų kategorijų asmens duomenis, pavyzdžiui, IP adresus, universaliuosius išteklių adresus (URL), domenų vardus, el. pašto adresus ir, kai jose atskleidžiami asmens duomenys, laiko žymas. Kompetentingų institucijų, bendrųjų kontaktinių punktų ir CSIRT vykdomas asmens duomenų tvarkymas galėtų būti teisinė prievolė arba būti laikomas būtinu siekiant atlikti užduotį viešojo intereso labui arba vykdant duomenų valdytojui pagal Reglamento (ES) 2016/679 6 straipsnio 1 dalies c arba e punktą ir 6 straipsnio 3 dalį pavestas viešosios valdžios funkcijas, arba siekiant teisėtų esminių ir svarbių subjektų interesų, kaip nurodyta to Reglamento 6 straipsnio 1 dalies f punkte. Be to, nacionalinėje teisėje galėtų būti nustatytos taisyklės, pagal kurias kompetentingoms institucijoms, bendriesiems kontaktiniams punktams ir CSIRT būtų leidžiama tiek, kiek tai būtina ir proporcinga siekiant užtikrinti esminių ir svarbių subjektų tinklų ir informacinių sistemų saugumą, tvarkyti specialių kategorijų asmens duomenis pagal Reglamento (ES) 2016/679 9 straipsnį, visų pirma numatant tinkamas ir konkrečias fizinių asmenų pagrindinių teisių ir interesų apsaugos priemones, įskaitant tokių duomenų pakartotinio naudojimo techninius apribojimus ir pažangiausių saugumo bei privatumo apsaugos priemonių, pavyzdžiui, pseudonimų suteikimo arba šifravimo, kai nuasmeninimas gali daryti didelį poveikį siekiamam tikslui, naudojimą;

(122) siekiant sustiprinti priežiūros įgaliojimus ir priemones, padedančius užtikrinti veiksmingą reikalavimų laikymąsi, šioje direktyvoje turėtų būti nustatytas būtiniausias priežiūros priemonių ir būdų, kuriais kompetentingos institucijos galėtų atlikti esminių ir svarbių subjektų priežiūrą, sąrašas. Be to, šioje direktyvoje turėtų būti nustatyta skirtinga esminių ir svarbių subjektų priežiūros tvarka, siekiant užtikrinti teisingą tiek subjektų, tiek kompetentingų institucijų pareigų pusiausvyrą. Todėl esminiams subjektams turėtų būti taikoma išsami *ex ante* ir *ex post* priežiūros tvarka, o svarbiems subjektams turėtų būti taikoma negriežta, tik *ex post*, priežiūros tvarka. Todėl iš svarbių subjektų neturėtų būti reikalaujama sistemingai dokumentuoti atitikties kibernetinio saugumo rizikos valdymo priemonėms, o kompetentingos institucijos turėtų įgyvendinti reaktyvųjį *ex post* požiūrį į priežiūrą, todėl neturėtų turėti bendros pareigos prižiūrėti tuos subjektus. Svarbių subjektų *ex post* priežiūra gali būti pradėta remiantis kompetentingoms institucijoms pateiktais įrodymais, duomenimis ar informacija, kurie, tų institucijų manymu, rodo galimus šios direktyvos pažeidimus. Pavyzdžiui, tai galėtų būti tokios pačios rūšies įrodymai, duomenys ar informacija, kuriuos kompetentingoms institucijoms pateikia kitos institucijos, subjektai, piliečiai, žiniasklaida ar kiti šaltiniai, viešai prieinama informacija arba informacija, kurią kompetentingos institucijos galėtų gauti vykdydamos kitą jų užduotims atlikti reikalingą veiklą;

(123) kompetentingoms institucijoms vykdant priežiūros užduotis neturėtų būti be reikalo trukdoma atitinkamo subjekto verslo veiklai. Kai kompetentingos institucijos vykdo savo su esminiais subjektais susijusias priežiūros užduotis, įskaitant patikrinimus vietoje ir priežiūrą ne vietoje, šios direktyvos pažeidimų tyrimą, saugumo auditus ar saugumo patikrinimus, jos turėtų kuo labiau sumažinti poveikį atitinkamo subjekto verslo veiklai;

(124) vykdydamos *ex ante* priežiūrą, kompetentingos institucijos turėtų galėti nuspręsti nustatyti prioritetus dėl proporcingo jų turimų priežiūros priemonių ir būdų naudojimo. Tai reiškia, kad kompetentingos institucijos gali nuspręsti dėl tokių prioritetų nustatymo remdamosi priežiūros metodikomis, pagal kurias turėtų būti laikomasi rizika grindžiamo požiūrio. Konkrečiau, tokios metodikos galėtų apimti esminių subjektų klasifikavimo pagal rizikos kategorijas kriterijus ar lyginamuosius standartus ir atitinkamas priežiūros priemones bei būdus, rekomenduojamus kiekvienai rizikos kategorijai, pavyzdžiui, patikrinimų vietoje, tikslinių saugumo auditų ar saugumo patikrinimų naudojimą, dažnumą ar rūšį, prašomos pateikti informacijos rūšį ir tos informacijos išsamumo lygį. Kartu su tokiomis priežiūros metodikomis taip pat galėtų būti parengiamos darbo programos ir jos

galėtų būti reguliariai vertinamos bei peržiūrimos, be kita ko, atsižvelgiant į tokius aspektus kaip išteklių paskirstymas ir poreikiai. Viešojo administravimo subjektų atžvilgiu priežiūros įgaliojimais turėtų būti naudojamasi laikantis nacionalinių teisėkūros ir institucinių sistemų;

(125) kompetentingos institucijos turėtų užtikrinti, kad su esminiais ir svarbiais subjektais susijusias jų priežiūros užduotis vykdytų kvalifikuoti specialistai, kurie turėtų turėti toms užduotims atlikti reikiamų įgūdžių, visų pirma susijusių su patikrinimų vietoje ir priežiūros ne vietoje vykdymu, įskaitant duomenų bazių, aparatinės įrangos, užkardų, šifravimo ir tinklų trūkumų nustatymą. Tie patikrinimai ir priežiūra turėtų būti vykdomi objektyviai;

(126) tinkamai pagrįstais atvejais, kai kompetentinga institucija žino apie didelę kibernetinę grėsmę arba iškilusią riziką, ji turėtų turėti galimybę nedelsiant priimti vykdymo užtikrinimo sprendimus, kad užkirstų kelią incidentui arba į jį reaguotų;

(127) kad vykdymo užtikrinimas būtų veiksmingas, turėtų būti nustatytas būtinas vykdymo užtikrinimo galių, kurias galima įgyvendinti už šioje direktyvoje nustatytų kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti pažeidimą, sąrašas, kuriuo būtų sukurta aiški ir nuosekli tokio vykdymo užtikrinimo visoje Sąjungoje sistema. Turėtų būti deramai atsižvelgta į šios direktyvos pažeidimo pobūdį, rimtumą ir trukmę, padarytą turtinę ar neturtinę žalą, į tai, ar pažeidimas buvo padarytas tyčia ar dėl neatsargumo, veiksmus, kurių imtasi siekiant užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti, atsakomybės laipsnį ar bet kokius atitinkamus ankstesnius pažeidimus, bendradarbiavimo su kompetentinga institucija laipsnį ir visas kitas atsakomybę sunkinančias arba švelninančias aplinkybes. Vykdymo užtikrinimo priemonės, įskaitant administracines baudas, turėtų būti proporcingos ir jas skiriant turėtų būti taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės principus ir Europos Sąjungos pagrindinių teisių chartiją (toliau – Chartija), įskaitant teisę į veiksmingą teisinę gynybą bei teisingą bylos nagrinėjimą, nekaltumo prezumpciją ir teisę į gynybą;

(128) pagal šią direktyvą nereikalaujama, kad valstybės narės numatytų fizinių asmenų, atsakingų už tai, kad subjektas laikytųsi šios direktyvos, baudžiamąją ar civilinę atsakomybę dėl žalos, kurią trečiosios šalys patyrė dėl šios direktyvos pažeidimo;

(129) siekiant užtikrinti veiksmingą šioje direktyvoje nustatytų pareigų vykdymą, kiekvienai kompetentingai institucijai turėtų būti suteikti įgaliojimai skirti administracines baudas arba prašyti jas skirti;

(130) jei administracinė bauda skiriama esminiam ar svarbiam subjektui, kuris yra įmonė, tais tikslais įmonė turėtų būti suprantama kaip įmonė, apibrėžta SESV 101 ir 102 straipsniuose. Jei administracinė bauda skiriama 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. Administracinės baudos skyrimas neturi įtakos kompetentingų institucijų kitų įgaliojimų ar kitų sankcijų, nustatytų nacionalinėse taisyklėse, kuriomis ši direktyva perkeliama į nacionalinę teisę, taikymui;

(131) valstybės narės turėtų galėti nustatyti taisykles dėl baudžiamųjų sankcijų už nacionalinių taisyklių, kuriomis ši direktyva perkeliama į nacionalinę teisę, pažeidimus. Tačiau skiriant baudžiamąsias sankcijas už tokių nacionalinių taisyklių pažeidimus ir susijusias administracines sankcijas neturėtų būti pažeistas ne *bis in idem* principas, kaip jį aiškina Europos Sąjungos Teisingumo Teismas;

(132) kai šia direktyva administracinės sankcijos nėra suderintos arba kai tai yra būtina kitais atvejais, pavyzdžiui, sunkaus šios direktyvos pažeidimo atveju, valstybės narės turėtų įgyvendinti sistemą, pagal kurią numatomos veiksmingos, proporcingos ir atgrasomos sankcijos. Tokių sankcijų pobūdis ir tai, ar jos yra baudžiamosios, ar administracinės, turėtų būti nustatyta nacionalinėje teisėje;

(133) siekiant dar labiau sustiprinti vykdymo užtikrinimo priemonių, taikomų šios direktyvos pažeidimams, veiksmingumą ir atgrasomumą, kompetentingoms institucijoms turėtų būti suteikti įgaliojimai laikinai sustabdyti arba reikalauti laikinai sustabdyti sertifikavimą ar leidimą, susijusį su dalimi ar visomis atitinkamomis esminio subjekto teikiamomis paslaugomis arba vykdoma veikla, ir reikalauti nustatyti laikiną draudimą bet kuriam generalinio direktoriaus arba teisinio atstovo lygmens vadovaujamas pareigas einančiam fiziniam asmeniui eiti vadovaujamas pareigas. Atsižvelgiant į tokių laikinų sustabdymų ar draudimų griežtumą ir poveikį subjektų veiklai ir galiausiai vartotojams, jie turėtų būti taikomi tik proporcingai atsižvelgiant į pažeidimo sunkumą ir į kiekvieno konkretaus atvejo aplinkybes, įskaitant tai, ar pažeidimas padarytas tyčia ar dėl neatsargumo, ir veiksmus, kurių galimai imtasi siekiant užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti. Tokie laikini sustabdymai ar draudimai turėtų būti taikomi tik kaip kraštutinė priemonė, t. y. tik po to, kai išnaudojamos kitos šioje direktyvoje nustatytos atitinkamos vykdymo užtikrinimo priemonės, ir tik tol, kol atitinkamas subjektas imasi reikiamų veiksmų trūkumams ištaisyti arba kompetentingos institucijos reikalavimams, dėl kurių taikomi tokie laikini sustabdymai ar draudimai, įvykdyti. Skiriant tokius laikinus sustabdymus ar draudimus, turėtų būti taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės ir Chartijos principus, įskaitant teisę į veiksmingą teisinę gynybą bei teisingą bylos nagrinėjimą, nekaltumo prezumpciją ir teisę į gynybą;

(134) siekdamos užtikrinti, kad subjektai laikytųsi savo pareigų, nustatytų šioje direktyvoje, valstybės narės turėtų bendradarbiauti ir padėti viena kitai priežiūros ir vykdymo užtikrinimo priemonių srityje, visų pirma tais atvejais, kai subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba kai jo tinklų ir informacinės sistemos yra kitoje valstybėje narėje nei ta, kurioje jis teikia paslaugas. Prašymą gavusi kompetentinga institucija, teikdama pagalbą, turėtų imtis priežiūros arba vykdymo užtikrinimo priemonių laikydamasi nacionalinės teisės. Siekdamos užtikrinti sklandų savitarpio pagalbos pagal šią direktyvą veikimą, kompetentingos institucijos turėtų naudotis Bendradarbiavimo grupe kaip forumu atvejams ir konkretiems pagalbos prašymams aptarti;

(135) siekiant užtikrinti veiksmingą priežiūrą ir vykdymo užtikrinimą, visų pirma, kai situacija yra tarpvalstybinio pobūdžio, valstybė narė, gavusi savitarpio pagalbos prašymą, turėtų, neviršydama to prašymo ribų, imtis tinkamų priežiūros ir vykdymo užtikrinimo priemonių subjekto, kuris yra to prašymo objektas ir kuris teikia paslaugas arba turi tinklų ir informacinę sistemą tos valstybės narės teritorijoje;

(136) šia direktyva turėtų būti nustatytos kompetentingų institucijų ir priežiūros institucijų pagal Reglamentą (ES) 2016/679 bendradarbiavimo taisyklės, siekiant nagrinėti šios direktyvos pažeidimus, susijusius su asmens duomenimis;

(137) šia direktyva turėtų būti siekiama užtikrinti aukšto lygio esminių ir svarbių subjektų atsakomybę už kibernetinio saugumo rizikos valdymo priemones ir pareigas pranešti. Todėl esminių ir svarbių subjektų valdymo organai turėtų patvirtinti kibernetinio saugumo rizikos valdymo priemones ir prižiūrėti jų įgyvendinimą;

(138) siekiant užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje šios direktyvos pagrindu, pagal SESV 290 straipsnį Komisijai turėtų būti deleguoti įgaliojimai priimti aktus dėl šios direktyvos papildymo, nurodant, iš kokių kategorijų esminių ir svarbių subjektų reikalaujama naudoti tam tikrus sertifikuotus IRT produktus, IRT paslaugas ir IRT procesus arba gauti sertifikatą pagal Europos kibernetinio saugumo sertifikavimo schemą. 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 ([22]) 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;

([22]) OL L 123, 2016 5 12, p. 1.

(139) siekiant užtikrinti vienodas šios direktyvos įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai nustatyti Bendradarbiavimo grupės veikimui būtiną procedūrinę tvarką ir techninius bei metodinius, taip pat sektorinius reikalavimus, susijusius su kibernetinio saugumo rizikos valdymo priemonėmis, ir išsamiau apibrėžti pranešimų apie incidentus, kibernetinę grėsmę ir vos neįvykusius incidentus bei informuojant apie didelę kibernetinę grėsmę pateikiamos informacijos rūšį, formą ir tvarką, taip pat atvejus, kuriais incidentas turi būti laikomas dideliu. Tais įgaliojimais turėtų būti naudojamasi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011 ([23]);

(140) Komisija, pasikonsultavusi su suinteresuotaisiais subjektais, turėtų periodiškai peržiūrėti šią direktyvą, visų pirma siekdama nustatyti, ar tikslinga siūlyti pakeitimus atsižvelgiant į kintančias visuomenines, politines, technologines ar rinkos sąlygas. Atlikdama tas peržiūras, Komisija turėtų įvertinti susijusių subjektų dydžio ir šios direktyvos prieduose nurodytų sektorių, subsektorių ir subjektų rūšių svarbą ekonomikos ir visuomenės veikimui kibernetinio saugumo atžvilgiu. Komisija turėtų, *inter alia*, įvertinti, ar paslaugų teikėjai, kuriems taikoma ši direktyva, pripažinti kaip labai didelės interneto platformos, kaip tai suprantama Europos Parlamento ir Tarybos reglamento (ES) 2022/2065 ([24]) 33 straipsnyje, gali būti identifikuoti kaip esminiai subjektai pagal šią direktyvą;

(141) šia direktyva sukuriamos naujos ENISA užduotys, taip sustiprinant jos vaidmenį, ir dėl to ENISA gali būti keliami reikalavimai vykdyti savo esamas užduotis pagal Reglamentą (ES) 2019/881 aukštesniu lygiu nei anksčiau. Siekiant užtikrinti, kad ENISA turėtų finansinių ir žmogiškųjų išteklių, kurių reikia, kad ji vykdytų esamas ir naujas užduotis, taip pat atitiktų bet kokį aukštesnį tų užduočių vykdymo lygį, susijusį su jos sustiprintu vaidmeniu, jos biudžetas turėtų būti atitinkamai padidintas. Be to, siekiant užtikrinti veiksmingą išteklių panaudojimą, ENISA turėtų būti suteikta daugiau lankstumo, sudarant jai sąlygas skirstyti išteklius viduje siekiant, kad ji veiksmingai vykdytų savo užduotis ir patenkintų lūkesčius;

(142) kadangi šios direktyvos tikslo, t. y. užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje, valstybės narės negali deramai pasiekti, o dėl siūlomo 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 šia direktyva neviršijama to, kas būtina nurodytam tikslui pasiekti;

(143) šia direktyva paisoma pagrindinių teisių ir laikomasi principų, pripažįstamų Chartijoje, visų pirma teisės į tai, kad būtų gerbiamas privatus gyvenimas bei komunikacijos slaptumas, teisės į asmens duomenų apsaugą, laisvės užsiimti verslu, teisės į nuosavybę, teisės į veiksmingą teisinę gynybą ir teisingą bylos nagrinėjimą, nekaltumo prezumpcijos ir teisės į gynybą. Teisė į veiksmingą teisinę gynybą užtikrinama ir esminių ir svarbių subjektų teikiamų paslaugų gavėjams. Ši direktyva turėtų būti įgyvendinta atsižvelgiant į tas teises ir principus;

(144) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([25]) 42 straipsnio 1 dalimi buvo pasikonsultuota su Europos duomenų apsaugos priežiūros pareigūnu, ir 2021 m. kovo 11 d. jis pateikė savo nuomonę ([26]),

([23]) 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).

([24]) 2022 m. spalio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2065 dėl skaitmeninių paslaugų bendrosios rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB (Skaitmeninių paslaugų aktas) (OL L 277, 2022 10 27, p. 1).

([25]) 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).

([26]) OL C 183, 2021 5 11, p. 3.

PRIĖMĖ ŠIĄ DIREKTYVĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas

1. Šia direktyva nustatomos priemonės, kuriomis siekiama užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje, kad būtų pagerintas vidaus rinkos veikimas.

2. Tuo tikslu šia direktyva nustatomos:

a) pareigos, kuriomis iš valstybių narių reikalaujama priimti nacionalines kibernetinio saugumo strategijas ir paskirti arba įsteigti kompetentingas institucijas, kibernetinių krizių valdymo institucijas, bendruosius kibernetinio saugumo kontaktinius punktus (toliau – bendrieji kontaktiniai punktai) ir reagavimo į kompiuterių saugumo incidentus tarnybas (CSIRT);

b) kibernetinio saugumo rizikos valdymo priemonės ir pareigos pranešti, taikomos I ar II priede nurodytos rūšies subjektams, taip pat subjektams, identifikuotiems kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557;

c) dalijimosi kibernetinio saugumo informacija taisyklės ir pareigos ja dalytis;

d) valstybių narių pareigos priežiūros ir vykdymo užtikrinimo srityse.

2 straipsnis

Taikymo sritis

1. Ši direktyva taikoma I ar II priede nurodytos rūšies viešiesiems ar privatiesiems subjektams, kurie laikomi vidutinėmis įmonėmis pagal Rekomendacijos 2003/361/EB priedo 2 straipsnį arba kurie viršija to straipsnio 1 dalyje nustatytas viršutines ribas, ir kurie teikia paslaugas arba vykdo veiklą Sąjungoje.

Šios direktyvos tikslais tos rekomendacijos priedo 3 straipsnio 4 dalis netaikoma.

2. Nepaisant subjektų dydžio, ši direktyva taip pat taikoma I ar II priede nurodytos rūšies subjektams, kai:

a) paslaugas teikia:

   i) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai;

   ii) patikimumo užtikrinimo paslaugų teikėjai;

   iii) aukščiausio lygio domenų vardų registrai ir domenų vardų sistemos paslaugų teikėjai;

b) subjektas yra vienintelis paslaugos, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ar ekonominės veiklos vykdymą, teikėjas valstybėje narėje;

c) paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai;

d) paslaugos, kurią teikia subjektas, sutrikimas galėtų kelti didelę sisteminę riziką visų pirma sektoriuose, kuriuose toks sutrikimas galėtų daryti tarpvalstybinį poveikį;

e) subjektas yra ypatingos svarbos atsižvelgiant į jo konkrečią svarbą konkrečiam sektoriui ar paslaugos rūšiai arba kitiems tarpusavyje priklausomiems sektoriams valstybėje narėje nacionaliniu ar regioniniu lygmeniu;

f) subjektas yra:

i) centrinės valdžios, kaip valstybė narė apibrėžė pagal nacionalinę teisę viešojo administravimo subjektas, arba

ii) regioninio lygmens, kaip valstybė narė apibrėžė pagal nacionalinę teisę, kuris, atlikus rizika grindžiamą vertinimą, teikia paslaugas, kurių sutrikimas galėtų daryti didelį poveikį ypatingos svarbos visuomeninei ar ekonominei veiklai, viešojo administravimo subjektas.

3. Nepriklausomai nuo jų dydžio, ši direktyva taikoma subjektams, identifikuotiems kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557.

4. Nepriklausomai nuo jų dydžio, ši direktyva taikoma subjektams, teikiantiems domenų vardų registravimo paslaugas.

5. Valstybės narės gali numatyti, kad ši direktyva taikoma:

a) viešojo administravimo subjektams vietos lygmeniu;

b) švietimo įstaigoms, visų pirma tais atvejais, kai jos vykdo ypatingos svarbos mokslinių tyrimų veiklą.

6. Šia direktyva nedaromas poveikis valstybių narių atsakomybei užtikrinti nacionalinį saugumą ir jų įgaliojimams apsaugoti kitas esmines valstybines funkcijas, įskaitant valstybės teritorinio vientisumo užtikrinimą ir viešosios tvarkos palaikymą.

7. Ši direktyva netaikoma viešojo administravimo subjektams, vykdantiems savo veiklą, nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas.

8. Valstybės narės gali atleisti nuo 21 ir 23 straipsniuose nustatytų pareigų konkrečius subjektus, vykdančius veiklą nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas, arba kurie teikia paslaugas išimtinai šio straipsnio 7 dalyje nurodytiems viešojo administravimo subjektams, tos veiklos ar paslaugų atžvilgiu. Tokiais atvejais VII skyriuje nurodytos priežiūros ir vykdymo užtikrinimo priemonės netaikomos tai konkrečiai veiklai ar paslaugoms. Kai subjektai vykdo tik šioje dalyje nurodytos rūšies veiklą arba teikia tik šioje dalyje nurodytos rūšies paslaugas, valstybės narės taip pat gali nuspręsti atleisti tuos subjektus nuo 3 ir 27 straipsniuose nustatytų pareigų.

9. 7 ir 8 dalys netaikomos, kai subjektas veikia kaip patikimumo užtikrinimo paslaugų teikėjas.

10. Ši direktyva netaikoma subjektams, kuriems valstybės narės netaiko Reglamento (ES) 2022/2554 pagal to reglamento 2 straipsnio 4 dalį.

11. Šioje direktyvoje nustatytos pareigos nereiškia, kad bus teikiama informacija, kurios atskleidimas prieštarautų esminiams valstybių narių nacionalinio saugumo, viešojo saugumo ar gynybos interesams.

12. Ši direktyva taikoma nedarant poveikio Reglamentui (ES) 2016/679, Direktyvai 2002/58/EB, Europos Parlamento ir Tarybos direktyvoms 2011/93/ES ([27]) ir 2013/40/ES ([28]) ir Direktyvai (ES) 2022/2557.

13. Nedarant poveikio SESV 346 straipsniui, informacija, kuri yra konfidenciali pagal Sąjungos ar nacionalines taisykles, kaip antai taisyklės dėl verslo konfidencialumo, turi būti pagal šią direktyvą keičiamasi su Komisija ir kitomis atitinkamomis institucijomis tik tais atvejais, kai toks keitimasis yra būtinas šios direktyvos taikymui. Keičiamasi tik tokia informacija, kuri atitinka keitimosi tikslą ir yra jam proporcinga. Keičiantis informacija saugomas tos informacijos konfidencialumas ir atitinkamų subjektų saugumo ir komerciniai interesai.

([27]) 2011 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyva 2011/93/ES dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR (OL L 335, 2011 12 17, p. 1).

([28]) 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL L 218, 2013 8 14, p. 8).

14. Subjektai, kompetentingos institucijos, bendrieji kontaktiniai punktai ir CSIRT tvarko asmens duomenis tiek, kiek tai būtina šios direktyvos tikslais ir laikydamiesi Reglamento (ES) 2016/679, ir toks tvarkymas visų pirma grindžiamas to reglamento 6 straipsniu.

Asmens duomenų tvarkymą pagal šią direktyvą viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai vykdo laikydamiesi Sąjungos duomenų apsaugos teisės ir Sąjungos privatumo teisės, visų pirma Direktyvos 2002/58/EB, nuostatų.

3 straipsnis

Esminiai ir svarbūs subjektai

1. Šios direktyvos taikymo tikslais esminiais subjektais laikomi šie subjektai:

a) I priede nurodytos rūšies subjektai, kurie viršija vidutinėms įmonėms nustatytas viršutines ribas, nustatytas Rekomendacijos 2003/361/EB priedo 2 straipsnio 1 dalyje;

b) kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai ir aukščiausio lygio domenų vardų registrai, taip pat DNS paslaugų teikėjai, nepriklausomai nuo jų dydžio;

c) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai, kurie laikomi vidutinėmis įmonėmis pagal Rekomendacijos 2003/361/EB priedo 2 straipsnį;

d) 2 straipsnio 2 dalies f punkto i papunktyje nurodyti viešojo administravimo subjektai;

e) visi kiti I arba II priede nurodytos rūšies subjektai, kuriuos valstybė narė identifikavo kaip esminius subjektus pagal 2 straipsnio 2 dalies b-e punktus;

f) subjektai, kurie pagal Direktyvą (ES) 2022/2557 identifikuoti kaip ypatingos svarbos subjektai, nurodyti šios direktyvos 2 straipsnio 3 dalyje;

g) jei valstybė narė taip numato, subjektai, kuriuos ta valstybė narė ne vėliau kaip 2023 m. sausio 16 d. identifikavo kaip esminių paslaugų operatorius pagal Direktyvą (ES) 2016/1148 arba nacionalinę teisę.

2. Šios direktyvos I arba II priede nurodytos rūšies subjektai, kurie nelaikomi esminiais subjektais pagal šio straipsnio 1 dalį, laikomi svarbiais subjektais. Tai apima subjektus, kuriuos valstybė narė identifikavo kaip esminius subjektus pagal 2 straipsnio 2 daliesb–e punktus.

3. Ne vėliau kaip 2025 m. balandžio 17 d. valstybės narės sudaro esminių ir svarbių subjektų bei domeno vardo registravimo paslaugas teikiančių subjektų sąrašą. Po tos datos valstybės narės reguliariai ir ne rečiau kaip kas dvejus metus peržiūri tą sąrašą ir, kai tinkama, jį atnaujina.

4. Siekdamos sudaryti 3 dalyje nurodytą sąrašą, valstybės narės reikalauja, kad toje dalyje nurodyti subjektai kompetentingoms institucijoms pateiktų bent šią informaciją:

a) subjekto pavadinimą;

b) adresą ir naujausius kontaktinius duomenis, įskaitant subjektų el. pašto adresus, IP adresų ruožus ir telefonų numerius;

c) kai taikytina, I arba II priede nurodytą atitinkamą sektorių ir subsektorių ir

d) kai taikytina, valstybių narių, kuriose jos teikia į šios direktyvos taikymo sritį patenkančias paslaugas, sąrašą.

3 dalyje nurodyti subjektai nedelsdami ir bet kuriuo atveju ne vėliau kaip per dvi savaites nuo pakeitimo dienos praneša apie bet kokius pagal šios dalies pirmą pastraipą pateiktų duomenų pakeitimus.

Komisija, padedant Europos Sąjungos kibernetinio saugumo agentūrai (toliau – ENISA), nepagrįstai nedelsdama pateikia gaires ir šablonus, susijusius su šioje dalyje nustatytomis pareigomis.

Valstybės narės gali nustatyti nacionalinius mechanizmus, pagal kuriuos subjektai galėtų užsiregistruoti patys.

5. Ne vėliau kaip 2025 m. balandžio 17 d., o vėliau – kas dvejus metus kompetentingos institucijos praneša:

a) Komisijai ir Bendradarbiavimo grupei esminių ir svarbių subjektų, įtrauktų į sąrašą vadovaujantis 3 dalimi pagal kiekvieną iš I arba II priede nurodytų sektorių ir subsektorių, skaičių, ir

b) Komisijai – atitinkamą informaciją apie esminių ir svarbių subjektų, identifikuotų pagal 2 straipsnio 2 dalies b–e punktus, skaičių, I arba II priede nurodytą sektorių ir subsektorių, kuriems jie priklauso, jų teikiamų paslaugų rūšį ir nuostatą iš įtvirtintųjų 2 straipsnio 2 dalies b–e punktuose, pagal kurią jie buvo identifikuoti.

6. Iki 2025 m. balandžio 17 d. ir Komisijai paprašius, valstybės narės gali pranešti Komisijai 5 dalies b punkte nurodytų esminių ir svarbių subjektų pavadinimus.

4 straipsnis

Konkretiems sektoriams taikomi Sąjungos teisės aktai

1. Jei pagal konkretiems sektoriams taikomus Sąjungos teisės aktus reikalaujama, kad esminiai arba svarbūs subjektai priimtų kibernetinio saugumo rizikos valdymo priemones arba praneštų apie didelius incidentus, ir jei tų reikalavimų poveikis yra bent lygiavertis šioje direktyvoje nustatytų pareigų poveikiui, atitinkamos šios direktyvos nuostatos, įskaitant VII skyriuje įtvirtintas nuostatas dėl priežiūros ir vykdymo užtikrinimo, tokiems subjektams netaikomos. Jei konkretiems sektoriams taikomi Sąjungos teisės aktai taikomi ne visiems konkretaus sektoriaus, kuriam taikoma ši direktyva, subjektams, atitinkamos šios direktyvos nuostatos toliau taikomos subjektams, kuriems netaikomi tie konkretiems sektoriams taikomi Sąjungos teisės aktai.

2. Šio straipsnio 1 dalyje nurodytų reikalavimų poveikis laikomas lygiaverčiu šioje direktyvoje nustatytų pareigų poveikiui, jeigu:

a) kibernetinio saugumo rizikos valdymo priemonių poveikis yra bent lygiavertis priemonių, nustatytų 21 straipsnio 1 ir 2 dalyse, poveikiui; arba

b) konkrečiam sektoriui taikomame Sąjungos teisės akte numatyta CSIRT, kompetentingų institucijų arba bendrųjų kontaktinių punktų pagal šią direktyvą neatidėliotina prieiga, kai tinkama, automatinė ir tiesioginė, prie pateiktų pranešimų apie incidentus ir jei reikalavimai pranešti apie didelius incidentus yra pagal poveikį bent lygiaverčiai šios direktyvos 23 straipsnio 1–6 dalyse nustatytiems reikalavimams.

3. Komisija ne vėliau kaip 2023 m. liepos 17 d. pateikia gaires, kuriomis paaiškinamas 1 ir 2 dalių taikymas. Komisija reguliariai peržiūri tas gaires. Rengdama tas gaires Komisija atsižvelgia į visas Bendradarbiavimo grupės ir ENISA pastabas.

5 straipsnis

Minimalus suderinimas

Šia direktyva valstybėms narėms netrukdoma priimti arba palikti toliau galioti nuostatų, kuriomis užtikrinamas aukštesnio lygio kibernetinis saugumas, su sąlyga, kad tokios nuostatos yra suderinamos su valstybių narių įsipareigojimais, nustatytais Sąjungos teisėje.

6 straipsnis

Terminų apibrėžtys

Šioje direktyvoje vartojamų terminų apibrėžtys:

1) tinklų ir informacinė sistema – tai:

   a) elektroninių ryšių tinklas, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 1 punkte;

b) bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba

c) skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami a ir b punktuose nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

2) tinklų ir informacinių sistemų saugumas – tinklų ir informacinių sistemų pajėgumas tam tikru patikimumo lygiu išlikti atspariems bet kokiam įvykiui, galinčiam sukelti pavojų saugomų, perduodamų ar tvarkomų duomenų, arba teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui;

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

4) nacionalinė kibernetinio saugumo strategija – nuosekli valstybės narės sistema, kurioje nustatyti tos valstybės narės kibernetinio saugumo srities strateginiai tikslai ir prioritetai ir jų įgyvendinimo valdymas;

5) vos neįvykęs incidentas – įvykis, kuriuo galėjo būti sukeltas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui, bet kuriam įvykti buvo sėkmingai užkirstas kelias arba kuris neįvyko;

6) incidentas – įvykis, kuriuo sukeliamas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui;

7) didelio masto kibernetinio saugumo incidentas – incidentas, į kurio sukeltą sutrikimą viena valstybė narė nepajėgia reaguoti arba kuris daro didelį poveikį ne mažiau kaip dviem valstybėms narėms;

8) incidento valdymas – visi veiksmai ir procedūros, kuriais siekiama užkirsti incidentui kelią, atskleisti, išanalizuoti ir sustabdyti incidentą arba į jį reaguoti ir atstatyti veiklą po incidento;

9) rizika – potencialus praradimas arba sutrikimas, kurį sukėlė incidentas, kuri turi būti išreikšta kaip tokio praradimo arba sutrikimo masto ir incidento pasikartojimo derinys;

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

11) didelė kibernetinė grėsmė – kibernetinė grėsmė, dėl kurios techninių charakteristikų galima daryti prielaidą, kad ji gali padaryti didelį neigiamą poveikį subjekto tinklų ir informacinėms sistemoms arba subjekto paslaugų naudotojų tinklų ir informacinėms sistemoms, sukeldama didelę turtinę arba neturtinę žalą;

12) IRT produktas – IRT produktas, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 12 punkte;

13) IRT paslauga – IRT paslauga, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 13 punkte;

14) IRT procesas – IRT procesas, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 14 punkte;

15) pažeidžiamumas – IRT produktų arba IRT paslaugų silpnoji vieta, jautrumas ar trūkumas, kuriais gali būti pasinaudota kibernetinei grėsmei kelti;

16) standartas – standartas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012 ([29]) 2 straipsnio 1 punkte;

17) techninė specifikacija – techninė specifikacija, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 4 punkte;

([29]) 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).

18) interneto duomenų srautų mainų taškas – tinklo įrenginys, kuris sudaro sąlygas sujungti daugiau nei du nepriklausomus tinklus (autonomines sistemas), visų pirma siekiant palengvinti interneto duomenų srautų mainus, kuris sujungia tik autonomines sistemas ir kuris nereikalauja, kad interneto duomenų srautai, perduodami tarp bet kurių naudojamų autonominių sistemų porų, būtų perduodami per bet kurią trečią autonominę sistemą ir nekeičia tokių srautų ar kitokiu būdu jų netrikdo;

19) domenų vardų sistema arba DNS – hierarchiškai paskirstyta vardų sistema, kurioje galima identifikuoti interneto paslaugas ir išteklius ir sudaromos sąlygos galutiniams naudotojams naudotis interneto maršruto parinkimo ir junglumo paslaugomis ir gauti tas paslaugas bei išteklius;

20) DNS paslaugų teikėjas – subjektas, kuris teikia:

a) viešai prieinamas rekursinio domenų vardų keitimo paslaugas galutiniams interneto naudotojams arba

b) patikimo domenų vardų keitimo paslaugas trečiųjų šalių reikmėms, išskyrus šakninio pavadinimo serverius;

21) aukščiausio lygio domenų vardų registras – subjektas, kuriam pavestas konkretus aukščiausio lygio domenas ir kuris atsako už aukščiausio lygio domeno administravimą, įskaitant to aukščiausio lygio domeno domenų vardų registraciją ir techninį to aukščiausio lygio domeno veikimą, įskaitant jo vardų serverių veikimą, duomenų bazių techninę priežiūrą ir aukščiausio lygio domenų zonos rinkmenų paskirstymą tarp vardų serverių, neatsižvelgiant į tai, ar bet kurias iš tų operacijų atlieka pats subjektas, ar tai yra užsakomosios paslaugos, tačiau neįtraukiant atvejų, kai registras aukščiausio lygio domenų vardus naudoja tik savo reikmėms;

22) domenų vardų registravimo paslaugas teikiantis subjektas – registratorius arba registratorių vardu veikiantis agentas, pavyzdžiui, privatumo ar įgaliotojo serverio registravimo paslaugų teikėjas arba perpardavėjas;

23) skaitmeninė paslauga – paslauga, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2015/1535 ([30]) 1 straipsnio 1 dalies b punkte;

24) patikimumo užtikrinimo paslauga – patikimumo užtikrinimo paslauga, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 16 punkte;

25) patikimumo užtikrinimo paslaugų teikėjas – patikimumo užtikrinimo paslaugų teikėjas, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 19 punkte;

26) kvalifikuota patikimumo užtikrinimo paslauga – kvalifikuota patikimumo užtikrinimo paslauga, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 17 punkte;

27) kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas – kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 20 punkte;

28) elektroninė prekyvietė – elektroninė prekyvietė, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2005/29/EB ([31]) 2 straipsnio n punkte;

29) interneto paieškos sistema – interneto paieškos sistema, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/1150 ([32]) 2 straipsnio 5 punkte;

30) debesijos kompiuterijos paslauga – skaitmeninė paslauga, kuri pagal poreikį suteikia administravimo paslaugas ir plataus masto nuotolinę prieigą prie kintamo masto pritaikomos bendrų ir paskirstytų kompiuterijos išteklių bazės, įskaitant atvejus, kai tokie ištekliai yra paskirstyti per kelias vietas;

([30]) 2015 m. rugsėjo 9 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/1535, kuria nustatoma informacijos apie techninius reglamentus ir informacinės visuomenės paslaugų taisykles teikimo tvarka (OL L 241, 2015 9 17, p. 1).

([31]) 2005 m. gegužės 11 d. Europos Parlamento ir Tarybos direktyva 2005/29/EB dėl nesąžiningos įmonių komercinės veiklos vartotojų atžvilgiu vidaus rinkoje ir iš dalies keičianti Tarybos direktyvą 84/450/EEB, Europos Parlamento ir Tarybos direktyvas 97/7/EB, 98/27/EB bei 2002/65/EB ir Europos Parlamento ir Tarybos reglamentą (EB) Nr. 2006/2004 („Nesąžiningos komercinės veiklos direktyva“) (OL L 149, 2005 6 11, p. 22).

([32]) 2019 m. birželio 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/1150 dėl verslo klientams teikiamų internetinių tarpininkavimo paslaugų sąžiningumo ir skaidrumo didinimo (OL L 186, 2019 7 11, p. 57).

31) duomenų centro paslauga – paslauga, kuri apima struktūras arba struktūrų grupes, skirtas IT ir tinklo įrangos centralizuotam pritaikymui, tarpusavio junglumui ir eksploatavimui, teikiant duomenų saugojimo, tvarkymo ir transportavimo paslaugas kartu su visa energijos paskirstymo ir aplinkos kontrolės įranga ir infrastruktūra;

32) turinio teikimo tinklas – geografiškai paskirstytų serverių tinklas, kurio paskirtis yra turinio ir paslaugų teikėjų vardu užtikrinti interneto naudotojams didelę skaitmeninio turinio ir paslaugų pasiūlą, prieinamumą arba greitą teikimą;

33) socialinių tinklų paslaugų platforma – platforma, kurioje galutiniams naudotojams sudaromos sąlygos prisijungti, dalytis, rasti vienas kitą ir bendrauti naudojant įvairius prietaisus, visų pirma per pokalbius, įrašus, vaizdo įrašus ir rekomendacijas;

34) atstovas – Sąjungoje įsisteigęs fizinis arba juridinis asmuo, paskirtas veikti tik DNS paslaugų teikėjo, aukščiausio lygio domenų vardų registro, domenų vardų registravimo paslaugas teikiančio subjekto, debesijos kompiuterijos paslaugų teikėjo, duomenų centro paslaugų teikėjo, turinio pristatymo tinklo paslaugų teikėjo, valdomų paslaugų teikėjo, valdomų saugumo paslaugų teikėjo, elektroninės prekyvietės paslaugų teikėjo, interneto paieškos sistemos paslaugų teikėjo arba socialinio tinklo paslaugų platformų paslaugų teikėjo, kuris nėra įsisteigęs Sąjungoje, vardu, į kurį kompetentinga institucija arba CSIRT gali kreiptis vietoj subjekto dėl to subjekto pareigų pagal šią direktyvą;

35) viešojo administravimo subjektas – valstybės narės subjektas, kuris valstybėje narėje pagal nacionalinę teisę yra pripažįstamas tokiu subjektu, išskyrus teismines institucijas, parlamentus ir centrinius bankus, ir kuris atitinka šiuos kriterijus:

   a) yra įsteigtas siekiant tikslo tenkinti bendrojo intereso poreikius, ir nėra pramoninio ar komercinio pobūdžio;

   b) turi juridinio asmens statusą arba pagal teisės aktus turi teisę veikti kito juridinio asmens statusą turinčio subjekto vardu;

   c) didžiąja dalimi yra finansuojamas valstybės, regioninių institucijų ar kitų viešosios teisės reglamentuojamų įstaigų lėšomis, arba jam taikoma tų institucijų ar įstaigų administracinė priežiūra, arba jis turi administracinį, valdymo ar priežiūros organą, kurio daugiau kaip pusę narių skiria valstybės, regioninės institucijos arba kitos viešosios teisės reglamentuojamos įstaigos;

   d) turi įgaliojimus priimti administracinius arba reguliavimo sprendimus dėl fizinių arba juridinių asmenų, kurie daro poveikį jų teisėms tarpvalstybinio asmenų, prekių, paslaugų ar kapitalo judėjimo srityje;

36) viešasis elektroninių ryšių tinklas – viešasis elektroninių ryšių tinklas, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 8 punkte;

37) elektroninių ryšių paslauga – elektroninių ryšių paslauga, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 4 punkte;

38) subjektas – fizinis asmuo arba juridinis asmuo, įsteigtas ir tokiu pripažintas pagal jo įsteigimo vietos nacionalinę teisę, kuris, veikdamas savo vardu, naudojasi teisėmis ir kuriam gali būti taikomos pareigos;

39) valdomų paslaugų teikėjas – subjektas, teikiantis paslaugas, susijusias su IRT produktų, tinklų, infrastruktūros, taikomųjų programų ar bet kurių kitų tinklų ir informacinių sistemų diegimu, valdymu, naudojimu ar technine priežiūra, teikdamas pagalbą arba aktyvaus administravimo paslaugas klientų patalpose arba nuotoliniu būdu;

40) valdomų saugumo paslaugų teikėjas – valdomų paslaugų teikėjas, vykdantis veiklą, susijusią su kibernetinio saugumo rizikos valdymu, arba teikiantis pagalbą tokiai veiklai;

41) mokslinių tyrimų organizacija – subjektas, kurio pagrindinis tikslas – vykdyti taikomuosius mokslinius tyrimus arba eksperimentinę plėtrą, siekiant panaudoti tų mokslinių tyrimų rezultatus komerciniais tikslais, tačiau kurio veikla neapima švietimo įstaigų.

II SKYRIUS

KOORDINUOTOS KIBERNETINĖS SISTEMOS

7 straipsnis

Nacionalinė kibernetinio saugumo strategija

1. Kiekviena valstybė narė priima nacionalinę kibernetinio saugumo strategiją, kurioje nustatomi strateginiai tikslai, reikiami ištekliai tiems tikslams pasiekti ir tinkamos politikos bei reguliavimo priemonės, kad būtų pasiektas ir išlaikytas aukšto lygmens kibernetinis saugumas. Nacionalinė kibernetinio saugumo strategija apima:

a) valstybės narės kibernetinio saugumo strategijos tikslus ir prioritetus, visų pirma apimančius I ir II prieduose nurodytus sektorius;

b) valdymo sistemą, kad būtų pasiekti šios dalies a punkte nurodyti tikslai ir įgyvendinti prioritetai, įskaitant 2 dalyje nurodytą politiką;

c) valdymo sistemą, pagal kurią paaiškinami atitinkamų suinteresuotųjų subjektų vaidmenys ir pareigos nacionaliniu lygmeniu, kuria grindžiamas kompetentingų institucijų, bendrųjų kontaktinių punktų ir CSIRT pagal šią direktyvą bendradarbiavimas ir veiklos koordinavimas nacionaliniu lygmeniu, taip pat tų įstaigų ir kompetentingų institucijų pagal konkretiems sektoriams taikomus Sąjungos teisės aktus veiklos koordinavimas ir jų bendradarbiavimas;

d) mechanizmą, pagal kurį nustatomi atitinkami objektai, ir kibernetinio saugumo rizikų toje valstybėje narėje vertinimą;

e) parengties, reagavimo į incidentus ir veiklos po incidento atstatymo priemonių, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą, nustatymą;

f) įvairių institucijų ir suinteresuotųjų subjektų, dalyvaujančių įgyvendinant nacionalinę kibernetinio saugumo strategiją, sąrašą;

g) politikos sistemą, padedančią užtikrinti geresnį kompetentingų institucijų pagal šią direktyvą ir kompetentingų institucijų pagal Direktyvą (ES) 2022/2557 koordinavimą siekiant dalytis informacija apie rizikas, kibernetines grėsmes, ir incidentus, taip pat apie nekibernetinę riziką, grėsmes ir incidentus bei, prireikus, vykdyti priežiūros užduotis;

h) planą, įskaitant būtinas priemones, piliečių informuotumo apie kibernetinį saugumą bendram lygiui didinti.

2. Nacionalinėje kibernetinio saugumo strategijoje valstybės narės visų pirma nustato:

a) politiką dėl IRT produktų ir IRT paslaugų, kuriuos subjektai naudoja teikdami savo paslaugas, tiekimo grandinių kibernetinio saugumo;

b) politiką dėl su kibernetiniu saugumu susijusių reikalavimų, taikomų IRT produktams ir IRT paslaugoms, įtraukimo ir specifikacijų viešuosiuose pirkimuose, įskaitant reikalavimus, susijusius su kibernetinio saugumo sertifikavimu, šifravimu ir atvirojo kodo kibernetinio saugumo produktų naudojimu;

c) pažeidžiamumų valdymo, apimančio koordinuoto pažeidžiamumų atskleidimo pagal 12 straipsnio 1 dalį skatinimą ir palengvinimą, politiką;

d) politiką, susijusią su bendru atvirojo interneto viešojo pagrindo prieinamumu, vientisumu ir konfidencialumu, įskaitant, kai tinkama, povandeninių ryšių kabelių kibernetinį saugumą;

e) atitinkamų pažangių technologijų, kuriomis siekiama įgyvendinti pažangiausias kibernetinio saugumo rizikos valdymo priemones, kūrimo ir integravimo skatinimo politiką;

f) švietimo ir mokymo kibernetinio saugumo klausimais, kibernetinio saugumo įgūdžių, informuotumo didinimo ir mokslinių tyrimų ir technologinės plėtros iniciatyvų, taip pat gerosios kibernetinės higienos praktikos ir kontrolės gairių, skirtų piliečiams, suinteresuotiesiems subjektams ir kitiems subjektams, skatinimo ir plėtros politiką;

g) politiką dėl akademinių ir mokslinių tyrimų institucijų rėmimo siekiant kurti, tobulinti ir diegti kibernetinio saugumo priemones ir saugią tinklų infrastruktūrą;

h) politiką, įskaitant atitinkamas procedūras ir tinkamas dalijimosi informacija priemones, siekiant remti savanorišką dalijimąsi kibernetinio saugumo informacija tarp subjektų laikantis Sąjungos teisės;

i) politiką, kuria stiprinami mažųjų ir vidutinių įmonių, visų pirma į šios direktyvos taikymo sritį nepatenkančių įmonių, kibernetinis atsparumas ir kibernetinės higienos bazinis lygis teikiant lengvai prieinamas gaires ir pagalbą jų konkretiems poreikiams tenkinti;

j) politiką, kuria skatinama aktyvi kibernetinė apsauga.

3. Valstybės narės per tris mėnesius nuo savo nacionalinių kibernetinio saugumo strategijų priėmimo apie jas praneša Komisijai. Valstybės narės į tokius pranešimus gali neįtraukti informacijos, kuri susijusi su jų nacionaliniu saugumu.

4. Valstybės narės, remdamosi pagrindiniais veiklos rezultatų rodikliais, reguliariai ir bent kas penkerius metus vertina savo nacionalines kibernetinio saugumo strategijas ir prireikus jas atnaujina. ENISA valstybių narių prašymu padeda joms parengti arba atnaujinti nacionalinę kibernetinio saugumo strategiją ir pagrindinius veiklos rezultatų rodiklius, skirtus tai strategijai įvertinti, siekiant ją suderinti su šioje direktyvoje nustatytais reikalavimais ir pareigomis.

8 straipsnis

Kompetentingos institucijos ir bendrieji kontaktiniai punktai

1. Kiekviena valstybė narė paskiria arba įsteigia vieną arba daugiau kompetentingų institucijų, atsakingų už kibernetinį saugumą ir VII skyriuje nustatytų priežiūros užduočių vykdymą (toliau – kompetentingos institucijos).

2. 1 dalyje nurodytos kompetentingos institucijos stebi šios direktyvos įgyvendinimą nacionaliniu lygmeniu.

3. Kiekviena valstybė narė paskiria arba įsteigia bendrąjį kontaktinį punktą. Kai valstybė narė pagal 1 dalį paskiria arba įsteigia tik vieną kompetentingą instituciją, ta kompetentinga institucija taip pat laikoma tos valstybės narės bendruoju kontaktiniu punktu.

4. Kiekvienas bendras kontaktinis punktas vykdo ryšių palaikymo funkciją, kad būtų užtikrintas jo valstybės narės institucijų tarpvalstybinis bendradarbiavimas su atitinkamomis kitų valstybių narių institucijomis ir, kai tinkama, Komisija bei ENISA, taip pat tarpsektorinis bendradarbiavimas su kitomis kompetentingomis institucijomis toje valstybėje narėje.

5. Valstybės narės užtikrina, kad jų kompetentingos institucijos ir bendrieji kontaktiniai punktai turėtų tinkamų išteklių, kad veiksmingai ir efektyviai vykdytų jiems pavestas užduotis ir taip įgyvendintų šios direktyvos tikslus.

6. Kiekviena valstybė narė nepagrįstai nedelsdama praneša Komisijai 1 dalyje nurodytos kompetentingos institucijos ir 3 dalyje nurodyto bendrojo kontaktinio punkto tapatybės duomenis, tų institucijų užduotis ir bet kokius vėlesnius jų pakeitimus. Kiekviena valstybė narė savo kompetentingos institucijos tapatybės duomenis paskelbia viešai. Komisija viešai paskelbia paskirtų bendrųjų kontaktinių punktų sąrašą.

9 straipsnis

Nacionalinės kibernetinių krizių valdymo sistemos

1. Kiekviena valstybė narė paskiria arba įsteigia vieną arba daugiau kompetentingų institucijų, kurios atsako už didelio masto kibernetinio saugumo incidentų ir krizių valdymą (toliau – kibernetinių krizių valdymo institucijos). Valstybės narės užtikrina, kad tos institucijos turėtų tinkamų išteklių, reikalingų veiksmingam ir efektyviam joms pavestų užduočių vykdymui. Valstybės narės užtikrina suderinamumą su esamomis nacionalinėmis bendro krizių valdymo sistemomis.

2. Jeigu valstybė narė paskiria arba įsteigia pagal 1 dalį daugiau nei vieną kibernetinių krizių valdymo instituciją, ji aiškiai nurodo, kuri iš tų institucijų yra koordinatorė valdant didelio masto kibernetinio saugumo incidentus ir krizes.

3. Kiekviena valstybė narė, taikydama šią direktyvą, nustato pajėgumus, objektus ir procedūras, kuriais galima pasinaudoti krizės atveju.

4. Kiekviena valstybė narė priima nacionalinį reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planą, kuriame išdėstomi didelio masto kibernetinio saugumo incidentų ir krizių valdymo tikslai ir tvarka. Tame plane visų pirma nustatomi:

a) nacionalinių pasirengimo priemonių ir veiksmų tikslai;

b) kibernetinių krizių valdymo institucijų užduotys ir pareigos;

c) kibernetinių krizių valdymo procedūros, įskaitant jų integravimą į nacionalinę bendro krizių valdymo sistemą, ir keitimosi informacija kanalai;

d) nacionalinės pasirengimo priemonės, įskaitant pratybas ir mokymo veiklą;

e) atitinkami viešieji ir privatieji suinteresuotieji subjektai ir naudojama infrastruktūra;

f) atitinkamų nacionalinių institucijų ir įstaigų nacionalinės procedūros ir susitarimai, kuriais siekiama užtikrinti, kad valstybė narė veiksmingai dalyvautų vykdant koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą Sąjungos lygmeniu ir jį remtų.

5. Per tris mėnesius nuo 1 dalyje nurodytos kibernetinių krizių valdymo institucijos paskyrimo arba įsteigimo kiekviena valstybė narė praneša Komisijai apie savo institucijos tapatybės duomenis ir apie visus vėlesnius jos pakeitimus. Valstybės narės pateikia Komisijai ir Europos ryšių palaikymo dėl kibernetinių krizių organizacinio tinklui (EU-CyCLONe) atitinkamą informaciją, susijusią su 4 dalies reikalavimais, apie savo nacionalinius reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planus per tris mėnesius nuo tų planų priėmimo. Valstybės narės gali nenurodyti konkrečios informacijos, jeigu tai yra būtina jų nacionaliniam saugumui ir tik tokiam saugumui būtinu mastu.

10 straipsnis

Reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT)

1. Kiekviena valstybė narė paskiria arba įsteigia vieną arba daugiau CSIRT. CSIRT gali būti paskirtos arba įsteigtos kompetentingoje institucijoje. CSIRT laikosi 11 straipsnio 1 dalyje išdėstytų reikalavimų, apima bent I ir II prieduose nurodytus sektorius, subsektorius ir subjektų rūšis ir atsako už incidentų valdymą pagal aiškiai apibrėžtą procesą.

2. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamų išteklių, kad galėtų veiksmingai vykdyti savo užduotis, nurodytas 11 straipsnio 3 dalyje.

3. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamą, saugią ir atsparią ryšių ir informacinę struktūrą, kuria naudodamosi jos galėtų keistis informacija su esminiais ir svarbiais subjektais ir kitais atitinkamais suinteresuotaisiais subjektais. Tuo tikslu valstybės narės užtikrina, kad kiekviena CSIRT prisidėtų prie saugaus dalijimosi informacija priemonių diegimo.

4. CSIRT pagal 29 straipsnį bendradarbiauja ir, kai tinkama, keičiasi atitinkama informacija su sektoriaus arba kelių sektorių esminių ir svarbių subjektų bendruomenėmis.

5. CSIRT dalyvauja tarpusavio vertinimuose, kurie organizuojami pagal 19 straipsnį.

6. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų jų CSIRT bendradarbiavimą CSIRT tinkle.

7. CSIRT gali užmegzti bendradarbiavimo ryšius su trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis. Palaikydamos tokius bendradarbiavimo santykius, valstybės narės sudaro palankesnes sąlygas veiksmingai, efektyviai ir saugiai keistis informacija su tomis trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis, naudodamos atitinkamus dalijimosi informacija protokolus, įskaitant Srauto kontrolės protokolą. CSIRT gali keistis atitinkama informacija su trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis, įskaitant asmens duomenis, laikydamosi Sąjungos duomenų apsaugos teisės.

8. CSIRT gali bendradarbiauti su trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis arba lygiavertėmis trečiųjų valstybių įstaigomis, visų pirma siekdamos teikti joms pagalbą kibernetinio saugumo srityje.

9. Kiekviena valstybė narė nepagrįstai nedelsdama praneša Komisijai šio straipsnio 1 dalyje nurodytos CSIRT ir CSIRT, paskirtos koordinatore pagal 12 straipsnio 1 dalį, tapatybės duomenis, jų atitinkamas užduotis, kurias jos vykdo esminių ir svarbių subjektų atžvilgiu, ir bet kokius vėlesnius jų pakeitimus.

10. Valstybės narės gali paprašyti ENISA padėti kurti jų CSIRT.

11 straipsnis

CSIRT keliami reikalavimai, techniniai pajėgumai ir užduotys

1. CSIRT turi atitikti šiuos reikalavimus:

a) CSIRT užtikrina, kad jų ryšio kanalai būtų lengvai prieinami išvengiant kritinių funkcionavimo trikties taškų, taip pat nustato keletą būdų, kaip bet kuriuo metu susisiekti su jomis ir su kitais subjektais; jos aiškiai nurodo ryšių kanalus ir apie juos informuoja savo klientus ir bendradarbiavimo partnerius;

b) CSIRT biurai ir pagalbinės informacinės sistemos turi būti saugiose vietose;

c) CSIRT aprūpinamos tinkama prašymų valdymo ir nukreipimo sistema, visų pirma siekiant palengvinti veiksmingą ir efektyvų perdavimą;

d) CSIRT užtikrina savo veiklos konfidencialumą ir patikimumą;

e) CSIRT turi turėti pakankamai darbuotojų, kad būtų užtikrintas pasiekiamumas bet kuriuo metu, ir jos turi užtikrinti tinkamą savo darbuotojų mokymą;

f) CSIRT aprūpinamos antrinėmis sistemomis ir atsargine darbo erdve, kad būtų užtikrintas jų paslaugų tęstinumas;

CSIRT gali dalyvauti tarptautiniuose bendradarbiavimo tinkluose.

2. Valstybės narės užtikrina, kad jų CSIRT bendrai turėtų techninių pajėgumų, būtinų, kad galėtų veiksmingai vykdyti savo užduotis, nurodytas 3 dalyje. Valstybės narės užtikrina, kad CSIRT būtų skirta pakankamai išteklių siekiant užtikrinti tinkamą darbuotojų skaičių, kad CSIRT galėtų plėtoti savo techninius pajėgumus.

3. CSIRT vykdo šias užduotis:

a) stebi ir analizuoja kibernetines grėsmes, pažeidžiamumus ir incidentus nacionaliniu lygmeniu, ir, gavusios prašymą, teikia pagalbą atitinkamiems esminiams ir svarbiems subjektams, susijusią su jų tinklų ir informacinių sistemų stebėjimu tikruoju laiku arba beveik tikruoju laiku;

b) teikia ankstyvuosius perspėjimus, įspėjimus, pranešimus ir platina informaciją apie kibernetines grėsmes, pažeidžiamumus ir incidentus esminiams ir svarbiems subjektams, taip pat kompetentingoms institucijoms ir kitiems atitinkamiems suinteresuotiesiems subjektams, jei įmanoma, beveik tikruoju laiku;

c) reaguoja į incidentus ir, kai tikslinga, teikia pagalbą atitinkamiems esminiams ir svarbiems subjektams;

d) renka ir analizuoja teismo ekspertizės duomenis ir teikia dinaminę rizikos bei incidentų analizę, taip pat užtikrina informuotumą apie padėtį kibernetinio saugumo srityje;

e) esminio ar svarbaus subjekto prašymu aktyviai tikrina atitinkamo subjekto tinklų ir informacines sistemas, kad būtų galima atskleisti pažeidžiamumus, galinčius daryti didelį poveikį;

f) dalyvauja CSIRT tinkle ir teikia savitarpio pagalbą pagal savo pajėgumus ir kompetenciją kitiems CSIRT tinklo nariams jų prašymu;

g) kai taikytina, atlieka koordinatoriaus funkcijas koordinuoto pažeidžiamumo atskleidimo tikslais pagal 12 straipsnio 1 dalį;

h) prisideda prie saugaus dalijimosi informacija priemonių diegimo pagal 10 straipsnio 3 dalį.

CSIRT gali atlikti aktyvų neintervencinį esminių ir svarbių subjektų viešai prieinamų tinklų ir informacinių sistemų tikrinimą. Toks tikrinimas atliekamas siekiant aptikti pažeidžiamas arba nesaugiai sukonfigūruotas tinklų ir informacines sistemas ir informuoti atitinkamus subjektus. Toks tikrinimas nedaro jokio neigiamo poveikio subjektų paslaugų veikimui.

Vykdydamos pirmoje pastraipoje nurodytas užduotis, CSIRT gali teikti pirmenybę konkrečioms užduotims remdamosi rizika grindžiamu požiūriu.

4. CSIRT užmezga bendradarbiavimo ryšius su atitinkamais privačiojo sektoriaus suinteresuotaisiais subjektais, kad būtų pasiekti šios direktyvos tikslai.

5. Siekdamos palengvinti bendradarbiavimą, nurodytą 4 dalyje, CSIRT skatina priimti ir naudoti bendrą arba standartizuotą praktiką, klasifikavimo sistemas ir taksonomiją srityse, susijusiose su:

a) incidentų valdymo procedūromis;

b) krizių valdymu ir

c) koordinuotu pažeidžiamumų atskleidimu pagal 12 straipsnio 1 dalį.

12 straipsnis

Koordinuotas pažeidžiamumų atskleidimas ir Europos pažeidžiamumų duomenų bazė

1. Kiekviena valstybė narė paskiria vieną iš savo CSIRT koordinuoto pažeidžiamumų atskleidimo koordinatore. Koordinatore paskirta CSIRT veikia kaip patikimas tarpininkas, prireikus lengvinantis sąveiką tarp pranešimą apie pažeidžiamumą teikiančio fizinio ar juridinio asmens ir gamintojo arba potencialiai pažeidžiamų IRT produktų ar IRT paslaugų teikėjo bet kurios šalies prašymu. Koordinatore paskirtos CSIRT užduotys apima:

a) atitinkamų subjektų nustatymą ir susisiekimą su jais;

b) pagalbos teikimą pranešimus apie pažeidžiamumą teikiantiems fiziniams ar juridiniams asmenims ir

c) derybas dėl informacijos atskleidimo terminų ir pažeidžiamumų, kurie daro poveikį keliems subjektams, valdymą.

Valstybės narės užtikrina, kad fiziniai ar juridiniai asmenys, jei jie to prašo, galėtų anonimiškai pranešti koordinatore paskirtai CSIRT apie pažeidžiamumą. Koordinatore paskirta CSIRT užtikrina, kad būtų imtasi kruopščių tolesnių veiksmų dėl pažeidžiamumo, apie kurį pranešta, ir užtikrina fizinio ar juridinio asmens, teikiančio pranešimą apie pažeidžiamumą, anonimiškumą. Jeigu pažeidžiamumas, apie kurį pranešta, galėtų daryti didelį poveikį subjektams daugiau nei vienoje valstybėje narėje, kiekvienos susijusios valstybės narės koordinatore paskirta CSIRT, kai tinkama, CSIRT tinkle bendradarbiauja su kitomis koordinatorėmis paskirtomis CSIRT.

2. ENISA, pasikonsultavusi su Bendradarbiavimo grupe, sukuria ir tvarko Europos pažeidžiamumų duomenų bazę. Tuo tikslu ENISA sukuria ir tvarko tinkamas informacines sistemas, politiką ir procedūras ir priima Europos pažeidžiamumų duomenų bazės saugumui ir vientisumui užtikrinti būtinas technines ir organizacines priemones, visų pirma siekdama sudaryti sąlygas subjektams, nepriklausomai nuo to, ar jie patenka į šios direktyvos taikymo sritį, bei jų tinklų ir informacinių sistemų tiekėjams, savanoriškai atskleisti ir registruoti viešai žinomas IRT produktų ar IRT paslaugų pažeidžiamumus. Visiems suinteresuotiesiems subjektams suteikiama prieiga prie Europos pažeidžiamumų duomenų bazėje esančios informacijos apie pažeidžiamumus. Toje duomenų bazėje pateikiama:

a) informacija, kuria apibūdinamas pažeidžiamumas;

b) paveikti IRT produktai ar IRT paslaugos ir pažeidžiamumų rimtumas, atsižvelgiant į aplinkybes, kuriomis juo gali būti pasinaudota;

c) informacija apie susijusių pataisų prieinamumą ir, jei pataisų nėra, pažeidžiamų IRT produktų ir IRT paslaugų naudotojams skirtos kompetentingų institucijų arba CSIRT pateiktos gairės, kaip galima sumažinti dėl atskleistų pažeidžiamumų kylančią riziką.

13 straipsnis

Bendradarbiavimas nacionaliniu lygmeniu

1. Kai tos pačios valstybės narės kompetentingos institucijos, bendrasis kontaktinis punktas ir CSIRT yra atskiri, jie bendradarbiauja tarpusavyje, kad vykdytų šioje direktyvoje nustatytas pareigas.

2. Valstybės narės užtikrina, kad jų CSIRT arba, kai taikytina, kompetentingos institucijos gautų pranešimus apie didelius incidentus pagal 23 straipsnį ir incidentus, dideles kibernetines grėsmes ir vos neįvykusius incidentus pagal 30 straipsnį.

3. Valstybės narės užtikrina, kad jų CSIRT arba, kai taikytina, kompetentingos institucijos informuotų savo bendruosius kontaktinius punktus apie šioje direktyvoje nustatyta tvarka pateikiamus pranešimus apie incidentus, kibernetines grėsmes ir vos neįvykusius incidentus.

4. Siekiant užtikrinti, kad kompetentingų institucijų, bendrųjų kontaktinių punktų ir CSIRT užduotys ir pareigos būtų vykdomos veiksmingai, valstybės narės užtikrina tinkamą tų įstaigų ir teisėsaugos institucijų, duomenų apsaugos institucijų, nacionalinių institucijų pagal reglamentus (EB) Nr. 300/2008 ir (ES) 2018/1139, priežiūros įstaigų pagal Reglamentą (ES) Nr. 910/2014, kompetentingų institucijų pagal Reglamentą (ES) 2022/2554, nacionalinių reguliavimo institucijų pagal Direktyvą (ES) 2018/1972, kompetentingų institucijų pagal Direktyvą (ES) 2022/2557, taip pat kompetentingų institucijų pagal kitus konkretiems sektoriams taikomus Sąjungos teisės aktus bendradarbiavimą toje valstybėje narėje.

5. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą ir jų kompetentingos institucijos pagal Direktyvą (ES) 2022/2557 bendradarbiautų ir reguliariai keistųsi informacija, kiek tai susiję su ypatingos svarbos subjektų identifikavimu, apie riziką, kibernetines grėsmes, ir incidentus, taip pat apie nekibernetinę riziką, grėsmes ir incidentus, darančius poveikį subjektams, kurie pagal Direktyvą (ES) 2022/2557 identifikuoti kaip ypatingos svarbos subjektai, ir apie priemones, kurių imtasi reaguojant į tą riziką, grėsmes ir incidentus. Valstybės narės taip pat užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą ir jų kompetentingos institucijos pagal Reglamentą (ES) Nr. 910/2014, Reglamentą (ES) 2022/2554 ir Direktyvą (ES) 2018/1972 reguliariai keistųsi atitinkama informacija, be kita ko, susijusia su atitinkamais incidentais ir kibernetinėmis grėsmėmis.

6. Valstybės narės techninėmis priemonėmis supaprastina informacijos, susijusios su 23 ir 30 straipsniuose nurodytais pranešimais, teikimą.

III SKYRIUS

BENDRADARBIAVIMAS SĄJUNGOS IR TARPTAUTINIU LYGMENIMIS

14 straipsnis

Bendradarbiavimo grupė

1. Siekiant remti ir palengvinti strateginį bendradarbiavimą ir keitimąsi informacija tarp valstybių narių, taip pat sustiprinti pasitikėjimą ir patikimumą, sudaroma Bendradarbiavimo grupė.

2. Bendradarbiavimo grupė vykdo savo užduotis remdamasi dvimetėmis darbo programomis, nurodytomis 7 dalyje.

3. Bendradarbiavimo grupę sudaro valstybių narių, Komisijos ir ENISA atstovai. Europos išorės veiksmų tarnyba Bendradarbiavimo grupėje dalyvauja stebėtojos teisėmis. Europos priežiūros institucijos (EPI) ir kompetentingos institucijos pagal Reglamentą (ES) 2022/2554 gali dalyvauti Bendradarbiavimo grupės veikloje pagal to reglamento 47 straipsnio 1 dalį.

Prireikus Bendradarbiavimo grupė gali pakviesti Europos Parlamentą ir atitinkamų suinteresuotųjų subjektų atstovus dalyvauti jos darbe.

Komisija teikia sekretoriato paslaugas.

4. Bendradarbiavimo grupė vykdo šias užduotis:

a) teikia kompetentingoms institucijoms gaires dėl šios direktyvos perkėlimo į nacionalinę teisę ir įgyvendinimo;

b) teikia kompetentingoms institucijoms gaires, susijusias su koordinuoto pažeidžiamumų atskleidimo politikos plėtojimu ir įgyvendinimu, kaip nurodyta 7 straipsnio 2 dalies c punkte;

c) keičiasi geriausios praktikos pavyzdžiais ir informacija, susijusia su šios direktyvos įgyvendinimu, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, incidentais, pažeidžiamumais, vos neįvykusiais incidentais, informuotumo didinimo iniciatyvomis, mokymu, pratybomis ir įgūdžiais, gebėjimų stiprinimu, standartais ir techninėmis specifikacijomis, taip pat su esminių ir svarbių subjektų identifikavimu pagal 2 straipsnio 2 dalies b–e punktus;

d) keičiasi patarimais ir bendradarbiauja su Komisija dėl naujų kibernetinio saugumo politikos iniciatyvų ir bendro konkretiems sektoriams taikomų kibernetinio saugumo reikalavimų nuoseklumo;

e) keičiasi patarimais ir bendradarbiauja su Komisija dėl deleguotųjų arba įgyvendinimo aktų, priimamų pagal šią direktyvą, projektų;

f) keičiasi geriausios praktikos pavyzdžiais ir informacija su atitinkamomis Sąjungos institucijomis, įstaigomis, organais ir agentūromis;

g) keičiasi nuomonėmis dėl konkretiems sektoriams taikomų Sąjungos teisės aktų, kuriuose yra nuostatų dėl kibernetinio saugumo, įgyvendinimo;

h) kai tinkama, aptaria 19 straipsnio 9 dalyje nurodytas tarpusavio vertinimo ataskaitas ir parengia išvadas ir rekomendacijas;

i) atlieka koordinuojamus ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimus pagal 22 straipsnio 1 dalį;

j) aptaria savitarpio pagalbos atvejus, įskaitant patirtį ir rezultatus, susijusius su bendrais tarpvalstybiniais priežiūros veiksmais, kaip nurodyta 37 straipsnyje;

k) vienos ar daugiau atitinkamų valstybių narių prašymu aptaria konkrečius savitarpio pagalbos prašymus, nurodytus 37 straipsnyje;

l) teikia strategines gaires CSIRT tinklui ir EU–CyCLONe konkrečiais kylančiais klausimais;

m) keičiasi nuomonėmis dėl politikos dėl tolesnių veiksmų po didelio masto kibernetinio saugumo incidentų ir krizių remiantis CSIRT tinklo ir EU-CyCLONe patirtimi;

n) prisideda prie kibernetinio saugumo pajėgumų visoje Sąjungoje palengvindama nacionalinių pareigūnų mainus pagal gebėjimų stiprinimo programą, kurioje dalyvauja kompetentingų institucijų arba CSIRT darbuotojai;

o) organizuoja nuolatinius bendrus susitikimus su atitinkamais privačiais suinteresuotaisiais subjektais iš visos Sąjungos, kad aptartų Bendradarbiavimo grupės vykdomą veiklą ir surinktų informacijos apie naujus politikos uždavinius;

p) aptaria su kibernetinio saugumo pratybomis susijusį darbą, įskaitant ENISA atliktą darbą;

q) nustato 19 straipsnio 1 dalyje nurodytų tarpusavio vertinimų metodiką ir organizacinius aspektus, taip pat, padedant Komisijai ir ENISA, pagal 19 straipsnio 5 dalį nustato valstybėms narėms savęs vertinimo metodiką, ir, bendradarbiaudama su Komisija ir ENISA, parengia elgesio kodeksus, kuriais grindžiami pagal 19 straipsnio 6 dalį paskirtų kibernetinio saugumo ekspertų darbo metodai;

r) 40 straipsnyje nurodytos peržiūros tikslais rengia Komisijai strateginiu lygmeniu ir atliekant tarpusavio vertinimus sukauptos patirties ataskaitas;

s) aptaria ir reguliariai vertina kibernetinių grėsmių ar incidentų, pavyzdžiui, susijusių su išpirkos reikalavimo programine įranga, padėtį.

Bendradarbiavimo grupė teikia pirmos pastraipos r punkte nurodytas ataskaitas Komisijai, Europos Parlamentui ir Tarybai.

5. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų savo atstovų Bendradarbiavimo grupėje bendradarbiavimą.

6. Bendradarbiavimo grupė gali prašyti, kad CSIRT tinklas parengtų techninę ataskaitą pasirinktomis temomis.

7. Ne vėliau kaip 2024 m. vasario 1 d., o vėliau – kas dvejus metus Bendradarbiavimo grupė parengia darbo programą, skirtą veiksmams, kurių reikia imtis jos tikslams ir užduotims įgyvendinti.

8. Komisija gali priimti įgyvendinimo aktus, kuriais nustatoma procedūrinė tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti.

Tie įgyvendinimo aktai priimami laikantis 39 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

Komisija keičiasi rekomendacijomis ir bendradarbiauja su Bendradarbiavimo grupe dėl šios dalies pirmoje pastraipoje nurodytų įgyvendinimo aktų projektų pagal 4 dalies e punktą.

9. Bendradarbiavimo grupė nuolat ir ne rečiau kaip kartą per metus susitinka su Ypatingos svarbos subjektų atsparumo klausimų grupe, sudaryta pagal Direktyvą (ES) 2022/2557, kad skatintų ir palengvintų strateginį bendradarbiavimą ir keitimąsi informacija.

15 straipsnis

CSIRT tinklas

1. Siekiant prisidėti prie pasitikėjimo ir atsakomybės didinimo, taip pat skatinti greitą ir veiksmingą valstybių narių operatyvinį bendradarbiavimą, sukuriamas nacionalinių CSIRT tinklas.

2. CSIRT tinklą sudaro pagal 10 straipsnį paskirtų arba įsteigtų CSIRT ir Sąjungos institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos (CERT-EU) atstovai. Komisija dalyvauja CSIRT tinklo veikloje stebėtojos teisėmis. ENISA teikia sekretoriato paslaugas ir aktyviai teikia pagalbą CSIRT tarpusavio bendradarbiavimo srityje.

3. CSIRT tinklas vykdo šias užduotis:

a) keičiasi informacija apie CSIRT pajėgumus;

b) padeda CSIRT tarpusavyje dalytis technologijomis ir atitinkamomis priemonėmis, politika, įrankiais, procesais, geriausios praktikos pavyzdžiais ir sistemomis ir juos perduoti bei jais keistis;

c) keičiasi svarbia informacija apie incidentus, vos neįvykusius incidentus, kibernetines grėsmes, riziką ir pažeidžiamumus;

d) keičiasi informacija apie kibernetinio saugumo leidinius ir rekomendacijas;

e) užtikrina sąveikumą, susijusį su dalijimosi informacija specifikacijomis ir protokolais;

f) CSIRT tinklo, kuris galėjo būti paveiktas incidento, nario prašymu keičiasi informacija, susijusia su tuo incidentu ir atitinkamomis kibernetinėmis grėsmėmis, rizika ir pažeidžiamumais, ir ją aptaria;

g) CSIRT tinklo nario prašymu aptaria ir, kai įmanoma, įgyvendina koordinuotą atsaką į incidentą, nustatytą tos valstybės narės jurisdikcijoje;

h) teikia valstybėms narėms pagalbą šalinant tarpvalstybinius incidentus pagal šią direktyvą;

i) bendradarbiauja, keičiasi geriausios praktikos pavyzdžiais ir teikia pagalbą pagal 12 straipsnio 1 dalį koordinatorėmis paskirtoms CSIRT, kiek tai susiję su koordinuoto pažeidžiamumų, galinčių daryti didelį poveikį subjektams daugiau nei vienoje valstybėje narėje, atskleidimo valdymu;

j) aptaria ir nustato tolesnes operatyvinio bendradarbiavimo formas, be kita ko, susijusias su:

   i) kibernetinių grėsmių ir incidentų kategorijomis;

   ii) ankstyvaisiais perspėjimais;

   iii) savitarpio pagalba;

   iv) koordinavimo principais ir tvarka reaguojant į tarpvalstybinę riziką ir incidentus;

   v) pagalba rengiant nacionalinį reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planą, nurodytą 9 straipsnio 4 dalyje, teikiama valstybės narės prašymu;

k) informuoja Bendradarbiavimo grupę apie savo veiklą ir tolesnes operatyvinio bendradarbiavimo formas, aptartas pagal j punktą, ir prireikus prašo tuo klausimu pateikti rekomendacijų;

l) įvertina kibernetinio saugumo pratybas, įskaitant ENISA organizuojamas pratybas;

m) atskiros CSIRT prašymu aptaria tos CSIRT pajėgumus ir parengtį;

n) bendradarbiauja ir keičiasi informacija su regioniniais ir Sąjungos lygmens saugumo operacijų centrais (SOC), kad pagerintų bendrą informuotumą apie padėtį, susijusią su incidentais ir grėsmėmis visoje Sąjungoje;

o) kai tinkama, aptaria 19 straipsnio 9 dalyje nurodytas tarpusavio vertinimo ataskaitas;

p) teikia gaires siekiant palengvinti operatyvinės praktikos konvergenciją taikant šio straipsnio nuostatas dėl operatyvinio bendradarbiavimo.

4. Ne vėliau kaip 2025 m. sausio 17 d., o vėliau – kas dvejus metus CSIRT tinklas 40 straipsnyje nurodytos priežiūros tikslais įvertina padarytą pažangą operatyvinio bendradarbiavimo srityje ir patvirtina ataskaitą. Ataskaitoje visų pirma pateikiamos išvados ir rekomendacijos, grindžiamos 19 straipsnyje nurodytų tarpusavio vertinimų, atliktų dėl nacionalinių CSIRT, rezultatais. Ta ataskaita pateikiama Bendradarbiavimo grupei.

5. CSIRT tinklas priima savo darbo tvarkos taisykles.

6. CSIRT tinklas ir EU-CyCLONe susitaria dėl procedūrinės tvarkos ir ja remdamiesi bendradarbiauja.

16 straipsnis

Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas (EU-CyCLONe)

1. Siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą operatyviniu lygmeniu ir užtikrinti reguliarų keitimąsi svarbia informacija tarp valstybių narių ir Sąjungos institucijų, įstaigų, organų ir agentūrų, įsteigiamas EU-CyCLONe.

2. EU-CyCLONe sudaro valstybių narių kibernetinių krizių valdymo institucijų atstovai, taip pat tais atvejais, kai galimas arba vykstantis didelio masto kibernetinio saugumo incidentas turi arba gali turėti didelį poveikį paslaugoms ir veiklai, kurioms taikoma ši direktyva – Komisijos atstovai. Kitais atvejais Komisija dalyvauja EU-CyCLONe veikloje stebėtojo teisėmis.

ENISA teikia EU-CyCLONe sekretoriato paslaugas ir padeda saugiai keistis informacija, taip pat teikia būtinas priemones valstybių narių tarpusavio bendradarbiavimui remti, užtikrinančias saugų keitimąsi informacija.

Kai tikslinga, EU-CyCLONe gali pakviesti atitinkamų suinteresuotųjų subjektų atstovus dalyvauti jo darbe stebėtojų teisėmis.

3. EU-CyCLONe vykdo šias užduotis:

a) didina pasirengimo valdyti didelio masto kibernetinio saugumo incidentus ir krizes lygį;

b) plėtoja bendrą informuotumą apie padėtį, susijusią su didelio masto kibernetinio saugumo incidentais ir krizėmis;

c) įvertina atitinkamų didelio masto kibernetinio saugumo incidentų pasekmes ir poveikį ir siūlo galimas švelninimo priemones;

d) koordinuoja didelio masto kibernetinio saugumo incidentų ir krizių valdymą ir padeda politiniu lygmeniu priimti sprendimus, susijusius su tokiais incidentais ir krizėmis;

e) atitinkamos valstybės narės prašymu aptaria 9 straipsnio 4 dalyje nurodytus nacionalinius reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planus.

4. EU-CyCLONe priima savo darbo tvarkos taisykles.

5. EU-CyCLONe reguliariai teikia ataskaitas Bendradarbiavimo grupei apie didelio masto kibernetinio saugumo incidentų ir krizių valdymą, taip pat apie tendencijas, ypatingą dėmesį skirdamas jų poveikiui esminiams ir svarbiems subjektams.

6. EU-CyCLONe su CSIRT tinklu bendradarbiauja remdamasis sutartomis procedūrinėmis taisyklėmis, numatytomis 15 straipsnio 6 dalyje.

7. Ne vėliau kaip 2024 m. liepos 17 d., o vėliau – kas 18 mėnesių EU-CyCLONe teikia Europos Parlamentui ir Tarybai savo darbo įvertinimo ataskaitą.

17 straipsnis

Tarptautinis bendradarbiavimas

Pagal SESV 218 straipsnį Sąjunga, kai tinkama, gali sudaryti tarptautinius susitarimus su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis, pagal kuriuos joms būtų leidžiama dalyvauti tam tikroje Bendradarbiavimo grupės, CSIRT tinklo ir EU-CyCLONe veikloje ir toks dalyvavimas būtų organizuojamas. Tokie susitarimai turi atitikti Sąjungos duomenų apsaugos teisės aktus.

18 straipsnis

Kibernetinio saugumo būklės Sąjungoje ataskaita

1. ENISA, bendradarbiaudama su Komisija ir Bendradarbiavimo grupe, kas dvejus metus patvirtina kibernetinio saugumo Sąjungoje būklės ataskaitą ir tą ataskaitą pateikia ir pristato Europos Parlamentui. Ataskaita, *inter alia*, paskelbiama kaip kompiuterio skaitomi duomenys ir į ją turi būti įtraukti šie aspektai:

a) Sąjungos lygmens kibernetinio saugumo rizikos vertinimas, kuriame atsižvelgiama į kibernetinių grėsmių padėtį;

b) kibernetinio saugumo pajėgumų plėtojimo viešajame ir privačiajame sektoriuose visoje Sąjungoje vertinimas;

c) piliečių ir subjektų, įskaitant mažąsias ir vidutines įmones, bendro informuotumo apie kibernetinį saugumą ir kibernetinės higienos lygio vertinimas;

d) 19 straipsnyje nurodytų tarpusavio vertinimų rezultatų apibendrintas vertinimas;

e) apibendrintas kibernetinio saugumo pajėgumų ir išteklių brandos lygio visoje Sąjungoje, be kita ko, sektorių lygmeniu, taip pat valstybių narių nacionalinių kibernetinio saugumo strategijų suderinimo masto vertinimas.

2. Ataskaitoje pateikiamos konkrečios politikos rekomendacijos, kaip pašalinti trūkumus ir padidinti kibernetinio saugumo lygį visoje Sąjungoje, ir konkretaus laikotarpio išvadų santrauka iš agentūros ES kibernetinio saugumo techninės padėties ataskaitų dėl incidentų ir kibernetinių grėsmių, kurias pagal Reglamento (ES) 2019/881 7 straipsnio 6 dalį parengė ENISA.

3. ENISA, bendradarbiaudama su Komisija, Bendradarbiavimo grupe ir CSIRT tinklu, parengia metodiką, į kurią būtų įtraukiami atitinkami 1 dalies e punkte nurodyto apibendrinto vertinimo kintamieji, pavyzdžiui, kiekybiniai ir kokybiniai rodikliai.

19 straipsnis

Tarpusavio vertinimai

1. Bendradarbiavimo grupė, padedant Komisijai ir ENISA bei, kai tinkama, CSIRT, ne vėliau kaip 2025 m. sausio 17 d. nustato tarpusavio vertinimų metodiką ir organizacinius aspektus, kad būtų galima pasimokyti iš bendros patirties, stiprinti tarpusavio pasitikėjimą, pasiekti aukštą bendrą kibernetinio saugumo lygį, taip pat stiprinti valstybių narių kibernetinio saugumo pajėgumus ir politiką, būtinus šiai direktyvai įgyvendinti. Dalyvavimas tarpusavio vertinimuose yra savanoriškas. Tarpusavio vertinimus atlieka kibernetinio saugumo ekspertai. Kibernetinio saugumo ekspertus skiria bent dvi valstybės narės, kurios nėra vertinamosios valstybės narės.

Tarpusavio vertinimai apima bent vieną iš šių aspektų:

a) kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti, įtvirtintų 21 ir 23 straipsniuose, įgyvendinimo lygį;

b) gebėjimų lygį, įskaitant turimus finansinius, techninius ir žmogiškuosius išteklius, ir kompetentingų institucijų užduočių vykdymo veiksmingumą;

c) CSIRT operatyvinius pajėgumus;

d) 37 straipsnyje nurodytos savitarpio pagalbos įgyvendinimo lygį;

e) 29 straipsnyje nurodytų keitimosi kibernetinio saugumo informacija susitarimų įgyvendinimo lygį;

f) konkrečius tarpvalstybinio arba tarpsektorinio pobūdžio klausimus.

2. 1 dalyje nurodyta metodika apima objektyvius, nediskriminacinius, sąžiningus ir skaidrius kriterijus, kuriais remdamosi valstybės narės paskiria kibernetinio saugumo ekspertus, atitinkančius reikalavimus tarpusavio vertinimui atlikti. Komisija ir ENISA dalyvauja tarpusavio vertinimuose stebėtojų teisėmis.

3. Valstybės narės gali nustatyti konkrečius 1 dalies f punkte nurodytus klausimus tarpusavio vertinimui.

4. Prieš pradėdamos 1 dalyje nurodytą tarpusavio vertinimą, valstybės narės praneša dalyvaujančioms valstybėms narėms jo apimtį, įskaitant konkrečius klausimus, nustatytus pagal 3 dalį.

5. Prieš pradėdamos tarpusavio vertinimą, valstybės narės gali pačios įvertinti vertinamus aspektus ir pateikti tą įsivertinimą paskirtiems kibernetinio saugumo ekspertams. Bendradarbiavimo grupė, padedant Komisijai ir ENISA, nustato valstybių narių įsivertinimo metodiką.

6. Tarpusavio vertinimai apima fizinius arba virtualius apsilankymus vietoje ir keitimąsi informacija ne vietoje. Laikantis gero bendradarbiavimo principo, valstybės narės, kurioms taikomas tarpusavio vertinimas, pateikia paskirtiems kibernetinio saugumo ekspertams vertinimui atlikti reikalingą informaciją; tai daroma nedarant poveikio Sąjungos ar nacionalinei teisei dėl konfidencialios ar įslaptintos informacijos apsaugos ir esminių valstybės funkcijų, pavyzdžiui, nacionalinio saugumo, apsaugai. Bendradarbiavimo grupė, bendradarbiaudama su Komisija ir ENISA, parengia atitinkamus elgesio kodeksus, kuriais grindžiami paskirtų kibernetinio saugumo ekspertų darbo metodai. Visa per tarpusavio vertinimą gauta informacija naudojama tik tam vertinimui. Tarpusavio vertinime dalyvaujantys kibernetinio saugumo ekspertai neatskleidžia jokios per tą tarpusavio vertinimą gautos neskelbtinos ar konfidencialios informacijos jokioms trečiosioms šalims.

7. Atlikus tarpusavio vertinimą, tų pačių valstybėje narėje peržiūrėtų aspektų tolesnis tarpusavio vertinimas toje valstybėje narėje dvejus metus po tarpusavio vertinimo pabaigos neatliekamas, nebent valstybė narė prašytų arba Bendradarbiavimo grupei pasiūlius būtų susitarta kitaip.

8. Valstybės narės užtikrina, kad bet kokia su paskirtais kibernetinio saugumo ekspertais susijusi interesų konflikto rizika būtų atskleista kitoms valstybėms narėms, Bendradarbiavimo grupei, Komisijai ir ENISA prieš pradedant tarpusavio vertinimą. Valstybė narė, kuriai taikomas tarpusavio vertinimas, gali dėl tinkamai pagrįstų priežasčių, apie kurias pranešta paskiriančiai valstybei narei, paprieštarauti tam, kad būtų paskirti konkretūs kibernetinio saugumo ekspertai.

9. Tarpusavio vertinimuose dalyvaujantys kibernetinio saugumo ekspertai parengia per tarpusavio vertinimus nustatytų faktų ir išvadų ataskaitas. Valstybės narės, kurioms taikomas tarpusavio vertinimas, gali teikti pastabas dėl su jomis susijusių ataskaitų projektų ir tokios pastabos pridedamos prie ataskaitų. Ataskaitose pateikiamos rekomendacijos, kaip pagerinti aspektus, kuriuos apėmė tarpusavio vertinimas. Kai tinkama, ataskaitos pateikiamos Bendradarbiavimo grupei ir CSIRT tinklui. Valstybė narė, kuriai taikomas tarpusavio vertinimas, gali nuspręsti savo ataskaitą arba jos redaguotą versiją padaryti viešai prieinamą.

IV SKYRIUS

KIBERNETINIO SAUGUMO RIZIKOS VALDYMO PRIEMONĖS IR PAREIGOS PRANEŠTI

20 straipsnis

Valdymas

1. Valstybės narės užtikrina, kad esminių ir svarbių subjektų valdymo organai patvirtintų kibernetinio saugumo rizikos valdymo priemones, kurių ėmėsi tie subjektai, siekdami laikytis 21 straipsnio, prižiūrėtų jo įgyvendinimą ir galėtų būti patraukti atsakomybėn už tai, kad subjektai pažeidžia tą straipsnį.

Šios dalies taikymu nedaromas poveikis nacionalinės teisės aktams, susijusiems su atsakomybės taisyklėmis, taikomomis viešosioms institucijoms, taip pat valstybės tarnautojų ir renkamų ar paskirtų pareigūnų atsakomybe.

2. Valstybės narės užtikrina, kad esminių ir svarbių subjektų valdymo organų nariai turėtų dalyvauti mokymuose, ir skatina esminius ir svarbius subjektus reguliariai siūlyti panašius mokymus savo darbuotojams, kad jie įgytų pakankamai žinių ir įgūdžių, kad galėtų nustatyti riziką ir įvertinti kibernetinio saugumo rizikos valdymo praktiką bei jos poveikį subjekto teikiamoms paslaugoms.

21 straipsnis

Kibernetinio saugumo rizikos valdymo priemonės

1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai imtųsi tinkamų ir proporcingų techninių, operatyvinių ir organizacinių priemonių, siekdami valdyti tinklų ir informacinių sistemų, kurias tie subjektai naudoja savo veiklai arba teikdami savo paslaugas, saugumui kylančią riziką ir užkirsti kelią incidentų poveikiui jų paslaugų gavėjams ir kitoms paslaugoms arba juos sumažinti iki minimumo.

Atsižvelgiant į naujausius technikos laimėjimus ir, kai taikytina, atitinkamus Europos ir tarptautinius standartus, taip pat į įgyvendinimo sąnaudas, pirmoje pastraipoje nurodytomis priemonėmis užtikrinamas toks tinklų ir informacinių sistemų saugumo lygis, kuris atitinka kilusią riziką. Vertinant tų priemonių proporcingumą, tinkamai atsižvelgiama į subjekto galimybės patirti riziką laipsnį, subjekto dydį ir incidentų tikimybę bei jų sunkumą, įskaitant jų socialinį ir ekonominį poveikį.

2. 1 dalyje nurodytos priemonės grindžiamos visus pavojus apimančiu požiūriu, kuriuo siekiama apsaugoti tinklų ir informacines sistemas bei jų fizinę aplinką nuo incidentų, ir jos apima bent šiuos elementus:

a) rizikos analizės ir informacinių sistemų saugumo politiką;

b) incidentų valdymą;

c) veiklos tęstinumą, pvz., atsarginių kopijų valdymą ir veiklos atkūrimą po ekstremaliųjų įvykių, ir krizių valdymą;

d) tiekimo grandinės saugumą, įskaitant su saugumu susijusius aspektus, susijusius su kiekvieno subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykiais;

e) tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumą, įskaitant pažeidžiamumo valdymą ir atskleidimą;

f) politiką ir procedūras, skirtas kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti;

g) pagrindinę kibernetinės higienos praktiką ir kibernetinio saugumo mokymus;

h) kriptografijos ir, kai taikytina, šifravimo naudojimo politiką ir procedūras;

i) žmogiškųjų išteklių saugumą, prieigos kontrolės politiką ir turto valdymą;

j) kai taikytina, kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą.

3. Valstybės narės užtikrina, kad, subjektai, svarstydami, kurios šio straipsnio 2 dalies d punkte nurodytos priemonės yra tinkamos, atsižvelgtų į kiekvieno tiesioginio tiekėjo ir paslaugų teikėjo pažeidžiamumą ir į jų tiekėjų ir paslaugų teikėjų produktų bendrą kokybę ir kibernetinio saugumo praktiką, įskaitant jų saugumo plėtojimo procedūras. Valstybės narės taip pat užtikrina, kad subjektai, svarstydami, kurios tame punkte nurodytos priemonės yra tinkamos, privalėtų atsižvelgti į pagal 22 straipsnio 1 dalį atliktų koordinuojamų ypatingos svarbos tiekimo grandinių rizikos vertinimų rezultatus.

4. Valstybės narės užtikrina, kad subjektas, kuris nustato, kad jis nesilaiko 2 dalyje numatytų priemonių, nepagrįstai nedelsdamas imtųsi visų būtinų, tinkamų ir proporcingų taisomųjų priemonių.

5. Komisija ne vėliau kaip 2024 m. spalio 17 d. priima įgyvendinimo aktus, kuriais nustatomi 2 dalyje nurodytų priemonių techniniai ir metodiniai reikalavimai, taikomi DNS paslaugų teikėjams, aukščiausio lygio domenų vardų registrams, debesijos kompiuterijos paslaugų teikėjams, duomenų centrų paslaugų teikėjams, turinio teikimo tinklo teikėjams, valdomų paslaugų teikėjams, valdomų saugumo paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų ir patikimumo užtikrinimo paslaugų teikėjams.

Komisija gali priimti įgyvendinimo aktus, kuriais nustatomi 2 dalyje nurodytų priemonių būtinieji techniniai ir metodiniai reikalavimai, taip pat sektoriams taikomi reikalavimai, taikomi kitiems esminiams ir svarbiems subjektams nei nurodytieji šios dalies pirmoje pastraipoje.

Rengdama šios dalies pirmoje ir antroje pastraipose nurodytus įgyvendinimo aktus, Komisija, kiek įmanoma, laikosi Europos ir tarptautinių standartų bei atitinkamų techninių specifikacijų. Komisija keičiasi rekomendacijomis ir bendradarbiauja su Bendradarbiavimo grupe ir ENISA dėl įgyvendinimo aktų projektų pagal 14 straipsnio 4 dalies e punktą.

Tie įgyvendinimo aktai priimami laikantis 39 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

22 straipsnis

Sąjungos lygmeniu koordinuojami ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimai

1. Bendradarbiavimo grupė, bendradarbiaudama su Komisija ir ENISA, gali atlikti koordinuotus konkrečių ypatingos svarbos IRT paslaugų, IRT sistemų ar IRT produktų tiekimo grandinių saugumo rizikos vertinimus, atsižvelgdama į techninius ir, kai tinkama, netechninius rizikos veiksnius.

2. Komisija, pasikonsultavusi su Bendradarbiavimo grupe ir ENISA bei prireikus su atitinkamais suinteresuotaisiais subjektais, nustato konkrečias ypatingos svarbos IRT paslaugas, IRT sistemas ar IRT produktus, dėl kurių gali būti atliekamas 1 dalyje nurodytas koordinuotas saugumo rizikos vertinimas.

23 straipsnis

Pareigos pranešti

1. Kiekviena valstybė narė užtikrina, kad esminiai ir svarbūs subjektai nepagrįstai nedelsdami praneštų valstybės narės CSIRT arba, kai taikytina, jos kompetentingai institucijai pagal 4 dalį apie bet kokį incidentą, darantį didelį poveikį jų paslaugų teikimui, kaip nurodyta 3 dalyje (toliau – didelis incidentas). Kai tinkama, atitinkami subjektai nepagrįstai nedelsdami praneša jų paslaugų gavėjams apie didelius incidentus, kurie gali turėti neigiamos įtakos tų paslaugų teikimui. Kiekviena valstybė narė užtikrina, kad tie subjektai, *inter alia*, praneštų visą informaciją, pagal kurią CSIRT arba, kai taikytina, kompetentinga institucija galėtų nustatyti tarpvalstybinį incidento poveikį. Vien dėl pranešimo veiksmo negali būti padidinama pranešančiojo subjekto atsakomybė.

Jei atitinkami subjektai praneša kompetentingai institucijai apie didelį incidentą pagal pirmą pastraipą, valstybė narė užtikrina, kad ta kompetentinga institucija, gavusi pranešimą, perduotų jį CSIRT.

Tarpvalstybinio arba tarpsektorinio didelio incidento atveju valstybės narės užtikrina, kad jų bendrieji kontaktiniai punktai laiku gautų atitinkamą informaciją, apie kurią pranešta pagal 4 dalį.

2. Kai taikytina, valstybės narės užtikrina, kad esminiai ir svarbūs subjektai nepagrįstai nedelsdami informuotų savo paslaugų gavėjus, kuriuos didelė kibernetinė grėsmė galėjo paveikti, apie visas priemones ar teisių gynimo priemones, kurių tie gavėjai gali imtis reaguodami į tą grėsmę. Atitinkamais atvejais subjektai taip pat praneša tiems gavėjams apie pačią didelę kibernetinę grėsmę.

3. Incidentas laikomas dideliu, jeigu:

a) dėl jo atitinkamas subjektas patyrė arba gali patirti didelių paslaugų teikimo sutrikimų arba finansinių nuostolių;

b) jis paveikė arba gali paveikti kitus fizinius ar juridinius asmenis sukeldamas didelę turtinę arba neturtinę žalą.

4. Valstybės narės užtikrina, kad 1 dalyje nurodyto pranešimo tikslais atitinkami subjektai CSIRT arba, kai taikytina, kompetentingai institucijai pateiktų:

a) nepagrįstai nedelsdami ir bet kuriuo atveju per 24 valandas nuo tada, kai sužinojo apie didelį incidentą, – ankstyvąjį perspėjimą, kuriame, kai taikytina, nurodoma, ar didelį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis galėtų daryti tarpvalstybinį poveikį;

b) nepagrįstai nedelsdami ir bet kuriuo atveju per 72 valandas nuo tada, kai sužinojo apie didelį incidentą, – pranešimą apie incidentą, kuriame, kai taikytina, atnaujinama a) punkte nurodyta informacija ir nurodomas didelio incidento, įskaitant jo sunkumą ir poveikį, pradinis vertinimas, taip pat nurodomi užvaldymo rodikliai, jei tokių yra;

c) CSIRT arba, kai taikytina, kompetentingos institucijos prašymu – tarpinę ataskaitą apie atitinkamus atnaujintus duomenis apie padėtį;

d) ne vėliau kaip per vieną mėnesį nuo b punkte nurodyto pranešimo apie incidentą – galutinę ataskaitą, kurioje pateikiama ši informacija:

   i) išsamus incidento, įskaitant jo sunkumą ir poveikį, aprašymas;

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

   iii) taikomos ir įgyvendinamos poveikio mažinimo priemonės;

   iv) kai taikytina, tarpvalstybinis incidento poveikis;

e) tuo atveju, jei d punkte nurodytos galutinės ataskaitos pateikimo metu incidentas tebevyksta, valstybės narės užtikrina, kad atitinkami subjektai tuo metu pateiktų pažangos ataskaitą, o galutinę ataskaitą – per vieną mėnesį nuo tada, kai suvaldė incidentą.

Nukrypstant nuo pirmos pastraipos b punkto, patikimumo užtikrinimo paslaugų teikėjas didelių incidentų, darančių poveikį jo patikimumo užtikrinimo paslaugų teikimui, atveju nepagrįstai nedelsdamas ir bet kuriuo atveju per 24 valandas nuo tada, kai sužinojo apie didelį incidentą, apie tai praneša CSIRT arba, kai taikytina, kompetentingai institucijai.

5. CSIRT arba kompetentinga institucija nepagrįstai nedelsdama ir, kai įmanoma, – per 24 valandas nuo 4 dalies a punkte nurodyto ankstyvojo perspėjimo gavimo pateikia atsakymą pranešančiajam subjektui, įskaitant pirminę grįžtamąją informaciją apie didelį incidentą, ir, subjekto prašymu – galimų rizikos mažinimo priemonių įgyvendinimo gaires arba operacinių patarimų. Jei CSIRT nėra pradinis 1 dalyje nurodyto pranešimo gavėjas, gaires teikia kompetentinga institucija, bendradarbiaudama su CSIRT. CSIRT teikia papildomą techninę pagalbą, jei to prašo atitinkamas subjektas. Jei įtariama, kad didelis incidentas yra baudžiamojo pobūdžio, CSIRT arba kompetentinga institucija taip pat teikia gaires dėl pranešimo apie didelį incidentą teisėsaugos institucijoms.

6. Kai taikytina ir visų pirma tuomet, kai didelis incidentas yra susijęs su dviem ar daugiau valstybių narių, CSIRT, kompetentinga institucija arba bendrasis kontaktinis punktas nepagrįstai nedelsdami informuoja apie didelį incidentą kitas paveiktas valstybes nares, ir ENISA. Tokia informacija apima pagal 4 dalį gautos informacijos rūšį. Tai darydami CSIRT, kompetentinga institucija ar bendrasis kontaktinis punktas, laikydamiesi Sąjungos arba nacionalinės teisės, saugo subjekto saugumo ir komercinius interesus, taip pat pateiktos informacijos konfidencialumą.

7. Kai visuomenės informuotumas yra būtinas siekiant užkirsti kelią dideliam incidentui ar reaguoti į besitęsiantį didelį incidentą arba kai didelio incidento atskleidimas kitais atvejais atitinka viešąjį interesą, valstybės narės CSIRT arba, kai taikytina, jos kompetentinga institucija ir atitinkamais atvejais kitų atitinkamų valstybių narių CSIRT arba kompetentingos institucijos, gali, pasikonsultavusios su atitinkamu subjektu, informuoti visuomenę apie incidentą arba pareikalauti, kad tą padarytų subjektas.

8. CSIRT arba kompetentingos institucijos prašymu bendrasis kontaktinis punktas perduoda pagal 1 dalį gautus pranešimus kitų paveiktų valstybių narių bendriesiems kontaktiniams punktams.

9. Bendrasis kontaktinis punktas kas tris mėnesius teikia ENISA suvestinę ataskaitą, į kurią įtraukiami nuasmeninti ir suvestiniai duomenys apie didelius incidentus, incidentus, kibernetines grėsmes ir vos neįvykusius incidentus, apie kuriuos pranešta pagal šio straipsnio 1 dalį ir pagal 30 straipsnį. Siekdama prisidėti prie palyginamos informacijos teikimo ENISA gali priimti technines gaires dėl į suvestinę ataskaitą įtrauktos informacijos parametrų. ENISA kas šešis mėnesius informuoja Bendradarbiavimo grupę ir CSIRT tinklą apie savo išvadas dėl gautų pranešimų.

10. CSIRT arba, kai taikytina, kompetentingos institucijos teikia kompetentingoms institucijoms pagal Direktyvą (ES) 2022/2557 informaciją apie didelius incidentus, incidentus, kibernetines grėsmes ir vos neįvykusius incidentus, apie kuriuos pagal šio straipsnio 1 dalį ir 30 straipsnį pranešė subjektai, identifikuoti kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557

11. Komisija gali priimti įgyvendinimo aktus, kuriais išsamiau nustatoma pagal šio straipsnio 1 dalį ir 30 straipsnį pateikiamo pranešimo ir pagal šio straipsnio 2 dalį pateikiamos informacijos rūšis, formatas ir procedūra.

Komisija ne vėliau kaip 2024 m. spalio 17 d. priima įgyvendinimo aktus dėl DNS paslaugų teikėjų, aukšto lygio domenų vardų registrų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, taip pat elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų teikėjų, kuriais išsamiau apibrėžiami atvejai, kuriais incidentas laikomas dideliu, kaip nurodyta 3 dalyje. Komisija gali priimti tokius įgyvendinimo aktus dėl kitų esminių ir svarbių subjektų.

Komisija keičiasi rekomendacijomis ir bendradarbiauja su Bendradarbiavimo grupe dėl šios dalies pirmoje ir antroje pastraipose nurodytų įgyvendinimo aktų projektų pagal 14 straipsnio 4 dalies e punktą.

Tie įgyvendinimo aktai priimami laikantis 39 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

24 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų naudojimas

1. Siekdamos įrodyti atitiktį tam tikriems 21 straipsnio reikalavimams, valstybės narės gali reikalauti, kad esminiai ir svarbūs subjektai naudotų konkrečius esminių ar svarbių subjektų sukurtus arba iš trečiųjų šalių nupirktus IRT produktus, IRT paslaugas ir IRT procesus, kurie sertifikuoti pagal Europos kibernetinio saugumo sertifikavimo schemas, priimtas pagal Reglamento (ES) 2019/881 49 straipsnį. Be to, valstybės narės skatina esminius ir svarbius subjektus naudotis kvalifikuotomis patikimumo užtikrinimo paslaugomis.

2. Komisijai pagal 38 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais ši direktyva papildoma nustatant, kokių kategorijų esminiai ir svarbūs subjektai privalo naudoti tam tikrus sertifikuotus IRT produktus, IRT paslaugas ir IRT procesus arba gauti sertifikatą pagal Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Reglamento (ES) 2019/881 49 straipsnį. Tie deleguotieji aktai priimami tais atvejais, kai nustatomi nepakankami kibernetinio saugumo lygiai, ir į tuos aktus įtraukiamas įgyvendinimo laikotarpis.

Prieš priimdama tokius deleguotuosius aktus, Komisija atlieka poveikio vertinimą ir vykdo konsultacijas pagal Reglamento (ES) 2019/881 56 straipsnį.

3. Kai šio straipsnio 2 dalies tikslais nėra tinkamos Europos kibernetinio saugumo sertifikavimo schemos, Komisija, pasikonsultavusi su Bendradarbiavimo grupe ir Europos kibernetinio saugumo sertifikavimo grupe, gali prašyti ENISA parengti potencialią schemą pagal Reglamento (ES) 2019/881 48 straipsnio 2 dalį.

25 straipsnis

Standartizacija

1. Siekdamos skatinti vienodą 21 straipsnio 1 ir 2 dalių įgyvendinimą, valstybės narės, nereikalaudamos taikyti kokios nors konkrečios rūšies technologijos ir nesuteikdamos jai pirmenybės, skatina naudotis Europos ir tarptautiniais standartais ir techninėmis specifikacijomis, kurie yra svarbūs tinklų ir informacinių sistemų saugumui.

2. ENISA, bendradarbiaudama su valstybėmis narėmis ir, kai tikslinga, pasikonsultavusi su atitinkamais suinteresuotaisiais subjektais, parengia rekomendacijas ir gaires dėl techninių sričių, kurios turi būti apsvarstytos atsižvelgiant į 1 dalį, taip pat dėl jau galiojančių standartų, be kita ko, nacionalinių standartų, kuriuose būtų numatyta įtraukti tas sritis.

V SKYRIUS

JURISDIKCIJA IR REGISTRACIJA

26 straipsnis

Jurisdikcija ir teritoriškumas

1. Laikoma, kad subjektai, patenkantys į šios direktyvos taikymo sritį, laikomi priklausančiais valstybės narės, kurioje jie yra įsisteigę, jurisdikcijai, išskyrus:

a) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjus, kurie laikomi priklausančiais valstybės narės, kurioje jie teikia savo paslaugas, jurisdikcijai;

b) DNS paslaugų teikėjus, aukščiausio lygio domenų vardų registrus, domenų vardų registravimo paslaugas teikiančius subjektus, debesijos kompiuterijos paslaugų teikėjus, duomenų centrų paslaugų teikėjus, turinio teikimo tinklo paslaugų teikėjus, valdomų paslaugų teikėjus, valdomų saugumo paslaugų teikėjus, taip pat elektroninių prekyviečių, interneto paieškos sistemų ar socialinio tinklo paslaugų platformų paslaugų teikėjus, kurie laikomi priklausančiais valstybės narės, kurioje yra jų pagrindinė buveinė Sąjungoje, jurisdikcijai;

c) viešojo administravimo subjektus, kurie laikomi priklausančiais valstybės narės, kuri juos įsteigė, jurisdikcijai.

2. Šios direktyvos tikslais laikoma, kad 1 dalies b punkte nurodyto subjekto pagrindinė buveinė Sąjungoje yra valstybėje narėje, kurioje daugiausia priimami su kibernetinio saugumo rizikos valdymo priemonėmis susiję sprendimai. Jei tokios valstybės narės neįmanoma nustatyti arba jei tokie sprendimai nepriimami Sąjungoje, laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje vykdomos kibernetinio saugumo operacijos. Jei tokios valstybės narės neįmanoma nustatyti, laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje atitinkamas subjektas turi padalinį, kuriame dirba daugiausia darbuotojų Sąjungoje.

3. Jei 1 dalies b punkte nurodytas subjektas nėra įsisteigęs Sąjungoje, bet teikia paslaugas Sąjungoje, jis paskiria atstovą Sąjungoje. Atstovas turi būti įsisteigęs vienoje iš tų valstybių narių, kuriose siūlomos paslaugos. Laikoma, kad toks subjektas priklauso valstybės narės, kurioje yra įsisteigęs jo atstovas, jurisdikcijai. Jei Sąjungoje nėra pagal šią dalį paskirto atstovo, bet kuri valstybė narė, kurioje subjektas teikia paslaugas, gali imtis teisinių veiksmų prieš subjektą dėl šios direktyvos pažeidimo.

4. 1 dalies b punkte nurodyto subjekto atstovo paskyrimu nedaromas poveikis teisiniams veiksmams, kurie galėtų būti inicijuoti prieš patį subjektą.

5. Valstybės narės, gavusios savitarpio pagalbos prašymą dėl 1 dalies b punkte nurodyto subjekto, gali, neviršydamos to prašymo ribų, imtis tinkamų priežiūros ir vykdymo užtikrinimo priemonių, susijusių su atitinkamu subjektu, teikiančiu paslaugas arba turinčiu tinklų ir informacinę sistemą jų teritorijoje.

27 straipsnis

Subjektų registras

1. ENISA sukuria ir tvarko DNS paslaugų teikėjų, aukščiausio lygio domenų vardų registrų, domenų vardų registravimo paslaugas teikiančių subjektų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo paslaugų teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, taip pat internetinių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų paslaugų teikėjų registrą, remdamasi iš bendrųjų kontaktinių punktų pagal 4 dalį gauta informacija. Gavusi prašymą, ENISA suteikia kompetentingoms institucijoms prieigą prie to registro, kartu, kai taikytina, užtikrindama informacijos konfidencialumo apsaugą.

2. Valstybės narės reikalauja, kad 1 dalyje nurodyti subjektai kompetentingoms institucijoms ne vėliau kaip 2025 m. sausio 17 d. pateiktų šią informaciją:

a) subjekto pavadinimą;

b) I arba II priede nurodytą atitinkamą sektorių, subsektorių ir subjekto rūšį, jei taikoma;

c) subjekto pagrindinės buveinės adresą ir kitus juridinius padalinius Sąjungoje arba, jei jie nėra įsisteigę Sąjungoje, pagal 26 straipsnio 3 dalį paskirto atstovo adresą;

d) naujausius kontaktinius duomenis, įskaitant subjekto ir, kai taikytina, pagal 26 straipsnio 3 dalį paskirto jo atstovo el. pašto adresus ir telefono numerius;

e) valstybes nares, kuriose subjektas teikia paslaugas, ir

f) subjekto IP adresų ruožus.

3. Valstybės narės užtikrina, kad 1 dalyje nurodyti subjektai nedelsdami ir bet kuriuo atveju ne vėliau kaip per tris mėnesius nuo pakeitimo dienos praneštų kompetentingai institucijai apie bet kokius jų pagal 2 dalį pateiktos informacijos pakeitimus.

4. Gavęs 2 ir 3 dalyse nurodytą informaciją, išskyrus 2 dalies f punkte nurodytą informaciją, atitinkamos valstybės narės bendrasis kontaktinis punktas, nepagrįstai nedelsdamas ją persiunčia ENISA.

5. Kai taikytina, šio straipsnio 2 ir 3 dalyse nurodyta informacija teikiama naudojantis 3 straipsnio 4 dalies ketvirtoje pastraipoje nurodytu nacionaliniu mechanizmu.

28 straipsnis

Domenų vardų registracijos duomenų bazė

1. Siekdamos prisidėti prie DNS saugumo, stabilumo ir atsparumo, valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai rūpestingai rinktų ir specialioje duomenų bazėje saugotų tikslius ir išsamius domenų vardų registracijos duomenis, laikydamiesi Sąjungos duomenų apsaugos teisės aktų dėl duomenų, kurie yra asmens duomenys.

2. 1 dalies tikslais valstybės narės reikalauja, kad domenų vardų registracijos duomenų bazėse būtų būtina informacija, pagal kurią būtų galima nustatyti domenų vardų turėtojus ir kontaktinius punktus, administruojančius aukščiausio lygio domenų vardais pažymėtus domenų vardus, ir su jais susisiekti. Tokia informacija apima:

a) domeno vardą;

b) registracijos datą;

c) registruotojo pavadinimą, pavardę, kontaktinį el. pašto adresą ir telefono numerį;

d) domeno vardą administruojančio kontaktinio punkto el. pašto adresą ir telefono numerį, jei jie skiriasi nuo registruotojo duomenų.

3. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai taikytų politiką ir procedūras, įskaitant tikrinimo procedūras, kuriomis užtikrinama, kad 1 dalyje nurodytose duomenų bazėse būtų pateikiama tiksli ir išsami informacija. Valstybės narės reikalauja, kad tokia politika ir procedūros būtų skelbiamos viešai.

4. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai nepagrįstai nedelsdami po domeno vardo užregistravimo viešai paskelbtų domeno vardo registracijos duomenis, kurie nėra asmens duomenys.

5. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai, gavę teisėtus ir tinkamai pagrįstus teisėtų prieigos prašančių subjektų prašymus, suteiktų prieigą prie konkrečių domenų vardų registracijos duomenų, laikydamiesi Sąjungos duomenų apsaugos teisės aktų. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai, atsakytų nepagrįstai nedelsdami ir bet kuriuo atveju per 72 valandas nuo tada, kai gaunamas prašymas suteikti prieigą. Valstybės narės reikalauja, kad tokių duomenų atskleidimo politika ir procedūros būtų skelbiamos viešai.

6. Dėl to, kad laikomasi 1–5 dalyse nustatytų pareigų, neturi būti dubliuojamas domenų vardų registracijos duomenų rinkimas. Tuo tikslu valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai bendradarbiautų tarpusavyje.

VI SKYRIUS

DALIJIMASIS INFORMACIJA

29 straipsnis

Dalijimosi kibernetinio saugumo informacija susitarimai

1. Valstybės narės užtikrina, kad subjektai, patenkantys į šios direktyvos taikymo sritį, ir, kai tinkama, kiti subjektai, nepatenkantys į šios direktyvos taikymo sritį, galėtų savanoriškai tarpusavyje keistis svarbia kibernetinio saugumo informacija, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, vos neįvykusiais incidentais, pažeidžiamumais, metodais ir procedūromis, užvaldymo rodikliais, priešiška taktika, konkrečių grėsmių ir dalyvių informacija, kibernetinio saugumo įspėjimais ir rekomendacijomis dėl kibernetinio saugumo priemonių konfigūracijos siekiant aptikti kibernetinius išpuolius, kai tokiu dalijimusi informacija:

a) siekiama užkirsti kelią incidentams, juos atskleisti, į juos reaguoti ar po jų atstatyti veiklą, arba sumažinti jų poveikį;

b) didinamas kibernetinis saugumas, visų pirma didinant informuotumą apie kibernetines grėsmes, ribojant arba sustabdant tokių grėsmių plitimo galimybes, remiant įvairius gynybos pajėgumus, pažeidžiamumų ištaisymą ir atskleidimą, grėsmių nustatymo, sustabdymo ir prevencijos metodus, švelninimo strategijas ar reagavimo ir veiklos atstatymo etapus, arba skatinant viešųjų ir privačiųjų subjektų atliekamus bendradarbiavimu grindžiamus kibernetinių grėsmių mokslinius tyrimus.

2. Valstybės narės užtikrina, kad informacija būtų keičiamasi esminių ir svarbių subjektų ir, kai tinkama, jų tiekėjų ar paslaugų teikėjų bendruomenėse. Toks keitimasis vykdomas taikant dalijimosi kibernetinio saugumo informacija susitarimus, susijusius su galimai neskelbtina informacija, kuria dalijamasi.

3. Valstybės narės sudaro palankesnes sąlygas sudaryti šio straipsnio 2 dalyje nurodytus dalijimosi kibernetinio saugumo informacija susitarimus. Tokiuose susitarimuose gali būti nustatyti veiklos elementai, įskaitant specialių IT platformų ir automatizavimo priemonių naudojimą, dalijimosi informacija susitarimų turinys ir sąlygos. Nustatydamos išsamią informaciją apie valdžios institucijų dalyvavimą tokiuose susitarimuose, valstybės narės gali nustatyti sąlygas dėl informacijos, kurią turi pateikti kompetentingos institucijos arba CSIRT. Valstybės narės teikia pagalbą tokių susitarimų taikymui pagal 7 straipsnio 2 dalies h punkte nurodytą savo politiką.

4. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai kompetentingoms institucijoms praneša apie savo dalyvavimą 2 dalyje nurodytuose dalijimosi informacija susitarimuose sudarydami tokius susitarimus arba, kai tinkama, apie pasitraukimą iš tokių susitarimų, kai toks pasitraukimas įsigalioja.

5. ENISA teikia pagalbą sudarant 2 dalyje nurodytų dalijimosi kibernetinio saugumo informacija susitarimus, teikdama geriausios praktikos pavyzdžius ir gaires.

30 straipsnis

Savanoriškas pranešimas apie svarbią informaciją

1. Valstybės narės užtikrina, kad, be 23 straipsnyje numatytos pranešimų teikimo pareigos, pranešimus CSIRT arba, kai taikytina, kompetentingoms institucijoms, savanoriškai galėtų teikti:

a) esminiai ir svarbūs subjektai apie incidentus, kibernetines grėsmes ir vos neįvykusius incidentus;

b) kiti nei a punkte nurodyti subjektai, nepriklausomai nuo to, ar jie patenka į šios direktyvos taikymo sritį – apie didelius incidentus, kibernetines grėsmes ir vos neįvykusius incidentus.

2. Valstybės narės tvarko šio straipsnio 1 dalyje nurodytus pranešimus laikydamosi procedūros, nustatytos 23 straipsnyje. Valstybės narės gali teikti pirmenybę privalomų pranešimų tvarkymui, palyginti su savanoriškais pranešimais.

Prireikus CSIRT ir, kai taikytina, kompetentingos institucijos teikia bendriesiems kontaktiniams punktams informaciją apie pagal šį straipsnį gautus pranešimus, kartu užtikrindamos pranešimą teikiančio subjekto pateiktos informacijos konfidencialumą ir tinkamą apsaugą. Nedarant poveikio nusikalstamų veikų prevencijai, tyrimui, jų atskleidimui ir baudžiamajam persekiojimui už jas, dėl savanoriško pranešimo pranešimą teikiančiam subjektui nenustatoma jokių papildomų pareigų, kurios jam nebūtų taikomos, jei jis nebūtų pateikęs pranešimo.

VII SKYRIUS

PRIEŽIŪRA IR VYKDYMO UŽTIKRINIMAS

31 straipsnis

Bendrieji aspektai, susiję su priežiūra ir vykdymo užtikrinimu

1. Valstybės narės užtikrina, kad jų kompetentingos institucijos veiksmingai vykdytų priežiūrą ir imtųsi priemonių, būtinų siekiant užtikrinti, kad būtų laikomasi šios direktyvos.

2. Valstybės narės gali leisti savo kompetentingoms institucijoms nustatyti užduočių prioritetus priežiūros srityje. Prioritetai nustatomi vadovaujantis rizika grindžiamu požiūriu. Tuo tikslu, vykdydamos savo priežiūros užduotis, numatytas 32 ir 33 straipsniuose, kompetentingos institucijos gali nustatyti priežiūros metodikas, pagal kurias būtų galima nustatyti tokių užduočių prioritetus, laikantis rizika grindžiamo požiūrio.

3. Kompetentingos institucijos, nagrinėdamos incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su priežiūros institucijomis pagal Reglamentą (ES) 2016/679, nedarant poveikio priežiūros institucijų kompetencijai ir užduotims pagal tą reglamentą.

4. Nedarant poveikio nacionalinėms teisėkūros ir institucinėms sistemoms, valstybės narės užtikrina, kad, vykdydamos priežiūrą, kaip viešojo administravimo subjektai laikosi šios direktyvos, ir taikydamos vykdymo užtikrinimo priemones šios direktyvos pažeidimų atveju, kompetentingos institucijos turėtų atitinkamus įgaliojimus vykdyti tokias užduotis naudodamosi veiklos nepriklausomumu nuo prižiūrimų viešojo administravimo subjektų. Valstybės narės gali nuspręsti dėl tinkamų, proporcingų ir veiksmingų priežiūros ir vykdymo užtikrinimo priemonių nustatymo tų subjektų atžvilgiu pagal nacionalines teisines ir institucines sistemas.

32 straipsnis

Esminių subjektų priežiūros ir vykdymo užtikrinimo priemonės

1. Valstybės narės užtikrina, kad priežiūros ar vykdymo užtikrinimo priemonės, taikomos esminiams subjektams šioje direktyvoje nustatytų pareigų atžvilgiu, būtų veiksmingos, proporcingos ir atgrasomos, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes.

2. Valstybės narės užtikrina, kad kompetentingos institucijos, vykdydamos savo priežiūros užduotis, susijusias su esminiais subjektais, turėtų bent šiuos įgaliojimus taikyti tiems subjektams:

a) atlikti patikrinimus vietoje ir priežiūrą ne vietoje, įskaitant atsitiktinius patikrinimus, kuriuos atlieka apmokyti specialistai;

b) atlikti reguliarius ir tikslinius saugumo auditus, kuriuos vykdo nepriklausoma įstaiga arba kompetentinga institucija;

c) atlikti *ad hoc* auditus, be kita ko, kai tai pateisinama dėl didelio incidento arba esminio subjekto padaryto šios direktyvos pažeidimo atveju;

d) atlikti saugumo patikrinimus, pagrįstus objektyviais, nediskriminaciniais, sąžiningais ir skaidriais rizikos vertinimo kriterijais, bendradarbiaudamos, kai to reikia, su atitinkamu subjektu;

e) prašyti pateikti informaciją, būtiną atitinkamo subjekto priimtoms kibernetinio saugumo rizikos valdymo priemonėms įvertinti, įskaitant dokumentais pagrįstą kibernetinio saugumo politiką, taip pat informacijos teikimo pareigos kompetentingoms institucijoms pagal 27 straipsnį laikymąsi;

f) prašyti leisti susipažinti su duomenimis, dokumentais ir informacija, reikalinga jų priežiūros užduotims atlikti;

g) prašyti pateikti kibernetinio saugumo politikos įgyvendinimo įrodymus, pavyzdžiui, kvalifikuoto auditoriaus atliktų saugumo auditų rezultatus ir atitinkamus pagrindinius įrodymus.

Pirmos pastraipos b punkte nurodyti tiksliniai saugumo auditai grindžiami kompetentingos institucijos arba audituojamo subjekto atliktais rizikos vertinimais arba kita turima su rizika susijusia informacija.

Bet kokio tikslinio saugumo audito rezultatai pateikiami kompetentingai institucijai. Tokio tikslinio saugumo audito, kurį atlieka nepriklausoma įstaiga, išlaidas padengia audituojamas subjektas, išskyrus tinkamai pagrįstus atvejus, kai kompetentinga institucija nusprendžia kitaip.

3. Naudodamosi savo įgaliojimais pagal 2 dalies e, f arba g punktą, kompetentingos institucijos nurodo prašymo tikslą ir tiksliai apibrėžia prašomą informaciją.

4. Valstybės narės užtikrina, kad jų kompetentingos institucijos, naudodamosi savo vykdymo užtikrinimo įgaliojimais esminių subjektų atžvilgiu, turėtų bent šiuos įgaliojimus:

a) teikti įspėjimus, kad atitinkami subjektai pažeidžia šią direktyvą;

b) priimti privalomus nurodymus, įskaitant nurodymus dėl priemonių, kurių reikia siekiant užkirsti kelią incidentui arba jam išspręsti, ir tokių priemonių įgyvendinimo bei ataskaitų apie jų įgyvendinimą terminus, arba įsakymą, kuriuo reikalaujama, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šios direktyvos pažeidimus;

c) nurodyti atitinkamiems subjektams nutraukti veiksmus, kurie pažeidžia šią direktyvą, ir tokių veiksmų nebekartoti;

d) nurodyti atitinkamiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų kibernetinio saugumo rizikos valdymo priemonės atitiktų 21 straipsnį arba kad jie įvykdytų 23 straipsnyje nustatytas pareigas pranešti;

e) įpareigoti atitinkamus subjektus informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę;

f) įpareigoti atitinkamus subjektus per pagrįstą terminą įgyvendinti saugumo audito metu pateiktas rekomendacijas;

g) paskirti stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip atitinkami subjektai laikosi 21 ir 23 straipsnių;

h) įpareigoti atitinkamus subjektus konkrečiu būdu viešai paskelbti šios direktyvos pažeidimo aspektus;

i) skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal nacionalinę teisę skirtų administracinę baudą pagal 34 straipsnį, kartu su bet kuriomis šios dalies a–h punktuose nurodytomis priemonėmis.

5. Jei pagal 4 dalies a–d ir f punktus patvirtintos vykdymo užtikrinimo priemonės yra neveiksmingos, valstybės narės užtikrina, kad jų kompetentingos institucijos turėtų įgaliojimus nustatyti terminą, iki kurio esminis subjektas turi imtis būtinų veiksmų trūkumams pašalinti arba tų institucijų reikalavimams įvykdyti. Jei per nustatytą terminą nesiimama prašomų veiksmų, valstybės narės užtikrina, kad jų kompetentingos institucijos turėtų įgaliojimus:

a) laikinai sustabdyti arba prašyti, kad sertifikavimo arba leidimus išduodanti įstaiga, arba teismas pagal nacionalinę teisę laikinai sustabdytų sertifikavimą arba įgaliojimą, susijusį su dalimi arba visomis esminio subjekto teikiamomis atitinkamomis paslaugomis ar vykdoma veikla;

b) reikalauti, kad atitinkamos įstaigos arba teismai pagal nacionalinę teisę nustatytų laikiną draudimą bet kuriam esminiame subjekte generalinio direktoriaus ar teisinio atstovo lygmens vadovaujamas pareigas einančiam fiziniam asmeniui eiti vadovaujamas pareigas tame subjekte.

Laikini sustabdymai arba draudimai, nustatyti pagal šią dalį, taikomi tik tol, kol atitinkamas subjektas nesiims būtinų veiksmų trūkumams pašalinti arba kompetentingos institucijos reikalavimams, dėl kurių taikytos tokios vykdymo užtikrinimo priemonės, įvykdyti. Skiriant tokius laikinus sustabdymus ar draudimus, turi būti taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės ir Chartijos principus, įskaitant teisę į veiksmingą teisinę gynybą bei teisingą bylos nagrinėjimą, nekaltumo prezumpciją ir teisę į gynybą.

Šioje dalyje numatytos vykdymo užtikrinimo priemonės netaikomos viešojo administravimo subjektams, kuriems taikoma ši direktyva.

6. Valstybės narės užtikrina, kad fizinis asmuo, atsakingas už esminį subjektą arba veikiantis kaip jo teisinis atstovas, remdamasis jam suteiktais įgaliojimais atstovauti tam subjektui, įgaliojimu priimti sprendimus jo vardu arba įgaliojimu vykdyti jo kontrolę, turėtų įgaliojimus užtikrinti, kad subjektas laikytųsi šios direktyvos. Valstybės narės užtikrina, kad tie fiziniai asmenys galėtų būti traukiami atsakomybėn už jų pareigų užtikrinti šios direktyvos laikymąsi.

Viešojo administravimo subjektų atžvilgiu šia dalimi nedaromas poveikis nacionalinės teisės aktams, susijusiems su valstybės tarnautojų ir renkamų ar paskirtų pareigūnų atsakomybe.

7. Imdamosi bet kurios iš 4 dalyje nurodytų vykdymo užtikrinimo priemonių kompetentingos institucijos gerbia teisę į gynybą ir atsižvelgia į kiekvieno konkretaus atvejo aplinkybes ir tinkamai atsižvelgia bent į:

a) pažeidimo sunkumą ir pažeistų nuostatų svarbą; sunkiais pažeidimais, *inter alia*, bet kuriuo atveju laikomi:

   i) pakartotiniai pažeidimai;

   ii) nepranešimas apie didelius incidentus;

   iii) trūkumų pagal kompetentingų institucijų privalomus vykdyti nurodymus neištaisymas;

   iv) trukdymas vykdyti audito ar stebėsenos veiklą, kurią įpareigojo atlikti kompetentinga institucija nustačius pažeidimą;

   v) neteisingos ar labai netikslios informacijos, susijusios su kibernetinio saugumo rizikos valdymo priemonėmis arba pareigomis pranešti, nustatytomis 21 ir 23 straipsniuose, pateikimas;

b) pažeidimo trukmę;

c) atitinkamo subjekto įvykdytus svarbius ankstesnius pažeidimus;

d) padarytą turtinę arba neturtinę žalą, įskaitant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų naudotojų skaičių;

e) tai, ar pažeidimą įvykdęs asmuo veikė tyčia ar dėl neatsargumo;

f) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti;

g) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;

h) atsakingais laikomų fizinių ar juridinių asmenų bendradarbiavimo su kompetentingomis institucijomis lygį.

8. Kompetentingos institucijos išsamiai pagrindžia savo vykdymo užtikrinimo priemones. Prieš priimdamos tokias priemones kompetentingos institucijos atitinkamiems subjektams praneša apie savo preliminarias išvadas. Jos taip pat suteikia tiems subjektams pagrįstą laikotarpį pastaboms pateikti, išskyrus tinkamai pagrįstus atvejus, kai tai trukdytų imtis neatidėliotinų incidentų prevencijos arba reagavimo į juos veiksmų.

9. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą informuotų toje pačioje valstybėje narėje esančias atitinkamas kompetentingas institucijas pagal Direktyvą (ES) 2022/2557, kai jos naudojasi savo priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad subjektas, kuris pagal Direktyvą (ES) 2022/2557 identifikuotas kaip ypatingos svarbos subjektas, laikytųsi šios direktyvos. Kai taikytina, kompetentingos institucijos pagal Direktyvą (ES) 2022/2557 gali prašyti kompetentingų institucijų pagal šią direktyvą naudotis savo priežiūros ir vykdymo užtikrinimo įgaliojimais subjekto, kuris identifikuojamas kaip ypatingos svarbos subjektas pagal Direktyvą (ES) 2022/2557, atžvilgiu.

10. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą bendradarbiautų su atitinkamomis atitinkamos valstybės narės kompetentingomis institucijomis pagal Reglamentą (ES) 2022/2554 Visų pirma valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą informuotų Priežiūros forumą, įsteigtą pagal Reglamento (ES) 2022/2554 32 straipsnio 1 dalį, kai jos naudojasi priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad esminis subjektas, paskirtas ypatingai svarbiu trečiųjų šalių IRT paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šios direktyvos.

33 straipsnis

Svarbių subjektų priežiūros ir jų pareigų vykdymo užtikrinimo priemonės

1. Gavusios įrodymų, duomenų ar informacijos, kad svarbus subjektas, kaip įtariama, nesilaiko šios direktyvos, visų pirma jos 21 ir 23 straipsnių, valstybės narės užtikrina, kad kompetentingos institucijos prireikus imtųsi veiksmų taikydamos *ex post* priežiūros priemones. Valstybės narės užtikrina, kad tos priemonės būtų veiksmingos, proporcingos ir atgrasomos, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes.

2. Valstybės narės užtikrina, kad kompetentingos institucijos, vykdydamos savo priežiūros užduotis, susijusias su svarbiais subjektais, turėtų bent šiuos įgaliojimus taikyti tiems subjektams:

a) atlikti patikrinimus vietoje ir vykdyti *ex post* priežiūrą ne vietoje, kuriuos atlieka apmokyti specialistai;

b) atlikti tikslinius saugumo auditus, kuriuos vykdo kvalifikuota nepriklausoma įstaiga arba kompetentinga institucija;

c) atlikti saugumo patikrinimus, pagrįstus objektyviais, nediskriminaciniais, sąžiningais ir skaidriais rizikos vertinimo kriterijais, bendradarbiaudamos, kai to reikia, su atitinkamu subjektu;

d) prašyti pateikti informaciją, būtiną atitinkamo subjekto priimtoms kibernetinio saugumo rizikos valdymo priemonėms įvertinti *ex post*, įskaitant dokumentais pagrįstą kibernetinio saugumo politiką, taip pat pareigos teikti informaciją kompetentingoms institucijoms pagal 28 straipsnį laikymąsi;

e) prašyti leisti susipažinti su duomenimis, dokumentais ir informacija, reikalinga priežiūros užduotims atlikti;

f) prašyti pateikti kibernetinio saugumo politikos įgyvendinimo įrodymus, pavyzdžiui, kvalifikuoto auditoriaus atliktų saugumo auditų rezultatus ir atitinkamus pagrindinius įrodymus.

Pirmos pastraipos b punkte nurodyti tiksliniai saugumo auditai grindžiami kompetentingos institucijos arba audituojamo subjekto atliktais rizikos vertinimais arba kita turima su rizika susijusia informacija.

Bet kokio tikslinio saugumo audito rezultatai pateikiami kompetentingai institucijai. Tokio tikslinio saugumo audito, kurį atlieka nepriklausoma įstaiga, išlaidas padengia audituojamas subjektas, išskyrus tinkamai pagrįstus atvejus, kai kompetentinga institucija nusprendžia kitaip.

3. Naudodamosi savo įgaliojimais pagal 2 dalies d, e arba f punktą, kompetentingos institucijos nurodo prašymo tikslą ir patikslina prašomą informaciją.

4. Valstybės narės užtikrina, kad kompetentingos institucijos, naudodamosi savo vykdymo užtikrinimo įgaliojimais svarbių subjektų atžvilgiu, turėtų bent šiuos įgaliojimus:

a) teikti įspėjimus, kad atitinkami subjektai pažeidžia šią direktyvą;

b) priimti privalomus nurodymus arba įsakymą, kuriuo reikalaujama, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šios direktyvos pažeidimą;

c) nurodyti atitinkamiems subjektams nutraukti veiksmus, kurie pažeidžia šią direktyvą, ir tokių veiksmų nebekartoti;

d) nurodyti atitinkamiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų kibernetinio saugumo rizikos valdymo priemonės atitiktų 21 straipsnį arba kad jie įvykdytų 23 straipsnyje nustatytas pareigas pranešti;

e) įpareigoti atitinkamus subjektus informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo veiklą ir kuriuos gali paveikti didelė kibernetinė grėsmė, apie grėsmės pobūdį, taip pat apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę;

f) įpareigoti atitinkamus subjektus per pagrįstą terminą įgyvendinti saugumo audito metu pateiktas rekomendacijas;

g) įpareigoti atitinkamus subjektus konkrečiu būdu viešai paskelbti šios direktyvos pažeidimo aspektus;

h) skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal nacionalinę teisę skirtų administracinę baudą pagal 34 straipsnį, kartu su bet kuriomis šios dalies a–g punktuose nurodytomis priemonėmis.

5. 32 straipsnio 6, 7 ir 8 dalys *mutatis mutandis* taikomos šiame straipsnyje numatytoms priežiūros ir vykdymo užtikrinimo priemonėms, skirtoms svarbiems subjektams.

6. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą bendradarbiautų su atitinkamomis atitinkamos valstybės narės kompetentingomis institucijomis pagal Reglamentą (ES) 2022/2554. Visų pirma valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą informuotų Priežiūros forumą, įsteigtą pagal Reglamento (ES) 2022/2554 32 straipsnio 1 dalį, kai jos naudojasi priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad svarbus subjektas, paskirtas ypatingai svarbiu trečiųjų šalių IRT paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šios direktyvos.

34 straipsnis

Bendrosios administracinių baudų skyrimo esminiams ir svarbiems subjektams sąlygos

1. Valstybės narės užtikrina, kad už šios direktyvos pažeidimus esminiams ir svarbiems subjektams skiriamos administracinės baudos pagal šį straipsnį kiekvienu atskiru atveju būtų veiksmingos, proporcingos ir atgrasomos, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes.

2. Administracinės baudos skiriamos kartu su 32 straipsnio 4 dalies a–h punktuose, 32 straipsnio 5 dalyje ir 33 straipsnio 4 dalies a–g punktuose nurodytomis priemonėmis.

3. Sprendžiant, ar skirti administracinę baudą, ir kiekvienu konkrečiu atveju priimant sprendimą dėl jos dydžio, deramai atsižvelgiama bent į 32 straipsnio 7 dalyje nurodytus aspektus.

4. Valstybės narės užtikrina, kad už 21 arba 23 straipsnio pažeidimus pagal šio straipsnio 2 ir 3 dalis esminiams subjektams būtų skiriamos administracinės baudos, kurių didžiausia būtų bent 10 000 000 EUR arba kurių didžiausia būtų bent 2 proc. įmonės, kuriai tas esminis subjektas priklauso, bendros pasaulinės metinės apyvartos praėjusiais finansiniais metais, atsižvelgiant į tai, kuri suma yra didesnė.

5. Valstybės narės užtikrina, kad už 21 arba 23 straipsnio pažeidimus pagal šio straipsnio 2 ir 3 dalis svarbiems subjektams būtų skiriamos administracinės baudos, kurių didžiausia būtų bent 7 000 000 EUR arba kurių didžiausia būtų bent 1,4 proc. įmonės, kuriai tas svarbus subjektas priklauso, bendros pasaulinės metinės apyvartos praėjusiais finansiniais metais, atsižvelgiant į tai, kuri suma yra didesnė.

6. Valstybės narės gali numatyti įgaliojimą skirti periodines baudas, siekiant priversti esminį arba svarbų subjektą nutraukti šios direktyvos pažeidimą, remiantis išankstiniu kompetentingos institucijos sprendimu.

7. Nedarant poveikio kompetentingų institucijų įgaliojimams pagal 32 ir 33 straipsnius, kiekviena valstybė narė gali nustatyti taisykles dėl to, ar ir kokiu mastu administracinės baudos gali būti skiriamos viešojo administravimo subjektams, kuriems taikomos šioje direktyvoje nustatytos pareigos.

8. Jei valstybės narės teisės sistemoje nenumatoma administracinių baudų, ta valstybė narė užtikrina, kad šis straipsnis galėtų būti taikomas taip, kad baudą inicijuotų kompetentinga institucija, o ją skirtų kompetentingi nacionaliniai teismai arba specialios jurisdikcijos teismai, sykiu užtikrinant, kad tos teisių gynimo priemonės būtų veiksmingos ir turėtų kompetentingų institucijų skiriamoms administracinėms baudoms lygiavertį poveikį. Bet kuriuo atveju skiriamos baudos turi būti veiksmingos, proporcingos ir atgrasomosios. Valstybė narė ne vėliau kaip 2024 m. spalio 17 d. praneša Komisijai apie įstatymų, kuriuos ji priima pagal šią dalį, nuostatas ir nedelsdama praneša apie visus vėlesnius tas nuostatas keičiančius teisės aktus arba joms įtakos turinčius pakeitimus.

35 straipsnis

Pažeidimai, susiję su asmens duomenų saugumo pažeidimu

1. Jeigu, vykdydamos priežiūrą ar vykdymo užtikrinimą, kompetentingos institucijos išsiaiškina, kad dėl esminio arba svarbaus subjekto padaryto šios direktyvos 21 ir 23 straipsniuose nustatytų pareigų pažeidimo gali būti padarytas asmens duomenų saugumo pažeidimas, kaip apibrėžta Reglamento (ES) 2016/679 4 straipsnio 12 punkte, apie kurį turi būti pranešta pagal to reglamento 33 straipsnį, jos, nepagrįstai nedelsdamos, informuoja priežiūros institucijas, kaip nurodyta to reglamento 55 arba 56 straipsnyje.

2. Jeigu priežiūros institucijos, kaip nurodyta Reglamento (ES) 2016/679 55 arba 56 straipsnyje, skiria administracinę baudą pagal to reglamento 58 straipsnio 2 dalies i punktą, kompetentingos institucijos negali skirti administracinės baudos pagal šios direktyvos 34 straipsnį už šio straipsnio 1 dalyje nurodytą pažeidimą, įvykdytą tuo pačiu elgesiu, už kurį buvo skirta administracinė bauda pagal Reglamento (ES) 2016/679 58 straipsnio 2 dalies i punktą. Tačiau kompetentingos institucijos gali taikyti šios direktyvos 32 straipsnio 4 dalies a–h punktuose, 32 straipsnio 5 dalyje ir 33 straipsnio 4 dalies a–g punktuose numatytas vykdymo užtikrinimo priemones.

3. Jeigu priežiūros institucija, kompetentinga pagal Reglamentą (ES) 2016/679, yra įsteigta kitoje valstybėje narėje nei kompetentinga institucija, kompetentinga institucija apie 1 dalyje nurodytą galimą duomenų pažeidimą informuoja jos pačios valstybėje narėje įsteigtą priežiūros instituciją.

36 straipsnis

Sankcijos

Valstybės narės nustato sankcijų, taikomų pažeidus pagal šią direktyvą priimtas nacionalines nuostatas, taisykles ir imasi visų būtinų priemonių užtikrinti, kad šios sankcijos būtų įgyvendinamos. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos. Valstybės narės ne vėliau kaip 2025 m. sausio 17 d. praneša Komisijai apie tas taisykles ir priemones ir nepagrįstai nedelsdamos informuoja ją apie visus vėlesnius joms įtakos turinčius pakeitimus.

37 straipsnis

Savitarpio pagalba

1. Kai subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba teikia paslaugas vienoje ar daugiau valstybių narių, o jo tinklų ir informacinės sistemos yra vienoje ar daugiau kitų valstybių narių, atitinkamų valstybių narių kompetentingos institucijos viena su kita bendradarbiauja ir padeda viena kitai. Tas bendradarbiavimas apima bent tai, kad:

a) valstybės narės kompetentingos institucijos, taikančios priežiūros arba vykdymo užtikrinimo priemones, per bendrąjį kontaktinį punktą informuoja kitų atitinkamų valstybių narių kompetentingas institucijas ir su jomis konsultuojasi dėl priežiūros ir vykdymo užtikrinimo priemonių, kurių imtasi;

b) kompetentinga institucija gali prašyti kitos kompetentingos institucijos imtis priežiūros arba vykdymo užtikrinimo priemonių;

c) kompetentinga institucija, gavusi kitos kompetentingos institucijos pagrįstą prašymą, teikia kitai kompetentingai institucijai savitarpio pagalbą, proporcingą jos pačios turimiems ištekliams, kad priežiūros ar vykdymo užtikrinimo priemonės galėtų būti įgyvendinamos veiksmingai, efektyviai ir nuosekliai.

Pirmos pastraipos c punkte nurodyta savitarpio pagalba gali apimti prašymus pateikti informaciją ir priežiūros priemones, įskaitant prašymus atlikti patikrinimus vietoje arba priežiūrą ne vietoje, arba tikslinius saugumo auditus. Kompetentinga institucija, kuriai pateiktas pagalbos prašymas, negali atmesti to prašymo, išskyrus atvejus, kai nustatoma, kad ji neturi kompetencijos teikti prašomą pagalbą, prašoma pagalba nėra proporcinga kompetentingos institucijos priežiūros atliekamų užduočių atžvilgiu arba prašymas yra susijęs su informacija arba apima veiklą, kuri, ją atskleidus arba atlikus, prieštarautų tos valstybės narės nacionaliniam saugumui, visuomenės saugumui ar gynybai. Prieš atsisakydama patenkinti tokį prašymą, kompetentinga institucija konsultuojasi su kitomis atitinkamomis kompetentingomis institucijomis, taip pat, vienos iš atitinkamų valstybių narių prašymu, su Komisija ir ENISA.

2. Kai tinkama ir bendru sutarimu, skirtingų valstybių narių kompetentingos institucijos gali vykdyti bendrus priežiūros veiksmus.

VIII SKYRIUS

DELEGUOTIEJI IR ĮGYVENDINIMO AKTAI

38 straipsnis

Įgaliojimų delegavimas

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

2. 24 straipsnio 2 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo 2023 m. sausio 16 d.

3. Europos Parlamentas arba Taryba gali bet kada atšaukti 24 straipsnio 2 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 24 straipsnio 2 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.

39 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.

IX SKYRIUS

BAIGIAMOSIOS NUOSTATOS

40 straipsnis

Peržiūra

Komisija ne vėliau kaip 2027 m. spalio 17 d. peržiūri šios direktyvos taikymą ir teikia ataskaitą Europos Parlamentui ir Tarybai. Ataskaitoje visų pirma įvertinama susijusių subjektų dydžio ir I ir II prieduose nurodytų sektorių, subsektorių ir subjektų rūšių svarba ekonomikos ir visuomenės veikimui kibernetinio saugumo atžvilgiu. Tuo tikslu ir siekiant tolesnės pažangos vykdant strateginį ir operatyvinį bendradarbiavimą, Komisija atsižvelgia į Bendradarbiavimo grupės ir CSIRT tinklo ataskaitas apie patirtį, įgytą strateginiu ir operatyviniu lygmenimis. Kai būtina, prie ataskaitos pridedamas pasiūlymas dėl teisėkūros procedūra priimamo akto.

41 straipsnis

Perkėlimas į nacionalinės teisės aktus

1. Valstybės narės ne vėliau kaip 2024 m. spalio 17 d., priima ir paskelbia nuostatas, būtinas, kad būtų laikomasi šios direktyvos. Apie tai jos nedelsdamos praneša Komisijai.

Tas nuostatas jos taiko nuo 2024 m. spalio 18 d..

2. Valstybės narės, priimdamos 1 dalyje nurodytas nuostatas, daro jose nuorodą į šią direktyvą arba tokia nuoroda daroma jas oficialiai skelbiant. Nuorodos darymo tvarką nustato valstybės narės.

42 straipsnis

Reglamento (ES) Nr. 910/2014 dalinis pakeitimas

Reglamento (ES) Nr. 910/2014 19 straipsnis išbraukiamas nuo 2024 m. spalio 18 d.

43 straipsnis

Direktyvos (ES) 2018/1972 dalinis pakeitimas

Direktyvos (ES) 2018/1972 40 ir 41 straipsniai išbraukiami nuo 2024 m. spalio 18 d.

44 straipsnis

Panaikinimas

Direktyva (ES) 2016/1148 panaikinama nuo 2024 m. spalio 18 d.

Nuorodos į panaikintą direktyvą laikomos nuorodomis į šią direktyvą ir skaitomos pagal III priede pateiktą atitikties lentelę.

45 straipsnis

Įsigaliojimas

Ši direktyva įsigalioja dvidešimtą dieną po jos paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

46 straipsnis

Adresatai

Ši direktyva skirta valstybėms narėms.

Priimta Strasbūre 2022 m. gruodžio 14 d.

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkė	*Pirmininkas*
R. METSOLA	M. BEK

I PRIEDAS

YPATINGOS SVARBOS SEKTORIAI

Sektorius	Subsektorius	Subjekto rūšis
1. Energetika	a) Elektra	— Elektros energijos įmonės, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2019/944 ([1])2 straipsnio 57 punkte, vykdančios „tiekimo“ funkciją, kaip apibrėžta tos direktyvos 2 straipsnio 12 punkte
		— Skirstymo sistemos operatoriai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 29 punkte
		— Perdavimo sistemos operatoriai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 35 punkte
		— Gamintojai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 38 punkte
		— Paskirtieji elektros energijos rinkos operatoriai, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/943 ([2]) 2 straipsnio 8 punkte — Elektros energijos rinkos dalyviai, kaip apibrėžta Reglamento (ES) 2019/943 2 straipsnio 25 punkte, teikiantys telkimo, reguliavimo apkrovos arba energijos kaupimo paslaugas, nurodytas Direktyvos (ES) 2019/944 2 straipsnio 18, 20 ir 59 punktuose — Įkrovimo prieigos operatoriui, atsakingi už įkrovimo prieigos, kuri naudojama įkrovimo paslaugai galutiniams naudotojams teikti, taip pat ir judumo paslaugų teikėjo vardu bei jo pavedimu, valdymą ir eksploatavimą
	b) Centralizuotas šilumos ir vėsumos tiekimas	— Centralizuoto šilumos tiekimo arba centralizuoto vėsumos tiekimo, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2018/2001 ([3])2 straipsnio 19 punkte, operatoriai
	c) Nafta	— Naftotiekių operatoriai
		— Naftos gamybos, perdirbimo ir apdorojimo įrenginių, laikymo ir perdavimo operatoriai
		— Centrinės atsargų saugyklos, kaip apibrėžta Tarybos direktyvos 2009/119/EB ([4])2 straipsnio f punkte
	d) Dujos	— Tiekimo įmonės, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/73/EB ([5])2 straipsnio 8 punkte
		— Skirstymo sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 6 punkte
		— Perdavimo sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 4 punkte
		— Laikymo sistemų operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 10 punkte
		— SGD sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 12 punkte
		— Gamtinių dujų įmonės, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 1 punkte
		— Gamtinių dujų perdirbimo ir apdorojimo įrenginių operatoriai
	e) Vandenilis	— Vandenilio gamybos, laikymo ir perdavimo operatoriai

Sektorius	Subsektorius	Subjekto rūšis
2. Transportas	a) Oro transportas	— Oro vežėjai, kaip apibrėžta Reglamento (EB) Nr. 300/2008 3 straipsnio 4 punkte, naudojami komerciniais tikslais
		— Oro uosto valdymo organai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/12/EB ([6])2 straipsnio 2 punkte, oro uostai, kaip apibrėžta tos direktyvos 2 straipsnio 1 punkte, įskaitant Europos Parlamento ir Tarybos reglamento (ES) Nr. 1315/2013 ([7])II priedo 2 skirsnyje išvardytus pagrindinius oro uostus, ir subjektai, eksploatuojantys oro uostuose esančius pagalbinius įrenginius
		— Skrydžių valdymo operatoriai, teikiantys skrydžių valdymo (ATC) paslaugas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (EB) Nr. 549/2004 ([8])2 straipsnio 1 punkte
	b) Geležinkelių transportas	— Infrastruktūros valdytojai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2012/34/ES ([9])3 straipsnio 2 punkte
		— Geležinkelio įmonės, kaip apibrėžta Direktyvos 2012/34/ES 3 straipsnio 1 punkte, įskaitant paslaugų įrenginių operatorius, kaip apibrėžta tos direktyvos 3 straipsnio 12 punkte
	c) Vandens transportas	— Vidaus vandenų, jūrų ir priekrantės keleivinio ir krovininio vandens transporto bendrovės, kaip apibrėžta jūrų transporto atžvilgiu Europos Parlamento ir Tarybos reglamento (EB) Nr. 725/2004 ([10]) I priede, neįskaitant tų bendrovių eksploatuojamų atskirų laivų
		— Uostų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2005/65/EB ([11])3 straipsnio 1 punkte, įskaitant jų uosto įrenginius, kaip apibrėžta Reglamento (EB) Nr. 725/2004 2 straipsnio 11 punkte, direkcijos ir subjektai, eksploatuojantys uostuose esančias įmones ir įrenginius
		— Laivų eismo tarnybų (LET), kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2002/59/EB ([12]) 3 straipsnio o punkte, operatoriai
	d) Kelių transportas	— Kelių direkcijos, kaip apibrėžta Komisijos deleguotojo reglamento (ES) 2015/962 ([13]) 2 straipsnio 12 punkte, atsakingos už eismo valdymo kontrolę, išskyrus viešuosius subjektus, kuriems eismo valdymo arba intelektinių transporto sistemų operatoriaus veikla yra tik neesminė jų bendrosios veiklos dalis
		— Intelektinių transporto sistemų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2010/40/ES ([14]) 4 straipsnio 1 punkte, operatoriai
3. Bankininkystė		Kredito įstaigos, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 575/2013 ([15])4 straipsnio 1 punkte
4. Finansų rinkų infrastruktūros objektai		— Prekybos vietų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2014/65/ES ([16])4 straipsnio 24 punkte, operatoriai
		— Pagrindinės sandorio šalys (PSŠ), kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 648/2012 ([17]) 2 straipsnio 1 punkte

Sektorius	Subsektorius	Subjekto rūšis
5. Sveikatos priežiūra		— Sveikatos priežiūros paslaugų teikėjai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2011/24/ES ([18])3 straipsnio g punkte
		— ES etaloninės laboratorijos, nurodytos Europos Parlamento ir Tarybos reglamento (ES) 2022/2371 ([19]) 15 straipsnyje
		— Subjektai, vykdantys vaistų, apibrėžtų Europos Parlamento ir Tarybos direktyvos 2001/83/EB ([20])1 straipsnio 2 punkte, mokslinių tyrimų ir kūrimo veiklą — Subjektai, gaminantys pagrindinius farmacijos produktus ir farmacijos preparatus, nurodytus NACE 2 red. C skirsnio 21 skyriuje — Subjektai, gaminantys medicinos priemones, kurios laikomos ypatingos svarbos ekstremaliosios visuomenės sveikatos situacijos atveju (ypatingos svarbos medicinos priemonių ekstremaliosios visuomenės sveikatos situacijos atveju sąrašas), kaip tai suprantama Europos Parlamento ir Tarybos reglamento (ES) 2022/123 ([21]) 22 straipsnyje
6. Geriamasis vanduo		Žmonėms vartoti skirto vandens, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2020/2184 ([22]) 2 straipsnio 1 punkto a papunktyje, tiekėjai ir skirstytojai, išskyrus skirstytojus, kuriems žmonėms vartoti skirto vandens skirstymas yra neesminė jų bendrosios kitų prekių ir produktų paskirstymo veiklos dalis
7. Nuotekos		Miesto nuotekas, buitines nuotekas ir pramonines nuotekas, nurodytas Tarybos direktyvos 91/271/EEB ([23]) 2 straipsnio 1, 2 ir 3 punktuose, renkančios, šalinančios ar valančios įmonės, išskyrus įmones, kurioms miesto nuotekų, buitinių nuotekų ar pramoninių nuotekų rinkimas, šalinimas ar valymas yra neesminė jų bendrosios veiklos dalis
8. Skaitmeninė infrastruktūra		— Interneto duomenų srautų mainų taško teikėjai
		— DNS paslaugų teikėjai, išskyrus šakninio pavadinimo serverių operatorius
		— Aukščiausio lygio domenų vardų registrai
		— Debesijos kompiuterijos paslaugų teikėjai
		— Duomenų centrų paslaugų teikėjai
		— Turinio teikimo tinklo teikėjai
		— Patikimumo užtikrinimo paslaugų teikėjai
		— Viešųjų elektroninių ryšių tinklų teikėjai
		— Viešai prieinamų elektroninių ryšių paslaugų teikėjai
9. IRT paslaugų valdymas (verslas verslui)		— Valdomų paslaugų teikėjai — Valdomų saugumo paslaugų teikėjai

Sektorius	Subsektorius	Subjekto rūšis
10. Viešasis administravimas		— Centrinės valdžios viešojo administravimo subjektai, kaip valstybė narė apibrėžė pagal nacionalinę teisę
		— Regioninio lygmens viešojo administravimo subjektai, kaip valstybė narė apibrėžė pagal nacionalinę teisę
11. Kosmosas		Valstybėms narėms arba privačiosioms šalims priklausančios, jų valdomos ir eksploatuojamos antžeminės infrastruktūros operatoriai, kurie remia kosminių paslaugų teikimą, išskyrus viešųjų elektroninių ryšių tinklų teikėjus

([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).
([2]) 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/943 dėl elektros energijos vidaus rinkos (OL L 158, 2019 6 14, p. 54).
([3]) 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/2001 dėl skatinimo naudoti atsinaujinančių išteklių energiją (OL L 328, 2018 12 21, p. 82).
([4]) 2009 m. rugsėjo 14 d. Tarybos direktyva 2009/119/EB, kuria valstybės narės įpareigojamos išlaikyti privalomąsias žalios naftos ir (arba) naftos produktų atsargas (OL L 265, 2009 10 9, p. 9).
([5]) 2009 m. liepos 13 d. Europos Parlamento ir Tarybos direktyva 2009/73/EB dėl gamtinių dujų vidaus rinkos bendrųjų taisyklių, panaikinanti Direktyvą 2003/55/EB (OL L 211, 2009 8 14, p. 94).
([6]) 2009 m. kovo 11 d. Europos Parlamento ir Tarybos direktyva 2009/12/EB dėl oro uostų mokesčių (OL L 70, 2009 3 14, p. 11).
([7]) 2013 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1315/2013 dėl Sąjungos transeuropinio transporto tinklo plėtros gairių, kuriuo panaikinamas Sprendimas Nr. 661/2010/ES (OL L 348, 2013 12 20, p. 1).
([8]) 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 549/2004, nustatantis bendro Europos dangaus sukūrimo pagrindą (pagrindų reglamentas) (OL L 96, 2004 3 31, p. 1).
([9]) 2012 m. lapkričio 21 d. Europos Parlamento ir Tarybos direktyva 2012/34/ES, kuria sukuriama bendra Europos geležinkelių erdvė (OL L 343, 2012 12 14, p. 32).
([10]) 2004 m. kovo 31 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 725/2004 dėl laivų ir uostų įrenginių apsaugos stiprinimo(OL L 129, 2004 4 29, p. 6).
([11]) 2005 m. spalio 26 d. Europos Parlamento ir Tarybos direktyva 2005/65/EB dėl uostų apsaugos stiprinimo (OL L 310, 2005 11 25, p. 28).
([12]) 2002 m. birželio 27 d. Europos Parlamento ir Tarybos direktyva 2002/59/EB, įdiegianti Bendrijos laivų eismo stebėsenos ir informacijos sistemą ir panaikinanti Tarybos direktyvą 93/75/EEB (OL L 208, 2002 8 5, p. 10).
([13]) 2014 m. gruodžio 18 d. Komisijos deleguotasis reglamentas (ES) 2015/962, kuriuo papildomos Europos Parlamento ir Tarybos direktyvos 2010/40/ES nuostatos, susijusios su visoje Europos Sąjungoje teikiamomis tikralaikės eismo informacijos paslaugomis (OL L 157, 2015 6 23, p. 21).
([14]) 2010 m. liepos 7 d. Europos Parlamento ir Tarybos direktyva 2010/40/ES dėl kelių transporto ir jo sąsajų su kitų rūšių transportu srities intelektinių transporto sistemų diegimo sistemos (OL L 207, 2010 8 6, p. 1).
([15]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 575/2013 dėl prudencinių reikalavimų kredito įstaigoms, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 (OL L 176, 2013 6 27, p. 1).
([16]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/65/ES dėl finansinių priemonių rinkų, kuria iš dalies keičiamos Direktyva 2002/92/EB ir Direktyva 2011/61/ES (OL L 173, 2014 6 12, p. 349).
([17]) 2012 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų (OL L 201, 2012 7 27, p. 1).
([18]) 2011 m. kovo 9 d. Europos Parlamento ir Tarybos direktyva 2011/24/ES dėl pacientų teisių į tarpvalstybines sveikatos priežiūros paslaugas įgyvendinimo (OL L 88, 2011 4 4, p. 45).

([19]) 2022 m. lapkričio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2371 dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai, kuriuo panaikinamas Sprendimas Nr. 1082/2013/ES (OL L 314, 2022 12 6, p. 26).
([20]) 2001 m. lapkričio 6 d. Europos Parlamento ir Tarybos direktyva 2001/83/EB dėl Bendrijos kodekso, reglamentuojančio žmonėms skirtus vaistus (OL L 311, 2001 11 28, p. 67).
([21]) 2022 m. sausio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/123 dėl didesnio Europos vaistų agentūros vaidmens pasirengimo vaistų ir medicinos priemonių krizei ir jos valdymo srityje (OL L 20, 2022 1 31, p. 1)
([22]) 2020 m. gruodžio 16 d. Europos Parlamento ir Tarybos direktyva (ES) 2020/2184 dėl žmonėms vartoti skirto vandens kokybės (OL L 435, 2020 12 23, p. 1).
([23]) 1991 m. gegužės 21 d. Tarybos direktyva 91/271/EEB dėl miesto nuotėkų valymo (OL L 135, 1991 5 30, p. 40).

II PRIEDAS

KITI ITIN SVARBŪS SEKTORIAI

Sektorius	Subsektorius	Subjekto rūšis
1. Pašto ir kurjerių paslaugos		Pašto paslaugų teikėjai, kaip apibrėžta Direktyvos 97/67/EB 2 straipsnio 1a punkte, įskaitant kurjerių paslaugų teikėjus
2. Atliekų tvarkymas		Atliekas, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2008/98/EB ([1]) 3 straipsnio 9 punkte, tvarkančios įmonės, išskyrus įmones, kurių pagrindinė ekonominė veikla nėra atliekų tvarkymas
3. Cheminių medžiagų gamyba ir platinimas		Chemines medžiagas gaminančios ir chemines medžiagas ar mišinius platinančios įmonės, kaip nurodyta Europos Parlamento ir Tarybos reglamento (EB) Nr. 1907/2006 ([2]) 3 straipsnio 9 ir 14 punktuose, ir gaminius, kaip apibrėžta to reglamento 3 straipsnio 3 punkte, iš tų medžiagų ar mišinių gaminančios įmonės
4. Maisto gamyba, perdirbimas ir platinimas		Maisto verslo įmonės, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (EB) Nr. 178/2002 ([3]) 3 straipsnio 2 punkte, vykdančios didmeninio platinimo ir pramoninės gamybos bei perdirbimo veiklą
5. Gamyba	a) Medicinos priemonių ir *in vitro* diagnostikos medicinos priemonių gamyba	Medicinos priemones, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2017/745 ([4]) 2 straipsnio 1 punkte, gaminantys subjektai, ir *in vitro* diagnostikos medicinos priemones, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2017/746 ([5]) 2 straipsnio 2 punkte, gaminantys subjektai, išskyrus šios direktyvos I priedo 5 punkto penktoje įtraukoje nurodytas medicinos priemones gaminančius subjektus.
	b) Kompiuterinių, elektroninių ir optinių gaminių gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 26 skyriuje
	c) Elektros įrangos gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 27 skyriuje
	d) Niekur kitur nepriskirtų mašinų ir įrangos gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 28 skyriuje
	e) Motorinių transporto priemonių, priekabų ir puspriekabių gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 29 skyriuje
	f) Kitos transporto įrangos gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 30 skyriuje

Sektorius	Subsektorius	Subjekto rūšis
6. Skaitmeninių paslaugų teikėjai		— Elektroninių prekyviečių teikėjai
		— Paieškos sistemų teikėjai
		— Socialinių tinklų paslaugų platformos teikėjai
7. Moksliniai tyrimai		Mokslinių tyrimų organizacijos

([1]) 2008 m. lapkričio 19 d. Europos Parlamento ir Tarybos direktyva 2008/98/EB dėl atliekų ir panaikinanti kai kurias direktyvas (OL L 312, 2008 11 22, p. 3).

([2]) 2006 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1907/2006 dėl cheminių medžiagų registracijos, įvertinimo, autorizacijos ir apribojimų (REACH), įsteigiantis Europos cheminių medžiagų agentūrą, iš dalies keičiantis Direktyvą 1999/45/EB bei panaikinantis Tarybos reglamentą (EEB) Nr. 793/93, Komisijos reglamentą (EB) Nr. 1488/94, Tarybos direktyvą 76/769/EEB ir Komisijos direktyvas 91/155/EEB, 93/67/EEB, 93/105/EB bei 2000/21/EB (OL L 396, 2006 12 30, p. 1).

([3]) 2002 m. sausio 28 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 178/2002, nustatantis maistui skirtų teisės aktų bendruosius principus ir reikalavimus, įsteigiantis Europos maisto saugos tarnybą ir nustatantis su maisto saugos klausimais susijusias procedūras (OL L 31, 2002 2 1, p. 1).

([4]) 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).

([5]) 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).

III PRIEDAS

ATITIKTIES LENTELĖ

Direktyva (ES) 2016/1148	Ši direktyva
1 straipsnio 1 dalis	1 straipsnio 1 dalis
1 straipsnio 2 dalis	1 straipsnio 2 dalis
1 straipsnio 3 dalis	-
1 straipsnio 4 dalis	2 straipsnio 12 dalis
1 straipsnio 5 dalis	2 straipsnio 13 dalis
1 straipsnio 6 dalis	2 straipsnio 6 ir 11 dalys
1 straipsnio 7 dalis	4 straipsnis
2 straipsnis	2 straipsnio 14 dalis
3 straipsnis	5 straipsnis
4 straipsnis	6 straipsnis
5 straipsnis	-
6 straipsnis	-
7 straipsnio 1 dalis	7 straipsnio 1 ir 2 dalys
7 straipsnio 2 dalis	7 straipsnio 4 dalis
7 straipsnio 3 dalis	7 straipsnio 3 dalis
8 straipsnio 1–5 dalys	8 straipsnio 1–5 dalys
8 straipsnio 6 dalis	13 straipsnio 4 dalis
8 straipsnio 7 dalis	8 straipsnio 6 dalis
9 straipsnio 1, 2 ir 3 dalys	10 straipsnio 1, 2 ir 3 dalys
9 straipsnio 4 dalis	10 straipsnio 9 dalis
9 straipsnio 5 dalis	10 straipsnio 10 dalis
10 straipsnio 1, 2 dalys ir 3 dalies pirma pastraipa	13 straipsnio 1, 2 ir 3 dalys
10 straipsnio 3 dalies antra pastraipa	23 straipsnio 9 dalis
11 straipsnio 1 dalis	14 straipsnio 1 ir 2 dalys
11 straipsnio 2 dalis	14 straipsnio 3 dalis
11 straipsnio 3 dalis	14 straipsnio 4 dalies pirmos pastraipos a–q ir s punktai bei 7 dalis
11 straipsnio 4 dalis	14 straipsnio 4 dalies pirmos pastraipos r punktas ir antra pastraipa
11 straipsnio 5 dalis	14 straipsnio 8 dalis
12 straipsnio 1–5 dalys	15 straipsnio 1–5 dalys
13 straipsnis	17 straipsnis
14 straipsnio 1 ir 2 dalys	21 straipsnio 1–4 dalys
14 straipsnio 3 dalis	23 straipsnio 1 dalis
14 straipsnio 4 dalis	23 straipsnio 3 dalis
14 straipsnio 5 dalis	23 straipsnio 5, 6 ir 8 dalys

Direktyva (ES) 2016/1148	Ši direktyva
14 straipsnio 6 dalis	23 straipsnio 7 dalis
14 straipsnio 7 dalis	23 straipsnio 11 dalis
15 straipsnio 1 dalis	31 straipsnio 1 dalis
15 straipsnio 2 dalies pirmos pastraipos a punktas	32 straipsnio 2 dalies e punktas
15 straipsnio 2 dalies pirmos pastraipos b punktas	32 straipsnio 2 dalies g punktas
15 straipsnio 2 dalies antra pastraipa	32 straipsnio 3 dalis
15 straipsnio 3 dalis	32 straipsnio 4 dalies b punktas
15 straipsnio 4 dalis	31 straipsnio 3 dalis
16 straipsnio 1 ir 2 dalys	21 straipsnio 1–4 dalys
16 straipsnio 3 dalis	23 straipsnio 1 dalis
16 straipsnio 4 dalis	23 straipsnio 3 dalis
16 straipsnio 5 dalis	-
16 straipsnio 6 dalis	23 straipsnio 6 dalis
16 straipsnio 7 dalis	23 straipsnio 7 dalis
16 straipsnio 8 ir 9 dalys	21 straipsnio 5 dalis ir 23 straipsnio 11 dalis
16 straipsnio 10 dalis	-
16 straipsnio 11 dalis	2 straipsnio 1, 2 ir 3 dalys
17 straipsnio 1 dalis	33 straipsnio 1 dalis
17 straipsnio 2 dalies a punktas	32 straipsnio 2 dalies e punktas
17 straipsnio 2 dalies b punktas	32 straipsnio 4 dalies b punktas
17 straipsnio 3 dalis	37 straipsnio 1 dalies a ir b punktai
18 straipsnio 1 dalis	26 straipsnio 1 dalies b punktas ir 2 dalis
18 straipsnio 2 dalis	26 straipsnio 3 dalis
18 straipsnio 3 dalis	26 straipsnio 4 dalis
19 straipsnis	25 straipsnis
20 straipsnis	30 straipsnis
21 straipsnis	36 straipsnis
22 straipsnis	39 straipsnis
23 straipsnis	40 straipsnis
24 straipsnis	-
25 straipsnis	41 straipsnis
26 straipsnis	45 straipsnis
27 straipsnis	46 straipsnis
I priedo 1 punktas	11 straipsnio 1 dalis
I priedo 2 punkto a papunkčio i–iv punktai	11 straipsnio 2 dalies a–d punktai

Direktyva (ES) 2016/1148	Ši direktyva
I priedo 2 punkto a papunkčio v punktas	11 straipsnio 2 dalies f punktas
I priedo 2 punkto b papunktis	11 straipsnio 4 dalis
I priedo 2 punkto c papunkčio i ir ii punktai	11 straipsnio 5 dalies a punktas
II priedas	I priedas
III priedo 1 ir 2 punktai	II priedo 6 punktas
III priedo 3 punktas	I priedo 8 punktas

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2022/2556

2022 m. gruodžio 14 d.

kuria iš dalies keičiamos direktyvos 2009/65/EB, 2009/138/EB, 2011/61/ES, 2013/36/ES, 2014/59/ES, 2014/65/ES, (ES) 2015/2366 ir (ES) 2016/2341 dėl finansų sektoriaus skaitmeninės veiklos atsparumo

(Tekstas svarbus EEE)

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 53 straipsnio 1 dalį ir 114 straipsnį,

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

atsižvelgdami į Europos Centrinio Banko nuomonę ([1]),

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę ([2]),

laikydamiesi įprastos teisėkūros procedūros ([3]),

kadangi:

(1) Sąjunga turi tinkamai ir visapusiškai spręsti skaitmeninės rizikos, kylančios visiems finansų sektoriaus subjektams dėl to, kad teikiant finansines paslaugas ir jomis naudojantis vis dažniau naudojamos informacinės ir ryšių technologijos (IRT), problemą, tokiu būdu padėdama išnaudoti skaitmeninių finansų potencialą skatinti inovacijas ir skatinti konkurenciją saugioje skaitmeninėje aplinkoje;

(2) finansų sektoriaus subjektai kasdienėje veikloje yra labai priklausomi nuo naudojimosi skaitmeninėmis technologijomis. Todėl labai svarbu užtikrinti jų skaitmeninės veiklos atsparumą IRT rizikai. Šis poreikis tapo dar aktualesnis dėl proveržio technologijų, visų pirma technologijų, sudarančių sąlygas skaitmeninę vertės arba teisių išraišką perleisti ir saugoti elektroniniu būdu, naudojant paskirstytojo registro ar panašią technologiją (kriptoturtą), ir su tuo turtu susijusių paslaugų augimo rinkoje;

([1]) OL C 343, 2021 8 26, p. 1.
([2]) OL C 155, 2021 4 30, p. 38.
([3]) 2022 m. lapkričio 10 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2022 m. lapkričio 28 d. Tarybos sprendimas.

(3) Sąjungos lygmens reikalavimai, susiję su IRT rizikos finansų sektoriui valdymu, šiuo metu yra numatyti Europos Parlamento ir Tarybos direktyvose 2009/65/EB ([4]), 2009/138/EB ([5]), 2011/61/ES ([6]), 2013/36/ES ([7]), 2014/59/ES ([8]), 2014/65/ES ([9]), (ES) 2015/2366 ([10]) ir (ES) 2016/2341 ([11]).

Tie reikalavimai yra nevienodi ir tam tikrais atvejais neišsamūs. Kai kuriais atvejais IRT riziką siekta mažinti tik netiesiogiai kaip operacinės rizikos dalį, o kitais atvejais jai visai neskirta dėmesio. Tos problemos yra sprendžiamos priimant Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 ([12]). Todėl tos direktyvos turėtų būti iš dalies pakeistos, kad būtų užtikrintas suderinamumas su tuo reglamentu. Šia direktyva įtvirtinami pakeitimai, kurie yra būtini siekiant užtikrinti teisinį aiškumą ir nuoseklumą tada, kai finansų sektoriaus subjektai, gavę veiklos leidimus ir prižiūrimi pagal tas direktyvas, taiko įvairius skaitmeninės veiklos atsparumo reikalavimus, būtinus jų veiklai vykdyti ir paslaugoms teikti, taip užtikrinant sklandų vidaus rinkos veikimą. Reikia užtikrinti tų reikalavimų adekvatumą rinkos pokyčiams, kartu skatinant proporcingumą, visų pirma finansų sektoriaus subjektų dydžio ir konkretaus režimo, kuris jiems taikomas, atžvilgiu, siekiant sumažinti reikalavimų laikymosi išlaidas;

(4) banko paslaugų sričiai Direktyvoje 2013/36/ES šiuo metu nustatytos tik bendrosios vidaus valdymo taisyklės ir operacinės rizikos nuostatos, kuriose nustatyti reikalavimai nenumatytų atvejų ir veiklos tęstinumo planams, kuriais netiesiogiai remiamasi sprendžiant IRT rizikos klausimus. Tačiau, siekiant IRT rizikos klausimą spręsti aiškiai ir nedviprasmiškai, reikalavimai nenumatytų atvejų ir veiklos tęstinumo planams turėtų būti iš dalies pakeisti, kad taip pat būtų įtraukti veiklos tęstinumo planai ir reagavimo ir veiklos atkūrimo planai, taikomi IRT rizikos atveju, laikantis Reglamente (ES) 2022/2554 nustatytų reikalavimų. Be to, vertinant operacinę riziką IRT rizika tik netiesiogiai įtraukiama į priežiūrinio tikrinimo ir vertinimo procesą (SREP), kurį atlieka kompetentingos institucijos, o jos vertinimo kriterijai šiuo metu apibrėžti Europos priežiūros institucijos (Europos bankininkystės institucijos) (EBI), įsteigtos pagal Europos Parlamento ir Tarybos reglamentą (ES) Nr. 1093/2010 ([13]), gairėse dėl IRT rizikos vertinimo per priežiūrinio tikrinimo ir vertinimo procesą (SREP). Siekiant suteikti teisinį aiškumą ir užtikrinti, kad

([4]) 2009 m. liepos 13 d. Europos Parlamento ir Tarybos direktyva 2009/65/EB dėl įstatymų ir kitų teisės aktų, susijusių su kolektyvinio investavimo į perleidžiamus vertybinius popierius subjektais (KIPVPS), derinimo (OL L 302, 2009 11 17, p. 32).

([5]) 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/138/EB dėl draudimo ir perdraudimo veiklos pradėjimo ir jos vykdymo (Mokumas II) (OL L 335, 2009 12 17, p. 1).

([6]) 2011 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2011/61/ES dėl alternatyvaus investavimo fondų valdytojų, kuria iš dalies keičiami direktyvos 2003/41/EB ir 2009/65/EB bei reglamentai (EB) Nr. 1060/2009 ir (ES) Nr. 1095/2010 (OL L 174, 2011 7 1, p. 1).

([7]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyva 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų ir investicinių įmonių priežiūros, kuria iš dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB (OL L 176, 2013 6 27, p. 338).

([8]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/59/ES, kuria nustatoma kredito įstaigų ir investicinių įmonių gaivinimo ir pertvarkymo sistema ir iš dalies keičiamos Tarybos direktyva 82/891/EEB, direktyvos 2001/24/EB, 2002/47/EB, 2004/25/EB, 2005/56/EB, 2007/36/EB, 2011/35/ES, 2012/30/ES bei 2013/36/ES ir Europos Parlamento ir Tarybos reglamentai (ES) Nr. 1093/2010 bei (ES) Nr. 648/2012 (OL L 173, 2014 6 12, p. 190).

([9]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/65/ES dėl finansinių priemonių rinkų, kuria iš dalies keičiamos Direktyva 2002/92/EB ir Direktyva 2011/61/ES (OL L 173, 2014 6 12, p. 349).

([10]) 2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 dėl mokėjimo paslaugų vidaus rinkoje, kuria iš dalies keičiamos direktyvos 2002/65/EB, 2009/110/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 ir panaikinama Direktyva 2007/64/EB (OL L 337, 2015 12 23, p. 35).

([11]) 2016 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/2341 dėl profesinių pensijų įstaigų veiklos ir priežiūros (PPĮ) (OL L 354, 2016 12 23, p. 37).

([12]) 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 (žr. šio Oficialiojo leidinio p. 1).

([13]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1093/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos bankininkystės institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/78/EB (OL L 331, 2010 12 15, p. 12).

bankų priežiūros institucijos veiksmingai nustatytų IRT riziką ir stebėtų, kaip ją valdo finansų sektoriaus subjektai pagal naująją skaitmeninės veiklos atsparumo sistemą, SREP taikymo sritis taip pat turėtų būti iš dalies pakeista, kad būtų aiškiai įtraukti Reglamente (ES) 2022/2554 nustatyti reikalavimai ir ji visų pirma apimtų riziką, nustatytą remiantis pranešimais apie didelius su IRT susijusius incidentus ir pagal tą reglamentą finansų sektoriaus subjektų atlikto skaitmeninės veiklos atsparumo testavimo rezultatais;

(5) skaitmeninės veiklos atsparumas yra labai svarbus siekiant išsaugoti finansų sektoriaus subjekto ypatingos svarbos funkcijas ir pagrindines verslo linijas jo pertvarkymo atveju ir taip išvengti realiosios ekonomikos ir finansų sistemos sutrikdymo. Dideli operaciniai incidentai gali trukdyti finansų sektoriaus subjektui toliau vykdyti veiklą ir kelti grėsmę pertvarkymo tikslams. Tam tikri sutartimi įforminti susitarimai dėl IRT paslaugų naudojimo yra labai svarbūs siekiant užtikrinti veiklos tęstinumą ir teikti būtinus duomenis pertvarkymo atveju. Kad Direktyva 2014/59/ES būtų suderinta su Sąjungos veiklos atsparumo sistemos tikslais, ji atitinkamai turėtų būti iš dalies pakeista siekiant užtikrinti, kad planuojant finansų sektoriaus subjektų pertvarkymą ir vertinant pertvarkymo galimybes būtų atsižvelgiama į su veiklos atsparumu susijusią informaciją;

(6) Direktyvoje 2014/65/ES nustatytos griežtesnės IRT rizikos taisyklės investicinėms įmonėms ir prekybos vietoms, kurios vykdo algoritminę prekybą. Duomenų teikimo paslaugoms ir sandorių duomenų saugykloms taikomi ne tokie išsamūs reikalavimai. Be to, Direktyvoje 2014/65/ES nepakankamai minimos informacijos tvarkymo sistemų kontrolės ir apsaugos priemonės ir mažai kalbama apie atitinkamų sistemų, išteklių ir procedūrų naudojimą verslo paslaugų tęstinumui ir reguliarumui užtikrinti. Ta direktyva taip pat turėtų būti suderinta su Reglamentu (ES) 2022/2554, kiek tai susiję su investicinių paslaugų teikimo ir investicinės veiklos tęstinumu bei reguliarumu, veiklos atsparumu, prekybos sistemų pajėgumu, veiklos tęstinumo priemonių veiksmingumu ir rizikos valdymu;

(7) Direktyvoje (ES) 2015/2366 nustatytos specialios IRT saugumo kontrolės taisyklės ir rizikos mažinimo elementai, susiję su veiklos leidimo teikti mokėjimo paslaugas gavimu. Tos veiklos leidimų suteikimo taisyklės turėtų būti iš dalies pakeistos, siekiant jas suderinti su Reglamentu (ES) 2022/2554. Be to, siekiant sumažinti administracinę naštą ir išvengti sudėtingumo ir besidubliuojančių pranešimų teikimo reikalavimų, toje direktyvoje nustatytos pranešimų apie incidentus teikimo taisyklės nebeturėtų būti taikomos mokėjimo paslaugų teikėjams, kurie yra reguliuojami pagal tą direktyvą, ir kuriems taip pat taikomas Reglamentas (ES) 2022/2554, tokiu būdu sudarant sąlygas tiems mokėjimo paslaugų teikėjams naudotis vienu visiškai suderintu pranešimų apie incidentus teikimo mechanizmu dėl visų su mokėjimu susijusių operacinių ar saugumo incidentų nepriklausomai nuo to, ar tokie incidentai yra susiję su IRT;

(8) IRT rizika iš dalies aptariama direktyvų 2009/138/EB ir (ES) 2016/2341 bendrosiose valdymo ir rizikos valdymo nuostatose, o tam tikrus reikalavimus reikia patikslinti deleguotuosiuose aktuose, darant konkrečias nuorodas į IRT riziką arba ne. Panašiai tik bendrosios taisyklės taikomos alternatyvaus investavimo fondų valdytojams, kuriems taikoma Direktyva 2011/61/ES, ir valdymo įmonėms, kurioms taikoma Direktyva 2009/65/EB. Todėl tos direktyvos turėtų būti suderintos su Reglamente (ES) 2022/2554 nustatytais IRT sistemų ir priemonių valdymo reikalavimais;

(9) daugeliu atvejų papildomi IRT rizikos reikalavimai jau buvo nustatyti deleguotuosiuose ir įgyvendinimo aktuose, priimtuose remiantis kompetentingos Europos priežiūros institucijos parengtais reguliavimo techninių standartų projektais ir įgyvendinimo techninių standartų projektais. Kadangi Reglamento (ES) 2022/2554 nuostatos bus finansų sektoriaus subjektų IRT rizikos teisine sistema, direktyvose 2009/65/EB, 2009/138/EB, 2011/61/ES ir 2014/65/ES nustatyti atitinkami įgaliojimai priimti deleguotuosius įgyvendinimo aktus turėtų būti iš dalies pakeisti pašalinant IRT rizikos nuostatas iš tų įgaliojimų taikymo srities;

(10) siekiant užtikrinti nuoseklų naujos finansų sektoriaus skaitmeninės veiklos atsparumo sistemos įgyvendinimą, valstybės narės turėtų taikyti nacionalinės teisės aktų, kuriais į nacionalinę teisę perkeliama ši direktyva, nuostatas nuo Reglamento (ES) 2022/2554 taikymo dienos;

(11) Direktyvos 2009/65/EB, 2009/138/EB, 2011/61/ES, 2013/36/ES, 2014/59/ES, 2014/65/ES, (ES) 2015/2366 ir (ES) 2016/2341 buvo priimtos remiantis Sutarties dėl Europos Sąjungos veikimo (SESV) 53 straipsnio 1 dalimi ar 114 straipsniu, arba remiantis abiem straipsniais. Dėl pakeitimų dalyko ir tikslų tarpusavio sąsajų šia direktyva padaryti pakeitimai buvo įtraukti į vieną teisėkūros procedūra priimamą aktą. Todėl ši direktyva turėtų būti priimta remiantis SESV 53 straipsnio 1 dalimi ir 114 straipsniu;

(12) kadangi šios direktyvos tikslų valstybės narės negali deramai pasiekti, nes jais siekiama direktyvose jau nustatytų reikalavimų suderinimo, o dėl veiksmo masto ir poveikio tų tikslų būtų geriau siekti Sąjungos lygmeniu, laikydamasi Europos Sąjungos sutarties 5 straipsnyje nustatyto subsidiarumo principo, Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šia direktyva neviršijama to, kas būtina nurodytiems tikslams pasiekti;

(13) pagal 2011 m. rugsėjo 28 d. bendrą valstybių narių ir Komisijos politinį pareiškimą dėl aiškinamųjų dokumentų ([14]) valstybės narės įsipareigojo pagrįstais atvejais prie pranešimų apie perkėlimo priemones pridėti vieną ar daugiau dokumentų, kuriuose paaiškinamos direktyvos sudėtinių dalių ir nacionalinių perkėlimo priemonių atitinkamų dalių sąsajos. Šios direktyvos atveju teisės aktų leidėjas laikosi nuomonės, kad tokių dokumentų perdavimas yra pagrįstas,

PRIĖMĖ ŠIĄ DIREKTYVĄ:

1 straipsnis

Direktyvos 2009/65/EB daliniai pakeitimai

Direktyvos 2009/65/EB 12 straipsnis iš dalies keičiamas taip:

1) 1 dalies antroje pastraipoje a punktas pakeičiamas taip:

„a) laikytųsi patikimų administravimo ir apskaitos procedūrų, elektroninio duomenų apdorojimo kontrolės ir apsaugos tvarkos, įskaitant tinklų ir informacines sistemas, įdiegtas ir valdomas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 (*), taip pat taikytų tinkamus vidaus kontrolės mechanizmus, įskaitant visų pirma darbuotojų asmeninių sandorių taisykles arba taisykles, taikomas investicijų į finansines priemones turėjimui ar valdymui siekiant investuoti savo vardu, kuriomis užtikrinama bent tai, kad visus su KIPVPS susijusius sandorius būtų galima atkurti pagal jų kilmę, šalis, pobūdį, įvykdymo laiką ir vietą ir kad valdymo įmonės valdomo KIPVPS turtas būtų investuojamas pagal fondo taisykles arba steigimo dokumentus ir galiojančias teisės nuostatas;

(*) 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).“;

2) 3 dalis pakeičiama taip:

„3. Nedarant poveikio 116 straipsnio taikymui, Komisija, laikydamasi 112a straipsnio, deleguotaisiais teisės aktais patvirtina priemones, kuriose nurodoma:

a) 1 dalies antros pastraipos a punkte nurodytos procedūros ir tvarka, išskyrus procedūras ir tvarką, skirtas tinklų ir informacinėms sistemoms;

b) 1 dalies antros pastraipos b punkte nurodytos struktūros ir organizaciniai reikalavimai, kuriais siekiama kuo labiau sumažinti interesų konfliktų skaičių.“.

([14]) OL C 369, 2011 12 17, p. 14.

2 straipsnis

Direktyvos 2009/138/EB daliniai pakeitimai

Direktyva 2009/138/EB iš dalies keičiama taip:

1) 41 straipsnio 4 dalis pakeičiama taip:

„4. Draudimo ir perdraudimo įmonės imasi pagrįstų veiksmų, įskaitant nenumatytų atvejų planų rengimą, siekdamos užtikrinti savo veiklos tęstinumą ir reguliarumą. Tuo tikslu įmonės naudoja tinkamas ir proporcingas sistemas, išteklius ir procedūras ir visų pirma įdiegia ir valdo tinklų ir informacines sistemas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 (*).

(*) 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).“;

2) 50 straipsnio 1 dalies a ir b punktai pakeičiami taip:

„a) 41 straipsnyje, 44 straipsnyje, visų pirma 44 straipsnio 2 dalyje išvardytos sritys, ir 46 bei 47 straipsniuose nurodytų sistemų elementai, išskyrus elementus, susijusius su informacinių ir ryšių technologijų rizikos valdymu;

b) 44, 46, 47 ir 48 straipsniuose nurodytos funkcijos, išskyrus funkcijas, susijusias su informacinių ir ryšių technologijų rizikos valdymu.“.

3 straipsnis

Direktyvos 2011/61/ES dalinis pakeitimas

Direktyvos 2011/61/ES 18 straipsnis pakeičiamas taip:

„*18 straipsnis*

Bendrieji principai

1. Valstybės narės reikalauja, kad AIFV visada naudotų pakankamus ir tinkamus žmogiškuosius ir techninius išteklius, kurių reikia, kad AIF būtų tinkamai valdomi.

Visų pirma AIFV buveinės valstybės narės kompetentingos institucijos, atsižvelgdamos ir į AIFV valdomų AIF pobūdį, reikalauja, kad AIFV taikytų patikimas administravimo ir apskaitos procedūras, elektroninio duomenų apdorojimo kontrolės ir apsaugos tvarką, įskaitant tinklų ir informacinėms sistemoms, įdiegtoms ir valdomoms pagal Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 (*), taip pat tinkamus vidaus kontrolės mechanizmus, įskaitant, visų pirma, darbuotojų asmeninių sandorių taisykles arba taisykles, taikomas investicijų į finansines priemones turėjimui ar valdymui siekiant investuoti savo vardu, kuriomis užtikrinama bent tai, kad visus su AIF susijusius sandorius būtų galima atkurti pagal jų kilmę, šalis, pobūdį, įvykdymo laiką ir vietą ir kad AIFV valdomų AIF turtas būtų investuojamas pagal AIF taisykles arba steigimo dokumentus ir galiojančias teisės nuostatas.

2. Komisija, naudodamasi teise priimti deleguotuosius aktus pagal 56 straipsnį ir laikydamasi 57 ir 58 straipsniuose nustatytų sąlygų, patvirtina priemones, kuriomis nustatomos šio straipsnio 1 dalyje nurodytos procedūros ir tvarka, išskyrus procedūras ir tvarką, skirtas tinklų ir informacinėms sistemoms.

(*) 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).“.

4 straipsnis

Direktyvos 2013/36/ES daliniai pakeitimai

Direktyva 2013/36/ES iš dalies keičiama taip:

1) 65 straipsnio 3 dalies a punkto vi papunktis pakeičiamas taip:

„vi) trečiosios šalys, kurioms i–iv papunkčiuose nurodyti subjektai perdavė funkcijų ar veiklos vykdymą, įskaitant IRT paslaugas teikiančias trečiąsias šalis, nurodytas Europos Parlamento ir Tarybos reglamento (ES) 2022/2554 (*) V skyriuje;

(*) 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).“;

2) 74 straipsnio 1 dalies pirma pastraipa pakeičiama taip:

„Įstaigose turi būti nustatytos patikimos valdymo priemonės, įskaitant aiškią organizacinę struktūrą, užtikrinant tiksliai apibrėžtą, skaidrią ir nuoseklią atsakomybę, veiksmingi rizikos, su kuria kredito įstaiga susiduria arba gali susidurti, nustatymo, valdymo, stebėsenos ir pranešimo apie tokią riziką procesai, tinkami vidaus kontrolės mechanizmai, įskaitant patikimas administravimo ir apskaitos procedūras, taip pat tinklų ir informacines sistemas, įdiegtas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554, ir atlygio politika bei praktika, deranti su patikimu ir veiksmingu rizikos valdymu ir skatinanti tokį valdymą.“;

3) 85 straipsnio 2 dalis pakeičiama taip:

„2. Kompetentingos institucijos užtikrina, kad įstaigos turėtų tinkamus nenumatytų atvejų ir veiklos tęstinumo politikos priemones ir planus, įskaitant IRT veiklos tęstinumo politiką ir planus ir IRT reagavimo ir veiklos atkūrimo planus, susijusius su technologija, kuria jos naudojasi perduodamos informaciją, ir kad tie planai būtų parengti, valdomi ir testuojami pagal Reglamento (ES) 2022/2554 11 straipsnį, kad įstaigos galėtų toliau veikti rimto veiklos sutrikimo atveju ir sumažinti dėl tokio sutrikimo patiriamus nuostolius.“;

4) 97 straipsnio 1 dalis papildoma šiuo punktu:

„d) rizika, nustatyta atliekant skaitmeninės veiklos atsparumo testavimą pagal Reglamento (ES) 2022/2554 IV skyrių.“.

5 straipsnis

Direktyvos 2014/59/ES daliniai pakeitimai

Direktyva 2014/59/ES iš dalies keičiama taip:

1) 10 straipsnis iš dalies keičiamas taip:

a) 7 dalies c punktas pakeičiamas taip:

„c) paaiškinimas, kaip būtų galima teisiškai ir ekonomiškai atskirti ypatingos svarbos funkcijas ir pagrindines verslo linijas, kiek tai būtina, nuo kitų funkcijų, kad būtų užtikrintas tęstinumas ir skaitmeninės veiklos atsparumas įstaigos žlugimo atveju;“;

b) 7 dalies q punktas pakeičiamas taip:

„q) pagrindinių operacijų ir sistemų, skirtų nepertraukiamam įstaigos veiklos procesų veikimui užtikrinti, įskaitant tinklų ir informacines sistemas, kaip nurodyta Europos Parlamento ir Tarybos reglamente (ES) 2022/2554 (*), aprašas;“;

(*) 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).“;

c) 9 dalis papildoma šia pastraipa:

„Pagal Reglamento (ES) Nr. 1093/2010 10 straipsnį EBI peržiūri ir, jei tikslinga, atnaujina techninius reguliavimo standartus, *inter alia*, kad būtų atsižvelgta į Reglamento (ES) 2022/2554 II skyriaus nuostatas.“;

2) priedas iš dalies keičiamas taip:

a) A skirsnio 16 punktas pakeičiamas taip:

„16. tvarka ir priemonės, būtinos užtikrinant nepertraukiamą įstaigos veiklos procesų veikimą, įskaitant tinklų ir informacines sistemas, įdiegtas ir valdomas pagal Reglamentą (ES) 2022/2554;“;

b) B skirsnis iš dalies keičiamas taip:

i) 14 punktas pakeičiamas taip:

„14. 13 punkte nurodytų sistemų savininkų tapatybė, su tomis sistemomis susiję susitarimai dėl paslaugų lygio, bet kokia programinė įranga ir sistemos ar licencijos, be kita ko, nurodant su jomis susijusius juridinius asmenis, ypatingos svarbos veiklą ir pagrindines verslo linijas, taip pat ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių, kaip apibrėžta Reglamento (ES) 2022/2554 3 straipsnio 23 punkte, tapatybė;“;

ii) įterpiamas šis punktas:

„14a. įstaigų skaitmeninės veiklos atsparumo testavimo pagal Reglamentą (ES) 2022/2554 rezultatai;“;

c) C skirsnis iš dalies keičiamas taip:

i) 4 punktas pakeičiamas taip:

„4. kokiu mastu įstaigos sudaryti paslaugų susitarimai, įskaitant sutartimi įformintus susitarimus dėl IRT paslaugų, yra patikimi ir visapusiškai užtikrinami įstaigos pertvarkymo atveju;“;

ii) įterpiamas šis punktas:

„4a. Tinklų ir informacinių sistemų, naudojamų įstaigos ypatingos svarbos funkcijoms ir pagrindinėms verslo linijoms palaikyti, skaitmeninės veiklos atsparumas, atsižvelgiant į pranešimus apie didelius su IRT susijusius incidentus ir skaitmeninės veiklos atsparumo testavimo pagal Reglamentą (ES) 2022/2554 rezultatus;“.

6 straipsnis

Direktyvos 2014/65/ES daliniai pakeitimai

Direktyva 2014/65/ES iš dalies keičiama taip:

1) 16 straipsnis iš dalies keičiamas taip:

a) 4 dalis pakeičiama taip:

„4. Investicinė įmonė imasi visų pagrįstų priemonių, siekdama užtikrinti investicinių paslaugų ir veiklos tęstinumą bei reguliarumą. Tuo tikslu investicinė įmonė naudoja atitinkamas ir proporcingas sistemas, įskaitant informacinių ir ryšių technologijų (IRT) sistemas, įdiegtas ir valdomas pagal Europos Parlamento ir Tarybos reglamento (ES) 2022/2554 (*) 7 straipsnį, taip pat atitinkamus ir proporcingus išteklius ir procedūras.

(*) 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).“;

b) 5 dalies antra ir trečia pastraipos pakeičiamos taip:

„Investicinė įmonė taiko patikimas administracines ir apskaitos procedūras, vidaus kontrolės mechanizmus ir veiksmingas rizikos vertinimo procedūras.

Nedarant poveikio kompetentingų institucijų galimybei reikalauti prieigos prie perduodamos informacijos pagal šią direktyvą ir Reglamentą (ES) Nr. 600/2014, investicinė įmonė taiko įdiegtus patikimus apsaugos mechanizmus, kad pagal Reglamento (ES) 2022/2554 reikalavimus užtikrintų informacijos perdavimo priemonių saugumą ir atpažintį, kuo labiau sumažintų duomenų iškraipymo ir neteisėtos prieigos riziką ir išvengtų informacijos nutekėjimo, visuomet išlaikydama duomenų konfidencialumą.“;

2) 17 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. Algoritmine prekyba užsiimanti investicinė įmonė taiko veiksmingas sistemas ir rizikos kontrolės priemones, kurios yra tinkamos jos vykdomos veiklos atžvilgiu, siekdama užtikrinti, kad jos prekybos sistemos būtų atsparios ir pakankamai pajėgios pagal Reglamento (ES) 2022/2554 II skyriuje nustatytus reikalavimus, kad joms būtų taikomos atitinkamos prekybos ribos ir apribojimai ir kad būtų išvengta klaidingų pavedimų siuntimo ar kitokių sistemos klaidų, galinčių rinkoje sukelti arba padidinti sąmyšį.

Be to, tokia įmonė taiko veiksmingas sistemas ir rizikos kontrolės priemones, siekdama užtikrinti, kad prekybos sistemos nebūtų naudojamos tokiems tikslams, kurie prieštarauja Reglamento (ES) Nr. 596/2014 nuostatoms arba prekybos vietos, su kuria ji yra susijusi, taisyklėms.

Investicinė įmonė turi įdiegti veiksmingas veiklos tęstinumo priemones, skirtas bet kokiems jos prekybos sistemų trikdžiams šalinti, įskaitant IRT veiklos tęstinumo politiką ir planus ir IRT reagavimo ir veiklos atkūrimo planus, parengtus pagal Reglamento (ES) 2022/2554 11 straipsnį, ir užtikrina, kad jos sistemos būtų visapusiškai testuojamos ir tinkamai stebimos siekiant užtikrinti jų atitiktį šioje dalyje nustatytiems bendriesiems reikalavimams ir visiems Reglamento (ES) 2022/2554 II ir IV skyriuose nustatytiems konkretiems reikalavimams.“;

b) 7 dalies a punktas pakeičiamas taip:

„a) išsamią 1–6 dalyse nustatytų organizacinių reikalavimų, išskyrus reikalavimus, susijusius su IRT rizikos valdymu, kurie turi būti taikomi investicinėms įmonėms, teikiančioms įvairias investicines paslaugas, vykdančioms investicinę veiklą, teikiančioms papildomas paslaugas arba įvairiais būdais derinančioms šias veiklas, tvarką, pagal kurią 5 dalyje nustatytų organizacinių reikalavimų specifikacijose nustatomi konkretūs tiesioginės rinkos prieigos ir suteiktosios prieigos reikalavimai taip, kad būtų užtikrinta, jog suteiktajai prieigai taikoma kontrolė būtų bent lygiavertė kontrolei, taikomai tiesioginei rinkos prieigai;“;

3) 47 straipsnio 1 dalis iš dalies keičiama taip:

a) b punktas pakeičiamas taip:

„b) turėtų tinkamas jai kylančios rizikos valdymo priemones, įskaitant IRT rizikos valdymo priemones pagal Reglamento (ES) 2022/2554 II skyrių, nustatytų tinkamas priemones ir sistemas, kurias taikant galima nustatyti didelę riziką, susijusią su jos veikimu, ir įgyvendintų priemones, kuriomis galima veiksmingai sumažinti tos rizikos poveikį;“;

b) c punktas išbraukiamas;

4) 48 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. Valstybės narės reikalauja, kad reguliuojama rinka nustatytų ir palaikytų veiklos atsparumą pagal Reglamento (ES) 2022/2554 II skyriuje nustatytus reikalavimus, siekdama užtikrinti, kad jos prekybos sistemos būtų atsparios, pakankamai pajėgios susidoroti su didžiausiais pavedimų ir pranešimų kiekiais, galėtų užtikrinti tvarkingą prekybą esant itin dideliam rinkos spaudimui, būtų visapusiškai testuojamos siekiant užtikrinti tokių sąlygų laikymąsi ir jose būtų taikomos veiksmingos veiklos tęstinumo priemonės, įskaitant IRT veiklos tęstinumo politiką ir planus ir IRT reagavimo ir veiklos atkūrimo planus, parengtus pagal Reglamento (ES) 2022/2554 11 straipsnį, siekiant užtikrinti jos paslaugų tęstinumą, jei įvyktų bet koks jos prekybos sistemų gedimas.“;

b) 6 dalis pakeičiama taip:

„6. Valstybės narės reikalauja, kad reguliuojama rinka taikytų veiksmingas sistemas, procedūras ir priemones, be kita ko, įpareigotų savo narius arba dalyvius atlikti tinkamą algoritmų testavimą ir suteiktų tokiam testavimui palankią aplinką pagal Reglamento (ES) 2022/2554 II ir IV skyriuose nustatytus reikalavimus, kad užtikrintų, kad algoritminės prekybos sistemos negalėtų sukurti arba paskatinti susidaryti tvarką pažeidžiančių prekybos sąlygų rinkoje ir valdytų tokių algoritminės prekybos sistemų iš tiesų sukeltas tvarką pažeidžiančias prekybos sąlygas, įskaitant sistemas, skirtas neįvykdytų pavedimų ir sandorių, kuriuos į sistemą gali įvesti narys arba dalyvis, santykiui riboti, kad turėtų galimybę sulėtinti pavedimų srautą, jei kyla pavojus, kad bus viršytas jos sistemos pajėgumas, ir nustatyti minimalų kainos pokyčio dydį, kuris rinkoje gali būti naudojamas vykdant pavedimus, ir užtikrinti jo taikymą.“;

c) 12 dalis iš dalies keičiama taip:

i) a punktas pakeičiamas taip:

„a) reikalavimai, skirti užtikrinti, kad reguliuojamos rinkos prekybos sistemos būtų atsparios ir pakankamai pajėgios, išskyrus reikalavimus, susijusius su skaitmeninės veiklos atsparumu;“;

ii) g punktas pakeičiamas taip:

„g) reikalavimai, skirti tinkamam algoritmų testavimui, išskyrus skaitmeninės veiklos atsparumo testavimą, užtikrinti, kuriais užtikrinama, kad algoritminės prekybos sistemos, įskaitant didelio dažnio algoritmines prekybos sistemas, negalėtų sukurti arba paskatinti susidaryti tvarką pažeidžiančių prekybos sąlygų rinkoje.“.

7 straipsnis

Direktyvos (ES) 2015/2366 daliniai pakeitimai

Direktyva (ES) 2015/2366 iš dalies keičiama taip:

1) 3 straipsnio j punktas pakeičiamas taip:

„j) paslaugoms, kurias teikia techninių paslaugų teikėjai, užtikrinantys mokėjimo paslaugų teikimą, bet niekada neįgyjantys pervedamų lėšų, įskaitant duomenų tvarkymą ir saugojimą, patikėjimo ir privatumo apsaugos paslaugas, duomenų ir subjekto autentiškumo patvirtinimą, informacinių ir ryšių technologijų (IRT) ir ryšių tinklo suteikimą, mokėjimo paslaugoms teikti naudojamų terminalų ir prietaisų suteikimą bei priežiūrą, išskyrus mokėjimo inicijavimo paslaugas ir informavimo apie sąskaitas paslaugas;“;

2) 5 straipsnio 1 dalis iš dalies keičiama taip:

a) pirma pastraipa iš dalies keičiama taip:

i) e punktas pakeičiamas taip:

„e) pareiškėjo taikomos valdymo tvarkos ir vidaus kontrolės mechanizmų, įskaitant administracines, rizikos valdymo ir apskaitos procedūras, taip pat susitarimus dėl IRT paslaugų naudojimo pagal Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 (*), aprašymą, įrodantį, kad ta valdymo tvarka ir tie vidaus kontrolės mechanizmai yra proporcingi, tinkami, patikimi ir pakankami;“;

(*) 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).“;

ii) f punktas pakeičiamas taip:

„f) nustatytos procedūros, pagal kurią stebimi saugumo incidentai ir su saugumu susiję klientų skundai, į juos reaguojama ir imamasi tolesnių veiksmų, įskaitant pranešimų apie incidentus teikimo mechanizmą, kurį taikant atsižvelgiama į Reglamento (ES) 2022/2554 III skyriuje nustatytas mokėjimo įstaigos pareigas pranešti, aprašymą;“;

iii) h punktas pakeičiamas taip:

„h) veiklos tęstinumo priemonių aprašymą, jame aiškiai nurodant ypatingos svarbos operacijas, veiksmingą IRT veiklos tęstinumo politiką ir planus bei IRT reagavimo ir veiklos atkūrimo planus ir reguliaraus tokių planų adekvatumo ir efektyvumo testavimo bei peržiūros procedūrą pagal Reglamentą (ES) 2022/2554;“;

b) trečia pastraipa pakeičiama taip:

„Pirmos pastraipos j punkte nurodytų saugumo kontrolės ir rizikos mažinimo priemonių aprašyme nurodoma, kaip jomis užtikrinamas aukštas skaitmeninės veiklos atsparumo lygis pagal Reglamento (ES) 2022/2554 II skyrių, visų pirma kiek tai susiję su techninio saugumo ir duomenų apsauga, įskaitant programinę įrangą ir IRT sistemas, kurias naudoja pareiškėjas arba įmonės, kurioms jis perduoda vykdyti visas savo operacijas arba jų dalį. Tos priemonės taip pat apima šios direktyvos 95 straipsnio 1 dalyje nustatytas saugumo priemones. Tomis priemonėmis atsižvelgiama į šios direktyvos 95 straipsnio 3 dalyje nurodytas EBI gaires dėl saugumo priemonių, kai jos bus priimtos.“;

3) 19 straipsnio 6 dalies antra pastraipa pakeičiama taip:

„Svarbių veiklos funkcijų, įskaitant IRT sistemas, vykdymas neperduodamas išorės subjektams taip, kad iš esmės pablogintų mokėjimo įstaigos vidaus kontrolės kokybę ir kompetentingų institucijų galimybes stebėti ir atsekti, kaip mokėjimo įstaiga laikosi visų šioje direktyvoje nustatytų pareigų.“;

4) 95 straipsnio 1 dalis papildoma šia pastraipa:

„Pirma pastraipa nedaro poveikio Reglamento (ES) 2022/2554 II skyriaus taikymui:

a) šios direktyvos 1 straipsnio 1 dalies a, b ir d punktuose nurodytiems mokėjimo paslaugų teikėjams;

b) šios direktyvos 33 straipsnio 1 dalyje nurodytiems informavimo apie sąskaitas paslaugos teikėjams;

c) mokėjimo įstaigoms, kurioms taikoma išimtis pagal šios direktyvos 32 straipsnio 1 dalį ir

d) elektroninių pinigų įstaigoms, kurios naudojasi netaikymo sąlyga, kaip nurodyta Direktyvos 2009/110/EB 9 straipsnio 1 dalyje.“;

5) 96 straipsnis papildomas šia dalimi:

„7. Valstybės narės užtikrina, kad šio straipsnio 1–5 dalys nebūtų taikomos:

a) šios direktyvos 1 straipsnio 1 dalies a, b ir d punktuose nurodytiems mokėjimo paslaugų teikėjams;

b) šios direktyvos 33 straipsnio 1 dalyje nurodytiems informavimo apie sąskaitas paslaugos teikėjams;

c) mokėjimo įstaigoms, kurioms taikoma išimtis pagal šios direktyvos 32 straipsnio 1 dalį, ir

d) elektroninių pinigų įstaigoms, kurios naudojasi išimtimi, kaip nurodyta Direktyvos 2009/110/EB 9 straipsnio 1 dalyje.“;

6) 98 straipsnio 5 dalis pakeičiama taip:

„5. Pagal Reglamento (ES) Nr. 1093/2010 10 straipsnį EBI peržiūri ir, jei tikslinga, reguliariai atnaujina reguliavimo techninius standartus, *inter alia*, kad būtų atsižvelgta į inovacijų ir technologinę plėtrą ir Reglamento (ES) 2022/2554 II skyriaus nuostatas.“.

8 straipsnis

Direktyvos (ES) 2016/2341 dalinis pakeitimas

Direktyvos (ES) 2016/2341 21 straipsnio 5 dalis pakeičiama taip:

„5. Valstybės narės užtikrina, kad PPĮ imtųsi pagrįstų veiksmų, įskaitant nenumatytų atvejų planų rengimą, kad užtikrintų savo veiklos tęstinumą ir reguliarumą. Tuo tikslu PPĮ naudoja tinkamas ir proporcingas sistemas, išteklius ir

procedūras ir, kai taikytina, visų pirma įdiegia ir valdo tinklų ir informacines sistemas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 (*).

(*) 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).“.

9 straipsnis

Perkėlimas į nacionalinę teisę

1. Valstybės narės ne vėliau kaip 2025 m. sausio 17 d. priima ir paskelbia nuostatas, būtinas, kad būtų laikomasi šios direktyvos. Apie tai jos nedelsdamos praneša Komisijai.

Tas nuostatas jos taiko nuo 2025 m. sausio 17 d.

Valstybės narės, priimdamos tas nuostatas, daro jose nuorodą į šią direktyvą arba tokia nuoroda daroma jas oficialiai skelbiant. Tokios nuorodos darymo tvarką nustato valstybės narės.

2. Įsigaliojus šiai direktyvai valstybės narės užtikrina, kad Komisijai būtų laiku pranešta apie visus įstatymų ir kitų teisės aktų projektus, kuriuos jos ketina priimti šios direktyvos taikymo srityje, kad Komisija galėtų pateikti pastabas.

10 straipsnis

Įsigaliojimas

Ši direktyva įsigalioja dvidešimtą dieną po jos paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

11 straipsnis

Adresatai

Ši direktyva skirta valstybėms narėms.

Priimta Strasbūre 2022 m. gruodžio 14 d.

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkė	*Pirmininkas*
R. METSOLA	M. BEK

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2022/2557

2022 m. gruodžio 14 d.

dėl ypatingos svarbos subjektų atsparumo, kuria panaikinama Tarybos direktyva 2008/114/EB

(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]),

atsižvelgdami į Regionų komiteto nuomonę ([2]),

laikydamiesi įprastos teisėkūros procedūros ([3]),

kadangi:

(1) ypatingos svarbos subjektai, kaip esminių paslaugų teikėjai, atlieka nepakeičiamą vaidmenį palaikant gyvybiškai svarbias visuomenės funkcijas ar ekonominę veiklą vidaus rinkoje, Sąjungos ekonomikai tampant vis glaudžiau susietai tarpusavio priklausomybės ryšiais. Todėl ypač svarbu nustatyti Sąjungos masto sistemą, kuria būtų siekiama tiek didinti ypatingos svarbos subjektų atsparumą vidaus rinkoje, nustatant suderintą būtinųjų taisyklių rinkinį, tiek padėti jiems pasitelkiant nuoseklias bei tikslines paramos ir priežiūros priemones;

(2) Tarybos direktyvoje 2008/114/EB ([4]) numatyta tvarka, pagal kurią energetikos ir transporto sektoriaus infrastruktūros objektai priskiriami Europos ypatingos svarbos infrastruktūros objektams, kurių veikimo sutrikdymas arba sunaikinimas sukeltų didelį tarpvalstybinį poveikį bent dviem valstybėms narėms. Toje direktyvoje daugiausia dėmesio skiriama tik tokių infrastruktūrų apsaugai. Tačiau 2019 m. atlikus direktyvos 2008/114/EB vertinimą nustatyta, kad veiklai, kurios tikslu naudojamasi ypatingos svarbos infrastruktūra, tampant vis glaudžiau tarpusavyje susietai ir vis labiau tarpvalstybinio pobūdžio, apsaugos priemonės, orientuotos tik į atskirą turtą, nėra pakankamos, kad būtų užkirstas kelias visiems sutrikimams. Todėl būtina požiūrį orientuoti labiau į pastangas

([1]) OL C 286, 2021 7 16, p. 170.
([2]) OL C 440, 2021 10 29, p. 99.
([3]) 2022 m. lapkričio 22 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2022 m. gruodžio 8 d. Tarybos sprendimas.
([4]) 2008 m. gruodžio 8 d. Tarybos direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo (OL L 345, 2008 12 23, p. 75).

užtikrinti, kad būtų labiau atsižvelgiama į riziką, būtų geriau apibrėžtas ir suderintas ypatingos svarbos subjektų, kaip paslaugų, kurios yra esminės vidaus rinkos veikimui, teikėjų vaidmuo ir pareigos ir būtų priimtos Sąjungos masto taisyklės, siekiant padidinti ypatingos svarbos subjektų atsparumą. Ypatingos svarbos subjektai turėtų turėti galimybes stiprinti savo gebėjimą užkirsti kelią incidentams, dėl kurių gali sutrikti esminių paslaugų teikimas, nuo jų apsaugoti, į juos reaguoti, juos atlaikyti, sušvelninti jų poveikį, juos įveikti, prisitaikyti prie jų ir po jų atstatyti veiklą;

(3) ypatingos svarbos infrastruktūros apsaugą Sąjungoje siekiama remti keliomis priemonėmis Sąjungos lygmeniu, tokiomis kaip Europos programa dėl ypatingos svarbos infrastruktūros objektų apsaugos, ir nacionaliniu lygmeniu, tačiau turėtų būti nuveikta daugiau, kad tokią infrastruktūrą eksploatuojantys subjektai būtų geriau pasirengę šalinti jų veiklai kylančią riziką, dėl kurios galėtų sutrikti esminių paslaugų teikimas. Taip pat turėtų būti nuveikta daugiau, kad tokie subjektai būtų geriau pasirengę, nes yra dinamiška grėsmių įvairovė, įskaitant kintančias hibridines ir terorizmo grėsmes, ir dėl to, kad didėja infrastruktūrų ir sektorių tarpusavio priklausomybė. Dar daugiau, didėja fizinė rizika, kylanti dėl gaivalinių nelaimių ir klimato kaitos, dėl kurios poveikio ekstremalių meteorologinių reiškinių dažnumas ir mastas didėja, atsiranda ilgalaikių vidutinių klimato sąlygų pokyčių ir, jei nebus imamasi prisitaikymo prie klimato kaitos priemonių, gali sumažėti tam tikrų rūšių infrastruktūros pajėgumas, veiksmingumas ir eksploatavimo trukmė. Be to, vidaus rinkai yra būdingas susiskaidymas, kiek tai susiję su ypatingos svarbos subjektų identifikavimu, nes atitinkami sektoriai ir atitinkamos subjektų kategorijos nėra visose valstybėse narėse nuosekliai pripažįstami kaip ypatingos svarbos. Todėl šia direktyva turėtų būti pasiektas patikimas suderinimo lygis, kiek tai susiję su tuo, kokie sektoriai ir subjektų kategorijos patenka į jos taikymo sritį;

(4) nors tam tikri ekonomikos sektoriai, tokie kaip energetikos ir transporto sektoriai, jau yra reglamentuojami konkretiems sektoriams taikomais Sąjungos teisės aktais, tų aktų nuostatos yra susijusios tik su tam tikrais šiuose sektoriuose veikiančių subjektų atsparumo aspektais. Siekiant visapusiškai spręsti šių subjektų, kurie yra ypatingos svarbos tinkamam vidaus rinkos veikimui, atsparumo klausimą, šia direktyva sukuriama visa apimanti sistema, kurioje sprendžiamas ypatingos svarbos subjektų atsparumo klausimas atsižvelgiant į visus pavojus, t. y. gaivalines ar žmogaus sukeltas nelaimes, atsitiktines ar tyčia sukeltas;

(5) didėjančią infrastruktūros ir sektorių tarpusavio priklausomybę lemia vis labiau tarpvalstybinio pobūdžio ir tarpusavyje priklausomas paslaugų teikimo tinklas, kuriame naudojamos pagrindinė visoje Sąjungoje esanti energetikos, transporto, bankų, geriamojo vandens, nuotekų, maisto gamybos, perdirbimo ir platinimo, sveikatos, kosmoso, finansų rinkos infrastruktūra ir skaitmeninės infrastruktūros sektoriai, taip pat tam tikri viešojo administravimo sektoriaus aspektai. Kosmoso sektoriui ši direktyva taikoma tiek, kiek tai susiję su tam tikrų paslaugų teikimu, grindžiamu antžeminėmis infrastruktūromis, kurios priklauso valstybėms narėms arba privatiems subjektams, yra jų valdomos arba eksploatuojamos, todėl ši direktyva neapima infrastruktūrų, kurios priklauso Sąjungai ar nuosavybės teise yra turimos jos vardu, yra Sąjungos ar jos vardu valdomos ar eksploatuojamos, jai įgyvendinant savo kosmoso programą.

Kalbant apie energetikos sektorių ir visų pirma elektros energijos gamybos ir perdavimo (tiekiant elektros energiją) metodus, suprantama, kad, kai tai laikoma tikslinga, elektros energijos gamyba gali apimti atominių elektrinių elektros energijos perdavimo dalis, tačiau neapima konkrečiai branduolinių elementų, kuriems taikomos sutartys ir Sąjungos teisė, įskaitant atitinkamus Sąjungos branduolinės energetikos srities teisės aktus. Maisto sektoriaus ypatingos svarbos subjektų identifikavimo procesas turėtų tinkamai atspindėti vidaus rinkos šiame sektoriuje pobūdį ir išsamias Sąjungos taisykles, susijusias su maisto srities teisės aktų ir maisto saugos bendraisiais principais ir reikalavimais. Todėl, siekiant užtikrinti proporcingą požiūrį ir tinkamai atspindėti šių subjektų vaidmenį ir svarbą nacionaliniu lygmeniu, maisto tvarkymo įmonės turėtų būti identifikuojamos kaip ypatingos svarbos subjektai tik jei tos maisto tvarkymo įmonės – neatsižvelgiant į tai, ar jos siekia pelno ar jo nesiekia, yra valstybinės ar privačios – užsiima tik logistika, didmeniniu platinimu, didelio masto pramonine gamyba ir perdirbimu ir joms tenka reikšminga, kaip nustatyta, rinkos dalis nacionaliniu lygmeniu. Ši tarpusavio priklausomybė reiškia, kad bet koks esminių paslaugų sutrikimas, net ir toks, kuris iš pradžių įvyksta tik viename subjekte arba sektoriuje, gali turėti platesnį grandininį poveikį ir sukelti plataus masto ir ilgalaikes neigiamas pasekmes paslaugų teikimui visoje vidaus rinkoje. Didelės krizės, kaip, pavyzdžiui, COVID-19 pandemija, parodė, kad mūsų vis labiau tarpusavyje priklausomos visuomenės yra pažeidžiamos susidūrus su mažai tikėtina didelio poveikio rizika;

(6) subjektams, kurie dalyvauja teikiant esmines paslaugas, taikoma vis daugiau skirtingų reikalavimų, nustatytų nacionalinės teisės aktuose. Tai, kad kai kurios valstybės narės yra nustačiusios ne tokius griežtus saugumo reikalavimus tiems subjektams, ne tik lemia skirtingus atsparumo lygius, bet ir gali sukelti neigiamą poveikį gyvybiškai svarbių visuomenės funkcijų arba ekonominės veiklos išlaikymui visoje Sąjungoje, taip pat sukuria kliūtis tinkamam vidaus rinkos veikimui. Investuotojai ir įmonės gali pasikliauti ir pasitikėti ypatingos svarbos subjektais, kurie yra atsparūs, o patikimumas ir pasitikėjimas yra gerai veikiančios vidaus rinkos kertiniai akmenys. Panašios rūšies subjektai vienose valstybėse narėse laikomi ypatingos svarbos subjektais, o kitose ne, be to, įvairiose valstybėse narėse subjektams, identifikuotiems kaip ypatingos svarbos subjektai, taikomi skirtingi reikalavimai. Taip tarpvalstybiniu mastu veikiančioms įmonėms, visų pirma veikiančioms valstybėse narėse, kuriose galioja griežtesni reikalavimai, susidaro papildoma ir nereikalinga administracinė našta. Todėl Sąjungos masto sistema taip pat padėtų suvienodinti ypatingos svarbos subjektų veiklos sąlygas visoje Sąjungoje;

(7) reikia nustatyti suderintas būtinąsias taisykles ir taip užtikrinti esminių paslaugų teikimą vidaus rinkoje, didinti ypatingos svarbos subjektų atsparumą ir gerinti kompetentingų institucijų tarpvalstybinį bendradarbiavimą. Svarbu, kad tos taisyklės būtų sumanytos ir įgyvendinamos taip, kad jos būtų parengtos ateities iššūkiams, sudarant sąlygas reikiamam lankstumui. Taip pat labai svarbu gerinti ypatingos svarbos subjektų pajėgumą teikti esmines paslaugas tais atvejais, kai susiduriama su keliomis skirtingomis rizikomis iš karto;

(8) kad pasiektų aukštą atsparumo lygį, valstybės narės turėtų identifikuoti ypatingos svarbos subjektus, kuriems bus taikomi specialūs reikalavimai ir priežiūra, ir kuriems bus teikiama ypatinga parama ir gairės kilus bet kokiai atitinkamai rizikai;

(9) kadangi siekiant ypatingos svarbos subjektų atsparumo itin svarbus yra kibernetinis saugumas, taip pat siekiant užtikrinti nuoseklumą, visais atvejais, kai tai įmanoma, turėtų būti užtikrintas suderintas požiūris tarp šios direktyvos ir Europos Parlamento ir Tarybos direktyvos (ES) 2022/2555 ([5]) Atsižvelgiant į kibernetinės rizikos padažnėjimą ir konkrečius jos ypatumus, Direktyvoje (ES) 2022/2555 nustatyti išsamūs įvairiems subjektams taikomi reikalavimai, kuriais siekiama užtikrinti jų kibernetinį saugumą. Atsižvelgiant į tai, kad kibernetinis saugumas Direktyvoje (ES) 2022/2555 aptartas pakankamai, toje direktyvoje nagrinėjami klausimai neturėtų patekti į šios direktyvos taikymo sritį, nedarant poveikio specialiai tvarkai, taikomai skaitmeninės infrastruktūros sektoriaus subjektams;

(10) jeigu pagal konkretiems sektoriams taikomus Sąjungos teisės aktų nuostatas reikalaujama, kad ypatingos svarbos subjektai imtųsi priemonių padidinti savo atsparumą, ir jeigu tuos reikalavimus valstybės narės pripažįsta bent jau lygiaverčiais šioje direktyvoje nustatytoms atitinkamoms pareigoms, atitinkamos šios direktyvos nuostatos neturėtų būti taikomos, kad būtų išvengta dubliavimo ir nereikalingos naštos. Tokiu atveju turėtų būti taikomos atitinkamos tokių Sąjungos teisės aktų nuostatos. Jeigu atitinkamos šios direktyvos nuostatos netaikomos, taip pat neturėtų būti taikomos šioje direktyvoje nustatytos nuostatos dėl priežiūros ir vykdymo užtikrinimo;

(11) šia direktyva nedaromas poveikis valstybių narių ir jų institucijų kompetencijai, kiek tai susiję su administraciniu savarankiškumu, arba jų atsakomybei užtikrinti nacionalinį saugumą ir gynybą ar jų įgaliojimams užtikrinti kitas esmines valstybės funkcijas, visų pirma susijusias su viešuoju saugumu, teritoriniu vientisumu ir viešosios tvarkos palaikymu. Ši direktyva neturėtų būti taikoma viešojo administravimo subjektams, kurie veiklą vykdo daugiausia nacionalinio saugumo, viešojo saugumo, gynybos ir teisėsaugos srityse, įskaitant nusikalstamų veikų tyrimą, nustatymą ir baudžiamąjį persekiojimą už jas. Tačiau ši direktyva turėtų būti taikoma viešojo administravimo subjektams, kurių veikla su tomis sritimis susijusi tik nežymiai. Šios direktyvos tikslais kompetenciją reglamentavimo srityje turintys subjektai nelaikomi subjektais, vykdančiais veiklą teisėsaugos srityje, todėl ši direktyva nėra jiems netaikoma tuo pagrindu. Ši direktyva netaikoma viešojo administravimo subjektams, kurie yra bendrai įsteigti su trečiąja valstybe pagal tarptautinį susitarimą. Ši direktyva netaikoma valstybių narių diplomatinėms atstovybėms ir konsulinėms įstaigoms trečiosiose valstybėse.

([5]) 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 80).

Tam tikri ypatingos svarbos subjektai vykdo veiklą nacionalinio saugumo, viešojo saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas, arba teikia paslaugas tik viešojo administravimo subjektams, kurių veikla daugiausia vykdoma tose srityse. Atsižvelgdamos į valstybių narių atsakomybę užtikrinti nacionalinį saugumą ir gynybą, valstybės narės turėtų galėti nuspręsti, kad ypatingos svarbos subjektams šioje direktyvoje nustatytos pareigos tiems ypatingos svarbos subjektams turėtų būti visiškai ar iš dalies netaikomos, jeigu jų paslaugos daugiausia teikiamos arba jų veikla daugiausia vykdoma nacionalinio saugumo, viešojo saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas. Ši direktyva vis tik turėtų būti taikoma ypatingos svarbos subjektams, kurių paslaugos ar veikla su tomis sritimis susijusios tik nežymiai. Jokia valstybė narė neturėtų privalėti teikti informacijos, kurios atskleidimas būtų priešingas esminiams jos nacionalinio saugumo interesams. Šiuo atveju aktualios yra Sąjungos arba nacionalinės taisyklės dėl įslaptintos informacijos apsaugos ir informacijos neatskleidimo susitarimai;

(12) siekiant nepakenkti nacionaliniam saugumui ar ypatingos svarbos subjektų saugumui ir komerciniams interesams, prieiga prie neskelbtinos informacijos, keitimasis ja ir jos tvarkymas turėtų būti vykdomi apdairiai, ypatingą dėmesį skiriant perdavimo kanalams ir saugojimo pajėgumams, kuriais bus naudojamasi;

(13) kiekviena valstybė narė, siekdama užtikrinti visapusišką požiūrį į ypatingos svarbos subjektų atsparumą, turėtų būti nustačiusi ypatingos svarbos subjektų atsparumo didinimo strategiją (toliau – strategija). Strategijoje turėtų būti išdėstyti strateginiai tikslai ir įgyvendintinos politikos priemonės. Siekiant nuoseklumo ir veiksmingumo, strategija turėtų būti parengta taip, kad būtų sklandžiai integruota esama politika, remiantis, kai įmanoma, atitinkamomis esamomis nacionalinėmis ir sektorinėmis strategijomis, planais ar panašiais dokumentais nacionaliniu ir sektorių lygmeniu. Siekdamos visapusiško požiūrio valstybės narės turėtų užtikrinti, kad jų strategijose būtų numatyta politikos sistema, pagal kurią kompetentingos institucijos pagal šią direktyvą, ir kompetentingos institucijos pagal Direktyvą (ES) 2022/2555 tvirčiau tarpusavyje koordinuotų veiklą joms dalijantis informacija apie kibernetiniam saugumui kylančią riziką, kibernetines grėsmes ir kibernetinius incidentus ir nekibernetinę riziką, grėsmes bei incidentus, taip pat joms vykdant priežiūros užduotis. Įgyvendindamos savo strategijas, valstybės narės turėtų tinkamai atsižvelgti į hibridinį grėsmių ypatingos svarbos subjektams pobūdį;

(14) valstybės narės turėtų pateikti savo strategijas ir jų esminius atnaujinimus Komisijai, visų pirma tam, kad Komisija galėtų įvertinti, ar ši direktyva nacionaliniu lygmeniu taikoma teisingai, kiek tai susiję su ypatingos svarbos subjektų atsparumui taikoma politika. Prireikus strategijos galėtų būti pateikiamos kaip įslaptinta informacija. Komisija turėtų parengti apibendrinamąją ataskaitą apie valstybių narių pateiktas strategijas, kad ja būtų galima remtis Ypatingos svarbos subjektų atsparumo klausimų grupės diskusijose, skirtose geriausiai praktikai ir bendro intereso klausimams nustatyti. Atsižvelgiant į agreguotos informacijos apibendrinamojoje ataskaitoje (nesvarbu, ar ta informacija įslaptinta, ar ne) neskelbtiną pobūdį, Komisija šią apibendrinamąją ataskaitą turėtų tvarkyti užtikrindama tinkamą sąmoningumo lygį ypatingos svarbos subjektų, valstybių narių ir Sąjungos saugumo klausimais. Apibendrinamoji ataskaita ir strategijos turėtų būti apsaugotos nuo neteisėtų ar piktavališkų veiksmų ir turėtų būti prieinamos tik įgaliotiems asmenims, kad būtų pasiekti šios direktyvos tikslai. Toks strategijų ir jų esminių atnaujinimų pateikimas taip pat turėtų padėti Komisijai suprasti požiūrių į ypatingos svarbos subjektų atsparumą pokyčius ir padėti stebėti šios direktyvos, kurią Komisija turi periodiškai peržiūrėti, poveikį ir pridėtinę vertę;

(15) valstybės narės, vykdydamos veiksmus, kuriais siekiama identifikuoti ypatingos svarbos subjektus ir padėti užtikrinti jų atsparumą, turėtų laikytis rizika grindžiamo požiūrio, kuriuo pastangos būtų telkiamos į subjektus, kurie yra svarbiausi gyvybiškai svarbių visuomenės funkcijų ar ekonominės veiklos vykdymui. Kad užtikrintų tokį tikslinį požiūrį, kiekviena valstybė narė, naudodamasi suderinta sistema, turėtų įvertinti aktualią gaivalinių ir žmogaus sukeltų nelaimių riziką, įskaitant tarpsektorinio ir tarpvalstybinio pobūdžio riziką, galinčią daryti poveikį esminių paslaugų teikimui, įskaitant avarijas, gaivalines nelaimes, ekstremaliąsias visuomenės sveikatos situacijas, pavyzdžiui, pandemijas ir hibridines grėsmes ar kitas priešiškų subjektų keliamas grėsmes, įskaitant teroristinius nusikaltimus, nusikalstamo pasaulio įsiskverbimą ir sabotažą (toliau – valstybės narės rizikos vertinimas). Atlikdamos valstybių narių rizikos vertinimus, valstybės narės turėtų atsižvelgti į kitus bendro pobūdžio arba konkretaus sektoriaus rizikos vertinimus, atliktus pagal kitus Sąjungos teisės aktus, ir turėtų įvertinti, kiek sektoriai priklausomi tarpusavyje, įskaitant priklausomybę nuo kitų valstybių narių ir trečiųjų valstybių sektorių. Valstybių

narių rizikos vertinimų rezultatai turėtų būti naudojami ypatingos svarbos subjektų identifikavimo procese ir padėti šiems subjektams laikytis jų atsparumo reikalavimų. Ši direktyva taikoma tik valstybėms narėms ir Sąjungoje veiklą vykdantiems ypatingos svarbos subjektams. Vis dėlto, kai tinkama ir laikantis taikytinų teisės aktų, kompetentingų institucijų patirtimi ir žiniomis, sukauptomis visų pirma atliekant rizikos vertinimus, taip pat Komisijos patirtimi ir žiniomis, sukauptomis visų pirma teikiant įvairių formų paramą ir vykdant bendradarbiavimą, galėtų būti pasinaudota trečiųjų valstybių, visų pirma esančių Sąjungos tiesioginėje kaimynystėje, labui, ta patirtimi ir žiniomis prisidedant prie esamo bendradarbiavimo atsparumo srityje;

(16) siekiant užtikrinti, kad šioje direktyvoje nustatyti atsparumo reikalavimai būtų taikomi visiems atitinkamiems subjektams, ir sumažinti skirtumus tuo atžvilgiu, svarbu nustatyti suderintas taisykles, kurios sudarytų sąlygas nuosekliai identifikuoti ypatingos svarbos subjektus visoje Sąjungoje, kartu taip pat sudarant sąlygas valstybėms narėms tinkamai atspindėti šių subjektų vaidmenį ir svarbą nacionaliniu lygmeniu. Kiekviena valstybė narė, taikydama šioje direktyvoje nustatytus kriterijus, turėtų identifikuoti subjektus, kurie teikia vieną ar daugiau esminių paslaugų ir kurie eksploatuoja ir turi ypatingos svarbos infrastruktūrą jos teritorijoje. Turėtų būti laikoma, kad subjektas veiklą vykdo valstybės narės teritorijoje, jeigu toje valstybėje narėje jis vykdo atitinkamai esminei paslaugai ar paslaugoms teikti būtiną veiklą ir jeigu joje yra tai paslaugai ar paslaugoms teikti naudojama (-os) to subjekto ypatingos svarbos infrastruktūra (-os). Jei valstybėje narėje nėra tuos kriterijus atitinkančių subjektų, ta valstybė narė neturėtų būti įpareigota atitinkamame sektoriuje ar subsektoriuje identifikuoti ypatingos svarbos subjektus. Siekiant veiksmingumo, efektyvumo, nuoseklumo ir teisinio tikrumo, turėtų būti nustatytos atitinkamos pranešimo subjektams, kad jie identifikuoti kaip kritiniai subjektai, taisyklės;

(17) valstybės narės turėtų pateikti Komisijai – tokiu būdu, kuris atitinka šios direktyvos tikslus, – esminių paslaugų sąrašą, nurodyti identifikuotų ypatingos svarbos subjektų skaičių pagal kiekvieną priede išdėstytą sektorių bei subsektorių ir pagal kiekvieno subjekto teikiamą esminę paslaugą ar paslaugas ir, jei taikoma, ribas. Turėtų būti galima tai pateikti atskirai arba agreguota forma, t. y. duomenys gali būti pateikti kaip vidurkiai pagal geografinę teritoriją, metus, sektorių, subsektorių ar kitokiu būdu ir gali apimti informaciją apie įvairius pateiktus rodiklius;

(18) turėtų būti nustatyti kriterijai, kurie padėtų apibrėžti trikdomojo poveikio, kurį sukelia incidentas, mastą. Tie kriterijai turėtų būti grindžiami Europos Parlamento ir Tarybos direktyvoje (ES) 2016/1148 ([6]) išdėstytais kriterijais siekiant pasinaudoti valstybių narių įdirbiu nustatant esminės paslaugos, kaip apibrėžta toje direktyvoje, operatorius ir tuo klausimu sukaupta patirtimi. Tokios didelės krizės, kaip COVID-19 pandemija, parodė, kaip svarbu užtikrinti tiekimo grandinės saugumą ir kaip jos sutrikimas gali turėti neigiamą ekonominį ir socialinį poveikį daugelyje sektorių ir tarpvalstybiniu mastu. Todėl nustatydamos kitų sektorių ir jų subsektorių priklausomybės nuo ypatingos svarbos subjekto teikiamos esminės paslaugos laipsnį, valstybės narės taip pat turėtų, kiek įmanoma, atsižvelgti į poveikį tiekimo grandinei;

(19) vadovaujantis taikytina Sąjungos ir nacionaline teise, įskaitant Europos Parlamento ir Tarybos reglamentą (ES) 2019/452 ([7]), kuriuo nustatoma tiesioginių užsienio investicijų į Sąjungą tikrinimo sistema, turi būti pripažinta potenciali grėsmė, kurią kelia ypatingos svarbos infrastruktūros patekimas užsieniečių nuosavybėn Sąjungoje, nes paslaugos, ekonomika bei laisvas Sąjungos piliečių judėjimas ir sauga priklauso nuo tinkamo ypatingos svarbos infrastruktūros veikimo;

(20) Direktyvoje (ES) 2022/2555 reikalaujama, kad skaitmeninės infrastruktūros sektoriaus subjektai, kurie pagal šią direktyvą galėtų būti identifikuoti kaip ypatingos svarbos subjektai, imtųsi tinkamų ir proporcingų techninių, operacinių ir organizacinių priemonių, kad būtų valdoma tinklų ir informacinių sistemų saugumui kylanti rizika, taip pat pranešama apie didelius incidentus ir dideles kibernetines grėsmes. Atsižvelgiant į tai, kad grėsmės tinklų ir informacinių sistemų saugumui gali būti skirtingos kilmės, Direktyvoje (ES) 2022/2555 taikomas visus pavojus apimantis požiūris, kuris apima tinklų ir informacinių sistemų, taip pat tų sistemų fizinių komponentų ir fizinės aplinkos atsparumą;

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

([7]) 2019 m. kovo 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/452, kuriuo nustatoma tiesioginių užsienio investicijų į Sąjungą tikrinimo sistema (OL L 79I, 2019 3 21, p. 1).

Kadangi reikalavimai, nustatyti Direktyvoje (ES) 2022/2555 tuo atžvilgiu, yra bent jau lygiaverčiai šioje direktyvoje išdėstytoms atitinkamoms pareigoms, siekiant išvengti dubliavimo ir nereikalingos administracinės naštos, skaitmeninės infrastruktūros sektoriaus subjektams šios direktyvos 11 straipsnyje ir III, IV bei VI skyriuose nustatyti reikalavimai neturėtų būti taikomi. Tačiau valstybės narės, atsižvelgdamos į skaitmeninės infrastruktūros sektoriaus subjektų paslaugų, teikiamų ypatingos svarbos subjektams, priklausantiems visiems kitiems sektoriams, svarbą, remdamosi šioje direktyvoje nustatytais kriterijais ir naudodamos joje numatytą procedūrą, turėtų skaitmeninės infrastruktūros sektoriaus subjektus identifikuoti kaip ypatingos svarbos subjektus. Todėl turėtų būti taikomos strategijos, valstybių narių rizikos vertinimai ir paramos priemonės, kaip nustatyta šios direktyvos II skyriuje. Valstybės narės turėtų galėti priimti arba palikti galioti nacionalinės teisės nuostatas aukštesniam tų ypatingos svarbos subjektų atsparumo lygiui užtikrinti, jei tos nuostatos atitinka taikytiną Sąjungos teisę;

(21) Sąjungos finansinių paslaugų teisėje yra nustatyti finansų subjektams taikomi išsamūs reikalavimai, susiję su visos jiems kylančios rizikos, įskaitant veiklos riziką, valdymu ir veiklos tęstinumo užtikrinimu. Ši teisė apima Europos Parlamento ir Tarybos reglamentus (ES) Nr. 648/2012 ([8]), (ES) Nr. 575/2013 ([9]) ir (ES) Nr. 600/2014 ([10]) ir Europos Parlamento ir Tarybos direktyvas 2013/36/ES ([11]) ir 2014/65/ES ([12]). Ta teisinė sistema papildyta Europos Parlamento ir Tarybos reglamentu (ES) 2022/2554 ([13]), kuriame nustatyti finansų įmonėms taikomi reikalavimai valdyti informacinių ir ryšių technologijų (IRT) riziką, įskaitant kiek tai susiję su fizinių IRT infrastruktūrų apsauga. Kadangi tų subjektų atsparumas yra visapusiškai joje aptartas, siekiant išvengti dubliavimo ir nereikalingos administracinės naštos, tiems subjektams šios direktyvos 11 straipsnis ir III, IV bei VI skyriai neturėtų būti taikomi.

Tačiau valstybės narės, atsižvelgdamos į finansų sektorių subjektų paslaugų, teikiamų ypatingos svarbos subjektams, priklausantiems visiems kitiems sektoriams, svarbą, remdamosi šioje direktyvoje nustatytais kriterijais ir naudodamos joje numatytą procedūrą, finansų sektorių subjektus turėtų identifikuoti kaip ypatingos svarbos subjektus. Todėl turėtų būti taikomos strategijos, valstybių narių rizikos vertinimai ir paramos priemonės, išdėstyti šios direktyvos II skyriuje. Valstybės narės turėtų galėti priimti arba palikti galioti nacionalinės teisės nuostatas aukštesniam tų ypatingos svarbos subjektų atsparumo lygiui užtikrinti, jei tos nuostatos atitinka taikytiną Sąjungos teisę;

(22) valstybės narės turėtų paskirti arba įsteigti institucijas, kurios būtų kompetentingos prižiūrėti šios direktyvos taisyklių taikymą ir, kai būtina, užtikrinti jų vykdymą, taip pat turėtų užtikrinti, kad toms institucijoms būtų suteikti tinkami įgaliojimai ir ištekliai. Atsižvelgiant į nacionalinių valdymo struktūrų skirtumus, siekiant apsaugoti nustatytą tvarką atskiruose sektoriuose arba Sąjungos priežiūros ir reguliavimo įstaigas ir išvengti dubliavimo, valstybės narės turėtų turėti galimybę paskirti arba įsteigti daugiau nei vieną kompetentingą instituciją. Jei valstybės narės paskiria ar įsteigia daugiau nei vieną kompetentingą instituciją, jos turėtų aiškiai atskirti atitinkamas konkrečių institucijų užduotis ir užtikrinti sklandų ir veiksmingą jų bendradarbiavimą. Visos kompetentingos institucijos taip pat turėtų bendradarbiauti platesniu mastu su kitomis atitinkamomis institucijomis Sąjungos ir nacionaliniu lygmenimis;

([8]) 2012 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų (OL L 201, 2012 7 27, p. 1).

([9]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 575/2013 dėl prudencinių reikalavimų kredito įstaigoms ir kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 (OL L 176, 2013 6 27, p. 1).

([10]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 600/2014 dėl finansinių priemonių rinkų, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 (OL L 173, 2014 6 12, p. 84).

([11]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyva 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų ir investicinių įmonių priežiūros, kuria iš dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB (OL L 176, 2013 6 27, p. 338).

([12]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/65/ES dėl finansinių priemonių rinkų, kuria iš dalies keičiamos Direktyva 2002/92/EB ir Direktyva 2011/61/ES (OL L 173, 2014 6 12, p. 349).

([13]) 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 (žr. šio Oficialiojo leidinio p. 1).

(23) siekiant palengvinti tarpvalstybinį bendradarbiavimą bei komunikaciją ir sudaryti sąlygas veiksmingam šios direktyvos įgyvendinimui, kiekviena valstybė narė turėtų, nedarydama poveikio konkretiems sektoriams taikomų Sąjungos teisės aktų reikalavimams, paskirti vieną bendrąjį kontaktinį punktą, kai aktualu, įsteigtą kompetentingoje institucijoje, atsakingą už koordinavimą klausimais, susijusiais su ypatingos svarbos subjektų atsparumu ir tarpvalstybiniu bendradarbiavimu Sąjungos lygmeniu (toliau – bendrasis kontaktinis punktas). Kiekvienas bendrasis kontaktinis punktas turėtų palaikyti ryšius ir koordinuoti komunikaciją, kai aktualu, su savo valstybės narės kompetentingomis institucijomis, kitų valstybių narių bendraisiais kontaktiniais punktais ir Ypatingos svarbos subjektų atsparumo klausimų grupe;

(24) kompetentingos institucijos pagal šią direktyvą ir kompetentingos institucijos pagal Direktyvą (ES) 2022/2555, turėtų bendradarbiauti ir keistis informacija dėl kibernetiniam saugumui kylančios rizikos, kibernetinių grėsmių ir kibernetinių incidentų ir nekibernetinės rizikos, grėsmių bei incidentų, darančių poveikį ypatingos svarbos subjektams, taip pat dėl atitinkamų priemonių, kurių ėmėsi kompetentingos institucijos pagal šią direktyvą ir kompetentingos institucijos pagal Direktyvą (ES) 2022/2555. Svarbu, kad valstybės narės užtikrintų, kad šioje direktyvoje ir Direktyvoje (ES) 2022/2555 numatyti reikalavimai būtų įgyvendinami taip, kad vieni kitus papildytų, ir kad ypatingos svarbos subjektams netektų didesnė administracinė našta, nei būtina siekiant įgyvendinti šios direktyvos ir tos direktyvos tikslus;

(25) valstybės narės turėtų remti ypatingos svarbos subjektus, įskaitant tuos, kurie laikomi mažosiomis arba vidutinėmis įmonėmis, jiems stiprinant savo atsparumą, laikydamosi šioje direktyvoje nustatytų valstybių narių pareigų ir kartu nedarant poveikio pačių ypatingos svarbos subjektų teisinei atsakomybei užtikrinti tokią atitiktį, ir tai darydamos jos turėtų užkirsti kelią pernelyg didelei administracinei naštai. Valstybės narės visų pirma galėtų parengti rekomendacinę medžiagą ir metodikas, padėti rengti pratybas siekiant išbandyti ypatingos svarbos subjektų atsparumą ir teikti patarimus ir mokymą ypatingos svarbos subjektų darbuotojams. Kai būtina ir pagrįsta viešojo intereso tikslais, valstybės narės galėtų teikti finansinius išteklius ir turėtų sudaryti palankias sąlygas ypatingos svarbos subjektams savanoriškai dalytis informacija ir keistis gerosios praktikos pavyzdžiais, nedarant poveikio Sutartyje dėl Europos Sąjungos veikimo (SESV) nustatytų konkurencijos taisyklių taikymui;

(26) siekiant padidinti valstybių narių identifikuotų ypatingos svarbos subjektų atsparumą ir sumažinti tiems ypatingos svarbos subjektams tenkančią administracinę naštą, kompetentingos institucijos turėtų tarpusavyje konsultuotis, kad užtikrintų nuoseklų šios direktyvos taikymą. Tos konsultacijos turėtų būti pradedamos bet kurios suinteresuotosios kompetentingos institucijos prašymu, ir jose daugiausia dėmesio turėtų būti skiriama tam, kad būtų užtikrintas suderintas požiūris į tarpusavyje susijusius ypatingos svarbos subjektus, kurie naudoja ypatingos svarbos infrastruktūrą, kuri yra fiziškai sujungta tarp dviejų ar daugiau valstybių narių, kurie priklauso toms pačioms grupėms ar įmonių struktūroms arba kurie yra identifikuoti kaip ypatingos svarbos subjektai vienoje valstybėje narėje ir kurie teikia esmines paslaugas kitoms valstybėms narėms arba kitose valstybėse narėse;

(27) kai pagal Sąjungos arba nacionalinės teisės nuostatas reikalaujama, kad ypatingos svarbos subjektai įvertintų riziką, aktualią siekiant šios direktyvos tikslų, ir imtųsi priemonių savo pačių atsparumui užtikrinti, į tuos reikalavimus turėtų būti tinkamai atsižvelgiama priežiūros, kaip ypatingos svarbos subjektai laikosi šios direktyvos, tikslais;

(28) ypatingos svarbos subjektai turėtų visapusiškai suprasti jiems kylančią atitinkamą riziką ir turėtų turėti pareigą tą riziką išanalizuoti. Tuo tikslu jie turėtų atlikti rizikos vertinimus, kai tai yra būtina atsižvelgiant į jų konkrečias aplinkybes ir tos rizikos raidą, ir bet kuriuo atveju rizika turėtų būti įvertinama kas keturis metus, kad būtų galima įvertinti visas aktualias rizikas, kurios gali sutrikdyti jų esminių paslaugų teikimą (toliau – ypatingos svarbos subjekto rizikos vertinimas). Jeigu ypatingos svarbos subjektai, laikydamiesi kituose teisės aktuose nustatytų pareigų, atliko rizikos vertinimus arba parengė dokumentus, kurie yra aktualūs jų ypatingos svarbos subjekto rizikos vertinimui, jie turėtų galėti naudoti tuos vertinimus ir dokumentus, kad įvykdytų šioje direktyvoje išdėstytus reikalavimus dėl ypatingos svarbos subjekto rizikos vertinimo. Kompetentinga institucija turėtų galėti paskelbti, kad esamas ypatingos svarbos subjekto atliktas rizikos vertinimas, kuriame nagrinėjamos aktualios rizikos ir priklausomybė, iš dalies arba visiškai atitinka šioje direktyvoje nustatytus reikalavimus;

(29) ypatingos svarbos subjektai turėtų imtis techninių, saugumo ir organizacinių priemonių, kurios būtų tinkamos ir proporcingos atsižvelgiant į jiems kylančią riziką, kad galėtų užkirsti kelią incidentui, apsisaugoti nuo jo, į jį reaguoti, atlaikyti tokį incidentą, jį sušvelninti, įveikti, prisitaikyti prie jo ir po jo atstatyti veiklą. Nors ypatingos svarbos subjektai turėtų imtis tų priemonių pagal šią direktyvą, tokių priemonių turinys ir jų mastas turėtų būti tokie, kad tinkamai ir proporcingai atspindėtų įvairią riziką, kurią kiekvienas ypatingos svarbos subjektas nustatė atlikdamas savo ypatingos svarbos subjekto rizikos vertinimą, ir tokio subjekto ypatumus. Kad paskatintų nuoseklų Sąjungos požiūrį, Komisija, pasikonsultavusi su Ypatingos svarbos subjektų atsparumo klausimų grupe, turėtų priimti neprivalomas gaires, kuriose būtų išsamiau išdėstytos tos techninės, saugumo ir organizacinės priemonės. Valstybės narės turėtų užtikrinti, kad kiekvienas ypatingos svarbos subjektas paskirtų ryšių palaikymo ar lygiavertį pareigūną kaip kontaktinį punktą ryšiams su kompetentingomis institucijomis;

(30) atsižvelgdami į veiksmingumą ir atskaitomybę, ypatingos svarbos subjektai turėtų atsparumo plane arba tokiam planui lygiaverčiame dokumente ar dokumentuose tiek išsamiai, kad tinkamai pasiektų veiksmingumo ir atskaitomybės tikslus, aprašyti priemones, kurių jie imasi, kartu atsižvelgdami į nustatytą riziką, ir tą planą taikyti praktikoje. Jei ypatingos svarbos subjektas, laikydamasis kitų teisės aktų, jau ėmėsi techninių, saugumo bei organizacinių priemonių ir parengė dokumentus, kurie yra aktualūs šioje direktyvoje nustatytoms atsparumo didinimo priemonėms, jis turėtų galėti naudotis tomis priemonėmis ir dokumentais įvykdyti šioje direktyvoje nustatytoms atsparumo didinimo priemonėms, kad būtų išvengta dubliavimo. Kad būtų išvengta dubliavimo, kompetentinga institucija turėtų galėti paskelbti, kad esamos atsparumo didinimo priemonės, kurių ėmėsi ypatingos svarbos subjektas, kuriomis vykdomos jo pareigos imtis techninių, saugumo bei organizacinių priemonių pagal šią direktyvą, iš dalies arba visiškai atitinka direktyvoje nustatytus reikalavimus;

(31) Europos Parlamento ir Tarybos reglamentuose (EB) Nr. 725/2004 ([14]) bei (EB) Nr. 300/2008 ([15]) ir Europos Parlamento ir Tarybos direktyvoje 2005/65/EB ([16]) nustatyti reikalavimai, kurie taikomi aviacijos ir jūrų transporto sektoriuose veikiantiems subjektams, siekiant užkirsti kelią incidentams, kuriuos sukelia neteisėti veiksmai, ir apsisaugoti nuo tokių incidentų pasekmių bei jas sušvelninti. Nors priemonės, kurių reikalaujama pagal šią direktyvą, yra platesnio pobūdžio atsižvelgiant į susijusią riziką ir taikytinų priemonių rūšis, šiuose sektoriuose veikiantys ypatingos svarbos subjektai savo atsparumo plane arba lygiaverčiuose dokumentuose turėtų aptarti priemones, kurių jie ėmėsi pagal tuos kitus Sąjungos teisės aktus. Ypatingos svarbos subjektai taip pat turėtų atsižvelgti į Europos Parlamento ir Tarybos direktyvą 2008/96/EB ([17]), pagal kurią numatyti viso tinklo kelių vertinimai eismo įvykių rizikos žemėlapiui sudaryti ir tiksliniai kelio saugumo patikrinimai siekiant nustatyti pavojingas sąlygas, defektus ir problemas, dėl kurių padidėja eismo įvykių ir sužalojimų rizika, vykdomi atliekant esamų kelių arba kelių ruožų apžiūras vietoje. Ypatingos svarbos subjektų apsaugos ir atsparumo užtikrinimas nepaprastai svarbus geležinkelių sektoriui, ir, įgyvendinant šioje direktyvoje nustatytas atsparumo priemones, ypatingos svarbos subjektai raginami vadovautis neprivalomomis gairėmis ir gerosios praktikos dokumentais, parengtais pagal sektorių darbo kryptis, pvz., Komisijos sprendimu 2018/C 232/03 ([18]) įsteigta ES geležinkelių keleivių saugumo platforma;

(32) vis didesnį nerimą kelia rizika, kad ypatingos svarbos subjektų arba jų rangovų darbuotojai piktnaudžiaus, pavyzdžiui, savo prieigos teisėmis ypatingos svarbos subjekto organizacijoje, kad pakenktų ir sukeltų žalą. Todėl valstybės narės turėtų nustatyti sąlygas, kuriomis ypatingos svarbos subjektams, tinkamai pagrįstais atvejais ir atsižvelgiant į valstybių narių rizikos vertinimus, būtų leidžiama pateikti prašymus, kad būtų atlikti asmenų, priklausančių konkrečioms jų darbuotojų kategorijoms, patikrinimai. Turėtų būti užtikrinta, kad prašymus atitinkamos institucijos įvertintų per pagrįstą laikotarpį ir jie būtų tvarkomi laikantis nacionalinės teisės aktų ir nacionalinių procedūrų, taip pat atitinkamos taikytinos Sąjungos teisės, įskaitant asmens duomenų apsaugos teisę. Siekdamos patvirtinti asmens, kuriam taikomas asmens patikrinimas, tapatybę, valstybės narės turėtų reikalauti tapatybę patvirtinančio įrodymo, pavyzdžiui, paso, nacionalinės tapatybės kortelės ar skaitmeninių formų tapatybę patvirtinančių įrodymų laikantis taikytinos teisės.

([14]) 2004 m. kovo 31 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 725/2004 dėl laivų ir uostų įrenginių apsaugos stiprinimo (OL L 129, 2004 4 29, p. 6).

([15]) 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių ir panaikinantis Reglamentą (EB) Nr. 2320/2002 (OL L 97, 2008 4 9, p. 72).

([16]) 2005 m. spalio 26 d. Europos Parlamento ir Tarybos direktyva 2005/65/EB dėl uostų apsaugos stiprinimo (OL L 310, 2005 11 25, p. 28).

([17]) 2008 m. lapkričio 19 d. Europos Parlamento ir Tarybos direktyva 2008/96/EB dėl kelių infrastruktūros saugumo valdymo (OL L 319, 2008 11 29, p. 59).

([18]) 2018 m. birželio 29 d. Komisijos sprendimas, kuriuo įsteigiama ES geležinkelių keleivių saugumo platforma 2018/C 232/03 (OL C 232, 2018 7 3, p. 10).

Asmens patikrinimas turėtų apimti informacijos apie atitinkamo asmens teistumą patikrinimą. Tuo tikslu valstybės narės turėtų naudotis Europos nuosprendžių registrų informacine sistema, laikydamosi Tarybos pamatiniame sprendime 2009/315/TVR ([19]) ir, kai tinkama ir taikytina, Europos Parlamento ir Tarybos reglamente (ES) 2019/816 ([20]) nustatytų procedūrų, kad gautų informaciją apie teistumą, esančią kitose valstybėse narėse. Be to, kai aktualu ir taikytina, valstybės narės gali remtis Europos Parlamento ir Tarybos reglamentu (ES) 2018/1862 ([21]) sukurtos antrosios kartos Šengeno informacinės sistemos (SIS II) duomenimis ir bet kuria kita esama objektyvia informacija, kuri gali būti būtina siekiant nustatyti, ar atitinkamas asmuo yra tinkamas eiti pareigas, dėl kurių ypatingos svarbos subjektas paprašė atlikti asmens patikrinimą;

(33) turėtų būti sukurtas pranešimo apie tam tikrus incidentus mechanizmas, kad kompetentingos institucijos galėtų greitai ir tinkamai reaguoti į incidentus ir susidaryti išsamų vaizdą apie incidento, su kuriuo susidūrė ypatingos svarbos subjektai, poveikį, pobūdį, priežastį ir galimus padarinius. Ypatingos svarbos subjektai turėtų nepagrįstai nedelsdami pranešti kompetentingoms institucijoms apie incidentus, dėl kurių stipriai sutrinka arba gali būti stipriai sutrikdytas esminių paslaugų teikimas. Išskyrus atvejus, kai veiklos požiūriu to padaryti neįmanoma, ypatingos svarbos subjektai pirmąjį pranešimą turėtų pateikti ne vėliau kaip per 24 valandas nuo tada, kai sužino apie incidentą. Pirmajame pranešime turėtų būti pateikta tik informacija, kurios būtinai reikia, kad kompetentinga institucija sužinotų apie incidentą, o ypatingos svarbos subjektas prireikus galėtų kreiptis pagalbos. Tokiame pranešime, kai įmanoma, turėtų būti nurodyta numanoma incidento priežastis. Valstybės narės turėtų užtikrinti, kad dėl reikalavimo pateikti tą pirmąjį pranešimą teikiančio ypatingos svarbos subjekto ištekliai nebūtų nukreipti nuo veiklos, susijusios su incidento valdymu, kuriam turėtų būti teikiama pirmenybė. Kai aktualu, pateikus pirmąjį pranešimą, ne vėliau kaip per mėnesį po incidento turėtų būti pateikiama išsami ataskaita. Išsami ataskaita turėtų papildyti pirmąjį pranešimą ir joje turėtų būti pateikta išsami incidento apžvalga;

(34) standartizavimo procesą ir toliau labiausiai turėtų skatinti rinka. Tačiau gali būti situacijų, kai yra tikslinga reikalauti laikytis specifinių standartų. Kai naudinga, valstybės narės taip pat turėtų skatinti taikyti Europos standartus ir tarptautinius standartus bei technines specifikacijas, susijusius su saugumo ir atsparumo priemonėmis, taikomomis ypatingos svarbos subjektams;

(35) nors ypatingos svarbos subjektai paprastai veikia naudodami vis labiau sujungtą paslaugų teikimo ir infrastruktūros tinklą, o esmines paslaugas dažnai teikia daugiau nei vienoje valstybėje narėje, kai kurie iš šių ypatingos svarbos subjektų Sąjungos ir jos vidaus rinkos mastu yra ypač reikšmingi, nes teikia esmines paslaugas šešioms ar daugiau valstybių narių arba šešiose ar daugiau valstybių narių, todėl Sąjungos lygmeniu joms galėtų būti teikiama speciali parama. Todėl turėtų būti nustatytos patariamųjų misijų taisyklės, taikomos tokiems Europos mastu ypač reikšmingiems ypatingos svarbos subjektams. Tos taisyklės nedaro poveikio šioje direktyvoje nustatytoms priežiūros ir vykdymo užtikrinimo taisyklėms;

(36) Komisijos arba vienos ar daugiau valstybių narių, kurioms ar kuriose teikiama esminė paslauga, motyvuotu prašymu, tais atvejais, kai reikia papildomos informacijos, kad būtų galima patarti ypatingos svarbos subjektui pareigų laikymosi pagal šią direktyvą klausimais arba įvertinti, ar Europos mastu ypač reikšmingas ypatingos svarbos subjektas vykdo pareigas, valstybė narė, kuri Europos mastu ypač reikšmingą ypatingos svarbos subjektą identifikavo kaip ypatingos svarbos subjektą, turėtų pateikti Komisijai tam tikro pobūdžio informaciją, kaip išdėstyta šioje direktyvoje. Pritarus valstybei narei, kuri Europos mastu ypač reikšmingą ypatingos svarbos subjektą identifikavo kaip ypatingos svarbos subjektą, Komisija turėtų galėti surengti patariamąją misiją, kad įvertintų to subjekto taikomas priemones. Siekiant užtikrinti, kad tokios patariamosios misijos būtų vykdomos tinkamai, turėtų būti nustatytos papildomos taisyklės, visų pirma dėl patariamųjų misijų organizavimo ir vykdymo, tolesnių veiksmų ir atitinkamų Europos mastu ypač reikšmingų ypatingos svarbos subjektų pareigų. Patariamoji misija, nedarant

([19]) 2009 m. vasario 26 d. Tarybos pamatinis sprendimas 2009/315/TVR dėl valstybių narių keitimosi informacija iš nuosprendžių registro organizavimo ir turinio (OL L 93, 2009 4 7, p. 23).

([20]) 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/816, kuriuo Europos nuosprendžių registrų informacinei sistemai papildyti sukuriama centralizuota valstybių narių, turinčių informacijos apie priimtus trečiųjų šalių piliečių ir asmenų be pilietybės apkaltinamuosius nuosprendžius, nustatymo sistema (ECRIS-TCN) ir kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1726 (OL L 135, 2019 5 22, p. 1).

([21]) 2018 m. lapkričio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1862 dėl Šengeno informacinės sistemos (SIS) sukūrimo, eksploatavimo ir naudojimo policijos bendradarbiavimui ir teisminiam bendradarbiavimui baudžiamosiose bylose, kuriuo iš dalies keičiamas ir panaikinamas Tarybos sprendimas 2007/533/TVR ir panaikinamas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1986/2006 ir Komisijos sprendimas 2010/261/ES (OL L 312, 2018 12 7, p. 56).

poveikio valstybių narių, kuriose vykdoma patariamoji misija, ir atitinkamo ypatingos svarbos subjekto poreikiui laikytis šios direktyvos taisyklių, turėtų būti vykdoma laikantis išsamių tos valstybės narės teisės taisyklių, pvz., dėl tikslių sąlygų, kurios turi būti įvykdomos siekiant gauti leidimą patekti į atitinkamas patalpas arba susipažinti su dokumentais, ir teisminės teisių gynimo tvarkos. Kai aktualu, specifinių ekspertinių žinių, reikalingų tokioms patariamosioms misijoms, būtų prašoma kreipiantis į Reagavimo į nelaimes koordinavimo centrą, įsteigtą Europos Parlamento ir Tarybos sprendimu Nr. 1313/2013/ES ([22]).

(37) siekiant paremti Komisiją ir palengvinti valstybių narių tarpusavio bendradarbiavimą ir keitimąsi informacija, be kita ko geriausios praktikos pavyzdžiais, susijusia su šioje direktyvoje aptartais klausimais, turėtų būti sudaryta Ypatingos svarbos subjektų atsparumo klausimų grupė, kuri veiktų kaip Komisijos ekspertų grupė. Valstybės narės turėtų stengtis užtikrinti praktišką ir efektyvų savo kompetentingų institucijų atstovų, paskirtų į Ypatingos svarbos subjektų atsparumo klausimų grupę, bendradarbiavimą, be kita ko, paskirdamos, kai tinkama, asmens patikimumo pažymėjimus turinčius atstovus. Ypatingos svarbos subjektų atsparumo klausimų grupė savo užduotis turėtų pradėti vykdyti kaip įmanoma greičiau, kad suteiktų papildomų priemonių tinkamam bendradarbiavimui užtikrinti šios direktyvos perkėlimo į nacionalinę teisę laikotarpiu. Ypatingos svarbos subjektų atsparumo klausimų grupė turėtų užtikrinti sąveiką su kitų aktualių sektorių ekspertų darbo grupėmis;

(38) ypatingos svarbos subjektų atsparumo klausimų grupė turėtų bendradarbiauti su Bendradarbiavimo grupe, sudaryta pagal Direktyvą (ES) 2022/2555, siekdama remti visapusišką ypatingos svarbos subjektų kibernetinio ir nekibernetinio atsparumo sistemą. Ypatingos svarbos subjektų atsparumo klausimų grupė ir Bendradarbiavimo grupė, sudaryta pagal Direktyvą (ES) 2022/2555, turėtų reguliariai palaikyti dialogą, kad skatintų kompetentingų institucijų pagal šią direktyvą ir kompetentingų institucijų pagal Direktyvą (ES) 2022/2555 bendradarbiavimą ir palengvintų keitimąsi informacija, visų pirma abiem grupėms svarbiomis temomis;

(39) siekdama šios direktyvos tikslų ir nedarydama poveikio valstybių narių ir ypatingos svarbos subjektų teisinei pareigai užtikrinti atitiktį jų atitinkamoms direktyvoje nustatytoms pareigoms, Komisija, kai, jos manymu, tai yra tinkama, turėtų remti kompetentingas institucijas ir ypatingos svarbos subjektus, siekdama palengvinti joms atitinkamų savo pareigų vykdymą. Komisija, teikdama paramą valstybėms narėms ir ypatingos svarbos subjektams vykdant savo pareigas pagal šią direktyvą, turėtų naudoti esamas struktūras ir priemones, pvz., nustatytas pagal Sąjungos civilinės saugos mechanizmą, sukurtą Sprendimu Nr. 1313/2013/ES, ir Europos ypatingos svarbos infrastruktūros apsaugos referenciniame tinkle. Be to, ji turėtų informuoti valstybes nares apie Sąjungos lygmeniu esamus išteklius, numatytus, pavyzdžiui, Vidaus saugumo fonde, nustatytame Europos Parlamento ir Tarybos reglamentu (ES) 2021/1149 ([23]), programoje „Europos horizontas“, sukurtoje Europos Parlamento ir Tarybos reglamentu (ES) 2021/695 ([24]), ar pagal kitas ypatingos svarbos subjektų atsparumui aktualias priemones;

(40) valstybės narės turėtų užtikrinti, kad jų kompetentingos institucijos turėtų tam tikrus konkrečius įgaliojimus, kad ši direktyva būtų tinkamai taikoma ir tinkamai užtikrinamas jos vykdymas ypatingos svarbos subjektų atžvilgiu, kai šie subjektai patenka į valstybių narių jurisdikciją, kaip nustatyta šioje direktyvoje. Šie įgaliojimai visų pirma turėtų apimti įgaliojimus atlikti patikrinimus ir auditą, įgaliojimus vykdyti priežiūrą ir įgaliojimus reikalauti, kad ypatingos svarbos subjektai pateiktų informaciją ir įrodymus, susijusius su priemonėmis, kurių jie ėmėsi, kad laikytųsi savo pareigų, ir, prireikus, įgaliojimus duoti nurodymus ištaisyti nustatytus pažeidimus. Duodamos tokius nurodymus, valstybės narės neturėtų reikalauti priemonių, kurios nėra būtinos ar neproporcingos siekiant užtikrinti atitinkamo ypatingos svarbos subjekto atitiktį, visų pirma atsižvelgiant į pažeidimo sunkumą ir atitinkamo ypatingos svarbos subjekto ekonominį pajėgumą. Bendriau tariant, šie įgaliojimai turėtų būti suteikiami užtikrinant tinkamas ir

([22]) 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (OL L 347, 2013 12 20, p. 924).

([23]) 2021 m. liepos 7 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/1149, kuriuo nustatomas Vidaus saugumo fondas (OL L 251, 2021 7 15, p. 94).

([24]) 2021 m. balandžio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/695, kuriuo sukuriama bendroji mokslinių tyrimų ir inovacijų programa „Europos horizontas“, nustatomos su ja susijusios dalyvavimo ir sklaidos taisyklės ir panaikinami reglamentai (ES) Nr. 1290/2013 ir (ES) Nr. 1291/2013 (OL L 170, 2021 5 12, p. 1).

veiksmingas apsaugos priemones, kurios turi būti nustatytos nacionalinėje teisėje laikantis Europos Sąjungos pagrindinių teisių chartijos. Vertindamos, kaip ypatingos svarbos subjektas laikosi šioje direktyvoje jam nustatytų pareigų, kompetentingos institucijos pagal šią direktyvą, turėtų galėti prašyti kompetentingų institucijų pagal Direktyvą (ES) 2022/2555 pasinaudoti savo priežiūros ir vykdymo užtikrinimo įgaliojimais subjekto pagal tą direktyvą, kuris identifikuotas kaip ypatingos svarbos subjektas pagal šią direktyvą, atžvilgiu. Tuo tikslu kompetentingos institucijos pagal šią direktyvą ir kompetentingos institucijos pagal Direktyvą (ES) 2022/2555 turėtų bendradarbiauti ir keistis informacija;

(41) kad ši direktyva būtų taikoma veiksmingai ir nuosekliai, pagal SESV 290 straipsnį Komisijai turėtų būti suteikti įgaliojimai priimti teisės aktus, kuriais ši direktyva būtų papildyta nustatant esminių paslaugų sąrašą. Tuo sąrašu kompetentingos institucijos turėtų naudotis atlikdamos valstybių narių rizikos vertinimus ir identifikuodamos ypatingos svarbos subjektus pagal šią direktyvą. Atsižvelgiant į šioje direktyvoje taikomą minimalaus suderinimo metodą, tas sąrašas nėra išsamus ir valstybės narės galėtų jį papildyti įtraukdamos papildomas esmines paslaugas nacionaliniu lygmeniu, kad būtų atsižvelgta į nacionalinius esminių paslaugų teikimo ypatumus. 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 ([25]) 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;

(42) siekiant užtikrinti vienodas šios direktyvos įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai. Tais įgaliojimais turėtų būti naudojamasi laikantis Reglamento (ES) Nr. 182/2011 ([26]);

(43) kadangi šios direktyvos tikslų, t. y. užtikrinti, kad esminės paslaugos, būtinos išlaikyti gyvybiškai svarbias visuomenės funkcijas arba ekonominę veiklą, vidaus rinkoje būtų teikiamos netrukdomai, ir didinti tokias paslaugas teikiančių ypatingos svarbos subjektų atsparumą, valstybės narės negali deramai pasiekti, o dėl veiksmo masto bei poveikio tų tikslų būtų geriau siekti Sąjungos lygmeniu, laikydamasi Europos Sąjungos sutarties 5 straipsnyje nustatyto subsidiarumo principo Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šia direktyva neviršijama to, kas būtina nurodytiems tikslams pasiekti;

(44) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([27]) 42 straipsnio 1 dalimi buvo konsultuotasi su Europos duomenų apsaugos priežiūros pareigūnu, ir jis pateikė nuomonę 2021 m. rugpjūčio 11 d.;

(45) todėl direktyva 2008/114/EB turėtų būti panaikinta,

([25]) OL L 123, 2016 5 12, p. 1.

([26]) 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).

([27]) 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).

PRIĖMĖ ŠIĄ DIREKTYVĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir taikymo sritis

1. Šia direktyva nustatomos:

a) valstybių narių pareigos imtis konkrečių priemonių, kuriomis siekiama užtikrinti netrukdomą esminių paslaugų, būtinų išlaikyti gyvybiškai svarbias visuomenės funkcijas arba ekonominę veiklą, patenkančių į SESV 114 straipsnio taikymo sritį, teikimą vidaus rinkoje, visų pirma pareigos identifikuoti ypatingos svarbos subjektus ir juos remti, kad jie galėtų vykdyti jiems nustatytas pareigas;

b) ypatingos svarbos subjektų pareigos didinti savo atsparumą ir gebėjimą teikti a punkte nurodytas paslaugas vidaus rinkoje;

c) taisyklės dėl:

   i) ypatingos svarbos subjektų priežiūros;

   ii) vykdymo užtikrinimo;

   iii) Europos mastu ypač reikšmingų ypatingos svarbos subjektų identifikavimo ir patariamųjų misijų, siekiant įvertinti priemones, kurias tokie subjektai įgyvendino, kad įvykdytų savo pareigas pagal III skyrių;

d) bendros bendradarbiavimo ir ataskaitų apie šios direktyvos taikymą teikimo procedūros;

e) priemonės, kuriomis siekiama aukšto ypatingos svarbos subjektų atsparumo lygio, kad būtų užtikrintas esminių paslaugų teikimas visoje Sąjungoje ir pagerintas vidaus rinkos veikimas.

2. Ši direktyva netaikoma klausimams, kuriems taikoma Direktyva (ES) 2022/2555, nedarant poveikio šios direktyvos 8 straipsniui. Atsižvelgdamos į ypatingos svarbos subjektų fizinio saugumo ir kibernetinio saugumo ryšį, valstybės narės užtikrina koordinuotą šios direktyvos ir Direktyvos (ES) 2022/2555 įgyvendinimą.

3. Jeigu pagal konkretiems sektoriams taikomus Sąjungos teisės aktus reikalaujama, kad ypatingos svarbos subjektai imtųsi priemonių savo atsparumui didinti, ir jeigu tie reikalavimai valstybių narių yra pripažįstami kaip bent jau lygiaverčiai atitinkamoms šioje direktyvoje nustatytoms pareigoms, atitinkamos šios direktyvos nuostatos, įskaitant VI skyriaus nuostatas dėl priežiūros ir vykdymo užtikrinimo, netaikomos.

4. Nedarant poveikio SESV 346 straipsniui, informacija, kuri yra konfidenciali pagal Sąjungos ar nacionalines taisykles, kaip antai taisyklės dėl verslo konfidencialumo, turi būti pagal šią direktyvą keičiamasi su Komisija ir kitomis atitinkamomis institucijomis tik tais atvejais, kai toks keitimasis yra būtinas šios direktyvos taikymui. Keičiamasi tik tokia informacija, kuri atitinka keitimosi tikslą ir yra jam proporcinga. Keičiantis informacija saugomas tos informacijos konfidencialumas ir ypatingos svarbos subjektų saugumo ir komerciniai interesai, kartu atsižvelgiant į valstybių narių saugumą.

5. Šia direktyva nedaromas poveikis valstybių narių atsakomybei užtikrinti nacionalinį saugumą bei gynybą ir jų įgaliojimams apsaugoti kitas esmines valstybines funkcijas, įskaitant valstybės teritorinio vientisumo užtikrinimą ir viešosios tvarkos palaikymą.

6. Ši direktyva netaikoma viešojo administravimo subjektams, vykdantiems savo veiklą nacionalinio saugumo, viešojo saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas.

7. Valstybės narės gali nuspręsti, kad 11 straipsnis ir III, IV ir VI skyriai visiškai ar iš dalies netaikomi konkretiems ypatingos svarbos subjektams, kurie vykdo veiklą nacionalinio saugumo, viešojo saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas, arba kurie teikia paslaugas tik šio straipsnio 6 dalyje nurodytiems viešojo administravimo subjektams.

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

9. Šia direktyva nedaromas poveikis Sąjungos teisei dėl asmens duomenų apsaugos, visų pirma Europos Parlamento ir Tarybos reglamentui (ES) 2016/679 ([28]) ir Europos Parlamento ir Tarybos direktyvai 2002/58/EB ([29]).

2 straipsnis

Terminų apibrėžtys

Šioje direktyvoje vartojamų terminų apibrėžtys:

1) ypatingos svarbos subjektas – viešasis arba privatusis subjektas, kurį valstybė narė pagal 6 straipsnį identifikavo kaip priklausantį vienai iš priedo lentelės trečioje skiltyje išdėstytų kategorijų;

2) atsparumas – ypatingos svarbos subjekto gebėjimas užkirsti kelią incidentui, apsisaugoti nuo jo, į jį reaguoti, jį atlaikyti, sušvelninti, įveikti, prisitaikyti prie jo ir po jo atstatyti veiklą;

3) incidentas – įvykis, kuris gali stipriai sutrikdyti, arba kuris sutrikdo, esminės paslaugos teikimą, be kita ko, kai tai daro poveikį nacionalinėms sistemoms, apsaugančioms teisinę valstybę;

4) ypatingos svarbos infrastruktūra – turtas, patalpos, įranga, tinklas ar sistema arba turto, patalpų, įrangos, tinklo ar sistemos dalis, būtini esminių paslaugų teikimui;

5) esminė paslauga – paslauga, kuri yra būtina siekiant palaikyti gyvybiškai svarbias visuomenės funkcijas, ekonominę veiklą, visuomenės sveikatą ir viešąjį saugumą arba aplinką;

6) rizika – potencialus nutrūkimas arba sutrikimas, kurį sukėlė incidentas; ji išreiškiama kaip tokio nutrūkimo arba sutrikimo masto ir to incidento tikimybės derinys;

7) rizikos vertinimas – bendras procesas siekiant nustatyti rizikos pobūdį ir mastą nustatant ir analizuojant atitinkamas potencialias grėsmes, pažeidžiamumus ir pavojus, dėl kurių galėtų kilti incidentas, ir įvertinant potencialų esminės paslaugos teikimo nutrūkimą arba sutrikimą, kurį sukėlė tas incidentas;

8) standartas – standartas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012 ([30]) 2 straipsnio 1 punkte;

([28]) 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).

([29]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).

([30]) 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).

9) techninė specifikacija – techninė specifikacija, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 4 punkte;

10) viešojo administravimo subjektas – valstybės narės subjektas, kuris valstybėje narėje pagal nacionalinę teisę yra pripažįstamas tokiu subjektu, išskyrus teismines institucijas, parlamentus ir centrinius bankus, ir kuris atitinka šiuos kriterijus:

a) yra įsteigtas siekiant tikslo tenkinti bendrojo intereso poreikius, ir nėra pramoninio ar komercinio pobūdžio;

b) turi juridinio asmens statusą arba pagal teisės aktus turi teisę veikti kito juridinio asmens statusą turinčio subjekto vardu;

c) didžiąja dalimi yra finansuojamas valstybės institucijų ar kitų viešosios teisės reglamentuojamų centrinio lygmens įstaigų lėšomis, jam taikoma tų institucijų ar įstaigų administracinė priežiūra arba jis turi administracinį, valdymo ar priežiūros organą, kurio daugiau kaip pusę narių skiria valstybės institucijos ar kitos viešosios teisės reglamentuojamos centrinio lygmens įstaigos;

d) turi įgaliojimus priimti administracinius arba reguliavimo sprendimus dėl fizinių arba juridinių asmenų, kurie daro poveikį jų teisėms tarpvalstybinio asmenų, prekių, paslaugų ar kapitalo judėjimo srityje.

3 straipsnis

Minimalus suderinimas

Šia direktyva valstybėms narėms netrukdoma priimti arba palikti toliau galioti nacionalinės teisės nuostatų aukštesniam ypatingos svarbos subjektų atsparumo lygiui užtikrinti, su sąlyga, kad tokios nuostatos yra suderinamos su valstybių narių įsipareigojimais, nustatytais Sąjungos teisėje.

II SKYRIUS

NACIONALINĖS YPATINGOS SVARBOS SUBJEKTŲ ATSPARUMO SISTEMOS

4 straipsnis

Ypatingos svarbos subjektų atsparumo strategija

1. Po konsultacijų, kuriose tiek, kiek praktiškai įmanoma, gali dalyvauti visi atitinkami suinteresuotieji subjektai, kiekviena valstybė narė ne vėliau kaip 2026 m. sausio 17 d. priima ypatingos svarbos subjektų atsparumo didinimo strategiją (toliau – strategija). Strategijoje nustatomi strateginiai tikslai ir politikos priemonės, remiantis atitinkamomis esamomis nacionalinėmis ir sektorinėmis strategijomis, planais ar panašiais dokumentais, siekiant užtikrinti ir išlaikyti aukštą ypatingos svarbos subjektų atsparumo lygį, į taikymo sritį įtraukiant bent priede išdėstytus sektorius.

2. Kiekviena strategija apima bent šiuos elementus:

a) strateginius tikslus ir prioritetus, kuriais siekiama didinti bendrą ypatingos svarbos subjektų atsparumą atsižvelgiant į tarpvalstybinę ir tarpsektorinę priklausomybę ir tarpusavio priklausomybę;

b) valdymo sistemą, padedančią siekti strateginių tikslų ir prioritetų, įskaitant įvairių institucijų, ypatingos svarbos subjektų ir kitų šalių, dalyvaujančių įgyvendinant strategiją, vaidmenų ir funkcijų aprašymą;

c) priemonių, kurios yra būtinos siekiant didinti bendrą ypatingos svarbos subjektų atsparumą, aprašymą, įskaitant 5 straipsnyje nurodytos rizikos vertinimo aprašymą;

d) ypatingos svarbos subjektų identifikavimo proceso aprašymą;

e) pagal ši skyrių teikiamos paramos ypatingos svarbos subjektams proceso aprašymą, įskaitant viešojo sektoriaus ir privačiojo sektoriaus bei viešųjų ir privačiųjų subjektų bendradarbiavimo stiprinimo priemones;

f) pagrindinių institucijų ir atitinkamų suinteresuotųjų subjektų, išskyrus ypatingos svarbos subjektus, dalyvaujančių įgyvendinant strategiją, sąrašą;

g) politinę sistemą, padedančią užtikrinti kompetentingų institucijų pagal šią direktyvą ir kompetentingų institucijų pagal Direktyvą (ES) 2022/2555 veiksmų koordinavimą siekiant dalytis informacija apie kibernetiniam saugumui kylančią riziką, kibernetines grėsmes bei kibernetinius incidentus ir nekibernetinę riziką, grėsmes bei incidentus ir vykdyti priežiūros užduotis;

h) jau įdiegtų priemonių, kuriomis siekiama sudaryti palankesnes sąlygas mažosioms ir vidutinėms įmonėms, kaip tai suprantama Komisijos rekomendacijos 2003/361/EB ([31]) priede, kurias atitinkama valstybė narė identifikavo kaip ypatingos svarbos subjektus, įgyvendinti pareigas pagal šios direktyvos III skyrių, aprašymą.

Po konsultacijų, kuriose tiek, kiek praktiškai įmanoma, gali dalyvauti visi atitinkami suinteresuotieji subjektai, valstybės narės atnaujina savo strategijas ne rečiau kaip kas ketverius metus.

3. Valstybės narės savo strategijas ir esminius jų atnaujinimus per tris mėnesius nuo jų priėmimo pateikia Komisijai.

5 straipsnis

Valstybių narių atliekamas rizikos vertinimas

1. Komisijai suteikiami įgaliojimai ne vėliau kaip 2023 m. lapkričio 17 d. priimti deleguotąjį aktą pagal 23 straipsnį, kuriuo ši direktyva papildoma nustatant nebaigtinį priede išdėstytuose sektoriuose ir subsektoriuose teikiamų esminių paslaugų sąrašą. Kompetentingos institucijos tą esminių paslaugų sąrašą naudoja, kad ne vėliau kaip 2026 m. sausio 17 d., o vėliau – prireikus, bet ne rečiau kaip kas ketverius metus atliktų rizikos vertinimą (toliau – valstybės narės rizikos vertinimas). Kompetentingos institucijos valstybių narių rizikos vertinimus naudoja, kad identifikuotų ypatingos svarbos subjektus pagal 6 straipsnį ir padėtų tiems ypatingos svarbos subjektams imtis priemonių pagal 13 straipsnį.

Valstybių narių rizikos vertinimuose atsižvelgiama į susijusią gaivalinę ir žmogaus sukeltą riziką, įskaitant tarpsektorinio ir tarpvalstybinio pobūdžio riziką, nelaimingus atsitikimus, gaivalines nelaimes, ekstremaliąsias visuomenės sveikatos situacijas bei hibridines grėsmes ir kitas priešiškų subjektų keliamas grėsmes, įskaitant teroristinius nusikaltimus, kaip numatyta Europos Parlamento ir Tarybos direktyvoje (ES) 2017/541 ([32]).

2. Atlikdamos valstybių narių rizikos vertinimus, valstybės narės atsižvelgia bent į:

a) bendrą rizikos vertinimą, atliktą pagal Sprendimo Nr. 1313/2013/ES 6 straipsnio 1 dalį;

b) kitus susijusius rizikos vertinimus, atliktus pagal atitinkamų konkretiems sektoriams taikomų Sąjungos teisės aktų reikalavimus, įskaitant Europos Parlamento ir Tarybos reglamentus (ES) 2017/1938 ([33]) ir (ES) 2019/941 ([34]) ir Europos Parlamento ir Tarybos direktyvas 2007/60/EB ([35]) ir 2012/18/ES ([36]);

([31]) 2003 m. gegužės 6 d. Komisijos rekomendacija 2003/361/EB dėl mikroįmonių, mažųjų ir vidutinių įmonių apibrėžimo (OL L 124, 2003 5 20, p. 36).
([32]) 2017 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva (ES) 2017/541 dėl kovos su terorizmu, pakeičianti Tarybos pamatinį sprendimą 2002/475/TVR ir iš dalies keičianti Tarybos sprendimą 2005/671/TVR (OL L 88, 2017 3 31, p. 6).
([33]) 2017 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/1938 dėl dujų tiekimo saugumo užtikrinimo priemonių, kuriuo panaikinamas Reglamentas (ES) Nr. 994/2010 (OL L 280, 2017 10 28, p. 1).
([34]) 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/941 dėl pasirengimo valdyti riziką elektros energijos sektoriuje, kuriuo panaikinama Direktyva 2005/89/EB (OL L 158, 2019 6 14, p. 1).
([35]) 2007 m. spalio 23 d. Europos Parlamento ir Tarybos direktyva 2007/60/EB dėl potvynių rizikos įvertinimo ir valdymo (OL L 288, 2007 11 6, p. 27).
([36]) 2012 m. liepos 4 d. Europos Parlamento ir Tarybos direktyva 2012/18/ES dėl didelių, su pavojingomis cheminėmis medžiagomis susijusių avarijų pavojaus kontrolės, iš dalies keičianti ir vėliau panaikinanti Tarybos direktyvą 96/82/EB (OL L 197, 2012 7 24, p. 1).

c) atitinkamą riziką, kuri atsiranda dėl priede išdėstytų sektorių tarpusavio priklausomybės, įskaitant priklausomybę nuo kitose valstybėse narėse ir trečiosiose valstybėse esančių subjektų, ir poveikį, kurį vieno sektoriaus stiprus sutrikdymas gali daryti kitiems sektoriams, įskaitant bet kokią didelę riziką piliečiams ir tarptautinei rinkai;

d) turimą informaciją apie incidentus, apie kuriuos pranešta pagal 15 straipsnį.

Pirmos pastraipos c punkto tikslais, valstybės narės atitinkamai bendradarbiauja su kitų valstybių narių kompetentingomis institucijomis ir trečiųjų valstybių kompetentingomis institucijomis.

3. Valstybės narės leidžia ypatingos svarbos subjektams, kuriuos jos identifikavo pagal 6 straipsnį, susipažinti, kai aktualu, per jų bendruosius kontaktinius punktus, su atitinkamais valstybių narių rizikos vertinimų elementais. Valstybės narės užtikrina, kad ypatingos svarbos subjektams suteikta informacija jiems padėtų atlikti savo rizikos vertinimus pagal 12 straipsnį ir imtis priemonių savo atsparumui užtikrinti pagal 13 straipsnį.

4. Per tris mėnesius po valstybės narės rizikos vertinimo atlikimo, valstybė narė pateikia Komisijai atitinkamą informaciją apie nustatytos rizikos rūšis ir tos valstybės narės rizikos vertinimo rezultatus pagal kiekvieną priede išdėstytą sektorių ir subsektorių.

5. Komisija, bendradarbiaudama su valstybėmis narėmis parengia savanorišką bendrą ataskaitų teikimo šabloną, siekiant laikytis 4 dalies reikalavimų.

6 straipsnis

Ypatingos svarbos subjektų identifikavimas

1. Ne vėliau kaip 2026 m. liepos 17 d. kiekviena valstybė narė identifikuoja priede išdėstytų sektorių ir subsektorių ypatingos svarbos subjektus.

2. Pagal 1 dalį identifikuodama ypatingos svarbos subjektus, valstybė narė atsižvelgia į valstybės narės rizikos vertinimo rezultatus bei savo strategiją ir taiko visus šiuos kriterijus:

a) subjektas teikia vieną arba daugiau esminių paslaugų;

b) subjektas veikia ir jo ypatingos svarbos infrastruktūra yra tos valstybės narės teritorijoje; ir

c) incidentas turėtų didelį trikdomąjį poveikį, kaip nustatyta pagal 7 straipsnio 1 dalį, subjekto vienos arba daugiau esminių paslaugų teikimui arba vienos arba daugiau kitų esminių paslaugų teikimui priede išdėstytuose sektoriuose, kurie yra priklausomi nuo tos esminės paslaugos.

3. Kiekviena valstybė narė sudaro pagal 2 dalį identifikuotų ypatingos svarbos subjektų sąrašą ir užtikrina, kad tiems ypatingos svarbos subjektams apie tai, kad jie identifikuoti kaip ypatingos svarbos subjektai, būtų pranešta per vieną mėnesį nuo tokio identifikavimo dienos. Valstybės narės šiems ypatingos svarbos subjektams praneša apie jų pareigas pagal III ir IV skyrius ir apie datą, nuo kurios jiems taikomos tos pareigos, nedarant poveikio 8 straipsniui. Valstybės narės informuoja ypatingos svarbos subjektus priedo lentelės 3, 4 ir 8 punktuose išdėstytuose sektoriuose, kad jie neturi pareigų pagal III ir IV skyrius, išskyrus atvejus, kai nacionalinėse nuostatose numatyta kitaip.

Atitinkamiems ypatingos svarbos subjektams III skyrius taikomas praėjus 10 mėnesių po šios dalies pirmoje pastraipoje nurodyto pranešimo dienos.

4. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą praneštų kompetentingoms institucijoms pagal Direktyvą (ES) 2022/2555 apie ypatingos svarbos subjektų, kuriuos jos identifikavo pagal šį straipsnį, tapatybę per vieną mėnesį nuo tokio identifikavimo dienos. Tame pranešime, kai taikytina, nurodoma, kad atitinkami ypatingos svarbos subjektai yra subjektai šios direktyvos priedo lentelės 3, 4 ir 8 punktuose išdėstytuose sektoriuose ir kad jie neturi pareigų pagal jos III ir IV skyrius.

5. Valstybės narės prireikus ir bet kuriuo atveju ne rečiau kaip kas ketverius metus peržiūri ir, kai tinkama, atnaujina 3 dalyje nurodytų identifikuotų ypatingos svarbos subjektų sąrašą. Jeigu po tokių atnaujinimų identifikuojami papildomi ypatingos svarbos subjektai, tiems papildomiems ypatingos svarbos subjektams taikomos 3 ir 4 dalys. Be to, valstybės narės užtikrina, kad ypatingos svarbos subjektams, kurie po tokio atnaujinimo nebeidentifikuojami kaip ypatingos svarbos subjektai, būtų pranešta laiku apie tai ir apie tai, kad jiems nuo to pranešimo dienos nebetaikomos pareigos pagal III skyrių.

6. Komisija, bendradarbiaudama su valstybėmis narėmis, parengia rekomendacijas ir neprivalomas gaires, kad padėtų valstybėms narėms identifikuoti ypatingos svarbos subjektus.

7 straipsnis

Didelis trikdomasis poveikis

1. Nustatydamos, ar trikdomasis poveikis yra didelis, kaip nurodyta 6 straipsnio 2 dalies c punkte, valstybės narės atsižvelgia į šiuos kriterijus:

a) naudotojų, kurie priklauso nuo atitinkamo subjekto teikiamos esminės paslaugos, skaičių;

b) priede išdėstytų kitų sektorių ir subsektorių priklausomybę nuo atitinkamos esminės paslaugos;

c) poveikį, kurį incidentai dėl savo masto ir trukmės galėtų padaryti ekonominei ir visuomenės veiklai, aplinkai, viešajam saugumui bei saugai ar gyventojų sveikatai;

d) subjekto rinkos dalį atitinkamos esminės paslaugos ar esminių paslaugų rinkoje;

e) geografinę teritoriją, kurioje incidentas galėtų daryti poveikį, įskaitant bet kokias tarpvalstybines pasekmes, atsižvelgiant į pažeidžiamumą dėl tam tikrų tipų geografinių teritorijų, pavyzdžiui, salų regionų, atokių regionų ar kalnuotų vietovių, tam tikro lygio izoliacijos;

f) subjekto svarbą pakankamam esminės paslaugos lygiui išlaikyti, atsižvelgiant į esamas tos esminės paslaugos teikimo alternatyvas.

2. Identifikavusios ypatingos svarbos subjektus pagal 6 straipsnio 1 dalį, kiekviena valstybė narė nepagrįstai nedelsdama pateikia Komisijai šią informaciją:

a) esminių paslaugų toje valstybėje narėje sąrašą, kai, palyginti su 5 straipsnio 1 dalyje nurodytu esminių paslaugų sąrašu, yra papildomų esminių paslaugų;

b) ypatingos svarbos subjektų, identifikuotų kiekviename priede nustatytame sektoriuje ir subsektoriuje ir kiekvienos esminės paslaugos atžvilgiu, skaičių;

c) bet kokias ribas, taikomas siekiant sukonkretinti vieną ar daugiau iš 1 dalyje išvardytų kriterijų.

Pirmos pastraipos c punkte nurodytos ribos gali būti pateiktos atskirai arba agreguota forma.

Valstybės narės pirmoje pastraipoje nurodytą informaciją paskui teikia prireikus, bet ne rečiau kaip kas ketverius metus.

3. Komisija, pasikonsultavusi su 19 straipsnyje nurodyta Ypatingos svarbos subjektų atsparumo klausimų grupe, atsižvelgdama į šio straipsnio 2 dalyje nurodytą informaciją, priima neprivalomas gaires, kad palengvintų šio straipsnio 1 dalyje nurodytų kriterijų taikymą.

8 straipsnis

Ypatingos svarbos subjektai bankininkystės, finansų rinkos infrastruktūros ir skaitmeninės infrastruktūros sektoriuose

Valstybės narės užtikrina, kad 11 straipsnis ir III, IV bei VI skyriai nebūtų taikomi jų identifikuotiems ypatingos svarbos subjektams sektoriuose, išdėstytuose priede pateiktos lentelės 3, 4 ir 8 punktuose. Valstybės narės gali priimti arba palikti galioti nacionalinės teisės nuostatas aukštesniam tų ypatingos svarbos subjektų atsparumo lygiui užtikrinti, su sąlyga, kad tos nuostatos atitinka taikytiną Sąjungos teisę.

9 straipsnis

Kompetentingos institucijos ir bendrieji kontaktiniai punktai

1. Kiekviena valstybė narė paskiria arba įsteigia vieną arba daugiau kompetentingų institucijų, atsakingų už tinkamą šioje direktyvoje išdėstytų taisyklių taikymą ir prireikus jų vykdymo užtikrinimą nacionaliniu lygmeniu.

Kalbant apie ypatingos svarbos subjektus šios direktyvos priede pateiktos lentelės 3 ir 4 punktuose išdėstytuose sektoriuose, kompetentingos institucijos iš esmės turi būti Reglamento (ES) 2022/2554 46 straipsnyje nurodytos kompetentingos institucijos. Kalbant apie ypatingos svarbos subjektus šios direktyvos priede pateiktos lentelės 8 punkte išdėstytame sektoriuje, kompetentingos institucijos iš esmės turi būti kompetentingos institucijos pagal Direktyvą (ES) 2022/2555. Valstybės narės gali šios direktyvos priede pateiktos lentelės 3, 4 ir 8 punktuose išdėstytų sektorių atžvilgiu pagal esamas nacionalines sistemas paskirti kitą kompetentingą instituciją.

Jei valstybės narės paskiria ar įsteigia daugiau nei vieną kompetentingą instituciją, jos aiškiai nustato konkrečias kiekvienos institucijos užduotis ir užtikrina, kad jos veiksmingai bendradarbiautų vykdydamos savo užduotis pagal šią direktyvą, įskaitant užduotis, susijusias su 2 dalyje nurodyto bendrojo kontaktinio punkto paskyrimu ir veikla.

2. Kiekviena valstybė narė paskiria ar įsteigia vieną bendrąjį kontaktinį punktą vykdyti ryšių palaikymo funkciją ir taip užtikrinti tarpvalstybinį bendradarbiavimą su kitų valstybių narių bendraisiais kontaktiniais punktais ir 19 straipsnyje nurodyta Ypatingos svarbos subjektų atsparumo klausimų grupe (toliau – bendrasis kontaktinis punktas). Kai aktualu, valstybė narė savo bendrąjį kontaktinį punktą paskiria kompetentingoje institucijoje. Kai aktualu, valstybė narė gali nustatyti, kad jos bendrasis kontaktinis punktas taip pat užtikrina ryšių su Komisija palaikymo funkciją ir bendradarbiavimą su trečiosiomis valstybėmis.

3. Ne vėliau kaip 2028 m. liepos 17 d., o vėliau – kas dvejus metus bendrieji kontaktiniai punktai pateikia Komisijai ir 19 straipsnyje nurodytai Ypatingos svarbos subjektų atsparumo klausimų grupei apibendrinamąją ataskaitą apie jų gautus pranešimus, be kita ko, nurodydami pranešimų skaičių, praneštų incidentų pobūdį ir veiksmus, kurių buvo imtasi pagal 15 straipsnio 3 dalį.

Komisija, bendradarbiaudama su Ypatingos svarbos subjektų atsparumo klausimų grupe, parengia bendrą ataskaitų teikimo šabloną. Kompetentingos institucijos teikdamos pirmoje pastraipoje nurodytas apibendrinamąsias ataskaitas gali savanoriškai naudotis tuo bendru ataskaitų teikimo šablonu.

4. Kiekviena valstybė narė užtikrina, kad jos kompetentinga institucija ir bendrasis kontaktinis punktas turėtų įgaliojimus ir tinkamų finansinių, žmogiškųjų ir techninių išteklių, kad galėtų veiksmingai ir efektyviai vykdyti jiems pavestas užduotis.

5. Kiekviena valstybė narė užtikrina, kad jos kompetentinga institucija, kai tinkama, ir laikydamasi Sąjungos ir nacionalinės teisės, konsultuotųsi ir bendradarbiautų su kitomis atitinkamomis nacionalinėmis institucijomis, įskaitant institucijas, atsakingas už civilinę saugą, teisėsaugą ir asmens duomenų apsaugą, taip pat su ypatingos svarbos subjektais ir atitinkamomis suinteresuotosiomis šalimis.

6. Kiekviena valstybės narė užtikrina, kad jos kompetentinga institucija pagal šią direktyvą bendradarbiautų ir keistųsi informacija su kompetentingomis institucijomis pagal Direktyvą (ES) 2022/2555 kibernetiniam saugumui kylančios rizikos, kibernetinių grėsmių ir kibernetinių incidentų ir nekibernetinės rizikos, grėsmių bei incidentų, darančių poveikį ypatingos svarbos subjektams, klausimais, taip pat dėl atitinkamų priemonių, kurių ėmėsi jos kompetentinga institucija ir kompetentingos institucijos pagal Direktyvą (ES) 2022/2555.

7. Per tris mėnesius nuo kompetentingos institucijos ir bendrojo kontaktinio punkto paskyrimo ar įsteigimo kiekviena valstybė narė praneša Komisijai apie jų tapatybę ir jų užduotis ir pareigas pagal šią direktyvą, jų kontaktinius duomenis ir bet kokius jų vėlesnius pakeitimus. Jei valstybės narės nusprendžia ypatingos svarbos subjektų priede pateiktos lentelės 3, 4 ir 8 punktuose išdėstytuose sektoriuose atžvilgiu kompetentingomis institucijomis paskirti kitas institucijas, nei kompetentingos institucijos, nurodytos 1 dalies antroje pastraipoje, jos apie tai informuoja Komisiją. Kiekviena valstybė narė viešai paskelbia savo kompetentingos institucijos ir bendrojo kontaktinio punkto tapatybę.

8. Komisija bendrųjų kontaktinių punktų sąrašą paskelbia viešai.

10 straipsnis

Valstybių narių parama ypatingos svarbos subjektams

1. Valstybės narės remia ypatingos svarbos subjektų pastangas didinti savo atsparumą. Ta parama gali apimti rekomendacinės medžiagos ir metodikos rengimą, pagalbą rengiant pratybas, kad būtų išbandytas ypatingos svarbos subjektų atsparumas, ir konsultacijų bei mokymo jų darbuotojams teikimą. Nedarant poveikio taikytinoms valstybės pagalbos taisyklėms, valstybės narės gali skirti finansinių išteklių ypatingos svarbos subjektams, kai tai būtina ir pagrįsta su viešuoju interesu susijusiais tikslais.

2. Kiekviena valstybė narė užtikrina, kad jos kompetentinga institucija bendradarbiautų ir keistųsi informacija bei gerosios praktikos pavyzdžiais su priede išdėstytų sektorių ypatingos svarbos subjektais.

3. Valstybės narės sudaro palankesnes sąlygas savanoriškam ypatingos svarbos subjektų dalijimuisi informacija į šią direktyvą įtrauktais klausimais, laikantis Sąjungos ir nacionalinės teisės, ypač įslaptintos ir neskelbtinos informacijos, konkurencijos ir asmens duomenų apsaugos srityje.

11 straipsnis

Valstybių narių tarpusavio bendradarbiavimas

1. Kai tai tikslinga, valstybės narės konsultuojasi tarpusavyje dėl ypatingos svarbos subjektų, kad užtikrintų nuoseklų šios direktyvos taikymą. Tokios konsultacijos rengiamos visų pirma dėl ypatingos svarbos subjektų, kurie:

a) naudoja ypatingos svarbos infrastruktūrą, kuri yra fiziškai sujungta tarp dviejų ar daugiau valstybių narių;

b) yra įmonių struktūrų, kurios yra sujungtos su ypatingos svarbos subjektais kitose valstybėse narėse arba prijungtos prie jų, dalis;

c) buvo identifikuoti kaip ypatingos svarbos subjektai vienoje valstybėje narėje ir teikia esmines paslaugas kitoms valstybėms narėms arba kitose valstybėse narėse.

2. 1 dalyje nurodytomis konsultacijomis turi būti siekiama didinti ypatingos svarbos subjektų atsparumą ir, kai įmanoma, sumažinti jiems tenkančią administracinę naštą.

III SKYRIUS

YPATINGOS SVARBOS SUBJEKTŲ ATSPARUMAS

12 straipsnis

Ypatingos svarbos subjektų atliekamas rizikos vertinimas

1. Nedarant poveikio 6 straipsnio 3 dalies antroje pastraipoje nustatytam terminui, valstybės narės užtikrina, kad ypatingos svarbos subjektai per devynis mėnesius po 6 straipsnio 3 dalyje nurodyto pranešimo gavimo dienos, o vėliau – prireikus, bet ne rečiau kaip kas ketverius metus, remdamiesi valstybių narių rizikos vertinimais ir kitais atitinkamais informacijos šaltiniais, įvertintų visą susijusią riziką, kuri galėtų sutrikdyti jų esminių paslaugų teikimą (toliau – ypatingos svarbos subjekto rizikos vertinimas).

2. Ypatingos svarbos subjekto rizikos vertinime atsižvelgiama į visas aktualias rizikas, dėl kurių galėtų kilti incidentas, įskaitant tarpsektorinio ir tarpvalstybinio pobūdžio incidentus, nelaimingus atsitikimus, gaivalines nelaimes, ekstremaliąsias visuomenės sveikatos situacijas bei hibridines grėsmes ir kitas priešiškų subjektų keliamas grėsmes, įskaitant teroristinius nusikaltimus, kaip numatyta Europos Parlamento ir Tarybos direktyvoje (ES) 2017/541. Ypatingos svarbos subjekto rizikos vertinime atsižvelgiama į kitų priede išdėstytų sektorių priklausomybę nuo ypatingos svarbos subjekto teikiamos esminės paslaugos ir į tai, kiek ypatingos svarbos subjektas, teikdamas esmines paslaugas, yra priklausomas nuo kitų tokių kitų sektorių subjektų, be kita ko, kai aktualu, kaimyninėse valstybėse narėse ir trečiosiose valstybėse.

Jei ypatingos svarbos subjektas atliko kitų rizikos vertinimų arba parengė dokumentų laikydamasis kituose teisės aktuose, kurie yra aktualūs jo ypatingos svarbos subjekto rizikos vertinimui, nustatytų pareigų, jis gali naudoti tuos vertinimus ir dokumentus, kad įvykdytų šiame straipsnyje nustatytus reikalavimus. Vykdydama priežiūros funkcijas, kompetentinga institucija gali paskelbti, kad esamas ypatingos svarbos subjekto atliktas rizikos vertinimas, kuriame nagrinėjama šios dalies pirmoje pastraipoje nurodyta rizika ir priklausomybė, iš dalies arba visiškai atitinka pareigas pagal šį straipsnį.

13 straipsnis

Ypatingos svarbos subjektų taikomos atsparumo priemonės

1. Valstybės narės užtikrina, kad ypatingos svarbos subjektai imtųsi tinkamų ir proporcingų techninių, saugumo ir organizacinių priemonių, kuriomis būtų užtikrintas jų atsparumas, remdamiesi valstybių narių pateikta atitinkama informacija apie valstybės narės rizikos vertinimą ir ypatingos svarbos subjekto rizikos vertinimo rezultatus, įskaitant priemones, kurios yra būtinos siekiant:

a) užkirsti kelią incidentams, tinkamai atsižvelgiant į nelaimių rizikos mažinimo ir prisitaikymo prie klimato kaitos priemones;

b) užtikrinti tinkamą fizinę savo patalpų ir ypatingos svarbos infrastruktūros apsaugą, tinkamai įvertinant, pavyzdžiui, tvorų ir kliūčių statymą, perimetro stebėsenos priemones ir taisykles, aptikimo įrangą ir prieigos kontrolę;

c) reaguoti į incidentų pasekmes, jas atlaikyti ir sušvelninti, tinkamai įvertinant rizikos ir krizės valdymo procedūrų ir protokolų įgyvendinimą ir perspėjimo taisykles;

d) atstatyti veiklą po incidentų, tinkamai įvertinant veiklos tęstinumo priemones ir alternatyvių tiekimo grandinių nustatymą, siekiant atnaujinti esminės paslaugos teikimą;

e) užtikrinti tinkamą darbuotojų saugumo valdymą, tinkamai įvertinant tokias priemones kaip ypatingos svarbos funkcijas vykdančių darbuotojų kategorijų nustatymas, prieigos prie patalpų, ypatingos svarbos infrastruktūros ir neskelbtinos informacijos teisių suteikimas, asmenų patikrinimo procedūrų pagal 14 straipsnį nustatymas ir asmenų kategorijų, kurioms reikia atlikti tokius asmenų patikrinimus, nustatymas ir tinkamų mokymo reikalavimų ir kvalifikacijų nustatymas;

f) didinti atitinkamų darbuotojų informuotumą apie a–e punktuose nurodytas priemones, tinkamai atsižvelgiant į mokymo kursus, informacinę medžiagą ir pratybas.

Pirmos pastraipos e punkto tikslais valstybės narės užtikrina, kad nustatydami ypatingos svarbos funkcijas vykdančių darbuotojų kategorijas, ypatingos svarbos subjektai atsižvelgtų į išorės paslaugų teikėjų darbuotojus.

2. Valstybės narės užtikrina, kad ypatingos svarbos subjektai turėtų parengtą ir taikytų atsparumo planą arba lygiavertį dokumentą (-us), kuriame (-iuose) būtų aprašytos priemonės, kurių imtasi pagal 1 dalį. Jei ypatingos svarbos subjektai parengė dokumentus arba ėmėsi priemonių laikydamiesi kituose teisės aktuose, kurie yra aktualūs šio straipsnio 1 dalyje nurodytų priemonių atžvilgiu, nustatytų pareigų, jie gali naudoti tuos dokumentus ir priemones, kad įvykdytų šiame straipsnyje nustatytus reikalavimus. Vykdydama priežiūros funkcijas kompetentinga institucija gali paskelbti, kad esamos ypatingos svarbos subjekto taikomos atsparumo didinimo priemonės, kuriomis tinkamai ir proporcingai atsižvelgiama į 1 dalyje nurodytas technines, saugumo ir organizacines priemones, iš dalies arba visiškai atitinka pareigas pagal šį straipsnį.

3. Valstybės narės užtikrina, kad kiekvienas ypatingos svarbos subjektas ryšių palaikymo arba lygiavertį pareigūną paskirtų kaip kontaktinį punktą ryšiams su kompetentingomis institucijomis.

4. Valstybės narės, kuri identifikavo ypatingos svarbos subjektą, prašymu ir atitinkamam ypatingos svarbos subjektui sutikus, Komisija rengia patariamąsias misijas pagal 18 straipsnio 6, 8 ir 9 dalyse nustatytą tvarką, kad patartų atitinkamam ypatingos svarbos subjektui, kaip vykdyti savo pareigas pagal III skyrių. Apie patariamosios misijos išvadas pranešama Komisijai, tai valstybei narei ir atitinkamam ypatingos svarbos subjektui.

5. Komisija, pasikonsultavusi su 19 straipsnyje nurodyta Ypatingos svarbos subjektų atsparumo klausimų grupe, priima neprivalomas gaires, kuriose išsamiau išdėsto techninės, saugumo ir organizacines priemones, kurių gali būti imtasi pagal šio straipsnio 1 dalį.

6. Siekdama nustatyti būtinas techninės ir metodines specifikacijas, susijusias su šio straipsnio 1 dalyje nurodytų priemonių taikymu, Komisija priima įgyvendinimo aktus. Tie įgyvendinimo aktai priimami laikantis 24 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

14 straipsnis

Asmenų patikrinimai

1. Valstybės narės nustato sąlygas, kuriomis ypatingos svarbos subjektui, tinkamai pagrįstais atvejais ir atsižvelgiant į valstybės narės rizikos vertinimą, būtų leidžiama pateikti prašymus, kad būtų atlikti patikrinimai asmenų, kurie:

a) atlieka didesnės rizikos funkcijas ypatingos svarbos subjekte arba jo naudai, ypač susijusias su to ypatingos svarbos subjekto atsparumu;

b) yra įgalioti turėti tiesioginę arba nuotolinę prieigą prie ypatingos svarbos subjekto patalpų, informacijos arba kontrolės sistemų, be kita ko, kiek tai susiję su to ypatingos svarbos subjekto saugumu;

c) yra kandidatai, kuriuos svarstoma įdarbinti eiti pareigas, kurioms taikomi a ar b punkte išdėstyti kriterijai.

2. Šio straipsnio 1 dalyje nurodyti prašymai įvertinami per pagrįstą laikotarpį ir tvarkomi laikantis nacionalinės teisės ir nacionalinių procedūrų ir atitinkamos ir taikytinos Sąjungos teisės, įskaitant Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 ir Europos Parlamento ir Tarybos direktyvą (ES) 2016/680 ([37]). Asmenų patikrinimai turi būti proporcingi ir griežtai apsiriboti tuo, kas būtina. Jie atliekami vieninteliu tikslu: įvertinti galimą saugumo riziką atitinkamam ypatingos svarbos subjektui.

3. Atliekant 1 dalyje nurodytus asmenų patikrinimus bent:

a) patvirtinama tikrinamo asmens tapatybė;

b) patikrinama informacija apie to asmens teistumą už nusikaltimus, kurie yra aktualūs einant konkrečias pareigas.

Atlikdamos asmenų patikrinimus, valstybės narės, siekdamos gauti informacijos apie teistumą iš kitų valstybių narių, naudojasi Europos nuosprendžių registrų informacine sistema, laikydamosi Pamatiniame sprendime 2009/315/TVR ir, kai aktualu ir taikytina, Reglamente (ES) 2019/816 nustatytų procedūrų. Pamatinio sprendimo 2009/315/TVR 3 straipsnio 1 dalyje ir Reglamento (ES) 2019/816 3 straipsnio 5 punkte nurodytos centrinės institucijos atsakymus į prašymus pateikti tokią informaciją pateikia per 10 darbo dienų nuo prašymo gavimo dienos, laikydamosi Pamatinio sprendimo 2009/315/TVR 8 straipsnio 1 dalies.

([37]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016 5 4, p. 89).

15 straipsnis

Pranešimas apie incidentus

1. Valstybės narės užtikrina, kad ypatingos svarbos subjektai nepagrįstai nedelsdami praneštų kompetentingai institucijai apie incidentus, kurie stipriai sutrikdo arba gali stipriai sutrikdyti esminių paslaugų teikimą. Valstybės narės užtikrina, kad išskyrus atvejus, kai veiklos požiūriu to padaryti neįmanoma, ypatingos svarbos subjektai pirmąjį pranešimą pateiktų ne vėliau kaip per 24 valandas nuo tada, kai sužino apie incidentą, o ne vėliau kaip per vieną mėnesį po to, kai aktualu, pateiktų išsamią ataskaitą. Siekiant nustatyti sutrikdymo reikšmingumą, visų pirma atsižvelgiama į šiuos parametrus:

a) sutrikdymo paveiktų naudotojų skaičių ir proporciją;

b) sutrikdymo trukmę;

c) sutrikdymo paveiktą geografinę vietovę, atsižvelgiant į tai, ar ta vietovė yra geografiškai izoliuota.

Jei incidentas daro arba gali daryti didelį poveikį esminių paslaugų teikimo tęstinumui šešiose ar daugiau valstybių narių, incidento paveiktų valstybių narių kompetentingos institucijos apie tą incidentą praneša Komisijai.

2. 1 dalies pirmoje pastraipoje nurodytuose pranešimuose pateikiama visa turima informacija, būtina tam, kad kompetentinga institucija galėtų suprasti incidento pobūdį, numanomą priežastį ir galimas pasekmes, be kita ko, visą įmanomą informaciją, reikalingą nustatyti bet kokį tarpvalstybinį incidento poveikį. Dėl tokių pranešimų ypatingos svarbos subjektams netaikoma didesnė atsakomybė.

3. Remdamasi ypatingos svarbos subjekto 1 dalyje nurodytame pranešime pateikta informacija, atitinkama kompetentinga institucija per bendrąjį kontaktinį punktą informuoja kitų paveiktų valstybių narių bendruosius kontaktinius punktus, jeigu incidentas daro arba galėtų daryti didelį poveikį ypatingos svarbos subjektams ir esminių paslaugų teikimo tęstinumui į vieną ar daugiau arba vienoje ar daugiau kitų valstybių narių.

Siųsdami ir gaudami informaciją pagal pirmą pastraipą, bendrieji kontaktiniai punktai pagal Sąjungos ar nacionalinės teisę tą informaciją tvarko taip, kad būtų paisoma jos konfidencialumo, taip pat užtikrinamas atitinkamo ypatingos svarbos subjekto saugumas ir apsaugomi jo komerciniai interesai.

4. Atitinkama kompetentinga institucija, gavusi 1 dalyje nurodytą pranešimą, kuo greičiau pateikia atitinkamam ypatingos svarbos subjektui atitinkamą informaciją dėl tolesnių veiksmų, įskaitant informaciją, kuri galėtų padėti tam ypatingos svarbos subjektui veiksmingai reaguoti į atitinkamą incidentą. Jei valstybės narės nustato, kad tai atitinka viešąjį interesą, jos informuoja visuomenę.

16 straipsnis

Standartai

Siekdamos skatinti vienodą šios direktyvos įgyvendinimą, valstybės narės, kai tai naudinga ir nereikalaudamos taikyti kokios nors konkrečios rūšies technologijos, taip pat nesuteikdamos jai pirmenybės, skatina naudotis Europos ir tarptautiniais standartais bei techninėmis specifikacijomis, kurie yra aktualūs ypatingos svarbos subjektui taikomoms saugumo ir atsparumo priemonėms.

IV SKYRIUS

EUROPOS MASTU YPAČ REIKŠMINGI YPATINGOS SVARBOS SUBJEKTAI

17 straipsnis

Europos mastu ypač reikšmingų ypatingos svarbos subjektų identifikavimas

1. Subjektas laikomas Europos mastu ypač reikšmingu ypatingos svarbos subjektu, jei:

a) pagal 6 straipsnio 1 dalį jis buvo identifikuotas kaip ypatingos svarbos subjektas;

b) jis teikia tas pačias arba panašias esmines paslaugas šešioms ar daugiau arba šešiose ar daugiau valstybių narių ir

c) apie jį pranešta pagal šio straipsnio 3 dalį.

2. Valstybės narės užtikrina, kad ypatingos svarbos subjektas, gavęs 6 straipsnio 3 dalyje nurodytą pranešimą, savo kompetentingą instituciją informuotų, kai jis teikia esmines paslaugas šešioms ar daugiau arba šešiose ar daugiau valstybių narių. Tokiu atveju valstybės narės užtikrina, kad ypatingos svarbos subjektas informuotų savo kompetentingą instituciją apie esmines paslaugas, kurias jis teikia toms valstybėms narėms arba tose valstybėse narėse, ir apie valstybes nares, kurioms arba kuriose jis teikia tas esmines paslaugas. Valstybė narė nepagrįstai nedelsdama praneša Komisijai tokių ypatingos svarbos subjektų tapatybes ir pagal šią dalį jų pateiktą informaciją.

Komisija konsultuojasi su valstybės narės, kuri identifikavo ypatingos svarbos subjektą, kaip nurodyta pirmoje pastraipoje, kompetentinga institucija, kitų atitinkamų valstybių narių kompetentinga institucija ir su atitinkamu ypatingos svarbos subjektu. Tose konsultacijose kiekviena valstybė narė praneša Komisijai, jei paslaugas, kurias jai teikia ypatingos svarbos subjektas, ta valstybė narė laiko esminėmis paslaugomis.

3. Jei Komisija, remdamasi šio straipsnio 2 dalyje nurodytomis konsultacijomis, nustato, kad atitinkamas ypatingos svarbos subjektas teikia esmines paslaugas šešioms ar daugiau arba šešiose ar daugiau valstybių narių, Komisija per to ypatingos svarbos subjekto kompetentingą instituciją jam praneša, kad jis laikomas Europos mastu ypač reikšmingu ypatingos svarbos subjektu, taip pat informuoja tą ypatingos svarbos subjektą apie jo pareigas pagal šį skyrių ir dieną, nuo kurios tos pareigos jam taikomos. Kai Komisija informuoja kompetentingą instituciją apie savo sprendimą tam tikrą ypatingos svarbos subjektą laikyti Europos mastu ypač reikšmingu ypatingos svarbos subjektu, kompetentinga institucija nepagrįstai nedelsdama persiunčia tą pranešimą tam ypatingos svarbos subjektui.

4. Šis skyrius atitinkamam Europos mastu ypač reikšmingam ypatingos svarbos subjektui taikomas nuo šio straipsnio 3 dalyje nurodyto pranešimo gavimo dienos.

18 straipsnis

Patariamosios misijos

1. Valstybės narės, kuri pagal 6 straipsnio 1 dalį Europos mastu ypač reikšmingą ypatingos svarbos subjektą identifikavo kaip ypatingos svarbos subjektą, prašymu Komisija surengia patariamąją misiją priemonėms, kurias tas ypatingos svarbos subjektas įdiegė, kad įvykdytų savo pareigas pagal III skyrių, įvertinti.

2. Savo iniciatyva ar vienos ar daugiau valstybių narių, kuriai (-ioms) arba kurioje (-iose) teikiama esminė paslauga, prašymu ir sutikus valstybei narei, kuri pagal 6 straipsnio 1 dalį Europos mastu ypač reikšmingą ypatingos svarbos subjektą identifikavo kaip ypatingos svarbos subjektą, Komisija surengia šio straipsnio 1 dalyje nurodytą patariamąją misiją.

3. Komisijos arba vienos ar daugiau valstybių narių, kurioms arba kuriose teikiama esminė paslauga, pagrįstu prašymu valstybė narė, kuri pagal 6 straipsnio 1 dalį Europos mastu ypač reikšmingą ypatingos svarbos subjektą identifikavo kaip ypatingos svarbos subjektą, Komisijai pateikia:

a) ypatingos svarbos objekto rizikos vertinimo atitinkamas dalis;

b) atitinkamų priemonių, kurių imtasi pagal 13 straipsnį, sąrašą;

c) informaciją apie priežiūros ar vykdymo užtikrinimo veiksmus, įskaitant atitikties vertinimus arba duotus nurodymus, kurių jos kompetentinga institucija dėl to ypatingos svarbos subjekto ėmėsi pagal 21 ir 22 straipsnius.

4. Apie patariamosios misijos išvadas per tris mėnesius po tos patariamosios misijos užbaigimo dienos pranešama Komisijai, valstybei narei, kuri pagal 6 straipsnio 1 dalį Europos mastu ypač reikšmingą ypatingos svarbos subjektą identifikavo kaip ypatingos svarbos subjektą, valstybėms narėms, kurioms arba kuriose teikiama esminė paslauga, ir atitinkamam ypatingos svarbos subjektui.

Valstybės narės, kurioms arba kuriose teikiama esminė paslauga, išanalizuoja pirmoje pastraipoje nurodytą pranešimą ir prireikus pataria Komisijai dėl to, ar atitinkamas Europos mastu ypač reikšmingas ypatingos svarbos subjektas laikosi savo pareigų pagal III skyrių, ir, kai tinkama, kokių priemonių būtų galima imtis to ypatingos svarbos subjekto atsparumui padidinti.

Komisija, remdamasi antroje pastraipoje nurodytais patarimais, valstybei narei, kuri pagal 6 straipsnio 1 dalį Europos mastu ypač reikšmingą ypatingos svarbos subjektą identifikavo kaip ypatingos svarbos subjektą, valstybėms narėms, kurioms arba kuriose teikiama esminė paslauga, ir tam ypatingos svarbos subjektui perduoda savo nuomonę apie tai, ar tas ypatingos svarbos subjektas laikosi savo pareigų pagal III skyrių, ir, kai tinkama, kokių priemonių būtų galima imtis to ypatingos svarbos subjekto atsparumui padidinti.

Valstybė narė kuri pagal 6 straipsnio 1 dalį Europos mastu ypač reikšmingą ypatingos svarbos subjektą identifikavo kaip ypatingos svarbos subjektą, užtikrina, kad jos kompetentinga institucija ir atitinkamas ypatingos svarbos subjektas deramai atsižvelgtų į šios dalies trečioje pastraipoje nurodytą nuomonę ir Komisijai bei valstybėms narėms, kurioms arba kuriose teikiama esminė paslauga, pateikia informaciją apie priemones, kurių ji ėmėsi vadovaudamasi ta nuomone.

5. Kiekvieną patariamąją misiją sudaro ekspertai iš valstybės narės, kurioje yra Europos mastu ypač reikšmingas ypatingos svarbos subjektas, ekspertai iš valstybių narių, kurioms arba kuriose teikiama esminė paslauga, ir Komisijos atstovai. Tos valstybės narės gali pasiūlyti patariamosios misijos dalyvių kandidatūras. Komisija, pasikonsultavusi su valstybe nare, kuri pagal 6 straipsnio 1 dalį Europos mastu ypač reikšmingą ypatingos svarbos subjektą identifikavo kaip ypatingos svarbos subjektą, kiekvienos patariamosios misijos narius atrenka ir paskiria atsižvelgdama į jų profesinę kompetenciją ir užtikrindama, kai įmanoma, geografiniu požiūriu proporcingą atstovavimą visoms toms valstybėms narėms. Prireikus patariamosios misijos nariai turi turėti galiojantį ir tinkamą asmens patikimumo pažymėjimą. Komisija padengia su dalyvavimu patariamojoje misijoje susijusias išlaidas.

Komisija pasirūpina, kad būtų parengta kiekvienos patariamosios misijos programa, ir tai daro konsultuodamasi su atitinkamos patariamosios misijos nariais ir susitarusi su valstybe nare, kuri pagal 6 straipsnio 1 dalį Europos mastu ypač reikšmingą ypatingos svarbos subjektą identifikavo kaip ypatingos svarbos subjektą.

6. Komisija priima įgyvendinimo aktą, kuriame nustato taisykles dėl prašymų organizuoti patariamąsias misijas pateikimo ir tų prašymų nagrinėjimo, dėl patariamųjų misijų vykdymo bei ataskaitų dėl jų rengimo ir dėl komunikacijos apie šio straipsnio 4 dalies trečioje pastraipoje nurodytą Komisijos nuomonę ir taikytas priemones valdymo procedūrinės tvarkos, tinkamai atsižvelgdama į atitinkamos informacijos konfidencialumą ir neskelbtiną komercinį pobūdį. Tas įgyvendinimo aktas priimamas laikantis 24 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

7. Valstybės narės užtikrina, kad atitinkami Europos mastu ypač reikšmingi ypatingos svarbos subjektai suteiktų patariamųjų misijų dalyviams prieigą prie informacijos, sistemų ir įrangos, susijusių su jų esminių paslaugų teikimu ir būtinų atitinkamai patariamajai misijai vykdyti.

8. Patariamosios misijos vykdomos laikantis valstybės narės, kurioje jos vyksta, taikytinos nacionalinės teisės, gerbiant tos valstybės narės atsakomybę už nacionalinį saugumą ir jos saugumo interesų apsaugą.

9. Rengdama patariamąsias misijas, Komisija atsižvelgia į bet kokių patikrinimų pagal reglamentus (EB) Nr. 725/2004 ir (EB) Nr. 300/2008 ir bet kokios stebėsenos pagal Direktyvą 2005/65/EB, kuriuos Komisija atliko atitinkamai dėl atitinkamo ypatingos svarbos subjekto, ataskaitas.

10. Kiekvieną kartą, kai rengiama patariamoji misija, Komisija apie tai informuoja 19 straipsnyje nurodytą Ypatingos svarbos subjektų atsparumo klausimų grupę. Valstybė narė, kurioje vyko patariamoji misija, ir Komisija Ypatingos svarbos subjektų atsparumo klausimų grupę taip pat informuoja apie patariamosios misijos pagrindines išvadas ir per ją įgytą patirtį, kad būtų skatinamas tarpusavio mokymasis.

V SKYRIUS

BENDRADARBIAVIMAS IR ATASKAITŲ TEIKIMAS

19 straipsnis

Ypatingos svarbos subjektų atsparumo klausimų grupė

1. Sudaroma Ypatingos svarbos subjektų atsparumo klausimų grupė. Ypatingos svarbos subjektų atsparumo klausimų grupė remia Komisiją ir palengvina valstybių narių tarpusavio bendradarbiavimą bei keitimąsi informacija su šia direktyva susijusiais klausimais.

2. Ypatingos svarbos subjektų atsparumo klausimų grupę sudaro valstybių narių ir Komisijos atstovai, kai tikslinga, turintys asmens patikimumo pažymėjimą. Ypatingos svarbos subjektų atsparumo klausimų grupė, kai tai yra svarbu vykdant jos užduotis, gali kviesti savo darbe dalyvauti atitinkamus suinteresuotuosius subjektus. Europos Parlamento prašymu Komisija gali pakviesti Ypatingos svarbos subjektų atsparumo klausimų grupės posėdžiuose dalyvauti Europos Parlamento ekspertus.

Ypatingos svarbos subjektų atsparumo klausimų grupės posėdžiams pirmininkauja Komisijos atstovas.

3. Ypatingos svarbos subjektų atsparumo klausimų grupė vykdo šias užduotis:

a) remia Komisiją padedant valstybėms narėms didinti jų gebėjimus prisidėti prie ypatingos svarbos subjektų atsparumo užtikrinimo pagal šią direktyvą;

b) analizuoja strategijas, kad nustatytų su strategijomis susijusią geriausią praktiką;

c) palengvina keitimąsi geriausios praktikos pavyzdžiais, susijusiais su valstybių narių atliekamu ypatingos svarbos subjektų identifikavimu pagal 6 straipsnio 1 dalį, be kita ko, atsižvelgiant į jų tarpvalstybinę ir tarpsektorinę priklausomybę, ir susijusiais su rizika bei incidentais;

d) kai tinkama, su šia direktyva susijusiais klausimais prisideda prie dokumentų, susijusių su atsparumu Sąjungos lygmeniu, rengimo;

e) prisideda rengiant 7 straipsnio 3 dalyje bei 13 straipsnio 5 dalyje nurodytas gaires ir, pagal prašymą, bet kokius pagal šią direktyvą priimtus deleguotuosius arba įgyvendinimo aktus;

f) analizuoja 9 straipsnio 3 dalyje nurodytas apibendrinamąsias ataskaitas siekiant skatinti dalijimąsi geriausios praktikos pavyzdžiais, susijusiais su veiksmais, kurių imtasi pagal 15 straipsnio 3 dalį;

g) keičiasi geriausios praktikos pavyzdžiais, susijusiais su 15 straipsnyje nurodytais pranešimais apie incidentus;

h) aptaria patariamųjų misijų apibendrinamąsias ataskaitas ir įgytą patirtį pagal 18 straipsnio 10 dalį;

i) keičiasi informacija ir geriausios praktikos pavyzdžiais inovacijų, mokslinių tyrimų ir plėtros srityse, kiek tai susiję su ypatingos svarbos subjektų atsparumu pagal šią direktyvą;

j) kai aktualu, keičiasi informacija su ypatingos svarbos subjektų atsparumu susijusiais klausimais su atitinkamomis Sąjungos institucijomis, įstaigomis, organais ir agentūromis.

4. Ypatingos svarbos subjektų atsparumo klausimų grupė ne vėliau kaip 2025 m. sausio 17 d., o vėliau – kas dvejus metus parengia darbo programą dėl veiksmų, kurių reikia imtis siekiant įgyvendinti jos tikslus ir užduotis. Ta darbo programa turi atitikti šios direktyvos reikalavimus ir tikslus.

5. Ypatingos svarbos subjektų atsparumo klausimų grupė reguliariai ir bent kartą per metus susitinka su Bendradarbiavimo grupe, sudaryta pagal Direktyvą (ES) 2022/2555, kad skatintų ir lengvintų bendradarbiavimą ir keitimąsi informacija.

6. Komisija gali priimti įgyvendinimo aktus, kuriais nustatoma procedūrinė tvarka, būtina Ypatingos svarbos subjektų atsparumo klausimų grupės veikimui užtikrinti, laikantis 1 straipsnio 4 dalies Tie įgyvendinimo aktai priimami laikantis 24 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

7. Komisija pateikia Ypatingos svarbos subjektų atsparumo klausimų grupei ataskaitą, kurioje apibendrinama valstybių narių pagal 4 straipsnio 3 dalį ir 5 straipsnio 4 dalį pateikta informacija, ne vėliau kaip 2027 m. sausio 17 d., o vėliau – prireikus, bet ne rečiau kaip kas ketverius metus.

20 straipsnis

Komisijos parama kompetentingoms institucijoms ir ypatingos svarbos subjektams

1. Komisija, kai tinkama, remia valstybes nares ir ypatingos svarbos subjektus jiems vykdant savo pareigas pagal šią direktyvą. Komisija parengia tarpvalstybinės ir tarpsektorinės rizikos, kylančios esminių paslaugų teikimui, Sąjungos lygmens apžvalgą, rengia 13 straipsnio 4 dalyje ir 18 straipsnyje nurodytas patariamąsias misijas ir palengvina keitimąsi informacija tarp valstybių narių ir ekspertų visoje Sąjungoje.

2. Komisija papildo 10 straipsnyje nurodytą valstybių narių veiklą parengdama geriausios praktikos pavyzdžius, rekomendacinę medžiagą bei metodiką ir plėtodama tarpvalstybinę mokymo veiklą ir pratybas, siekiant išbandyti ypatingos svarbos subjektų atsparumą.

3. Komisija informuoja valstybes nares apie Sąjungos lygmens finansinius išteklius, kuriais valstybės narės gali naudotis ypatingos svarbos subjektų atsparumui didinti.

VI SKYRIUS

PRIEŽIŪRA IR VYKDYMO UŽTIKRINIMAS

21 straipsnis

Priežiūra ir vykdymo užtikrinimas

1. Valstybės narės, siekdamos įvertinti, kaip subjektai, kuriuos jos pagal 6 straipsnio 1 dalį identifikavo kaip ypatingos svarbos subjektus, laikosi pareigų pagal šią direktyvą, užtikrina, kad kompetentingos institucijos turėtų įgaliojimus ir priemones:

a) atlikti ypatingos svarbos infrastruktūros ir patalpų, kurias ypatingos svarbos subjektas naudoja teikdamas savo esmines paslaugas, patikrinimus vietoje ir vykdyti priemonių, kurių ėmėsi ypatingos svarbos subjektai, priežiūrą ne vietoje pagal 13 straipsnį;

b) atlikti arba nurodyti atlikti ypatingos svarbos subjektų auditą.

2. Valstybės narės užtikrina, kad kompetentingos institucijos turėtų įgaliojimus ir priemones tais atvejais, kai tai yra būtina jų užduotims pagal šią direktyvą atlikti, reikalauti, kad subjektai pagal Direktyvą (ES) 2022/2555, kuriuos valstybės narės identifikavo kaip ypatingos svarbos subjektus pagal šią Direktyvą, per tų institucijų nustatytą pagrįstą terminą pateiktų:

a) informaciją, kuri yra būtina siekiant įvertinti, ar priemonės, kurių tie subjektai ėmėsi savo atsparumui užtikrinti, atitinka 13 straipsnyje išdėstytus reikalavimus;

b) veiksmingo tų priemonių įgyvendinimo įrodymus, įskaitant audito, kurį to subjekto sąskaita atliko jo atrinktas nepriklausomas ir kvalifikuotas auditorius, rezultatus.

Kompetentingos institucijos, reikalaudamos pateikti tą informaciją, nurodo reikalavimo tikslą ir konkrečią reikalaujamą informaciją.

3. Nedarant poveikio galimybei nustatyti sankcijas pagal 22 straipsnį, kompetentingos institucijos po to, kai buvo atlikti šio straipsnio 1 dalyje nurodyti priežiūros veiksmai, arba įvertinus šio straipsnio 2 dalyje nurodytą informaciją gali duoti nurodymą atitinkamiems ypatingos svarbos subjektams per tų institucijų nustatytą pagrįstą terminą imtis būtinų ir proporcingų priemonių, kuriomis būtų ištaisytas nustatytas šios direktyvos pažeidimas, ir pateikti toms institucijoms informaciją apie priemones, kurių buvo imtasi. Duodant tuos nurodymus visų pirma atsižvelgiama į pažeidimo sunkumą.

4. Valstybė narė užtikrina, kad 1, 2 ir 3 dalyse numatyti įgaliojimai būtų įgyvendinami tik taikant tinkamas apsaugos priemones. Šiomis apsaugos priemonėmis visų pirma garantuojama, kad tokiais įgaliojimais būtų naudojamasi objektyviai, skaidriai ir proporcingai ir kad būtų tinkamai apsaugotos paveiktų ypatingos svarbos subjektų teisės ir teisėti interesai, pavyzdžiui, teisė į komercinių ir verslo paslapčių apsaugą, įskaitant jų teisę būti išklausytiems, teisę į gynybą ir veiksmingą teisių gynimą nepriklausomame teisme.

5. Valstybės narės užtikrina, kad kompetentinga institucija pagal šią direktyvą, pagal šį straipsnį įvertinusi ypatingos svarbos subjekto atitiktį, informuotų atitinkamos valstybės narės kompetentingas institucijas pagal Direktyvą (ES) 2022/2555. Tuo tikslu valstybės narės užtikrina, kad kompetentingos institucijos pagal šią direktyvą galėtų prašyti kompetentingų institucijų pagal Direktyvą (ES) 2022/2555, kad tos institucijos pasinaudotų savo priežiūros ir vykdymo užtikrinimo įgaliojimais subjekto, kuriam taikoma ta direktyva ir kuris buvo identifikuotas kaip ypatingos svarbos subjektas pagal šią direktyvą, atžvilgiu. Tuo tikslu valstybės narės užtikrina, kad kompetentingos institucijos pagal šią direktyvą bendradarbiautų ir keistųsi informacija su kompetentingomis institucijomis pagal Direktyvą (ES) 2022/2555.

22 straipsnis

Sankcijos

Valstybės narės nustato sankcijų, taikomų pažeidus pagal šią direktyvą priimtas nacionalines nuostatas, taisykles ir imasi visų būtinų priemonių užtikrinti, kad šios sankcijos būtų įgyvendinamos. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos. Valstybės narės ne vėliau kaip 2024 m. spalio 17 d. praneša apie tas taisykles ir tas priemones Komisijai ir nedelsdamos jai praneša apie visus vėlesnius joms įtakos turinčius pakeitimus.

VII SKYRIUS

DELEGUOTIEJI IR ĮGYVENDINIMO AKTAI

23 straipsnis

Įgaliojimų delegavimas

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

2. 5 straipsnio 1 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo 2023 m. sausio 16 d.

3. Europos Parlamentas arba Taryba gali bet kada atšaukti 5 straipsnio 1 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 5 straipsnio 1 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.

24 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.

VIII SKYRIUS

BAIGIAMOSIOS NUOSTATOS

25 straipsnis

Ataskaitų teikimas ir peržiūra

Ne vėliau kaip 2027 m. liepos 17 d. Komisija pateikia ataskaitą Europos Parlamentui ir Tarybai, kurioje įvertinama, kokiu mastu kiekviena valstybė narė ėmėsi būtinų priemonių, kad būtų laikomasi šios direktyvos.

Komisija periodiškai peržiūri šios direktyvos veikimą ir teikia ataskaitas Europos Parlamentui ir Tarybai. Toje ataskaitoje visų pirma įvertinama šios direktyvos pridėtinė vertė, jos poveikis užtikrinant ypatingos svarbos subjektų atsparumą ir tai, ar reikėtų iš dalies pakeisti šios direktyvos priedą. Pirmąją tokią ataskaitą Komisija pateikia ne vėliau kaip 2029 m. birželio 17 d. Pranešimo pagal šį straipsnį tikslu Komisija atsižvelgia į atitinkamus Ypatingos svarbos subjektų atsparumo klausimų grupės dokumentus.

26 straipsnis

Perkėlimas į nacionalinę teisę

1. Valstybės narės ne vėliau kaip 2024 m. spalio 17 d. priima ir paskelbia nuostatas, būtinas, kad būtų laikomasi šios direktyvos. Apie tai jos nedelsdamos praneša Komisijai.

Tas nuostatas jos taiko nuo 2024 m. spalio 18 d.

2. Valstybės narės, priimdamos pirmoje dalyje nurodytas nuostatas, daro jose nuorodą į šią direktyvą, arba tokia nuoroda daroma jas oficialiai skelbiant. Nuorodos darymo tvarką nustato valstybės narės.

27 straipsnis

Direktyvos 2008/114/EB panaikinimas

Direktyva 2008/114/EB panaikinama nuo 2024 m. spalio 18 d.

Nuorodos į panaikintą direktyvą laikomos nuorodomis į šią direktyvą.

28 straipsnis

Įsigaliojimas

Ši direktyva įsigalioja dvidešimtą dieną po jos paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

29 straipsnis

Adresatai

Ši direktyva skirta valstybėms narėms.

Priimta Strasbūre 2022 m. gruodžio 14 d.

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkė	*Pirmininkas*
R. METSOLA	M. BEK

PRIEDAS

SEKTORIAI, SUBSEKTORIAI IR SUBJEKTŲ KATEGORIJOS

Sektoriai	Subsektoriai	Subjektų kategorijos
1. Energetika	a) Elektros energija	— Elektros energijos įmonės, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2019/944 ([1]) 2 straipsnio 57 punkte, kurios vykdo tiekimo funkciją, kaip apibrėžta tos direktyvos 2 straipsnio 12 punkte
		— Skirstymo sistemos operatoriai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 29 punkte
		— Perdavimo sistemos operatoriai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 35 punkte
		— Gamintojai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 38 punkte
		— Paskirtieji elektros energijos rinkos operatoriai, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/943 ([2]) 2 straipsnio 8 punkte
		— Elektros energijos rinkos dalyviai, kaip apibrėžta Reglamento (ES) 2019/943 2 straipsnio 25 punkte, teikiantys telkimo, reguliavimo apkrova arba energijos kaupimo paslaugas, nurodytas Direktyvos (ES) 2019/944 2 straipsnio 18, 20 ir 59 punktuose
	b) Centralizuotas šilumos ir vėsumos tiekimas	— Centralizuotos šilumos arba vėsumos operatoriai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2018/2001 ([3]) 2 straipsnio 19 punkte
	c) Nafta	— Naftotiekių operatoriai
		— Naftos gamybos, perdirbimo ir apdorojimo įrenginių, laikymo ir perdavimo operatoriai
		— Centrinės atsargų saugyklos, kaip apibrėžta Tarybos direktyvos 2009/119/EB ([4]) 2 straipsnio f punkte

Sektoriai	Subsektoriai	Subjektų kategorijos
	d) Dujos	— Tiekimo įmonės, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/73/EB ([5]) 2 straipsnio 8 punkte
		— Skirstymo sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 6 punkte
		— Perdavimo sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 4 punkte
		— Laikymo sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 10 punkte
		— SGD sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 12 punkte
		— Gamtinių dujų įmonės, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 1 punkte
		— Gamtinių dujų perdirbimo ir apdorojimo įrenginių operatoriai
	e) Vandenilis	— Vandenilio gamybos, laikymo ir perdavimo operatoriai
2. Transportas	a) Oro transportas	— Oro vežėjai, kaip apibrėžta Reglamento (EB) Nr. 300/2008 3 straipsnio 4 punkte, naudojami komerciniais tikslais
		— Oro uosto valdymo organai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/12/EB ([6]) 2 straipsnio 2 punkte, oro uostai, kaip apibrėžta tos direktyvos 2 straipsnio 1 punkte, įskaitant Europos Parlamento ir Tarybos reglamento (ES) Nr. 1315/2013 ([7]) II priedo 2 skirsnyje išvardytus pagrindinius oro uostus, ir subjektai, eksploatuojantys oro uostuose esančius pagalbinius įrenginius
		— Eismo valdymo operatoriai, teikiantys skrydžių valdymo (ATC) paslaugas, nurodytas Europos Parlamento ir Tarybos reglamento (EB) Nr. 549/2004 ([8]) 2 straipsnio 1 punkte

Sektoriai	Subsektoriai	Subjektų kategorijos
	b) Geležinkelių transportas	— Infrastruktūros valdytojai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2012/34/ES ([9]) 3 straipsnio 2 punkte
		— Geležinkelio įmonės, kaip apibrėžta Direktyvos 2012/34/ES 3 straipsnio 1 punkte, ir paslaugų įrenginių operatoriai, kaip apibrėžta tos Direktyvos 3 straipsnio 12 punkte
	c) Vandens transportas	— Vidaus vandenų, jūrų ir pakrančių keleivinio ir krovininio vandens transporto bendrovės, kaip apibrėžta Reglamento (EB) Nr. 725/2004 I priede ir priskiriamos jūrų transporto sektoriui, neįskaitant tų bendrovių eksploatuojamų atskirų laivų
		— Uostų, nurodytų Direktyvos 2005/65/EB 3 straipsnio 1 punkte, įskaitant jų uosto įrenginius, kaip apibrėžta Reglamento (EB) Nr. 725/2004 2 straipsnio 11 punkte, valdymo įstaigos ir subjektai, eksploatuojantys uostuose esančias įmones ir įrenginius
		— Laivų eismo tarnybų (LET), kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2002/59/EB ([10]) 3 straipsnio o punkte, operatoriai
	d) Kelių transportas	— Kelių direkcijos, kaip apibrėžta Komisijos deleguotojo reglamento (ES) 2015/962 ([11]) 2 straipsnio 12 punkte, atsakingos už eismo valdymo kontrolę, išskyrus viešuosius subjektus, kuriems eismo valdymo arba intelektinių transporto sistemų operacijų veikla yra neesminė jų bendros veiklos dalis
		— Intelektinių transporto sistemų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2010/40/ES ([12]) 4 straipsnio 1 punkte, operatoriai
	e) Viešasis transportas	— Viešųjų paslaugų operatoriai, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (EB) Nr. 1370/2007 ([13]) 2 straipsnio d punkte
3. Bankininkystė		— Kredito įstaigos, kaip apibrėžta Reglamento (ES) Nr. 575/2013 4 straipsnio 1 punkte
4. Finansų rinkų infrastruktūros		— Prekybos vietų, kaip apibrėžta Direktyvos 2014/65/ES 4 straipsnio 24 punkte, operatoriai
		— Pagrindinės sandorio šalys, kaip apibrėžta Reglamento (ES) Nr. 648/2012 2 straipsnio 1 punkte

Sektoriai	Subsektoriai	Subjektų kategorijos
5. Sveikata		— Sveikatos priežiūros paslaugų teikėjai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2011/24/ES ([14]) 3 straipsnio g punkte
		— ES etaloninės laboratorijos, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2022/2371 ([15]) 15 straipsnyje
		— Subjektai, vykdantys vaistų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2001/83/EB ([16]) 1 straipsnio 2 punkte, mokslinių tyrimų ir kūrimo veiklą
		— Subjektai, gaminantys pagrindinius vaistus ir farmacinius preparatus, nurodytus NACE 2 red. C sekcijos 21 skyriuje
		— Subjektai, gaminantys medicinos priemones, kurios laikomos ypatingos svarbos ekstremaliosios visuomenės sveikatos situacijos atveju (ypatingos svarbos medicinos priemonių ekstremaliosios visuomenės sveikatos situacijos atveju sąrašas), kaip tai suprantama Europos Parlamento ir Tarybos reglamento (ES) 2022/123 ([17]) 22 straipsnyje
		— Subjektai, turintys platinimo leidimą, kaip nurodyta Direktyvos 2001/83/EB 79 straipsnyje
6. Geriamasis vanduo		— Žmonėms vartoti skirto vandens, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2020/2184 ([18]) 2 straipsnio 1 punkto a papunktyje, tiekėjai ir skirstytojai, išskyrus skirstytojus, kuriems žmonėms vartoti skirto vandens skirstymas yra neesminė jų bendrosios kitų prekių ir produktų paskirstymo veiklos dalis
7. Nuotekos		— Miesto, buitines ir gamybines nuotekas, kaip apibrėžta Tarybos direktyvos 91/271/EEB ([19]) 2 straipsnio 1, 2 ir 3 punktuose, renkančios, šalinančios arba valančios įmonės, išskyrus įmones, kurioms miesto, buitinių ir pramoninių nuotekų rinkimas, šalinimas arba valymas yra neesminė jų bendros veiklos dalis

Sektoriai	Subsektoriai	Subjektų kategorijos
8. Skaitmeninė infrastruktūra		— Interneto duomenų srautų mainų taško, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 18 punkte, teikėjai
		— DNS paslaugų teikėjai, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 20 punkte, išskyrus šakninio pavadinimo serverių operatorius
		— Aukščiausio lygio domeno vardų registrai, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 21 punkte
		— Debesijos kompiuterijos paslaugos, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 30 punkte, teikėjai
		— Duomenų centro paslaugos, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 31 punkte, teikėjai
		— Turinio teikimo tinklo, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 32 punkte, teikėjai
		— Patikimumo užtikrinimo paslaugų teikėjai, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 ([20]) 3 straipsnio 19 punkte
		— Viešųjų elektroninių ryšių tinklų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2018/1972 ([21]) 2 straipsnio 8 punkte, teikėjai
		— Elektroninių ryšių paslaugų, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 4 punkte, teikėjai, kai jų paslaugos yra viešai prieinamos
9. Viešasis administravimas		— Centrinės valdžios viešojo administravimo subjektai, kaip valstybės narės apibrėžė pagal nacionalinę teisę
10. Kosmosas		— Valstybėms narėms arba privačiosioms šalims priklausančios, jų valdomos ir eksploatuojamos antžeminės infrastruktūros operatoriai, kurie remia kosminių paslaugų teikimą, išskyrus viešųjų elektroninių ryšių tinklų, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 8 punkte, teikėjus

Sektoriai	Subsektoriai	Subjektų kategorijos
11. Maisto produktų gamyba, maisto perdirbimas ir platinimas		— Maisto verslai (verslo įmonės), kaip apibrėžta Europos Parlamento ir Tarybos reglamento (EB) Nr. 178/2002 ([22]) 3 straipsnio 2 punkte, užsiimančios tik logistika ir didmeniniu platinimu, didelio masto pramonine gamyba ir perdirbimu

([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).

([2]) 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/943 dėl elektros energijos vidaus rinkos (OL L 158, 2019 6 14, p. 54).

([3]) 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/2001 dėl skatinimo naudoti atsinaujinančiųjų išteklių energiją (OL L 328, 2018 12 21, p. 82).

([4]) 2009 m. rugsėjo 14 d. Tarybos direktyva 2009/119/EB, kuria valstybės narės įpareigojamos išlaikyti privalomąsias žalios naftos ir (arba) naftos produktų atsargas (OL L 265, 2009 10 9, p. 9).

([5]) 2009 m. liepos 13 d. Europos Parlamento ir Tarybos direktyva 2009/73/EB dėl gamtinių dujų vidaus rinkos bendrųjų taisyklių, panaikinanti Direktyvą 2003/55/EB (OL L 211, 2009 8 14, p. 94).

([6]) 2009 m. kovo 11 d. Europos Parlamento ir Tarybos direktyva 2009/12/EB dėl oro uostų mokesčių (OL L 70, 2009 3 14, p. 11).

([7]) 2013 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1315/2013 dėl Sąjungos transeuropinio transporto tinklo plėtros gairių, kuriuo panaikinamas Sprendimas Nr. 661/2010/ES (OL L 348, 2013 12 20, p. 1).

([8]) 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 549/2004, nustatantis bendro Europos dangaus sukūrimo pagrindą (pagrindų reglamentas) (OL L 96, 2004 3 31, p. 1).

([9]) 2012 m. lapkričio 21 d. Europos Parlamento ir Tarybos direktyva 2012/34/ES, kuria sukuriama bendra Europos geležinkelių erdvė (OL L 343, 2012 12 14, p. 32).

([10]) 2002 m. birželio 27 d. Europos Parlamento ir Tarybos direktyva 2002/59/EB, įdiegianti Bendrijos laivų eismo stebėsenos ir informacijos sistemą ir panaikinanti Tarybos direktyvą 93/75/EEB (OL L 208, 2002 8 5, p. 10).

([11]) 2014 m. gruodžio 18 d. Komisijos deleguotasis reglamentas (ES) 2015/962, kuriuo papildomos Europos Parlamento ir Tarybos direktyvos 2010/40/ES nuostatos, susijusios su visoje Europos Sąjungoje teikiamomis tikralaikės eismo informacijos paslaugomis (OL L 157, 2015 6 23, p. 21).

([12]) 2010 m. liepos 7 d. Europos Parlamento ir Tarybos direktyva 2010/40/ES dėl kelių transporto ir jo sąsajų su kitų rūšių transportu srities intelektinių transporto sistemų diegimo sistemos (OL L 207, 2010 8 6, p. 1).

([13]) 2007 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1370/2007 dėl keleivinio geležinkelių ir kelių transporto viešųjų paslaugų ir panaikinantis Tarybos reglamentus (EEB) Nr. 1191/69 ir Nr. 1107/70 (OL L 315, 2007 12 3, p. 1).

([14]) 2011 m. kovo 9 d. Europos Parlamento ir Tarybos direktyva 2011/24/ES dėl pacientų teisių į tarpvalstybines sveikatos priežiūros paslaugas įgyvendinimo (OL L 88, 2011 4 4, p. 45).

([15]) 2022 m. lapkričio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2371 dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai, kuriuo panaikinamas Sprendimas Nr. 1082/2013/ES (OL L 314, 2022 12 6, p. 26).

([16]) 2001 m. lapkričio 6 d. Europos Parlamento ir Tarybos direktyva 2001/83/EB dėl Bendrijos kodekso, reglamentuojančio žmonėms skirtus vaistus (OL L 311, 2001 11 28, p. 67).

([17]) 2022 m. sausio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/123 dėl didesnio Europos vaistų agentūros vaidmens pasirengimo vaistų ir medicinos priemonių krizei ir jos valdymo srityje (OL L 20, 2022 1 31, p. 1).

([18]) 2020 m. gruodžio 16 d. Europos Parlamento ir Tarybos direktyva (ES) 2020/2184 dėl žmonėms vartoti skirto vandens kokybės (OL L 435, 2020 12 23, p 1).

([19]) 1991 m. gegužės 21 d. Tarybos direktyva 91/271/EEB dėl miesto nuotėkų valymo (OL L 135, 1991 5 30, p. 40).

([20]) 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).

([21]) 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (OL L 321, 2018 12 17, p. 36).

([22]) 2002 m. sausio 28 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 178/2002, nustatantis maistui skirtų teisės aktų bendruosius principus ir reikalavimus, įsteigiantis Europos maisto saugos tarnybą ir nustatantis su maisto saugos klausimais susijusias procedūras (OL L 31, 2002 2 1, p. 1).

ISSN 1977-0723 (elektroninis leidimas)
ISSN 1725-5120 (popierinis leidimas)

Europos Sąjungos
leidinių biuras
L-2985 Liuksemburgas
LIUKSEMBURGAS

LT