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