3.11.2022 A9-0341/ 001-001

PAKEITIMAS 001-001
pateikė Ekonomikos ir pinigų politikos komitetas

Pranešimas
Billy Kelleher **A9-0341/2021**
Skaitmeniniai finansai: Skaitmeninės veiklos atsparumo aktas (DORA)

Pasiūlymas dėl reglamento (COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

Pakeitimas 1

EUROPOS PARLAMENTO PAKEITIMAI*

Komisijos pasiūlymas

2020/0266(COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014 ir (ES) Nr. 909/2014

(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,

---

* Pakeitimai: naujas ar pakeistas tekstas žymimas pusjuodžiu kursyvu, o išbrauktas tekstas nurodomas simboliu ▌.

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,

kadangi:

(1) skaitmeniniame amžiuje informacinėmis ir ryšių technologijomis (IRT) palaikomos sudėtingos sistemos, naudojamos kasdienei visuomeninei veiklai. Jos padeda mūsų ekonomikai pagrindiniuose sektoriuose, įskaitant finansų sektorių, ir stiprina bendrosios rinkos veikimą. Didesnis skaitmeninimas ir tarpusavio sąsajos taip pat didina IRT riziką, todėl visa visuomenė, o ypač finansų sistema, tampa labiau pažeidžiama kibernetinių grėsmių ar IRT sutrikimų atžvilgiu. Nors plačiai paplitęs IRT sistemų naudojimas ir didelis skaitmeninimas bei junglumas dabar yra pagrindiniai visos Sąjungos finansų sektoriaus subjektų veiklos bruožai, skaitmeninis atsparumas dar nėra pakankamai integruotas į jų veiklos sistemas;

(2) per pastaruosius dešimtmečius IRT naudojimas įgijo esminį vaidmenį finansų srityje ir šiandien yra ypatingai aktualus visų finansų sektoriaus subjektų įprastų kasdienių funkcijų vykdymui. Skaitmeninimas apima, pavyzdžiui, mokėjimus, kuriuos 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, ▌žalos administravimą ir netiesioginio aptarnavimo operacijas. ***IRT taip pat iš esmės pakeitė draudimo sektorių, pradedant skaitmeninių draudimo tarpininkų, veikiančių su „InsurTech“, atsiradimu, ir baigiant skaitmenine draudimo veikla ir sutarčių platinimu.*** Finansų sektorius ne tik tapo iš esmės skaitmeninis, bet skaitmeninimas padidino tarpusavio sąsajas ir priklausomybę pačiame finansų sektoriuje ir sąsajas su trečiųjų šalių infrastruktūra ir paslaugų teikėjais bei priklausomybę nuo jų;

(3) 2020 m. ataskaitoje dėl sisteminės kibernetinės rizikos[3] Europos sisteminės rizikos valdyba (ESRV) dar kartą patvirtino, kad dabartinės stiprios finansų sektoriaus subjektų, finansų rinkų ir finansų rinkos infrastruktūrų tarpusavio sąsajos, ypač jų IRT sistemų tarpusavio priklausomybė, galėtų virsti sisteminiu pažeidžiamumu, nes vienoje vietoje kilę kibernetiniai incidentai, nevaržomi jokių geografinių ribų, galėtų greitai išplisti iš bet kurio iš maždaug 22 000 Sąjungos finansų sektoriaus subjektų[4] į visą finansų

---

1 [*įrašyti nuorodą*] OL C , , p. .

2 OL L 155, 2021 4 30 p. 38.

3 2020 m. vasario mėn. ESRV ataskaita „Sisteminė kibernetinė rizika“, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

4 Remiantis poveikio vertinimu, pridedamu prie Europos priežiūros institucijų peržiūros (SWD(2017) 308), yra maždaug 5 665 kredito įstaigos, 5 934 investicinės įmonės, 2 666 draudimo įmonės, 1 573 profesinių pensijų įstaigų, 2 500 investicijų valdymo įmonių, 350 rinkos infrastruktūrų (pavyzdžiui, pagrindinių sandorio šalių, vertybinių popierių biržų, sistemingai sandorius savo viduje sudarančių tarpininkų, sandorių duomenų saugyklų ir daugiašalių prekybos sistemų), 45 kredito reitingų agentūros ir 2 500 veiklos leidimus turinčių mokėjimo įstaigų ir elektroninių pinigų įstaigų. Tai sudaro maždaug 21 233 subjektus ir neapima sutelktinio finansavimo subjektų, teisės

sistemą. Sunkūs IRT pažeidimai finansų srityje daro poveikį ne tik finansų sektoriaus subjektams. Jie taip pat sudaro sąlygas vienoje vietoje atsiradusioms pažeidžiamumo problemoms plisti finansiniais perdavimo kanalais ir gali turėti neigiamų padarinių Sąjungos finansų sistemos stabilumui, nes mažina likvidumą ir apskritai pasikliovimą ir pasitikėjimą finansų rinkomis;

(4) pastaraisiais metais IRT rizika sulaukė nacionalinių, Europos ir tarptautinių politikos formuotojų, reguliavimo institucijų ir standartus nustatančių įstaigų, siekiančių stiprinti atsparumą, nustatyti standartus ir koordinuoti reguliavimo ar priežiūros darbą, dėmesio. Tarptautiniu lygmeniu Bazelio bankų priežiūros komitetas, Mokėjimo ir rinkos infrastruktūrų komitetas, Finansinio stabilumo taryba, Finansinio stabilumo institutas, taip pat G 7 ir G 20 valstybių grupės siekia įvairių jurisdikcijų kompetentingoms institucijoms ir rinkos operatoriams suteikti priemonių jų finansų sistemų atsparumui stiprinti***. Todėl IRT riziką būtina vertinti glaudžiai tarpusavyje susijusios pasaulinės finansų sistemos kontekste, nes joje pirmenybė turi būti teikiama tarptautinio reguliavimo nuoseklumui ir kompetentingų institucijų bendradarbiavimui visame pasaulyje;***

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

(6) Komisijos 2018 m. „Fintech“ srities veiksmų plane[1] buvo pabrėžta, kad itin svarbu, jog Sąjungos finansų sektorius taptų atsparesnis ir 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 bankininkystės institucija (EBI), Europos vertybinių popierių ir rinkų institucija (ESMA) ir Europos draudimo ir profesinių pensijų institucija (EIOPA) (toliau kartu – Europos priežiūros institucijos, EPI) kartu paskelbė dvi technines rekomendacijas, ragindamos laikytis nuoseklaus požiūrio į IRT riziką finansų srityje ir rekomenduodamos proporcingai didinti finansinių paslaugų sektoriaus skaitmeninės veiklos atsparumą įgyvendinant Sąjungos konkrečiam sektoriui skirtą iniciatyvą;

(8) Sąjungos finansų sektorių reglamentuoja suderintas bendras taisyklių sąvadas ir

---

aktų nustatytą auditą atliekančių auditorių ir audito įmonių, kriptoturto paslaugų teikėjų ir lyginamųjų indeksų administratorių.

[1] Komisijos komunikatas Europos Parlamentui, Tarybai, Europos Centriniam Bankui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „FinTech“ srities veiksmų planas: konkurencingesnis ir novatoriškesnis Europos finansų sektorius“, COM/2018/0109 *final*, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

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 siekiant 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 šį komponentą, ***stiprinant*** finansų priežiūros institucijų ***įgaliojimus valdyti IRT riziką*** finansų ***sektoriuje, apsaugoti vidaus rinkos vientisumą ir efektyvumą bei sudaryti palankesnes sąlygas tvarkingam veikimui***;

(9) dėl teisės aktų skirtumų ir nevienodų nacionalinių reguliavimo ar priežiūros metodų, susijusių su IRT rizika, atsiranda bendrosios finansinių paslaugų rinkos kliūčių, dėl kurių tarpvalstybinę veiklą vykdantiems finansų sektoriaus subjektams trukdoma sklandžiai naudotis įsisteigimo laisve ir paslaugų teikimo laisve. Lygiai taip pat gali būti iškraipoma tos pačios rūšies finansų sektoriaus subjektų, veikiančių skirtingose valstybėse narėse, konkurencija. 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 sudaryti papildomų kliūčių bendrosios rinkos veikimui, o tai pakenktų rinkos dalyviams ir finansiniam stabilumui;

(10) su IRT rizika susijusios nuostatos Sąjungos lygmeniu tvarkytos nenuosekliai, todėl svarbiose srityse, pavyzdžiui, pranešimo apie su IRT susijusius incidentus ir skaitmeninės veiklos atsparumo testavimo srityse, stebimos spragos arba dalinis nuostatų sutapimas, o dėl priimamų skirtingų nacionalinių taisyklių arba ekonomiškai neefektyvaus iš dalies sutampančių taisyklių taikymo atsiranda nenuoseklumas. Tai ypač kenkia tokiam intensyviam IRT naudotojui kaip finansų sektorius, nes technologijų rizika neturi sienų, o finansų sektoriaus paslaugos teikiamos plačiai tarpvalstybiniu mastu 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 savarankiškai ir nuosekliai bei ekonomiškai efektyviai mažindami IRT riziką ir švelnindami IRT incidentų neigiamą poveikį;

(10a) tinkamos tinklų ir informacinės sistemos infrastruktūros sukūrimas ir palaikymas taip pat yra svarbi išankstinė veiksmingo rizikos duomenų kaupimo ir pranešimo apie riziką praktikos, kuri savo ruožtu yra būtina patikimam ir tvariam kredito įstaigų rizikos valdymui ir sprendimų priėmimo procesams, sąlyga. 2013 m. Bazelio bankų priežiūros komitetas (BBPK) paskelbė veiksmingo rizikos duomenų apibendrinimo ir pranešimo apie riziką principų rinkinį (BBPK 239), grindžiamą dviem bendraisiais valdymo ir IT infrastruktūros principais, kuris turėjo būti įgyvendintas iki 2016 m. pradžios. Remiantis 2018 m. gegužės mėn. Europos Centrinio banko (ECB) ataskaita dėl teminės peržiūros dėl veiksmingo rizikos duomenų apibendrinimo, 2018 m. gegužės mėn. rizikos ataskaita ir BBPK 2020 m. balandžio mėn. pažangos ataskaita daroma išvada, kad pasaulinės sisteminės svarbos bankų padaryta įgyvendinimo pažanga yra nepatenkinama ir kad tai kelia susirūpinimą. Siekdama palengvinti tarptautinių standartų laikymąsi ir suderinimą su jais, Komisija, glaudžiai bendradarbiaudama su ECB ir pasikonsultavusi su EBI bei ESRV, turėtų parengti

ataskaitą, kurioje būtų įvertinta, kaip BBPK 239 principai sąveikauja su šio reglamento nuostatomis ir, jei tinkama, kaip tie principai turėtų būti įtraukti į Sąjungos teisę;

(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. Pajėgumai ir bendras atsparumas, kuriuos finansų sektoriaus subjektai įgytų laikydamiesi tokių pagrindinių reikalavimų, kad nenukentėtų veiklos sutrikdymo atvejais, padėtų išsaugoti Sąjungos finansų rinkų stabilumą bei vientisumą ir užtikrinti aukštą investuotojų ir vartotojų apsaugos lygį Sąjungoje. Kadangi šiuo reglamentu siekiama prisidėti prie sklandaus bendrosios rinkos veikimo, jis turėtų būti grindžiamas SESV 114 straipsnio nuostatomis, atsižvelgiant į jų aiškinimą pagal nusistovėjusią Europos Sąjungos Teisingumo Teismo praktiką;

(12) šiuo reglamentu pirmiausia siekiama konsoliduoti ir atnaujinti IRT rizikos reikalavimus, kurie iki šiol buvo atskirai aptariami skirtinguose reglamentuose ir direktyvose. Nors tie Sąjungos teisės aktai apėmė pagrindines finansinės rizikos kategorijas (pvz., kredito riziką, rinkos riziką, sandorio šalies kredito riziką ir likvidumo riziką, elgesio rinkoje riziką), juos priimant nebuvo galima išsamiai atsižvelgti į visus veiklos atsparumo komponentus. Toliau plėtojant operacinės rizikos reikalavimus šiuose Sąjungos teisės aktuose dažnai pirmenybė teikta tradiciniam kiekybiniam rizikos mažinimo metodui (t. y. nustatant kapitalo reikalavimus IRT rizikai padengti), o ne siekiui įtvirtinti tikslinius kokybinius reikalavimus, kuriais didinami pajėgumai, pavyzdžiui, reikalavimus, kuriais užtikrinami apsaugos nuo su IRT susijusių incidentų, jų aptikimo, izoliavimo, veiklos atkūrimo ir taisymo pajėgumai, arba nustatyti pranešimų teikimo ir skaitmeninio testavimo pajėgumus. Tos direktyvos ir reglamentai visų pirma buvo skirti esminėms prudencinės priežiūros, rinkos vientisumo ar elgesio taisyklėms.

Šiame dokumente, kuriame konsoliduojamos ir atnaujinamos IRT rizikos taisyklės, visos nuostatos, susijusios su skaitmenine rizika finansų sektoriuje, būtų pirmą kartą sykiu nuosekliai išdėstytos viename teisėkūros procedūra priimame akte. Taigi šia iniciatyva turėtų būti užpildytos kai kurių tokių teisės aktų spragos arba pašalintas jų nenuoseklumas, įskaitant juose vartojamą terminiją, ir turėtų būti aiškiai įvardyta IRT rizika, numatant tikslines IRT rizikos valdymo pajėgumų, pranešimų teikimo ir testavimo bei trečiųjų šalių keliamos rizikos stebėsenos taisykles. ***Šia iniciatyva taip pat siekiama didinti informuotumą apie IRT riziką ir pripažįstama, kad IRT incidentai ir veiklos atsparumo stoka gali pakenkti finansų sektoriaus subjektų finansiniam patikimumui;***

(13) finansų sektoriaus subjektai, mažindami IRT riziką, turėtų laikytis to paties požiūrio ir tų pačių principinių taisyklių***, atsižvelgdami į savo dydį, pobūdį, sudėtingumą ir rizikos profilį***. 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 pagrindinės kibernetinės higienos taip pat turėtų būti išvengta didelių ekonomikos išlaidų, nes IRT sutrikimų poveikis ir išlaidos sumažėtų iki minimumo;

(14) priimant reglamentą padedama mažinti reglamentavimo sudėtingumą, skatinama priežiūros konvergencija ir didinamas teisinis tikrumas, kartu prisidedant ir prie reikalavimų laikymosi išlaidų, visų pirma patiriamų finansų sektoriaus subjektų, kurie vykdo tarpvalstybinę veiklą, apribojimo ir konkurencijos iškraipymo mažinimo. Todėl

reglamentas dėl bendros finansų sektoriaus subjektų skaitmeninės veiklos atsparumo sistemos sukūrimo yra tinkamiausias būdas užtikrinti vienodą ir nuoseklų visų IRT rizikos valdymo komponentų taikymą Sąjungos finansų sektoriuose;

(14a) tačiau šio reglamento įgyvendinimas neturėtų trukdyti inovacijoms finansų sektoriaus subjektams sprendžiant skaitmeninės veiklos atsparumo klausimus, laikantis reglamento nuostatų, nei jų teikiamoms paslaugoms arba IRT paslaugas teikiančių trečiųjų šalių siūlomoms paslaugoms;

(15) be finansinių paslaugų teisės aktų, Europos Parlamento ir Tarybos direktyva (ES) 2016/1148[1] dabar yra bendra Sąjungos lygmens kibernetinio saugumo sistema. Septyniuose ypatingos svarbos sektoriuose ta direktyva taip pat taikoma trijų rūšių finansų sektoriaus subjektams, t. y. kredito įstaigoms, prekybos vietoms ir pagrindinėms sandorio šalims. Tačiau, kadangi Direktyvoje (ES) 2016/1148 nustatytas esminių paslaugų operatorių identifikavimo nacionaliniu lygmeniu mechanizmas, faktiškai tik tam tikros valstybių narių nustatytos kredito įstaigos, prekybos vietos ir pagrindinės sandorio šalys patenka į jos taikymo sritį ir dėl to turi laikytis joje nustatytų IRT saugumo ir pranešimo apie incidentus reikalavimų;

(16) kadangi šiuo reglamentu didinamas skaitmeninio atsparumo komponentų suderinimas nustatant reikalavimus, taikomus IRT rizikos valdymui ir pranešimui apie su IRT susijusius incidentus, kurie yra griežtesni nei nustatytieji galiojančiuose Sąjungos finansinių paslaugų teisės aktuose, juo taip pat didinamas suderinimas, palyginti su Direktyvoje (ES) 2016/1148 nustatytais reikalavimais. Todėl ***finansų sektoriaus subjektams*** šis reglamentas yra *lex specialis* Direktyvos (ES) 2016/1148 atžvilgiu.

Labai svarbu išlaikyti tvirtą finansų sektoriaus ir Sąjungos horizontaliosios kibernetinio saugumo sistemos sąryšį ***siekiant užtikrinti suderinamumą*** su valstybių narių jau priimtomis kibernetinio saugumo strategijomis ***ir informuoti*** finansų priežiūros ***institucijas*** apie kibernetinius incidentus, darančius poveikį kitiems sektoriams, kuriems taikoma Direktyva (ES) 2016/1148;

(17) siekiant sudaryti sąlygas tarpsektorinio mokymosi procesui ir veiksmingai pasinaudoti kitų sektorių patirtimi kovojant su kibernetinėmis grėsmėmis, Direktyvoje (ES) 2016/1148 nurodyti finansų sektoriaus subjektai turėtų likti tos direktyvos „ekosistemos“ (pvz., TIS bendradarbiavimo grupės ir reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT)) dalimi.

EPI ir nacionalinėms kompetentingoms institucijoms turėtų būti suteikta galimybė atitinkamai dalyvauti strateginėse politikos diskusijose ir TIS bendradarbiavimo grupės techniniame darbe, keistis informacija ir toliau bendradarbiauti su bendraisiais informaciniais centrais, paskirtais pagal Direktyvą (ES) 2016/1148. Pagal šį reglamentą ***bendra priežiūros įstaiga, atsakingoji priežiūros institucija ir*** kompetentingos institucijos taip pat turėtų konsultuotis ir bendradarbiauti su nacionalinėmis CSIRT, paskirtomis pagal Direktyvos (ES) 2016/1148 9 straipsnį***.***

Be to, šiuo reglamentu turėtų būti užtikrinta, kad pagal Direktyvą (ES) 2016/1148 įsteigtam CSIRT tinklui būtų teikiama išsami informacija apie didelius su IRT susijusius incidentus;

---

[1] 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).

(18) taip pat svarbu užtikrinti suderinamumą ***tiek*** su Europos ypatingos svarbos infrastruktūros objektų direktyva, kuri šiuo metu peržiūrima siekiant padidinti ypatingos svarbos infrastruktūros objektų apsaugą ir atsparumą su kibernetine veikla nesusijusioms grėsmėms, ***tiek su direktyva dėl ypatingos svarbos subjektų atsparumo***[1], o tai gali turėti įtakos finansų sektoriui;

(19) debesijos paslaugų teikėjai yra viena iš skaitmeninių paslaugų teikėjų kategorijų, kuriai taikoma Direktyva (ES) 2016/1148. Jiems taikoma *ex post* priežiūra, kurią vykdo pagal tą direktyvą paskirtos nacionalinės institucijos ir kuri apima tik tame akte nustatytų IRT saugumo ir pranešimo apie incidentus reikalavimų laikymąsi. Kadangi šiuo reglamentu nustatoma priežiūros sistema taikoma visoms ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, įskaitant debesijos paslaugų teikėjus, kai jie teikia IRT paslaugas finansų sektoriaus subjektams, ši sistema laikytina papildančia pagal Direktyvą (ES) 2016/1148 vykdomą priežiūrą***, o esminiai ir procedūriniai reikalavimai, taikomi ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims pagal šį reglamentą, turėtų būti nuoseklūs ir suderinami su tais, kurie taikomi pagal tą direktyvą***. Be to, šiuo reglamentu nustatoma priežiūros sistema turėtų būti taikoma debesijos paslaugų teikėjams, kai nėra Sąjungos horizontaliosios visiems sektoriams taikomos sistemos, pagal kurią būtų įkurta skaitmeninės priežiūros institucija;

(20) siekdami 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 pranešimo apie su IRT susijusius incidentus, IRT sistemų testavimo, kontrolės priemonių ir procesų, taip pat trečiosios šalies keliamos IRT rizikos ***ir IRT rizikos grupės viduje*** valdymo mechanizmus ir politiką. Reikėtų kelti finansų sistemos skaitmeninės veiklos atsparumo kartelę, kartu sudarant sąlygas proporcingai taikyti reikalavimus***, atsižvelgiant į jų pobūdį, mastą, sudėtingumą ir bendrą rizikos profilį***;

(21) nacionalinio lygmens pranešimo apie su IRT susijusius incidentus ribos ir taksonomijos gerokai skiriasi. Nors bendrus principus galima nustatyti Europos Sąjungos kibernetinio saugumo agentūrai (ENISA)[2] ir TIS bendradarbiavimo grupei atliekant atitinkamą darbą finansų sektoriaus subjektų, kuriems taikoma Direktyva (ES) 2016/1148, atžvilgiu, likusiems finansų sektoriaus subjektams vis dar taikomi arba gali atsirasti skirtingi ribų ir taksonomijų metodai. Vadinasi, finansų sektoriaus subjektams gali būti taikoma daugybė reikalavimų, ypač tais atvejais, kai jie vykdo veiklą keliose Sąjungos jurisdikcijose ir yra finansų grupės dalis. Be to, šie 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, nes tai yra itin svarbu mažinant IRT riziką didelio masto išpuolių, galinčių turėti sisteminių padarinių, atveju;

(21a) siekiant sumažinti administracinę naštą ir išvengti pranešimų teikimo reikalavimų sudėtingumo ir dubliavimosi mokėjimo paslaugų teikėjams, kuriems taikomas šis reglamentas, Direktyvoje (ES) 2015/2366 numatyti pranešimo apie incidentus

---

1 2008 m. gruodžio 8 d. Tarybos direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo (OL L 345, 2008 12 23, p. 75).

2 ENISA orientacinė incidentų klasifikavimo taksonomija, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

reikalavimai nebeturėtų būti taikomi. Kredito įstaigos, elektroninių pinigų įstaigos ir mokėjimo įstaigos pagal šį reglamentą turėtų pranešti apie visus veiklos ar su mokėjimais susijusius ir su jais nesusijusius saugumo incidentus, apie kuriuos anksčiau buvo pranešama pagal Direktyvą (ES) 2015/2366, neatsižvelgiant į tai, ar incidentai yra susiję su IRT, ar ne;

(22) siekiant, kad kompetentingos institucijos galėtų vykdyti savo priežiūros funkcijas, galėdamos susidaryti visapusišką su IRT susijusių incidentų pobūdžio, dažnumo, svarbos ir poveikio vaizdą, ir tobulinti atitinkamų valdžios institucijų, įskaitant teisėsaugos institucijas ir pertvarkymo institucijas, keitimąsi informacija, būtina nustatyti taisykles, kuriomis ***būtų sukurta patikima*** pranešimo apie su IRT susijusius incidentus tvarka***, apimanti reikalavimus, padedančius šalinti spragas sektoriniuose finansinių paslaugų teisės aktuose, ir panaikinti*** visus dabar iš dalies sutampančius ir pasikartojančius reikalavimus, kad būtų sumažintos išlaidos. Todėl labai svarbu suderinti pranešimo apie su IRT susijusius incidentus tvarką reikalaujant, kad visi finansų sektoriaus subjektai pranešimus teiktų ▌ savo kompetentingoms institucijoms***, naudodamiesi viena bendra supaprastinta sistema, nustatyta šiame reglamente***. Be to, EPI turėtų būti suteikti įgaliojimai patikslinti pranešimo apie su IRT susijusius incidentus elementus, pavyzdžiui, taksonomiją, terminus, duomenų rinkinius, šablonus ir taikomas ribas;

(23) kai kuriuose finansų pasektoriuose buvo parengti skaitmeninės veiklos atsparumo testavimo reikalavimai, įtraukti į kelias ***ir kartais*** nekoordinuojamas nacionalines sistemas, tas pačias problemas sprendžiant skirtingai. Dėl to tarpvalstybiniai finansų sektoriaus subjektai patiria dvigubų išlaidų ***ir tai gali trukdyti abipusiam*** rezultatų ***pripažinimui***. Todėl dėl nekoordinuojamo testavimo gali būti skaidoma bendroji rinka;

(24) be to, tais atvejais, kai testavimas neprivalomas, pažeidžiamumo atvejai neaptinkami, todėl kyla didesnė rizika finansų sektoriaus subjektui ir galiausiai finansų sektoriaus stabilumui ir vientisumui. Be Sąjungos intervencijos skaitmeninės veiklos atsparumo testavimas toliau būtų fragmentiškas, o abipusis testavimo rezultatų pripažinimas skirtingose jurisdikcijose nevyktų. Be to, kadangi mažai tikėtina, kad kiti finansų pasektoriai galėtų priimti tokias schemas reikšmingu mastu, jie nepasinaudotų galimais privalumais, pavyzdžiui, nenustatytų pažeidžiamumo atvejų ir rizikos, netestuotų apsaugos pajėgumų ir veiklos tęstinumo ir neįgytų didesnio klientų, tiekėjų ir verslo partnerių pasitikėjimo. Siekiant pašalinti tokį reikalavimų dalinį sutapimą, skirtumus ir spragas, būtina nustatyti taisykles, kuriomis būtų siekiama, kad finansų sektoriaus subjektai ir kompetentingos institucijos koordinuotų testavimą, taip sudarant palankesnes sąlygas reikšmingų finansų sektoriaus subjektų pažangaus testavimo rezultatų tarpusavio pripažinimui;

(25) finansų sektoriaus subjektų priklausomybę nuo IRT paslaugų iš dalies lemia jų poreikis prisitaikyti prie besiformuojančios konkurencingos skaitmeninės pasaulinės ekonomikos, didinti savo veiklos efektyvumą ir tenkinti vartotojų paklausą. Pastaraisiais metais tokios priklausomybės pobūdis ir mastas nuolat kinta, todėl mažėja finansinio tarpininkavimo sąnaudos, sudaromos sąlygos verslo plėtrai ir finansinės veiklos įgyvendinimo didinimui, kartu siūlant įvairias IRT priemones sudėtingiems vidaus procesams valdyti;

(26) tokį intensyvų IRT paslaugų naudojimą liudija sudėtingi sutartimi įforminti susitarimai, kurių laikydamiesi 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, kai pastarosios yra įtvirtintos susitarimuose. Daugelyje tokių sutarčių taip pat nenumatoma pakankamų apsaugos priemonių, leidžiančių vykdyti visapusišką subrangos procesų stebėseną, todėl finansų sektoriaus subjektas praranda galimybę įvertinti šią susijusią riziką. Be to, kadangi IRT paslaugas teikiančios trečiosios šalys dažnai teikia standartines paslaugas skirtingų rūšių klientams, tokios sutartys ne visada gali būti tinkamai pritaikytos prie individualių ar konkrečių finansų sektoriaus dalyvių poreikių;

(27) nepaisant kai kurių bendrų veiklos rangai taikomų taisyklių, nustatytų kai kuriuose Sąjungos finansinių paslaugų teisės aktuose, 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 išorėje kylančios IRT rizikos problema. Todėl būtina nustatyti tam tikrus pagrindinius principus, kuriais finansų sektoriaus subjektai vadovautųsi valdydami trečiosios šalies keliamą IRT riziką, kartu su pagrindinėmis sutartinėmis teisėmis, susijusiomis su keliais sutarčių vykdymo ir nutraukimo elementais, siekiant įtvirtinti tam tikras minimalias apsaugos priemones, užtikrinančias finansų sektoriaus subjektų gebėjimą veiksmingai stebėti visą riziką, kylančią IRT paslaugas teikiančių trečiųjų šalių lygmeniu;

(28) trečiosios šalies keliamos IRT rizikos ir priklausomybės nuo IRT paslaugas teikiančių trečiųjų šalių atžvilgiu trūksta suderinimo ir konvergencijos. Nepaisant tam tikrų pastangų konkrečioje veiklos rangos srityje, pavyzdžiui, 2017 m. rekomendacijų dėl veiklos perdavimo debesijos paslaugų teikėjams[1], sisteminės rizikos, kuri gali kilti dėl to, kad finansų sektorių aptarnauja ribotas ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių skaičius, klausimas Sąjungos teisės aktuose beveik nesprendžiamas. Šį trūkumą Sąjungos lygmeniu dar labiau padidina tai, kad nėra konkrečių įgaliojimų ir priemonių, leidžiančių nacionalinėms priežiūros institucijoms gerai suprasti priklausomybę nuo IRT paslaugas teikiančių trečiųjų šalių ir tinkamai stebėti riziką, kylančią dėl tokios priklausomybės nuo IRT paslaugas teikiančių trečiųjų šalių koncentracijos;

(29) 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 leistų finansų priežiūros institucijoms kiekybiškai ir kokybiškai įvertinti bei ištaisyti IRT rizikos, su kuria susiduria ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys, padarinius, būtina sukurti tinkamą Sąjungos priežiūros sistemą, sudarančią sąlygas nuolat stebėti IRT paslaugas teikiančių trečiųjų šalių, kurios ***teikia*** ypatingai ***svarbias paslaugas*** finansų sektoriaus ***subjektams***, veiklą. ***Kadangi IRT paslaugų teikimas grupės viduje nekelia tokios pačios rizikos, IRT paslaugų teikėjai, priklausantys tai pačiai grupei ar institucinei apsaugos sistemai, neturėtų būti apibrėžiami kaip ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys;***

(30) kadangi IRT grėsmės tampa vis painesnės ir sudėtingesnės, geros 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, o tai savo ruožtu stiprina

[1] Rekomendacijos dėl veiklos perdavimo debesijos paslaugų teikėjams (EBA/REC/2017/03), panaikintos EBI veiklos rangos gairėmis (EBA/GL/2019/02).

finansų sektoriaus subjektų gebėjimą neleisti grėsmėms virsti realiais incidentais ir sudaro sąlygas finansų sektoriaus subjektams geriau suvaldyti su IRT susijusių incidentų poveikį ir veiksmingiau atkurti veiklą. Nesant rekomendacijų Sąjungos lygmeniu, regis, keli veiksniai trukdo dalytis žvalgybos informacija, visų pirma neaiškumas dėl atitikties duomenų apsaugos, antimonopolinėms ir atsakomybės taisyklėms***. Todėl svarbu stiprinti finansų sektoriaus subjektų ir kompetentingų institucijų bendradarbiavimo ir pranešimų teikimo tvarką, taip pat keitimąsi informacija su visuomene, siekiant sukurti atvirą dalijimosi žvalgybos informacija sistemą ir taikyti „pritaikytojo saugumo užtikrinimo“ principą, kurie yra būtini siekiant padidinti finansų sektoriaus veiklos atsparumą ir pasirengimą atremti IRT riziką. Keitimosi informacija susitarimuose visada turėtų būti tinkamai atsižvelgiama į galimą riziką kibernetinio saugumo, duomenų apsaugos ar komercinio konfidencialumo srityse;***

(31) be to, dėl dvejonių, kuria informacija galima dalytis su kitais rinkos dalyviais arba ne priežiūros institucijomis (pavyzdžiui, analitiniais duomenimis su ENISA arba teisėsaugos tikslais su Europolu), gali būti neteikiama naudinga informacija. Dalijimosi informacija mastas ir kokybė tebėra riboti, fragmentiški, o atitinkama informacija daugiausia keičiamasi vietos lygmeniu (vykdant nacionalines iniciatyvas) netaikant nuoseklių Sąjungos masto dalijimosi informacija schemų, pritaikytų integruoto finansų sektoriaus poreikiams. ***Todėl svarbu stiprinti tuos ryšių kanalus ir, kai būtina ir aktualu, užtikrinti, kad ne priežiūros institucijos per visą priežiūros ciklą teiktų informaciją;***

(32) ▌ finansų sektoriaus subjektai ***taip pat*** turėtų būti skatinami kolektyviai naudotis savo individualiomis žiniomis ir praktine patirtimi strateginiu, taktiniu ir veiklos lygmenimis, kad sustiprintų savo gebėjimus tinkamai įvertinti, stebėti, reaguoti į kibernetines grėsmes ir apsisaugoti nuo jų. Taigi būtina sudaryti sąlygas, kad Sąjungos lygmeniu būtų rengiamos savanoriško dalijimosi informacija schemos, kurias taikant patikimoje aplinkoje būtų padedama finansų bendruomenei užkirsti kelią grėsmėms ir kolektyviai į jas reaguoti, greitai apribojant IRT rizikos plitimą ir neleidžiant neigiamam poveikiui plisti finansiniais kanalais. Tokie mechanizmai turėtų būti įgyvendinami visiškai laikantis galiojančių Sąjungos konkurencijos teisės taisyklių[1] ir tokiu būdu, kad būtų visiškai laikomasi Sąjungos duomenų apsaugos taisyklių, iš esmės Europos Parlamento ir Tarybos reglamento (ES) 2016/679[2], visų pirma tvarkant asmens duomenis duomenų valdytojo arba trečiosios šalies teisėto intereso pagrindu, kaip nurodyta to reglamento 6 straipsnio 1 dalies f punkte;

(33) nepaisant šiame reglamente numatytos plačios taikymo srities, skaitmeninės veiklos atsparumo taisyklės***, įskaitant rizikos valdymo sistemos reikalavimus,*** turėtų būti taikomos atsižvelgiant į didelius finansų sektoriaus subjektų dydžio, ▌pobūdžio, ***sudėtingumo ir*** 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, ***pobūdį,***

---

1 Komisijos komunikatas „Sutarties dėl Europos Sąjungos veikimo 101 straipsnio taikymo horizontaliesiems bendradarbiavimo susitarimams gairės“ (2011/C 11/01).

2 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).

sudėtingumą*,** veiklos pobūdį ***ir susijusį rizikos profilį, o kompetentingos institucijos turėtų toliau vertinti ir peržiūrėti tokio paskirstymo metodą;

(34) kadangi didesni finansų sektoriaus subjektai gali turėti daugiau išteklių ir galėtų 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 pagal šį reglamentą nėra labai mažos įmonės. Tokie subjektai yra geriau pasirengę nustatyti specialias valdymo funkcijas, skirtas susitarimams su IRT paslaugas teikiančiomis trečiosiomis šalimis prižiūrėti arba krizių valdymo klausimams spręsti, organizuoti IRT rizikos valdymą pagal trijų gynybos linijų modelį arba priimti žmogiškųjų išteklių dokumentą, kuriame būtų visapusiškai paaiškinta prieigos teisių politika.

Be to, tik tokie finansų sektoriaus subjektai turėtų būti raginami atlikti išsamų vertinimą po svarbių tinklų ir informacinių sistemų infrastruktūrų bei procesų pakeitimų, reguliariai atlikti senųjų IRT sistemų rizikos analizę arba išplėsti veiklos tęstinumo ir reagavimo bei veiklos atkūrimo planų testavimą, kad galėtų nustatyti pirminės IRT infrastruktūros pakeitimo atsarginiais įrenginiais scenarijus;

(35) be to, kadangi turėtų būti reikalaujama, kad grėsmėmis grindžiamą skverbimosi testavimą atliktų tik tie finansų sektoriaus subjektai, kurie laikomi reikšmingais atliekant pažangų skaitmeninio atsparumo testavimą, tokiam testavimui atlikti reikalingi administraciniai procesai ir finansinės išlaidos turėtų tekti nedidelei finansų sektoriaus subjektų daliai. Galiausiai, siekiant sumažinti reglamentavimo naštą, tik finansų sektoriaus subjektų, kurie nėra labai mažos įmonės, turėtų būti prašoma reguliariai pranešti kompetentingoms institucijoms apie ***visas apskaičiuotas*** išlaidas ir nuostolius, patirtus dėl ***didelių*** IRT sutrikimų***, reikšmingų su IRT susijusių incidentų***, ir po ***tokių*** didelių IRT sutrikimų atliekamų patikrinimų rezultatus;

(36) siekiant užtikrinti visišką finansų sektoriaus subjektų veiklos strategijų ir atliekamo IRT rizikos valdymo suderinimą ir bendrą nuoseklumą, turėtų būti reikalaujama, kad valdymo organui tektų pagrindinis ir aktyvus vaidmuo valdant ir pritaikant IRT rizikos valdymo sistemą ir bendrą skaitmeninio atsparumo strategiją. Požiūris, kurio turi laikytis valdymo organas, 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;

(37) be to, visa valdymo organo atskaitomybė neatsiejama nuo pareigos užtikrinti tokį finansų sektoriaus subjekto investicijų į IRT ir bendro IRT biudžeto mastą, kuris leistų pasiekti pradinį skaitmeninės veiklos atsparumo lygį;

(38) šiuo reglamentu, paremtu atitinkamais kibernetinės rizikos valdymo tarptautiniais, nacionaliniais ir sektoriaus standartais, gairėmis, rekomendacijomis ar metodais[1],

[1] CPMI-IOSCO „Rekomendacijos dėl finansų rinkos infrastruktūrų kibernetinio atsparumo“ (angl. *Guidance on cyber resilience for financial market infrastructures*), https://www.bis.org/cpmi/publ/d146.pdf G 7 „Pagrindiniai finansų sektoriaus

skatinama naudoti funkcijų, padėsiančių sukurti bendrą IRT rizikos valdymo struktūrą, rinkinį. Jei pagrindiniai pajėgumai, kuriuos įdiegia finansų sektoriaus subjektai, atitinka šiame reglamente nustatytų funkcijų (identifikavimo, apsaugos ir prevencijos, aptikimo, reagavimo ir veiklos atkūrimo, mokymosi ir tobulėjimo bei komunikacijos) paskirties poreikius, finansų sektoriaus subjektai gali naudoti kitokios struktūros ar kategorijos IRT rizikos valdymo modelius;

(39) kad neatsiliktų nuo kintančios kibernetinių grėsmių aplinkos, finansų sektoriaus subjektai turėtų turėti atnaujinamas IRT sistemas, kurios yra patikimos ir pakankamai pajėgios ne tik užtikrinti duomenų tvarkymą, kiek tai būtina jų paslaugoms teikti, bet ir užtikrinti technologinį atsparumą, kad finansų sektoriaus subjektai galėtų tinkamai tenkinti papildomus tvarkymo poreikius, kurių gali atsirasti nepalankiausiomis rinkos sąlygomis arba kitomis nepalankiomis aplinkybėmis. Nors šiuo reglamentu nėra standartizuojamos konkrečios IRT sistemos, priemonės ar technologijos, jis grindžiamas tinkamu finansų sektoriaus subjektų Europos ir tarptautiniu mastu pripažintų techninių standartų (pvz., ISO) arba geriausios sektoriaus praktikos taikymu, jei toks taikymas visiškai atitinka konkrečius priežiūros nurodymus dėl tarptautinių standartų naudojimo ir įtraukimo;

(40) 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, ***atsižvelgiant į tai, ar funkcija yra ypatingos svarbos, ar svarbi,*** reikalingi veiksmingi veiklos tęstinumo ir veiklos atkūrimo planai. Tačiau, nors atsarginėse sistemose duomenys turėtų būti pradedami tvarkyti nepagrįstai nedelsiant, tokia pradžia neturėtų kelti jokio pavojaus tinklų ir informacinių sistemų vientisumui ir saugumui arba duomenų konfidencialumui;

(41) nors šiuo reglamentu finansų sektoriaus subjektams leidžiama lanksčiai nustatyti veiklos atkūrimo laiko tikslus ir tokiu būdu tokius tikslus nustatyti visapusiškai atsižvelgiant į atitinkamos funkcijos pobūdį ir ypatingą svarbą bei konkrečius verslo poreikius, nustatant tokius tikslus taip pat turėtų būti reikalaujama atlikti galimo bendro poveikio rinkos veiksmingumui vertinimą;

(42) didelis kibernetinių išpuolių poveikis sustiprėja finansų sektoriuje – srityje, kuriai būdinga gerokai didesnė rizika, kad ja bandys pasinaudoti piktavališki subjektai, siekiantys gauti finansinės naudos tiesiogiai iš šaltinio. Siekiant sumažinti tokią riziką ir neleisti, kad IRT sistemos prarastų vientisumą arba taptų neprieinamos ir būtų pažeistas konfidencialių duomenų saugumas arba padaryta žala fizinei IRT infrastruktūrai, reikėtų gerokai patobulinti finansų sektoriaus subjektų pranešimo apie didelius su IRT susijusius incidentus tvarką.

Visiems finansų sektoriaus subjektams turėtų būti taikoma suderinta pranešimo apie su IRT susijusius incidentus tvarka, pagal kurią jie būtų įpareigoti teikti pranešimus tik savo kompetentingoms institucijoms. Nors šis reikalavimas pranešti būtų taikomas

---

kibernetinio saugumo elementai“ (angl. *Fundamental Elements of Cybersecurity for the Financial Sector*), https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; NIST „Kibernetinio saugumo sistema“ (angl. *Cybersecurity Framework*), https://www.nist.gov/cyberframework; FST „Reagavimo į kibernetinius incidentus ir veiklos atkūrimo priemonių rinkinys“ (angl. *CIRR toolkit*),https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document

visiems finansų sektoriaus subjektams, ne visiems jiems turėtų būti daromas vienodas poveikis, nes atitinkamos reikšmingumo ribos ir terminai turėtų būti nustatomi taip, kad būtų fiksuojami tik dideli su IRT susiję incidentai. Tiesioginis pranešimų teikimas suteiktų galimybę finansų priežiūros institucijoms susipažinti su informacija apie su IRT susijusius incidentus. Vis dėlto finansų priežiūros institucijos turėtų šią informaciją perduoti ne finansų valdžios institucijoms (TIS kompetentingoms institucijoms, nacionalinėms duomenų apsaugos institucijoms ir teisėsaugos institucijoms, kai incidentai yra nusikalstamo pobūdžio). Su IRT susijusi informacija apie incidentus turėtų būti perduodama abipusiai: finansų priežiūros institucijos turėtų pateikti visą būtiną grįžtamąją informaciją arba rekomendacijas finansų sektoriaus subjektui, o EPI turėtų dalytis su įvykiu susijusiais anoniminiais duomenimis apie grėsmes ir pažeidžiamumo atvejus, siekdamos prisidėti prie platesnio masto kolektyvinės gynybos;

(43) reikėtų papildomai apsvarstyti galimybę centralizuoti pranešimų apie su IRT susijusius incidentus teikimą vienam pagrindiniam ***pranešimų apie didelius su IRT susijusius incidentus*** ES centrui, kuris arba gautų atitinkamus pranešimus tiesiogiai ir automatiškai informuotų nacionalines kompetentingas institucijas, arba tiesiog atliktų nacionalinių kompetentingų institucijų perduodamų pranešimų centralizavimo ir koordinavimo vaidmenį. Turėtų būti reikalaujama, kad EPI, konsultuodamosi su ECB ir ENISA, iki tam tikros datos parengtų bendrą ataskaitą, kurioje išnagrinėtų galimybę įsteigti tokį pagrindinį ES centrą;

(44) siekiant užtikrinti patikimą skaitmeninės veiklos atsparumą ir laikantis tarptautinių standartų (pvz., G 7 pagrindinių grėsmėmis grindžiamo skverbimosi testavimo elementų), finansų sektoriaus subjektai***, kurie nėra labai mažos įmonės,*** turėtų reguliariai testuoti savo IRT sistemų ir darbuotojų prevencinių, aptikimo, reagavimo ir veiklos atkūrimo pajėgumų veiksmingumą, kad atskleistų ir pašalintų galimus IRT pažeidžiamumo atvejus. Siekiant suvienodinti skirtingą finansų sektoriaus subjektų kibernetinio saugumo parengtį pačiuose finansų pasektoriuose 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 patikrinimais, klausimynais ir skenavimo programinės įrangos sprendimais, pirminio kodo patikrinimais, kai įmanoma; scenarijais grindžiamais testais, suderinamumo testavimu, veiklos efektyvumo testavimu ar ištisinio srauto (angl. *end-to-end*) testavimu) ir baigiant pažangesniu testavimu (pvz., TLPT testavimu, kurį turėtų atlikti pakankamos IRT brandos finansų sektoriaus subjektai). Taigi reikšmingiems finansų sektoriaus subjektams (pavyzdžiui, didelėms kredito įstaigoms, vertybinių popierių biržoms, centriniams vertybinių popierių depozitoriumams, pagrindinėms sandorio šalims ir pan.) turėtų būti taikomi griežtesni skaitmeninės veiklos atsparumo testavimo reikalavimai. Kartu skaitmeninės veiklos atsparumo testavimas taip pat turėtų būti aktualesnis kai kuriems pasektoriams, kurie atlieka esminį sisteminį vaidmenį (pvz., mokėjimų, bankininkystės, tarpuskaitos ir atsiskaitymo), ir mažiau aktualus kitiems pasektoriams (pvz., turto valdytojams, kredito reitingų agentūroms ir pan.). Tarpvalstybiniai finansų sektoriaus subjektai, kurie naudojasi įsisteigimo laisve arba paslaugų teikimo laisve Sąjungoje, turėtų laikytis vieno pažangaus testavimo reikalavimų rinkinio (pvz., TLPT testavimo) savo buveinės valstybėje narėje ir toks testavimas turėtų apimti IRT infrastruktūras visose jurisdikcijose, kuriose tarpvalstybinė grupė vykdo veiklą Sąjungoje, taip sudarant sąlygas tarpvalstybinėms grupėms patirti testavimo išlaidas tik vienoje jurisdikcijoje***. Be to, kad būtų sustiprintas***

bendradarbiavimas finansų sektoriaus subjektų atsparumo srityje su patikimomis trečiosiomis šalimis, Komisija ir kompetentingos institucijos turėtų stengtis sukurti grėsmėmis grindžiamo skverbimosi testavimo rezultatų tarpusavio pripažinimo sistemą.

Valstybės narės turėtų paskirti vieną valdžios instituciją, kuri nacionaliniu lygmeniu būtų atsakinga už grėsmėmis grindžiamą skverbimosi testavimą finansų sektoriuje. Tokia valdžios institucija, be kita ko, galėtų būti nacionalinė kompetentinga institucija arba valdžios institucija, paskirta pagal Direktyvos (ES) 2016/1148 (TIS) 8 straipsnį. Ši valdžios institucija būtų atsakinga už liudijimų, kad grėsmėmis grindžiamas skverbimosi testavimas buvo vykdomas laikantis reikalavimų, išdavimą. Tokie liudijimai sudarytų palankesnes sąlygas kompetentingų institucijų testavimo rezultatų tarpusavio pripažinimui.

Kai kurie finansų sektoriaus subjektai yra pajėgūs atlikti pažangų testavimą viduje, o kiti sudarys sutartis su Sąjungos arba trečiosios šalies išorės testuotojais. Dėl to svarbu, kad visiems testuotojams būtų taikomi tokie patys aiškūs reikalavimai. Kad būtų galima užtikrinti vidaus testuotojų nepriklausomumą, kompetentinga institucija turėtų suteikti leidimą naudotis jų paslaugomis.

Neturėtų būti nustatyta privaloma grėsmėmis grindžiamo skverbimosi testavimo metodika, tačiau turėtų būti laikoma, kad esamos TIBER-EU sistemos naudojimas atitinka šiame reglamente nustatytus grėsmėmis grindžiamo skverbimosi testavimo reikalavimus.

Iki šio reglamento įsigaliojimo ir kol įgaliotos EPI parengs ir priims grėsmėmis grindžiamo skverbimosi testavimo techninius reguliavimo standartus, finansų sektoriaus subjektai turėtų vadovautis tomis atitinkamomis Sąjungos gairėmis ir sistemomis, kurios taikomos žvalgybos informacija grindžiamiems skverbimosi testams, nes įsigaliojus šiam reglamentui jos bus taikomos ir toliau;

(44a) visa atsakomybė už grėsmėmis grindžiamo skverbimosi testavimo vykdymą (ir kibernetinio saugumo valdymą bei kibernetinių išpuolių prevenciją apskritai) turėtų tekti finansų sektoriaus subjektui, o valdžios institucijų liudijimai turėtų būti teikiami tik abipusio pripažinimo tikslu ir neturėtų trukdyti imtis tolesnių veiksmų, susijusių su IRT rizikos, kuri kyla finansų sektoriaus subjektui, lygiu, taip pat neturėtų būti laikomi jo IRT rizikos valdymo ir mažinimo pajėgumų patvirtinimu;

(45) siekiant užtikrinti patikimą trečiosios šalies keliamos IRT rizikos stebėseną, būtina nustatyti rinkinį principinių taisyklių, pagal kurias finansų sektoriaus subjektai galėtų stebėti riziką, kylančią dėl funkcijų, kurių vykdymas perduotas IRT paslaugas teikiančioms trečiosioms šalims, ***visų pirma kai tai susiję su ypatingos svarbos ar svarbių funkcijų teikimu trečiosios šalies IRT paslaugų teikėjams,*** ir apskritai dėl priklausomybės nuo IRT paslaugas teikiančių trečiųjų šalių;

(46) finansų sektoriaus subjektas visada turėtų būti visiškai atsakingas už šiame reglamente nustatytų pareigų vykdymą. Proporcinga rizikos, kylančios IRT paslaugas teikiančios trečiosios šalies lygmeniu, stebėsena turėtų būti organizuojama tinkamai atsižvelgiant į su IRT susijusios priklausomybės ***pobūdį,*** mastą, sudėtingumą ir svarbą, paslaugų, procesų ar funkcijų, kurioms taikomi sutartimi įforminti susitarimai, ypatingą svarbą ar svarbą ir galiausiai atidžiai įvertinus galimą poveikį finansinių paslaugų tęstinumui ir kokybei atitinkamai individualiu ir grupės lygmeniu***, taip pat atsižvelgiant į tai, ar IRT paslaugos teikiamos grupės viduje, ar jas teikia trečioji šalis***;

(47) vykdant tokią stebėseną turėtų būti laikomasi strateginio požiūrio į trečiosios šalies keliamą IRT riziką, įforminto finansų sektoriaus subjekto valdymo organui priėmus specialią strategiją, grindžiamą nuolatine atrankine visos tokios 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 šiuo reglamentu nustatytos priežiūros sistemos, finansų priežiūros institucijos turėtų reguliariai gauti esminę informaciją iš registrų ir galėti prašyti jų išrašų *ad hoc* pagrindu;

(48) sutartimi įforminti susitarimai turėtų būti oficialiai sudaromi tik atlikus išsamią ikisutartinę analizę, o ***korekcinių ir taisomųjų priemonių, kurios gali apimti visišką arba dalinį*** sutarčių nutraukimą***, turėtų būti imtasi tuo atveju, kai yra*** bent kelios aplinkybės, iš kurių būtų matyti ***dideli*** IRT paslaugas teikiančios trečiosios šalies trūkumai;

(49) siekiant spręsti IRT paslaugas teikiančių trečiųjų šalių koncentracijos rizikos sisteminio poveikio problemą, reikėtų skatinti subalansuotą sprendimą, laikantis lankstaus ir laipsniško požiūrio, nes griežtos viršutinės ribos arba griežti apribojimai galėtų trukdyti verslo etikai ir laisvei sudaryti sutartis. Finansų sektoriaus subjektai turėtų nuodugniai įvertinti sutartimi įformintus susitarimus, kad nustatytų tokios rizikos atsiradimo tikimybę, be kita ko**,** atlikdami išsamią susitarimų dėl veiklos subrangos analizę ▌. Šiame etape ir siekiant užtikrinti tinkamą pusiausvyrą tarp būtinybės išsaugoti laisvę sudaryti sutartis ir užtikrinti finansinį stabilumą, manoma, kad nustatyti griežtas IRT paslaugas teikiančių trečiųjų šalių rizikos pozicijų viršutines ribas ir apribojimus yra netikslinga. ***Bendra priežiūros institucija, vykdanti*** kiekvienos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies priežiūrą***, ir kasdienę priežiūrą vykdyti paskirta EPI*** (toliau – atsakingoji priežiūros institucija), ***vykdydamos*** priežiūros užduotis turėtų skirti ypatingą dėmesį tam, kad visapusiškai perprastų tarpusavio priklausomybės mastą ir nustatytų konkrečius atvejus, kai didelė ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių koncentracija Sąjungoje gali keli grėsmę Sąjungos finansų sistemos stabilumui ir vientisumui, ir turėtų numatyti dialogą su ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis, kai tokia rizika identifikuojama[1];

(50) siekiant, kad būtų galima reguliariai vertinti ir stebėti IRT paslaugas teikiančios trečiosios šalies gebėjimą saugiai teikti paslaugas finansų sektoriaus subjektui nedarant neigiamo poveikio pastarojo atsparumui, turėtų būti suderinti pagrindiniai sutarčių su IRT paslaugas teikiančiomis trečiosiomis šalimis įgyvendinimo elementai. Tie elementai apima tik minimalius sutartinius aspektus, kurie laikomi ypač svarbiais sudarant sąlygas finansų sektoriaus subjektui vykdyti visapusišką stebėseną, siekiant užtikrinti jo skaitmeninį atsparumą, kurį lemia IRT paslaugos stabilumas ir saugumas;

(51) sutartimi įformintuose susitarimuose visų pirma turėtų būti nurodyti išsamūs funkcijų ir paslaugų, vietų, kuriose vykdomos tokios funkcijos ir kuriuose tvarkomi duomenys, aprašymai, taip pat nurodomi išsamūs paslaugų lygio aprašymai kartu su kiekybiniais ir kokybiniais sutarto paslaugų lygio tiksliniais veiklos rezultatų rodikliais, kad finansų sektoriaus subjektas galėtų vykdyti veiksmingą stebėseną. Be to, esminiais finansų sektoriaus subjekto gebėjimo užtikrinti trečiosios šalies rizikos stebėseną elementais

[1] Be to, jei kiltų IRT paslaugas teikiančios trečiosios šalies, kuri laikoma dominuojančia, piktnaudžiavimo rizika, finansų sektoriaus subjektams taip pat turėtų būti suteikiama galimybė pateikti oficialų arba neoficialų skundą Europos Komisijai arba nacionalinėms konkurencijos tarnyboms.

taip pat turėtų būti laikomos nuostatos dėl asmens duomenų pasiekiamumo, prieinamumo, vientisumo, saugumo ir apsaugos, taip pat prieigos, veiklos atkūrimo ir grąžinimo garantijos IRT paslaugas teikiančios trečiosios šalies nemokumo, pertvarkymo ar veiklos nutraukimo ***arba sutartimi įformintų susitarimų nutraukimo*** atveju;

(52) siekiant užtikrinti, kad finansų sektoriaus subjektai ir toliau visiškai kontroliuotų visus pokyčius, kurie gali pakenkti jų IRT saugumui, turėtų būti nustatyti IRT paslaugas teikiančios trečiosios šalies įspėjimo terminai ir pareigos pranešti, taikomi įvykus pokyčiams, kurie gali turėti reikšmingos įtakos IRT paslaugas teikiančios trečiosios šalies gebėjimui veiksmingai atlikti ypatingos svarbos ar svarbias funkcijas, įskaitant pastarosios pareigą be papildomo mokesčio arba už iš anksto nustatyto dydžio mokestį teikti pagalbą įvykus su IRT susijusiam incidentui***, kuris yra svarbus paslaugoms, kurias užtikrindama sutartą paslaugų lygį teikia IRT paslaugas teikianti trečioji šalis finansų sektoriaus įstaigai***. ***Šis reglamentas netaikomas papildomoms IRT paslaugoms, nuo kurių finansų sektoriaus subjektai nėra priklausomi veiklos požiūriu.***

Be to, pagal šį reglamentą terminas „ypatingos svarbos arba svarbi funkcija“ taip pat turėtų apimti ypatingos svarbos funkcijas, apibrėžtas 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyvos 2014/59/ES[1] ***2 straipsnio 1 dalies 35 punkte. Atitinkamai funkcijos, kurios pagal Direktyvą (ES) 2014/59 apibrėžiamos kaip ypatingos svarbos funkcijos, turėtų ir pagal šį reglamentą būti apibrėžiamos kaip ypatingos svarbos ar svarbios funkcijos;***

(53) ***sutartimi įformintų susitarimų dėl ypatingos svarbos arba svarbių funkcijų atveju*** finansų sektoriaus subjekto arba paskirtos trečiosios šalies prieigos, patikrinimo ir audito teisės yra ypač svarbios finansų sektoriaus subjektų nuolatinės IRT paslaugas teikiančios trečiosios šalies veiklos efektyvumo stebėsenos priemonės, kurios derinamos su visapusišku pastarosios bendradarbiavimu atliekant patikrinimus. Taip pat ir ***bendra priežiūros įstaiga bei*** finansų sektoriaus subjekto ***atsakingoji priežiūros*** institucija turėtų turėti teisę, ***pateikusios*** įspėjimą ir ***laikydamosi*** konfidencialumo principo, patikrinti ir audituoti IRT paslaugas teikiančią trečiąją šalį***, sykiu imdamosi atsargumo priemonių, kad tikrinimas nesutrikdytų paslaugų, kurias ta IRT paslaugas teikianti trečioji šalis teikia kitiems klientams***. ***Tas finansų sektoriaus subjektas ir IRT paslaugas teikianti trečioji šalis turėtų galėti susitarti, kad prieigos, patikrinimo ir audito teisės gali būti perduotos nepriklausomai trečiajai šaliai;***

(54) sutartimi įformintuose susitarimuose turėtų būti numatytos aiškios sutarties nutraukimo teisės ir susiję minimalūs įspėjimo terminai, taip pat specialios pasitraukimo strategijos, pagal kurias visų pirma būtų galima nustatyti privalomus pereinamuosius laikotarpius, per kuriuos IRT paslaugas teikiančios trečiosios šalys turėtų toliau vykdyti atitinkamas funkcijas, kad sumažintų sutrikimų riziką finansų sektoriaus subjekto lygmeniu ar leistų

---

[1] ***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).***

pastarajam veiksmingai pakeisti IRT paslaugas teikiančias trečiąsias šalis arba pasinaudoti ***vidaus*** sprendimais, atitinkančiais teikiamos paslaugos sudėtingumą. ***Be to, kredito įstaigos turėtų užtikrinti, kad atitinkamos IRT sutartys būtų patikimos ir visapusiškai įgyvendinamos kredito įstaigos pertvarkymo atveju. Atsižvelgdamos į pertvarkymo institucijų lūkesčius, kredito įstaigos turėtų užtikrinti, kad atitinkamos IRT paslaugų sutartys būtų atsparios pertvarkymui. Tol, kol ypatingos svarbos ar svarbios IRT funkcijos tebevykdomos, tie finansų sektoriaus subjektai turėtų užtikrinti, kad sutartyse, be kitų reikalavimų, būtų numatytos draudimo nutraukti, sustabdyti arba pakeisti sutartį dėl restruktūrizavimo ar pertvarkymo sąlygos;***

(55) be to, savanoriškas Komisijos parengtų standartinių sutarčių sąlygų naudojimas debesijos paslaugoms gali suteikti daugiau pasitikėjimo finansų sektoriaus subjektams ir jiems IRT paslaugas teikiančioms trečiosioms šalims, nes būtų suteikta daugiau teisinio tikrumo dėl finansų sektoriuje naudojamų debesijos paslaugų, visiškai jas suderinant su finansinių paslaugų teisės aktais nustatytais reikalavimais ir lūkesčiais. Šis darbas grindžiamas priemonėmis, jau numatytomis 2018 m. „Fintech“ srities veiksmų plane, ***kuriame*** Komisija paskelbė apie ketinimą skatinti ir palengvinti standartinių sutarčių sąlygų dėl finansų sektoriaus subjektų debesijos paslaugų veiklos rangos parengimą, remiantis tarpsektorinių debesijos paslaugų suinteresuotųjų šalių indėliu, kurį Komisija užtikrino bendradarbiaudama su finansų sektoriumi;

(55a) EPI turėtų būti įgaliotos parengti techninių ir reguliavimo standartų projektus, kuriuose būtų nurodyti politikos lūkesčiai, susiję su trečiosios šalies IRT rizikos valdymu ir sutartiniais reikalavimais. Iki tų standartų įsigaliojimo finansų sektoriaus subjektai turėtų vadovautis atitinkamomis EPI ir kompetentingų institucijų paskelbtomis gairėmis ir kitomis priemonėmis;

(56) siekiant skatinti priežiūros metodų, taikomų trečiosios šalies keliamai IRT rizikai finansų sektoriuje, konvergenciją ir veiksmingumą, stiprinti finansų sektoriaus subjektų, kurie veiklos funkcijoms atlikti 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;

(57) specialioji tvarka turi būti taikoma tik ypatingos svarbos paslaugas teikiančioms trečiosioms šalims, todėl siekiant atsižvelgti į finansų sektoriaus priklausomybės nuo tokių IRT paslaugas teikiančių trečiųjų šalių aspektą ir pobūdį, reikėtų nustatyti Sąjungos priežiūros sistemos taikymui skirtą paskyrimo mechanizmą, t. y. kiekybinius ir kokybinius kriterijus, pagal kuriuos būtų nustatomi ypatingos svarbos parametrai, kuriais remiantis tokia trečioji šalis įtraukiama į priežiūros sistemą. Ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys, kurios nėra automatiškai paskiriamos taikant pirmiau minėtus kriterijus, turėtų turėti galimybę savanoriškai dalyvauti priežiūros sistemoje, o toms IRT paslaugas teikiančioms trečiosioms šalims, kurioms jau taikomos priežiūros mechanizmų sistemos, kuriomis padedama vykdyti Eurosistemos lygmens užduotis, nurodytas Sutarties dėl Europos Sąjungos veikimo 127 straipsnio 2 dalyje, turėtų būti taikoma išimtis. ***Panašiai pripažinimo ypatingai svarbiomis šalimis mechanizmas neturėtų būti taikomas įmonėms, kurios yra finansų grupės dalis ir teikia IRT paslaugas išimtinai tos pačios finansų grupės finansų sektoriaus subjektams;***

(58) reikalavimas, kad IRT paslaugas teikiančios trečiosios šalys, pripažintos ypatingai

svarbiomis, būtų įsisteigusios Sąjungoje, nėra duomenų vietos reikalavimas, nes šiuo reglamentu nenumatoma jokių papildomų reikalavimų dėl duomenų saugojimo ar tvarkymo Sąjungoje. ***Reikalavimu turėti įmonę, pavyzdžiui, Sąjungoje pagal valstybės narės teisę įsteigtą patronuojamąją įstaigą, siekiama užtikrinti, kad, viena vertus, IRT paslaugas teikianti trečioji šalis ir, kita vertus, atsakingoji priežiūros institucija ir bendra priežiūros įstaiga turėtų kontaktinį punktą ir kad atsakingoji priežiūros institucija ir bendra priežiūros įstaiga galėtų vykdyti savo pareigas ir priežiūros bei vykdymo užtikrinimo įgaliojimus, kaip numatyta šiame reglamente. Pagal paslaugų sutartį IRT paslaugas teikiančios trečiosios šalies paslaugos neturi būti teikiamos Sąjungoje įsteigto subjekto;***

(58a) dėl reikšmingo poveikio, kurį gali turėti IRT paslaugas teikiančių trečiųjų šalių priskyrimas ypatingos svarbos šalims, turėtų būti nustatytos išankstinio klausymo teisės kaip įpareigojimas EPI ir bendrai priežiūros įstaigai tinkamai atsižvelgti į bet kokią papildomą informaciją, kurią IRT paslaugas teikiančios trečiosios šalys teikia paskyrimo proceso metu;

(59) ***priežiūros*** sistema neturėtų būti daromas poveikis valstybių narių kompetencijai vykdyti nacionalinę IRT paslaugas teikiančių trečiųjų šalių, kurios nėra ypatingos svarbos paslaugų teikėjai pagal šį reglamentą, tačiau galėtų būti laikomos svarbiomis nacionaliniu lygmeniu, priežiūrą;

(60) siekiant pasinaudoti dabartine 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, ***pasitelkdamas naujai įsteigtą bendrą priežiūros įstaigą, priimančią tiek atskirus sprendimus, skirtus*** ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, tiek ***kolektyvines rekomendacijas***, visų pirma dėl ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūros programų lyginamosios analizės, ir ***nustatančią*** geriausią praktiką sprendžiant IRT koncentracijos rizikos klausimus;

(61) siekiant užtikrinti, kad IRT paslaugas teikiančios trečiosios šalys, atliekančios ypatingos svarbos vaidmenį finansų sektoriuje, būtų atitinkamai prižiūrimos Sąjungos mastu***, tiesioginei IRT paslaugas teikiančių trečiųjų šalių priežiūrai vykdyti turėtų būti įsteigta bendra priežiūros įstaiga***. ***Be to,*** viena iš EPI turėtų būti paskirta kiekvienos iš ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių atsakingąja priežiūros institucija***, kad ji vykdytų ir koordinuotų kasdienę priežiūrą ir tiriamąjį darbą, veiktų kaip vienas bendras kontaktinis centras ir užtikrintų tęstinumą***. ***Bendra priežiūros įstaiga ir atsakingoji priežiūros institucija turėtų dirbti sklandžiai, kad užtikrintų veiksmingą kasdienę priežiūrą ir kompleksinį požiūrį į sprendimų priėmimą ir rekomendacijas;***

(62) atsakingosioms priežiūros institucijoms turėtų būti suteikti reikiami įgaliojimai atlikti ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių tyrimus, patikrinimus vietoje ▌, patekti į visas atitinkamas patalpas ir vietas bei gauti išsamią ir atnaujintą informaciją, kad galėtų realiai įvertinti finansų sektoriaus subjektams ir galiausiai Sąjungos finansų sistemai gresiančios trečiosios šalies keliamos IRT rizikos rūšį, aspektą ir poveikį;

(62a) tiesioginės priežiūros pavedimas ***bendrai priežiūros įstaigai*** yra būtina sąlyga norint suprasti ir mažinti sisteminę IRT riziką finansų sektoriuje. Dėl ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių poveikio Sąjungoje ir su juo susijusių galimų IRT koncentracijos rizikos problemų reikia laikytis kolektyvinio Sąjungos lygmens požiūrio.

Jeigu daug kompetentingų institucijų atliktų daug atskirų auditų ir naudotųsi prieigos teisėmis, menkai koordinuodamos savo darbą arba jo visai nekoordinuodamos, nebūtų galima susidaryti išsamaus trečiosios šalies keliamos IRT rizikos vaizdo, o ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, kurios gautų daug tokių prašymų, tektų bereikalingas darbas, našta ir painiava;

(63) ***bendra priežiūros įstaiga*** turėtų turėti galimybę teikti rekomendacijas IRT rizikos ir tinkamų taisomųjų priemonių klausimais ir, be kita ko, išreikšti prieštaravimą tam tikriems sutartimi įformintiems susitarimams, kurie galiausiai daro poveikį finansų sektoriaus subjekto arba finansų sistemos stabilumui. Nacionalinės kompetentingos institucijos, vykdydamos savo funkcijas, susijusias su finansų sektoriaus subjektų prudencine priežiūra, turėtų tinkamai atsižvelgti į ***bendros*** priežiūros ***įstaigos*** nustatytų tokių esminių rekomendacijų laikymąsi. ***Prieš baigiant rengti tokias rekomendacijas, ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims turėtų būti suteikta galimybė pateikti informaciją, į kurią, jų pagrįstu manymu, reikėtų atsižvelgti prieš užbaigiant ir pateikiant rekomendaciją;***

(63a) siekdamos išvengti techninių ir organizacinių priemonių, kurios taikomos ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, dubliavimo ir prieštaravimų, atsakingosios priežiūros institucijos ir bendra priežiūros įstaiga, vykdydamos savo įgaliojimus pagal šiame reglamente nustatytą priežiūros sistemą, turėtų tinkamai atsižvelgti į Direktyvoje (ES) 2016/1148 nustatytą sistemą. Prieš naudodamosi tokiais įgaliojimais, bendra priežiūros įstaiga ir atsakingoji priežiūros institucija turėtų konsultuotis su atitinkamomis kompetentingomis institucijomis, kurios turi jurisdikciją pagal Direktyvą (ES) 2016/1148;

(64) priežiūros sistema jokiu būdu ar jokia dalimi nepakeičiamas finansų sektoriaus subjektų vykdomas rizikos, kylančios naudojantis trečiųjų šalių teikiamomis IRT paslaugomis, valdymas, įskaitant pareigą nuolat stebėti sutartimi įformintus susitarimus, sudarytus su ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis, ir nedaromas poveikis visai finansų sektoriaus subjektų atsakomybei laikytis visų šio reglamento ir atitinkamų finansinių paslaugų teisės aktų reikalavimų ir juos vykdyti. Siekiant išvengti pasikartojančio ir iš dalies sutampančio darbo, kompetentingos institucijos neturėtų savarankiškai taikyti jokių priemonių, skirtų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių rizikai stebėti. Visas tokias priemones reikėtų iš anksto koordinuoti ir suderinti pagal priežiūros sistemą;

(65) siekiant tarptautiniu lygmeniu skatinti geriausios praktikos, taikytinos tikrinant IRT paslaugas teikiančių trečiųjų šalių skaitmeninės rizikos valdymą, konvergenciją, EPI turėtų būti skatinamos sudaryti bendradarbiavimo susitarimus su atitinkamomis trečiųjų valstybių priežiūros ir reguliavimo kompetentingomis institucijomis, kad būtų sudarytos palankesnės sąlygos plėtoti geriausią praktiką, skirtą trečiosios šalies keliamai IRT rizikai mažinti;

(66) siekdamos pasinaudoti kompetentingų institucijų ekspertų techninėmis žiniomis operacinės ir IRT rizikos valdymo srityje***, vykdydamos bendruosius tyrimus ir patikrinimus vietoje*** atsakingosios priežiūros institucijos turėtų remtis nacionaline priežiūros patirtimi ir sukurti specialias kiekvienai ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai skirtas tyrimo grupes, jose suburdamos įvairių sričių specialistus, kurie padėtų rengti ir faktiškai vykdyti priežiūros veiklą, įskaitant ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių patikrinimus vietoje, ir imtųsi reikiamų tolesnių veiksmų;

(67) kompetentingos institucijos turėtų turėti visus būtinus priežiūros, tyrimo ir sankcijų taikymo įgaliojimus, kad užtikrintų šio reglamento taikymą. Iš esmės administracinės nuobaudos turėtų būti skelbiamos. Kadangi finansų sektoriaus subjektai ir IRT paslaugas teikiančios trečiosios šalys gali būti įsisteigę skirtingose valstybėse narėse ir prižiūrimi skirtingų sektorių kompetentingų institucijų, reikėtų užtikrinti glaudų atitinkamų kompetentingų institucijų, įskaitant ECB (kai tai susiję su Tarybos reglamentu (ES) Nr. 1024/2013[1] jam pavestais specialiais uždaviniais), bendradarbiavimą ir konsultavimąsi su EPI, tarpusavyje keičiantis informacija ir teikiant pagalbą, susijusią su priežiūros veikla. ***Bendra pertvarkymo valdyba, nors ji nėra kompetentinga institucija pagal šį reglamentą, vis dėlto turėtų būti įtraukta į tarpusavio keitimosi informacija apie subjektus, kuriems taikomas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 806/2014[2], mechanizmus;***

(68) siekiant toliau kiekybiškai ir kokybiškai įvertinti ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių paskyrimo kriterijus ir suderinti priežiūros mokesčius, Komisijai turėtų būti suteikti įgaliojimai šiais klausimais priimti aktus pagal Sutarties dėl Europos Sąjungos veikimo 290 straipsnį: patikslinant sisteminį poveikį, kurį IRT paslaugas teikiančios trečiosios šalies žlugimas galėtų turėti finansų sektoriaus subjektams, kuriems ji teikia paslaugas, pasaulinės sisteminės svarbos įstaigų (G-SII) ar kitų sisteminės svarbos įstaigų (O-SII), kurios priklauso nuo atitinkamos IRT paslaugas teikiančios trečiosios šalies, skaičių, konkrečioje rinkoje veiklą vykdančių IRT paslaugas teikiančių trečiųjų šalių skaičių, IRT paslaugas teikiančios trečiosios šalies pakeitimo išlaidas, valstybių narių, kuriose atitinkama IRT paslaugas teikianti trečioji šalis teikia paslaugas ir kuriose veiklą vykdo finansų sektoriaus subjektai, besinaudojantys atitinkamos IRT paslaugas teikiančios trečiosios šalies paslaugomis, skaičių, taip pat priežiūros mokesčių sumą ir jų mokėjimo būdą.

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[3] 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;

(69) kadangi šiame reglamente ir Europos Parlamento ir Tarybos direktyvoje (ES) 20xx/xx[4] konsoliduojamos IRT rizikos valdymo nuostatos, nustatytos įvairiuose Sąjungos finansinių paslaugų *acquis* reglamentuose ir direktyvose, įskaitant reglamentus (EB)

---

1 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).

2 ***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).***

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

4 [*Prašom įrašyti visą nuorodą*]

Nr. 1060/2009, (ES) Nr. 648/2012 (ES), Nr. 600/2014 ir (ES) Nr. 909/2014, siekiant užtikrinti visišką nuoseklumą, tie reglamentai turėtų būti iš dalies pakeisti paaiškinant, kad atitinkamos su IRT rizika susijusios nuostatos yra išdėstytos šiame reglamente.

EPI pateiktos arba šiuo metu rengiamos tų reglamentų ir direktyvų taikymo gairės turėtų būti persvarstomos ir tikslinamos vykdant konsolidavimo procesą, kad IRT rizikos reikalavimų teisinis pagrindas Sąjungos teisėje kiltų tik iš šio reglamento, jo įgyvendinimo aktų ir sprendimų bei rekomendacijų, priimtų remiantis šiuo reglamentu ir susijusių su subjektais, patenkančiais į jo taikymo sritį;

(69a) techniniais 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, testavimo ir pagrindinių trečiosios šalies keliamos IRT rizikos patikimos stebėsenos reikalavimų srityse. ***Rengdamos techninių reguliavimo standartų projektus, EPI turėtų deramai atsižvelgti į savo įgaliojimus, susijusius su proporcingumo aspektais, ir konsultuotis su atitinkamais patariamaisiais komitetais proporcingumo klausimais, visų pirma dėl šio reglamento taikymo MVĮ ir vidutinės kapitalizacijos įmonėms;***

(70) ypač svarbu, kad atlikdama parengiamąjį darbą Komisija tinkamai konsultuotųsi, taip pat ir su ekspertais. Komisija ir EPI turėtų užtikrinti, kad tuos standartus ir reikalavimus visi finansų sektoriaus subjektai galėtų taikyti tokiu būdu, kuris būtų proporcingas tų subjektų ir jų veiklos pobūdžiui, mastui ir sudėtingumui;

(71) siekiant gerinti pranešimų apie didelius su IRT susijusius incidentus palyginamumą ir užtikrinti sutartimi įformintų susitarimų dėl IRT paslaugas teikiančių trečiųjų šalių teikiamų paslaugų naudojimo skaidrumą, EPI turėtų būti įgaliotos parengti techninių įgyvendinimo standartų, kuriais nustatomi standartiniai šablonai, formos ir procedūros, skirti naudoti finansų sektoriaus subjektams pranešant apie didelį su IRT susijusį incidentą, taip pat standartiniai informacijos registro šablonai, projektus. Rengdamos šiuos standartus, EPI turėtų atsižvelgti į finansų sektoriaus subjektų ***pobūdį,*** dydį, sudėtingumą ir ***verslo profilį***, taip pat jų veiklos pobūdį ir rizikos dydį. Komisijai turėtų būti suteikti įgaliojimai priimti tuos techninius įgyvendinimo standartus įgyvendinimo aktais pagal SESV 291 straipsnį atitinkamų reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 15 straipsnyje nustatyta tvarka. Kadangi papildomi reikalavimai jau yra nustatyti deleguotaisiais ir įgyvendinimo aktais, pagrįstais atitinkamuose reglamentuose (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014 ir (ES) Nr. 909/2014 nustatytais techniniais reguliavimo ir įgyvendinimo standartais, tikslinga įpareigoti 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 kuriuose atnaujinamos dabartinės IRT rizikos valdymo taisyklės;

(72) dėl to reikės vėliau iš dalies pakeisti įvairiose finansinių paslaugų teisės aktų srityse priimtus deleguotuosius ir įgyvendinimo aktus. Operacinės rizikos straipsnių, kuriais tuose aktuose numatyti įgaliojimai priimti deleguotuosius ir įgyvendinimo aktus, taikymo sritis turėtų būti iš dalies pakeista siekiant į šį reglamentą perkelti visas šiandien tuose reglamentuose pateiktas nuostatas, taikomas skaitmeninės veiklos atsparumui;

(73) kadangi šio reglamento tikslų, t. y. užtikrinti visų finansų sektoriaus subjektų aukšto lygio skaitmeninės veiklos atsparumą, valstybės narės negali deramai pasiekti, nes tam

reikia suderinti daug skirtingų taisyklių, kurios šiuo metu egzistuoja kai kuriuose Sąjungos teisės aktuose arba įvairių valstybių narių teisinėse sistemose, o tų tikslų dėl jų 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.

PRIĖMĖ ŠĮ REGLAMENTĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas

1. Šiuo reglamentu nustatomi toliau nurodyti vienodi reikalavimai, taikomi finansų sektoriaus subjektų verslo procesus palaikančių tinklų ir informacinių sistemų saugumui, reikalingam aukštam bendram skaitmeninės veiklos atsparumo lygiui pasiekti:

a) finansų sektoriaus subjektams taikomi reikalavimai, susiję su:

– informacinių ir ryšių technologijų (IRT) rizikos valdymu;

– pranešimu kompetentingoms institucijoms apie didelius su IRT susijusius incidentus;

– finansinių subjektų, nurodytų 2 straipsnio 1 dalies a–c punktuose, pranešimu kompetentingoms institucijoms apie didelius operacinius ar su mokėjimais susijusius saugumo incidentus;

– skaitmeninės veiklos atsparumo testavimu;

– keitimusi informacija ir žvalgybos informacija apie kibernetines grėsmes ir pažeidžiamumo atvejus;

– priemonėmis, skirtomis finansų sektoriaus subjektams tinkamai valdyti trečiosios šalies keliamą IRT riziką;

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

c) ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūros sistema, taikoma, 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) 2016/1148 5 straipsnis, laikomi esminių paslaugų operatoriais, atžvilgiu šis reglamentas laikomas konkrečiam sektoriui taikomu Sąjungos teisės aktu pagal tos direktyvos 1 straipsnio 7 dalį.

2a. Šis reglamentas nedaro poveikio valstybių narių kompetencijai viešojo saugumo, gynybos ir nacionalinio saugumo palaikymo srityse.

2 straipsnis

Subjektinė taikymo sritis

1. Šis reglamentas taikomas šiems subjektams:

a) kredito įstaigoms,

b) mokėjimo įstaigoms,

c) elektroninių pinigų įstaigoms,

d) investicinėms įmonėms,

e) kriptoturto paslaugų teikėjams, kriptoturto emitentams, ***kriptoturto siūlytojams,*** su turtu susietų žetonų emitentams ***ir siūlytojams*** ir reikšmingų su turtu susietų žetonų emitentams,

f) centriniams vertybinių popierių depozitoriumams ***ir vertybinių popierių atsiskaitymų sistemų operatoriams***,

g) pagrindinėms sandorio šalims,

h) prekybos vietoms,

i) sandorių duomenų saugykloms,

j) alternatyvaus investavimo fondų valdytojams,

k) valdymo įmonėms,

l) duomenų teikimo paslaugų teikėjams,

m) draudimo ir perdraudimo įmonėms,

n) draudimo tarpininkams, perdraudimo tarpininkams ir papildomos draudimo veiklos tarpininkams***, kurie nėra labai mažos, mažosios ar vidutinės įmonės, nebent tos labai mažos, mažosios ar vidutinės įmonės yra išskirtinai priklausomos nuo organizuotos automatinės prekybos sistemų***,

o) profesinių pensijų įstaigoms ***(PPĮ), išskyrus atvejus, kai jos valdo pensijų sistemas, kuriose kartu nėra daugiau kaip 15 narių***,

p) kredito reitingų agentūroms,

q) teisės aktų nustatytą auditą atliekantiems auditoriams ir audito įmonėms***, kurios nėra labai mažos, mažosios ar vidutinės įmonės, išskyrus atvejus, kai tokios labai mažos, mažosios ar vidutinės įmonės teikia audito paslaugas šiame straipsnyje išvardytiems subjektams, išskyrus labai mažas, mažąsias ar vidutines įmones, kurios pagal Reglamento (ES) Nr. 537/2014 2 straipsnio 3 dalį yra pelno nesiekiantys audito subjektai, išskyrus atvejus, kai kompetentinga institucija nusprendžia, jog išimtis negalioja***,

r) ypatingos svarbos lyginamųjų indeksų administratoriams,

s) sutelktinio finansavimo paslaugų teikėjams,

t) pakeitimo vertybiniais popieriais duomenų saugykloms,

u) IRT paslaugas teikiančioms trečiosioms šalims.

1a. Šis reglamentas, išskyrus jo V skyriaus II skirsnį, taip pat taikomas IRT paslaugų grupės viduje teikėjams.

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

2a. Šiame reglamente, išskyrus V skyriaus II skirsnį, IRT paslaugas teikiančios trečiosios šalys ir IRT paslaugas grupės viduje teikiančios šalys bendrai vadinamos terminu „IRT paslaugas teikiančios trečiosios šalys“.

3 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) skaitmeninės veiklos atsparumas – finansų sektoriaus subjekto gebėjimas sukurti, užtikrinti ir peržiūrėti savo veiklos vientisumą, tiesiogiai ar netiesiogiai, naudojantis IRT paslaugas teikiančių trečiųjų šalių paslaugomis, užtikrinant ***nuolatinį finansinių paslaugų teikimą ir jų kokybę, atsižvelgiant į veiklos sutrikimus, darančius poveikį jo IRT pajėgumams***;

2) tinklų ir informacinė sistema – tinklų ir informacinė sistema, kaip apibrėžta Direktyvos (ES) 2016/1148 4 straipsnio 1 punkte;

3) tinklų ir informacinių sistemų saugumas – tinklų ir informacinių sistemų saugumas, kaip apibrėžta Direktyvos (ES) 2016/1148 4 straipsnio 2 punkte;

4) IRT rizika – bet kokia pagrįstai atpažįstama aplinkybė, susijusi su tinklų ir informacinių sistemų naudojimu, ▌kuriai susiklosčius gali būti ***pažeistas*** tinklų ir informacinių sistemų, bet kokios nuo ***IRT*** priklausančios priemonės ar proceso, operacijos ir proceso eigos arba paslaugų teikimo ***saugumas***;

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

6) su IRT susijęs incidentas – nenumatytas nustatytas ***incidentas arba keletas susijusių incidentų***, dėl ***kurių*** kyla pavojus tinklų ir informacinių sistemų saugumui▌ arba daromas neigiamas poveikis finansų sektoriaus subjekto teikiamų finansinių paslaugų prieinamumui, konfidencialumui, tęstinumui***, vientisumui*** ar autentiškumui;

6a) operacinis incidentas arba su mokėjimu susijęs saugumo incidentas – įvykis arba keletas susijusių įvykių, kurių nenumatė 2 straipsnio 1 dalies a–c punktuose nurodyti finansų sektoriaus subjektai ir kurie daro arba gali daryti neigiamą poveikį su mokėjimais susijusių paslaugų vientisumui, prieinamumui, konfidencialumui, autentiškumui ar tęstinumui;

7) didelis su IRT susijęs incidentas – su IRT susijęs incidentas, ***turintis arba*** galintis turėti didelį neigiamą poveikį tinklų ir informacinėms sistemoms, naudojamoms finansų sektoriaus subjekto ypatingos svarbos funkcijoms palaikyti;

7a) didelis operacinis incidentas arba su mokėjimu susijęs saugumo incidentas – operacinis incidentas arba su mokėjimu susijęs saugumo incidentas, atitinkantis 16 straipsnyje nustatytus kriterijus;

8) kibernetinė grėsmė – kibernetinė grėsmė, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/881[1] 2 straipsnio 8 punkte;

8a) didelė kibernetinė grėsmė – kibernetinė grėsmė, kurios savybės aiškiai rodo, kad ji gali sukelti didelį su IRT susijusį incidentą;

9) kibernetinis išpuolis – su IRT susijęs piktavališkas incidentas, kai priešiškas subjektas bando sunaikinti, atskleisti, pakeisti, išjungti, pavogti ar įgyti neteisėtą prieigą prie bet

[1] 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).

kokio turto arba neteisėtai juo naudotis;

10) žvalgybos informacija apie grėsmes – informacija, kuri siekiant priimti sprendimus yra apibendrinama, pertvarkoma, analizuojama, aiškinama arba patikslinama ir kuri sudaro sąlygas tinkamai ir pakankamai suprasti, kaip mažinti su IRT susijusio incidento ar kibernetinės grėsmės poveikį, įskaitant techninius kibernetinio išpuolio duomenis, už išpuolį atsakingus asmenis ir jų *modus operandi* bei motyvus;

11) pakopinė apsauga – su IRT susijusi strategija, pagal kurią pasitelkus žmones, procesus ir technologijas siekiama įvairiais būdais užkirsti kelią įsilaužimui skirtinguose subjekto lygmenyse ir lygiuose;

12) pažeidžiamumas – turto, sistemos, proceso ar kontrolės priemonės silpnoji vieta, jautrumas ar trūkumas, kuriais gali būti pasinaudota kibernetinei grėsmei kelti;

13) 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) subjekto ypatingos svarbos tikralaikių produkcijos sistemų bandymas;

14) 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;

15) IRT paslaugas teikianti trečioji šalis – ***IRT*** paslaugas teikianti įmonė, įskaitant ***IRT paslaugas teikiančius finansų sektoriaus subjektus, kurie yra įmonės, teikiančios įvairaus pobūdžio produktus ar paslaugas, dalis,*** išskyrus aparatinės įrangos komponentų teikėjus ir įmones, pagal Sąjungos teisę gavusias veiklos leidimą teikti elektroninių ryšių paslaugas, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2018/1972[1] 2 straipsnio 4 punkte;

15a) IRT paslaugų grupės viduje teikėjas – įmonė, priklausanti finansų grupei ir teikianti IRT paslaugas išskirtinai tos pačios grupės finansų sektoriaus subjektams arba tai pačiai institucinei užtikrinimo sistemai, įskaitant jų patronuojančiąsias įmones, patronuojamąsias įmones ir filialus ar kitus subjektus, kurie jiems bendrai priklauso arba yra jų kontroliuojami;

16) IRT paslaugos – skaitmeninės ir duomenų paslaugos, ***nuolat*** teikiamos naudojantis IRT sistemomis vienam ar keliems vidaus ar išorės naudotojams***, išskyrus telekomunikacijų paslaugų sutartis***;

17) ypatingos svarbos arba svarbi funkcija – ***veikla arba paslauga, kuri turi esminę reikšmę finansų sektoriaus subjekto veiklai ir kuriai sutrikus*** būtų reikšmingai pakenkta finansų sektoriaus subjekto ***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 galiojančius finansinių paslaugų teisės aktus nenutrūkstamam vykdymui***, įskaitant ypatingos svarbos funkcijas, kurios apibrėžtos Direktyvos 2014/59/ES 2 straipsnio 1 dalies 35 punkte***;

[1] 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (nauja redakcija) (OL L 321, 2018 12 17, p. 36).

18) ypatingos svarbos IRT paslaugas teikianti trečioji šalis – pagal ***28*** straipsnį paskirta IRT paslaugas teikianti trečioji šalis, kuriai taikoma ***29***–37 straipsniuose nurodyta priežiūros sistema;

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

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

21) 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 jų neprieinamumo, žlugimo ar kitokio pobūdžio trūkumo gali kilti pavojus ***visos Sąjungos finansiniam stabilumui arba*** finansų sektoriaus ***subjekto gebėjimui vykdyti*** ypatingos svarbos ***arba svarbias funkcijas*** arba ***jis gali patirti*** kitokio pobūdžio neigiamą poveikį, įskaitant didelius nuostolius;

22) 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, Direktyvos 2009/65/EB 2 straipsnio 1 dalies s punkte, Reglamento (ES) Nr. 909/2014 2 straipsnio 1 dalies 45 punkte, Europos Parlamento ir Tarybos reglamento (ES) 2016/1011[1] 3 straipsnio 1 dalies 20 punkte, Europos Parlamento ir Tarybos reglamento (ES) 20xx/xx[2] [MICA] 3 straipsnio 1 dalies ***18*** punkte, arba tokius pačius įgaliojimus turintys asmenys, kurie veiksmingai vadovauja subjektui arba vykdo pagrindines funkcijas pagal atitinkamus Sąjungos ar nacionalinės teisės aktus;

23) kredito įstaiga – kredito įstaiga, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 575/2013[3] 4 straipsnio 1 dalies 1 punkte;

23a) kredito įstaiga, kuriai taikoma išimtis pagal Direktyvą 2013/36/ES – kredito įstaiga, kuriai taikoma išimtis pagal Direktyvos 2013/36/ES 2 straipsnio 5 dalies 4–23 punktus;

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

24a) maža ir tarpusavyje nesusijusi investicinė įmonė – investicinė įmonė, atitinkanti Reglamento (ES) 2019/2033 12 straipsnio 1 dalyje nustatytas sąlygas;

25) mokėjimo įstaiga – mokėjimo įstaiga, kaip apibrėžta Direktyvos (ES) 2015/2366 1

---

1 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).

2 [*prašom įrašyti visą pavadinimą ir OL duomenis*]

3 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).

straipsnio 1 dalies d punkte;

25a) mokėjimo įstaiga, kuriai taikoma išimtis pagal Direktyvą (ES) 2015/2366 – mokėjimo įstaiga, kuriai taikoma išimtis pagal Direktyvos 2015/2366 32 straipsnio 1 dalį;

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

26a) elektroninių pinigų įstaiga, kuriai taikoma išimtis pagal Direktyvą 2009/110/EB – elektroninių pinigų įstaiga, kuriai taikoma išimtis pagal Direktyvos 2009/110/EB 9 straipsnį;

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

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

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

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

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

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

33) duomenų teikimo paslaugų teikėjas – duomenų teikimo paslaugų teikėjas, kaip apibrėžta Direktyvos 2014/65/ES 4 straipsnio 1 dalies 63 punkte;

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

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

36) draudimo tarpininkas – draudimo tarpininkas, kaip apibrėžta Direktyvos (ES) 2016/97 2 straipsnio ***1 dalies*** 3 punkte;

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

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

39) profesinių pensijų įstaiga – profesinių pensijų įstaiga, kaip apibrėžta Direktyvos 2016/2341/EB 6 straipsnio 1 punkte;

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

---

[1] 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).

41) teisės aktų nustatytą auditą atliekantis auditorius – teisės aktų nustatytą auditą atliekantis auditorius, kaip apibrėžta Direktyvos 2006/43/EB 2 straipsnio 2 punkte;

42) audito įmonė – audito įmonė, kaip apibrėžta Direktyvos 2006/43/EB 2 straipsnio 3 punkte;

43) kriptoturto paslaugų teikėjas – kriptoturto paslaugų teikėjas, kaip apibrėžta Reglamento (ES) 202x/xx 3 straipsnio 1 dalies ***8*** punkte [LB: įrašyti MICA reglamento nuorodą];

44) kriptoturto emitentas – kriptoturto emitentas, kaip apibrėžta [OL: įrašyti MICA reglamento nuorodą] 3 straipsnio 1 dalies ***6*** punkte;

44a) siūlytojas – siūlytojas, kaip apibrėžta [OL: įrašyti MICA reglamento nuorodą] 3 straipsnio 1 dalies [(XX)] punkte;

44b) kriptoturto siūlytojas – kriptoturto siūlytojas, kaip apibrėžta [OL: įrašyti MICA reglamento nuorodą] [3 straipsnio 1 dalies (XX) punkte];

45) su turtu susietų žetonų emitentas – su turtu susietų mokėjimo žetonų emitentas, kaip apibrėžta [OL: įrašyti MICA reglamento nuorodą] 3 straipsnio 1 dalies i punkte;

45a) su turtu susietų žetonų siūlytojas – su turtu susietų mokėjimo žetonų siūlytojas, kaip apibrėžta [OL: įrašyti MICA reglamento nuorodą] 3 straipsnio 1 dalies [(XX)] punkte;

46) reikšmingų su turtu susietų žetonų emitentas – reikšmingų su turtu susietų mokėjimo žetonų emitentas, kaip apibrėžta [OL: įrašyti MICA reglamento nuorodą] 3 straipsnio 1 dalies ***(XX)*** punkte;

47) ypatingos svarbos lyginamųjų indeksų administratorius – ypatingos svarbos lyginamųjų indeksų administratorius, kaip apibrėžta Reglamento ***2016/1011*** [OL: įrašyti Lyginamųjų indeksų reglamento nuorodą] ***3*** straipsnio ***25*** punkte;

48) sutelktinio finansavimo paslaugų teikėjas – sutelktinio finansavimo paslaugų teikėjas, kaip apibrėžta Reglamento (ES) ***2020/1503*** [LB: įrašyti Sutelktinio finansavimo reglamento nuorodą] ***2*** straipsnio ***1 dalies e*** punkte;

49) pakeitimo vertybiniais popieriais duomenų saugykla – pakeitimo vertybiniais popieriais duomenų saugykla, kaip apibrėžta Reglamento (ES) 2017/2402 2 straipsnio 23 punkte;

50) labai maža***, mažoji ar vidutinė*** įmonė – finansų sektoriaus subjektas, kaip apibrėžta Rekomendacijos 2003/361/EB priedo 2 ***straipsnyje***.

50a) pertvarkymo institucija – institucija, kurią paskiria valstybė narė pagal Direktyvos 2014/59/ES 3 straipsnį arba Bendra pertvarkymo valdyba, įsteigta pagal Reglamento (ES) Nr. 806/2014 42 straipsnį;

3a straipsnis

Proporcingumo principas

1. Finansų sektoriaus subjektai įgyvendina II, III ir IV skyriuose numatytas taisykles laikydamiesi proporcingumo principo, atsižvelgdami į savo įmonės dydį, paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą bei į bendrą rizikos profilį.

2. Laikantis proporcingumo principo šio reglamento 4–14 straipsniai netaikomi:

a) mažoms ir tarpusavyje nesusijusioms investicinėms įmonėms ar mokėjimo įstaigoms, kurioms taikoma išimtis pagal Direktyvą (ES) 2015/2366;

b) kredito įstaigoms, kurioms taikoma išimtis pagal Direktyvą 2013/36/ES;

c) elektroninių pinigų įstaigoms, kurioms taikoma išimtis pagal Direktyvą 2009/110/ES; arba

d) mažoms profesinių pensijų įstaigoms.

3. Remdamosi metine IRT rizikos valdymo sistemos peržiūros ataskaita, nurodyta 5 straipsnio 6 dalyje ir 14a straipsnio 2 dalyje, atitinkamos kompetentingos institucijos peržiūri ir įvertina, kaip finansų sektoriaus subjektas laikosi proporcingumo principo, ir nustato, ar finansų sektoriaus subjekto IRT rizikos valdymo sistema užtikrinamas patikimas valdymas, skaitmeninės veiklos atsparumas ir IRT rizikos padengimas. Atlikdamos šią peržiūrą ir vertinimą kompetentingos institucijos atsižvelgia į finansų sektoriaus subjekto dydį, jo paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą, taip pat į jo bendrą rizikos profilį.

4. Jei atitinkama kompetentinga institucija mano, kad finansų sektoriaus subjekto IRT rizikos valdymo sistema yra nepakankama ir neproporcinga, ji pradeda dialogą su finansų sektoriaus subjektu, kad pašalintų trūkumus ir užtikrintų visišką atitiktį II skyriui.

5. EPI parengia techninių reguliavimo standartų projektus, siekdamos:

a) nustatyti, kokiu mastu IRT rizikos valdymo įsipareigojimai taikomi kiekvienam iš 1 dalyje nurodytų finansų sektoriaus subjektų;

b) patikslinti 3 dalyje nurodytos IRT rizikos valdymo sistemos peržiūros metinės ataskaitos turinį ir formą;

c) nurodyti taisykles ir procedūras, kurių kompetentingos institucijos ir finansų sektoriaus subjektai turi laikytis palaikydami 4 dalyje nurodytą dialogą.

6. EPI 5 dalyje nurodytus techninių reguliavimo standartų projektus pateikia Komisijai iki [OL: įrašyti datą – vieni metai nuo įsigaliojimo dienos].

Komisijai suteikiami įgaliojimai priimti šio straipsnio 10 dalyje nurodytus techninius reguliavimo standartus atitinkamai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsnius.

II SKYRIUS

IRT RIZIKOS VALDYMAS

I SKIRSNIS

4 straipsnis

Valdymas ir organizavimas

1. Finansų sektoriaus subjektai įdiegia vidaus valdymo ir kontrolės ***sistemą, kuria*** užtikrinamas veiksmingas ir prudencinis visos IRT rizikos valdymas***, kad būtų užtikrintas aukštas skaitmeninės veiklos atsparumo lygis***.

2. Finansų sektoriaus subjekto valdymo organas nustato, tvirtina ir prižiūri visas priemones, susijusias su 5 straipsnio 1 dalyje nurodyta IRT rizikos valdymo sistema, ir atsako už jų įgyvendinimą.

   Taikant pirmą pastraipą, valdymo organas:

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

   aa) nustato procedūras ir politiką, kuriomis siekiama užtikrinti, kad būtų išlaikyti aukšti duomenų saugumo, konfidencialumo ir vientisumo standartai;

   b) nustato aiškias pareigas ir atsakomybę už visas su IRT susijusias funkcijas;

   c) nustato atitinkamą finansų sektoriaus subjektui priimtinos IRT rizikos lygį, kaip nurodyta 5 straipsnio 9 dalies b punkte;

   d) tvirtina, prižiūri ir periodiškai peržiūri finansų sektoriaus subjekto IRT veiklos tęstinumo politikos ir IRT veiklos atkūrimo po ekstremaliųjų įvykių plano, ***kuris gali būti patvirtintas kaip speciali atskira politika ir kaip neatsiejama platesnės finansų sektoriaus subjekto veiklos tęstinumo politikos ir veiklos atkūrimo po ekstremaliųjų įvykių plano dalis,*** kurie atitinkamai nurodyti 10 straipsnio 1 ir 3 dalyse, įgyvendinimą;

   e) tvirtina ir periodiškai peržiūri IRT audito planus, IRT auditą ir jų esminius pakeitimus;

   f) paskirsto ir periodiškai peržiūri atitinkamą biudžetą, kad būtų tenkinami finansų sektoriaus subjekto skaitmeninės veiklos atsparumo poreikiai, susiję su visų rūšių ištekliais, įskaitant ***atitinkamą*** visų ▌ darbuotojų mokymą IRT rizikos ir įgūdžių temomis;

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

   h) yra tinkamai informuotas apie susitarimus, sudarytus su IRT paslaugas teikiančiomis trečiosiomis šalimis dėl IRT paslaugų naudojimo, visus atitinkamus planuojamus esminius pakeitimus, susijusius su IRT paslaugas

teikiančiomis trečiosiomis šalimis, ir galimą tokių pokyčių poveikį ypatingos svarbos ar svarbioms funkcijoms, dėl kurių sudaryti tokie susitarimai, įskaitant teisę gauti rizikos analizės santrauką, kad galėtų įvertinti šių pokyčių poveikį;

i) yra ***reguliariai informuojamas bent*** apie didelius su IRT susijusius incidentus ir jų poveikį, taip pat apie reagavimo, veiklos atkūrimo ir taisomąsias priemones.

3. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, sukuria pareigybę, skirtą ***finansų sektoriaus subjekto*** susitarimų ***dėl IRT paslaugų naudojimo (ypač susitarimų, kurie sudaryti*** su IRT paslaugas teikiančiomis trečiosiomis šalimis***)*** stebėsenai, arba paskiria vyresniosios vadovybės narį, atsakingą už gresiančios susijusios rizikos priežiūrą ir atitinkamus dokumentus.

4. ***Finansų sektoriaus subjekto*** valdymo organo nariai ***aktyviai*** dalyvauja specialiuose mokymuose, kad įgytų ir turėtų naujausių pakankamų žinių ir įgūdžių IRT rizikai ir jos poveikiui finansų sektoriaus subjekto veiklai suprasti ir įvertinti***, be kita ko, reguliariai dalyvauja specialiuose mokymuose, kai tai proporcinga atsižvelgiant į valdomą IRT riziką***.

II SKIRSNIS

5 straipsnis

IRT rizikos valdymo sistema

1. Finansų sektoriaus subjektai turi patikimą, išsamią ir gerai dokumentais pagrįstą IRT rizikos valdymo sistemą, kuri jiems leidžia greitai, veiksmingai ir išsamiai mažinti IRT riziką bei užtikrinti aukštą skaitmeninės veiklos atsparumo lygį ▌.

2. 1 dalyje nurodyta IRT rizikos valdymo sistema apima strategijas, politiką, procedūras, IRT protokolus ir priemones, kurios yra būtinos siekiant tinkamai ir veiksmingai apsaugoti visus atitinkamus fizinius komponentus ir infrastruktūras, įskaitant aparatinę įrangą, serverius, taip pat visas atitinkamas patalpas, duomenų centrus ir jautrias specialias zonas, kad būtų užtikrinama, jog visi tie fiziniai elementai būtų tinkamai apsaugoti nuo rizikos, įskaitant žalą ir neteisėtą prieigą ar naudojimą.

3. Finansų sektoriaus subjektai mažina IRT rizikos poveikį, įgyvendindami atitinkamas strategijas, politiką, procedūras, protokolus ir priemones, kaip nustatyta IRT rizikos valdymo sistemoje. Jie pateikia išsamią ir atnaujintą informaciją apie IRT riziką ***ir apie IRT rizikos valdymo sistemą***, kurios reikalauja kompetentingos institucijos.

4. Pagal 1 dalyje nurodytą IRT rizikos valdymo sistemą finansų sektoriaus subjektai, išskyrus labai mažas įmones, įgyvendina informacijos saugumo valdymo sistemą, pagrįstą pripažintais tarptautiniais standartais ir atitinkančią priežiūros rekomendacijas***, jeigu jos jau prieinamos ir tinkamos, be kita ko, kaip nurodyta atitinkamose EPI parengtose gairėse***, bei reguliariai ją peržiūri.

5. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, ***priskiria atsakomybę už IRT rizikos valdymą ir priežiūrą kontrolės funkcijai ir užtikrina tos kontrolės funkcijos nepriklausomumą, kad būtų išvengta interesų konfliktų. Finansų sektoriaus subjektai*** užtikrina tinkamą IRT valdymo funkcijų, kontrolės funkcijų ir vidaus audito funkcijų nepriklausomumą pagal trijų apsaugos linijų modelį arba vidaus rizikos

valdymo ir kontrolės modelį.

6. 1 dalyje nurodyta IRT rizikos valdymo sistema pagrindžiama dokumentais ir peržiūrima ne rečiau kaip kartą per metus, taip pat įvykus dideliems su IRT susijusiems incidentams ir laikantis priežiūros nurodymų ar išvadų, padarytų atlikus atitinkamą skaitmeninės veiklos atsparumo testavimą arba auditą. Ji nuolat tobulinama remiantis įgyvendinimo ir stebėsenos patirtimi.

Kompetentingai institucijai kasmet pateikiama IRT rizikos valdymo sistemos peržiūros ataskaita.

7. ***Finansų sektoriaus subjektų, išskyrus labai mažas įmones, atveju*** 1 dalyje nurodytos IRT rizikos valdymo sistemos auditą reguliariai atlieka IRT auditoriai, turintys pakankamai žinių, įgūdžių ir patirties IRT rizikos srityje. IRT audito dažnumas ir tikrinami aspektai turi atitikti finansų sektoriaus subjekto IRT riziką.

8. Parengiamas oficialus tolesnių veiksmų procesas, įskaitant taisykles, pagal kurias laiku tikrinami ir taisomi esminiai IRT audito nustatyti faktai, atsižvelgiant į audito peržiūros išvadas. ▌

9. Į 1 dalyje nurodytą IRT rizikos valdymo sistemą įtraukiama ***skaitmeninės veiklos*** atsparumo strategija, kurioje nustatoma, kaip sistema įgyvendinama. Tuo tikslu ji apima IRT rizikos mažinimo ir konkrečių IRT tikslų įgyvendinimo metodus, nes ja:

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

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

   c) nustatomi aiškūs informacijos saugumo tikslai;

   d) paaiškinama IRT ▌architektūra ir visi pakeitimai, reikalingi konkretiems verslo tikslams pasiekti;

   e) nurodomi įvairūs mechanizmai, įdiegti tam, kad būtų galima aptikti su IRT susijusių incidentų poveikį, nuo jo apsisaugoti ir užkirsti jam kelią;

   f) nurodomas didelių su IRT susijusių incidentų, apie kuriuos pranešta, skaičius ir prevencinių priemonių veiksmingumas;

   g) nustatoma ***pagrindinė priklausomybė*** nuo IRT paslaugas teikiančių trečiųjų šalių ir ***nurodomos strategijos, kaip bus išsivaduota nuo tokios pagrindinės priklausomybės***;

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

   i) nurodoma komunikacijos strategija su IRT susijusių incidentų atveju***, kurią reikalaujama pateikti pagal 13 straipsnį***.

10. Gavę kompetentingų institucijų sutikimą, finansų sektoriaus subjektai gali ***perduoti***

išorės įmonėms tikrinti atitiktį IRT rizikos valdymo reikalavimams.

Pranešę kompetentingoms institucijoms, finansų sektoriaus subjektai gali pavesti grupės vidaus įmonėms tikrinti atitiktį IRT rizikos valdymo reikalavimams.

Kai įvyksta antroje pastraipoje nurodytas perdavimas, finansų sektoriaus subjektas ir toliau lieka visiškai atskaitingas už patikrinimą, ar laikomasi IRT rizikos valdymo reikalavimų.

6 straipsnis

IRT sistemos, protokolai ir priemonės

1. ***Siekdami mažinti ir valdyti IRT riziką,*** finansų sektoriaus subjektai naudoja ir prižiūri atnaujinamas IRT sistemas, protokolus ir priemones, atitinkančius šiuos reikalavimus:

   a) sistemos ir priemonės atitinka operacijų, kuriomis palaikomas jų veiklos vykdymas, mastą;

   b) jie yra patikimi;

   c) jie yra pakankamai pajėgūs, kad galėtų tiksliai tvarkyti duomenis, būtinus veiklai vykdyti ir paslaugoms teikti laiku, ir prireikus susidoroti su didžiausiais pavedimų, pranešimų ar sandorių kiekiais, įskaitant naujų technologijų diegimo atveju;

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

2. Kai finansų sektoriaus subjektai taiko tarptautiniu mastu pripažintus techninius standartus ir pažangiausią sektoriaus praktiką informacijos saugumo ir IRT vidaus kontrolės srityje, jie tuos standartus ir praktiką taiko vadovaudamiesi visomis atitinkamomis priežiūros rekomendacijomis dėl jų diegimo.

7 straipsnis

Identifikavimas

1. Pagal 5 straipsnio 1 dalyje nurodytą IRT rizikos valdymo sistemą finansų sektoriaus subjektai identifikuoja, klasifikuoja ir tinkamai pagrindžia dokumentais visas ***ypatingos svarbos ir svarbias*** su IRT susijusias veiklos funkcijas, šioms funkcijoms naudojamą informacinį turtą ir IRT sistemų konfigūracijas bei tarpusavio sąsajas su vidaus ir išorės IRT sistemomis. Prireikus ir bent kartą per metus finansų sektoriaus subjektai peržiūri ***su IRT susijusių veiklos funkcijų ypatingos svarbos ar svarbumo statusą ir*** informacinio turto klasifikavimo ir atitinkamų dokumentų tinkamumą.

2. Finansų sektoriaus subjektai nuolat identifikuoja visus IRT rizikos, visų pirma dėl kitų finansų subjektų kylančios ir jų keliamos rizikos, šaltinius ir vertina kibernetines grėsmes ir IRT pažeidžiamumus, susijusius su jų ***ypatingos svarbos ir svarbiomis*** IRT veiklos funkcijomis ir informaciniu 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***, kai taikytina,*** rizikos vertinimą po kiekvieno svarbaus tinklų ir informacinių sistemų infrastruktūros, procesų ar procedūrų, turinčių įtakos jų funkcijoms, pagalbiniams procesams ar informaciniam turtui, pakeitimo.

4. Finansų sektoriaus subjektai identifikuoja visas IRT sistemų paskyras, įskaitant esančias nutolusiose vietose, tinklo išteklius ir aparatinę įrangą ir grafiškai atvaizduoja fizinę įrangą, kuri laikoma ypatingai svarbia. Jie grafiškai atvaizduoja ***ypatingos svarbos ar svarbaus*** IRT turto konfigūraciją***, atsižvelgdami į jo paskirtį,*** ir skirtingo ***tokio*** IRT turto sąsajas ir tarpusavio priklausomybę.

5. Finansų sektoriaus subjektai identifikuoja ir dokumentais pagrindžia visus ***ypatingos svarbos ir svarbius*** procesus, kurie priklauso nuo IRT paslaugas teikiančių trečiųjų šalių, ir nustato tarpusavio sąsajas su IRT paslaugas teikiančiomis trečiosiomis šalimis***, kurios palaiko tas ypatingos svarbos ar svarbias funkcijas***.

6. Taikant 1, 4 ir 5 dalis, finansų sektoriaus subjektai tvarko ir reguliariai atnaujina atitinkamus aprašus.

7. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, reguliariai ir bent kartą per metus atlieka specialų visų senųjų IRT sistemų IRT rizikos vertinimą***, įskaitant sistemas, kurios vis dar naudojamos ir atlieka savo funkciją, bet:***

   a) yra senos arba jų gyvavimo ciklas baigiasi (aparatinės įrangos atveju),

   b) jų tiekėjas jų nebepalaiko ar nebeteikia techninės priežiūros arba

   c) jų atnaujinti neįmanoma arba neekonomiška. Atliekami metiniai senųjų IRT sistemų IRT rizikos ***vertinimai***, ypač iki ▌ technologijų, programų ar sistemų sujungimo ir po jo.

8 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 veikimą ir kuo labiau mažina tokios rizikos poveikį, diegdami tinkamas IRT saugumo priemones, politiką ir procedūras.

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

3. Kad pasiektų 2 dalyje nurodytus tikslus, finansų sektoriaus subjektai naudoja ▌ IRT technologijas ir procesus, kuriais:

   a) ***kuo labiau padidinamas*** informacijos perdavimo priemonių saugumas;

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

   c) užkertamas kelias informacijos nutekėjimui;

d) užtikrinama, kad duomenys būtų apsaugoti nuo ***vidinės IRT rizikos***, įskaitant ***netinkamą administravimą, tvarkymą ir žmogaus klaidas***.

4. Pagal 5 straipsnio 1 dalyje nurodytą IRT rizikos valdymo sistemą ***ir savo rizikos profilį*** finansų sektoriaus subjektai:

a) parengia ir dokumentais pagrindžia informacijos saugumo politiką, kurioje apibrėžiamos taisyklės, kaip apsaugoti jų klientų IRT išteklių, duomenų ir informacinio turto konfidencialumą, vientisumą ir prieinamumą***, sykiu užtikrinant visapusišką klientų IRT išteklių, duomenų ir informacinio turto apsaugą finansų sektoriaus subjektų nuosavose IRT sistemose***;

b) taikydami rizika grindžiamą metodą, nustato patikimą tinklų ir infrastruktūros valdymo tvarką, tam pasitelkdami tinkamus būdus, metodus ir protokolus – be kita ko, įgyvendindami ▌mechanizmus paveiktam informaciniam turtui izoliuoti kibernetinių išpuolių atveju;

c) įgyvendina politiką, ***procedūras ir kontrolės priemones, kuriomis*** fizinė ir virtualioji prieiga prie IRT sistemos išteklių ir duomenų suteikiama tik tiek, kiek tai reikalinga teisėtoms ir patvirtintoms funkcijoms ir veiklai▌ ;

d) įgyvendina griežtų tapatumo nustatymo mechanizmų ***ir kriptografinių raktų apsaugos*** politiką ir protokolus, pagrįstus atitinkamais standartais ir specialiomis kontrolės sistemomis▌ ;

e) įgyvendina IRT pakeitimų, įskaitant programinės įrangos, aparatinės įrangos, programinės aparatinės įrangos komponentų, sistemos ar saugumo pakeitimus, valdymo politiką, procedūras ir kontrolės priemones, grindžiamas rizikos vertinimo metodu ir įtrauktas į bendrą finansų sektoriaus subjekto pakeitimų valdymo procesą, siekiant užtikrinti, kad visi IRT sistemų pakeitimai būtų registruojami, testuojami, vertinami, tvirtinami, įgyvendinami ir tikrinami kontroliuojamu būdu;

f) turi tinkamą ir išsamią pataisų ir naujinių politiką.

Taikant b punktą, finansų sektoriaus subjektai tinklų ryšio infrastruktūrą kuria taip, kad būtų galimybė ją ***kuo skubiau*** atjungti, ir užtikrina jos suskaidymą ir segmentavimą, kad būtų kuo labiau sumažintas ir stabdomas neigiamo poveikio plitimas, ypač tarpusavyje susijusių finansinių procesų atveju.

Taikant e punktą, IRT pakeitimų valdymo procesą tvirtina atitinkami tiesioginiai vadovai, be to, parengiami specialūs protokolai, skirti pakeitimams ekstremaliosios situacijos atveju.

9 straipsnis

Aptikimas

1. Finansų sektoriaus subjektai turi mechanizmus neįprastai veiklai pagal 15 straipsnį, įskaitant IRT tinklo veikimo problemas ir su IRT susijusius incidentus, skubiai aptikti ir***, kai technologijų požiūriu įmanoma,*** visiems galimiems reikšmingiems bendriems gedimo taškams identifikuoti ***bei stebėti.***

Visi pirmoje pastraipoje nurodyti aptikimo mechanizmai reguliariai testuojami pagal 22 straipsnį.

2. 1 dalyje nurodytais aptikimo mechanizmais ***užtikrinama, kad būtų pradėti*** su IRT susijusių incidentų aptikimo ir reagavimo į su IRT susijusius incidentus ***procesai***, ***įskaitant automatinius*** įspėjimo ***mechanizmus*** atitinkamiems darbuotojams, atsakingiems už reagavimą į su IRT susijusius incidentus.

3. Finansų sektoriaus subjektai skiria pakankamai išteklių ir pajėgumų ▌ naudotojų veiklai, neįprastai IRT veiklai ir su IRT susijusiems incidentams, visų pirma kibernetiniams išpuoliams, stebėti.

3a Finansų sektoriaus subjektai registruoja visus su IRT susijusius incidentus, darančius poveikį finansinių paslaugų stabilumui, tęstinumui ar kokybei, įskaitant atvejus, kai incidentas padarė poveikį ar galėjo padaryti poveikį tokioms paslaugoms.

4. Be to, 2 straipsnio 1 dalies l punkte nurodyti finansų subjektai turi sistemas, kuriomis galima veiksmingai patikrinti prekybos pranešimų išsamumą, nustatyti praleistus duomenis bei akivaizdžias klaidas ir kuriose reikalaujama visus pranešimus, kuriuose yra klaidų, pateikti iš naujo.

10 straipsnis

Reagavimas ir veiklos atkūrimas

1. Pagal 5 straipsnio 1 dalyje nurodytą IRT rizikos valdymo sistemą, remdamiesi 7 straipsnyje nurodytais identifikavimo reikalavimais, finansų sektoriaus subjektai taiko ▌ išsamią IRT veiklos tęstinumo politiką, kuri ***gali būti patvirtinta kaip speciali atskira politika ir*** neatsiejama ***platesnės visos*** finansų sektoriaus subjekto veiklos tęstinumo politikos dalis.

IRT veiklos tęstinumo politikos tikslas – valdyti ir mažinti riziką, kuri galėtų turėti žalingą poveikį finansų sektoriaus subjektų IRT sistemoms ir IRT paslaugoms, ir prireikus palengvinti spartų veiklos atkūrimą. Rengdami savo IRT veiklos tęstinumo politiką, finansų sektoriaus subjektai konkrečiai atsižvelgia į riziką, kuri galėtų turėti žalingą poveikį IRT paslaugoms ir IRT sistemoms.

2. Finansų sektoriaus subjektai įgyvendina 1 dalyje nurodytą IRT veiklos tęstinumo politiką taikydami specialius, tinkamus ir dokumentais pagrįstus susitarimus, planus, procedūras ir mechanizmus, kurių paskirtis:

b) užtikrinti finansų sektoriaus subjekto ypatingos svarbos funkcijų tęstinumą;

c) greitai, tinkamai ir veiksmingai reaguoti į visus su IRT susijusius incidentus, visų pirma, be kita ko, kibernetinius išpuolius, ir juos spręsti taip, kad būtų daroma kuo mažesnė žala, o pirmenybė būtų teikiama veiklos atnaujinimo ir atkūrimo veiksmams;

d) nedelsiant pradėti įgyvendinti specialius planus, kuriais sudaromos sąlygos taikyti izoliavimo priemones, procesus ir technologijas, tinkamas visų rūšių su IRT susijusiems incidentams, ir užkirsti kelią tolesnei žalai, taip pat pagal 11 straipsnį nustatytas pritaikytas reagavimo ir veiklos atkūrimo procedūras;

e) įvertinti preliminarų poveikį, žalą ir nuostolius;

f) nustatyti komunikacijos ir krizių valdymo veiksmus, kuriais užtikrinama, kad atnaujinta informacija būtų perduodama visiems atitinkamiems vidaus

darbuotojams ir išorės suinteresuotosioms šalims pagal 13 straipsnį ir pateikiama kompetentingoms institucijoms pagal 17 straipsnį.

3. Pagal 5 straipsnio 1 dalyje nurodytą IRT rizikos valdymo sistemą finansų sektoriaus subjektai įgyvendina susijusį IRT veiklos atkūrimo po ekstremaliųjų įvykių planą, kurio peržiūrą atlieka nepriklausomas auditorius, išskyrus finansų subjektų, kurie yra labai mažos įmonės, atveju.

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

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

   a) bent kartą per metus ir po esminių ***ypatingos svarbos ar svarbių*** IRT sistemų pakeitimų testuoja IRT veiklos tęstinumo politiką ir IRT veiklos atkūrimo po ekstremaliųjų įvykių planą;

   b) testuoja pagal 13 straipsnį parengtus pranešimų krizės atveju planus.

   Taikant a punktą, 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 11 straipsnyje nustatytoms pareigoms įvykdyti, scenarijus.

   Finansų sektoriaus subjektai reguliariai peržiūri savo IRT veiklos tęstinumo politiką ir IRT veiklos atkūrimo po ekstremaliųjų įvykių planą, atsižvelgdami į pagal pirmą pastraipą atlikto testavimo rezultatus ir rekomendacijas, pateiktas atlikus audito patikras arba priežiūrinį tikrinimą.

6. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, turi krizių valdymo funkciją***, kuri yra speciali funkcija arba įeina į funkcijas, susijusias su reagavimu į incidentus ir jų valdymu. Vykdant šią krizių valdymo funkciją***, pradėjus įgyvendinti IRT veiklos tęstinumo politiką arba IRT veiklos atkūrimo po ekstremaliųjų įvykių planą, nustatomos aiškios vidaus ir išorės pranešimų krizės atveju valdymo procedūros pagal 13 straipsnį.

7. Finansų sektoriaus subjektai saugo ***atitinkamos*** veiklos prieš sutrikimo įvykius ir jų metu, kai pradedama įgyvendinti jų IRT veiklos tęstinumo politika arba IRT veiklos atkūrimo po ekstremaliųjų įvykių planas, įrašus. Suteikiama galimybė su tokiais įrašais nedelsiant susipažinti.

8. 2 straipsnio 1 dalies f punkte nurodyti finansų sektoriaus subjektai pateikia kompetentingoms institucijoms IRT veiklos tęstinumo testavimo ar panašių testų, atliktų per nagrinėjamą laikotarpį, rezultatų kopijas.

9. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, praneša kompetentingoms institucijoms apie visas ***apskaičiuotas finansines*** išlaidas ir nuostolius, patirtus dėl ***didelio*** IRT sutrikimo ir ***didelių*** su IRT susijusių incidentų.

9a. EPI Jungtiniame komitete parengia 9 dalyje nurodytų išlaidų apskaičiavimo ir kiekybinio nuostolių įvertinimo metodikos bendrąsias gaires.

11 straipsnis

Atsarginių kopijų politika ir veiklos atkūrimo metodai

1. Siekdami užtikrinti, kad IRT sistemos būtų atkuriamos kuo greičiau ir kuo mažiau jas sutrikdant, finansų sektoriaus subjektai į savo IRT rizikos valdymo sistemą įtraukia:

   a) atsarginių kopijų politiką, kurioje nurodoma duomenų, kurių atsarginės kopijos daromos, apimtis ir minimalus atsarginių kopijų darymo dažnumas, remiantis ypatinga informacijos svarba arba duomenų slaptumu;

   b) veiklos atkūrimo metodus.

2. ***Pagal 1 dalies a punkte nurodytą atsarginių kopijų politiką*** atsarginėse sistemose duomenys pradedami tvarkyti nepagrįstai nedelsiant, nebent tokia pradžia keltų pavojų tinklų ir informacinių sistemų saugumui arba duomenų vientisumui ar konfidencialumui.

3. Atkurdami atsarginius duomenis savo sistemose finansų sektoriaus subjektai naudoja IRT sistemas, ***fiziniais ar loginiais metodais atskirtas*** nuo ***jų*** pagrindinės ***IRT*** sistemos ▌ir ▌patikimai ***apsaugotas*** nuo bet kokios neteisėtos prieigos ar IRT sugadinimo.

   2 straipsnio 1 dalies g punkte nurodytų finansų sektoriaus subjektų atveju veiklos atkūrimo planais suteikiama galimybė atkurti visus sandorius sutrikimo momentu, kad pagrindinė sandorio šalis galėtų patikimai tęsti savo veiklą ir numatytą dieną atlikti atsiskaitymą.

4. Finansų sektoriaus subjektai ***įvertina poreikį turėti*** atsarginius IRT pajėgumus, kurių išteklių pajėgumai ir funkcijos ***būtų*** pakankami ir tinkami veiklos poreikiams tenkinti ***ir atitiktų veiklos atsparumo reikalavimus, kaip nustatyta šiame reglamente***.

5. 2 straipsnio 1 dalies f punkte nurodyti finansų sektoriaus subjektai turi arba užtikrina, kad jiems IRT paslaugas teikiančios trečiosios šalys turėtų bent vieną antrinę duomenų tvarkymo vietą, kuriai skirti ištekliai, pajėgumai, funkcijos ir aprūpinimo personalu tvarka būtų pakankami ir tinkami veiklos poreikiams tenkinti.

   Antrinė duomenų tvarkymo vieta:

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

   b) gali užtikrinti ypatingos svarbos paslaugų tęstinumą taip pat kaip ir pirminė vieta arba užtikrinti tokį paslaugų lygį, kuris būtinas, kad finansų sektoriaus subjektas galėtų atlikti savo ypatingos svarbos operacijas nenukrypdamas nuo veiklos atkūrimo tikslų;

   c) yra ▌prieinama finansų sektoriaus subjekto darbuotojams, kad būtų užtikrintas ypatingos svarbos ***ar svarbių funkcijų*** tęstinumas, jei pirminė duomenų tvarkymo vieta taptų neprieinama.

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

7. Atkurdami veiklą po su IRT susijusio incidento finansų sektoriaus subjektai ***užtikrina, kad duomenų vientisumo lygmuo būtų pats aukščiausias, pavyzdžiui,*** atlieka daug patikrinimų, įskaitant sutikrinimą. ***Tokie*** patikrinimai taip pat atliekami atkuriant išorės suinteresuotųjų šalių duomenis, siekiant užtikrinti, kad visi duomenys sistemose atitiktų.

12 straipsnis

Mokymasis ir tobulėjimas

1. Finansų sektoriaus subjektai turi 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 nustato, kad įvykus reikšmingam jų pagrindinės veiklos sutrikimui dėl IRT būtų atliekami ***didelių*** su IRT susijusių incidentų patikrinimai, per kuriuos būtų analizuojamos sutrikimo priežastys ir identifikuojami reikalingi IRT operacijų arba 10 straipsnyje nurodytos IRT veiklos tęstinumo politikos patobulinimai.

   Įgyvendindami pakeitimus***, susijusius su IRT rizikos, nustatytos per didelių su IRT susijusių incidentų patikrinimus, šalinimu***, finansų sektoriaus subjektai, išskyrus labai mažas įmones, apie ***visus svarbesnius*** pakeitimus praneša kompetentingoms institucijoms***, išsamiai aprašydami reikiamus patobulinimus ir tai, kaip jais siekiama užkirsti kelią sutrikimams arba sumažinti jų mastą ateityje***. ***Apie pakeitimus kompetentingoms institucijoms gali būti pranešama prieš pakeitimų įgyvendinimą arba po jo.***

   Atliekant pirmoje pastraipoje nurodytus patikrinimus po su IRT susijusių incidentų nustatoma, ar buvo laikomasi nustatytų procedūrų ir ar veiksmai, kurių imtasi, buvo veiksmingi, be kita ko, įvertinant:

   a) greitą reagavimą į įspėjimus apie saugumą ir su IRT susijusių incidentų poveikio ir jų rimtumo nustatymą;

   b) teismo ekspertizės atlikimo kokybę ir greitį;

   c) incidento sprendimo finansų sektoriaus subjekto viduje veiksmingumą;

   d) vidaus ir išorės komunikacijos veiksmingumą.

3. Į IRT rizikos vertinimo procesą nuolat tinkamai įtraukiama vykdant skaitmeninės veiklos atsparumo testavimą pagal 23 ir 24 straipsnius ir reaguojant į realius su IRT susijusius incidentus, visų pirma kibernetinius išpuolius, taip pat sprendžiant problemas, kilusias pradedant įgyvendinti veiklos tęstinumo arba veiklos atkūrimo planus, įgyta patirtis ir atitinkama informacija, kuria keistasi su sandorio šalimis ir kuri įvertinta priežiūrinio tikrinimo metu. Šių nustatytų faktų pagrindu tinkamai patikrinami atitinkami 5 straipsnio 1 dalyje nurodytos IRT rizikos valdymo sistemos komponentai.

4. Finansų sektoriaus subjektai stebi savo skaitmeninio atsparumo strategijos, nurodytos 5 straipsnio 9 dalyje, įgyvendinimo veiksmingumą. Jie chronologiškai atvaizduoja IRT rizikos pokyčius***, įskaitant tos rizikos tikimybę ypatingos svarbos arba svarbioms funkcijoms***, analizuoja su IRT susijusių incidentų, visų pirma kibernetinių išpuolių ir jų modelių, dažnumą, rūšis, mastą ir pokyčius, kad suprastų gresiančios IRT rizikos mastą ir sustiprintų finansų sektoriaus subjekto kibernetinę brandą ir parengtį.

5. Vyresnieji IRT darbuotojai bent kartą per metus valdymo organui praneša apie 3 dalyje nurodytus nustatytus faktus 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. ***Informuotumo apie IRT saugumą programos taikomos visiems darbuotojams. Skaitmeninės veiklos atsparumo mokymai*** taikomi ***bent*** visiems darbuotojams***, turintiems tiesioginės prieigos prie IRT sistemų teises,*** ir vyresniosios vadovybės nariams. ***Mokymo modulių sudėtingumas turi atitikti darbuotojo tiesioginės prieigos prie IRT sistemų lygį ir visų pirma turi būti atsižvelgiama į jo prieigą prie ypatingos svarbos ar svarbių funkcijų.***

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 susipažįsta su naujausiais IRT rizikos valdymo procesais, kuriais veiksmingai kovojama su esamų ar naujų formų kibernetiniais išpuoliais.

13 straipsnis

Komunikacija

1. Pagal 5 straipsnio 1 dalyje nurodytą IRT rizikos valdymo sistemą finansų sektoriaus subjektai turi komunikacijos planus, pagal kuriuos klientams ir partneriams bei prireikus visuomenei būtų galima atsakingai atskleisti informaciją ***bent*** apie ***didelius*** su IRT susijusius incidentus arba didelius pažeidžiamumus.

   Pirmoje pastraipoje nurodytais komunikacijos planais taip pat užtikrinama, kad klientams ir sandorio šalims kasmet būtų atskleidžiama visų su IRT susijusių incidentų santrauka. Atskleidžiant tokią informaciją visapusiškai laikomasi finansų sektoriaus subjekto ir jo klientų bei sandorio šalių verslo konfidencialumo principo ir nekeliamas pavojus 5 straipsnio 1 dalyje nurodytai IRT rizikos valdymo sistemai.

2. Pagal 5 straipsnio 1 dalyje nurodytą IRT rizikos valdymo sistemą finansų sektoriaus subjektai įgyvendina darbuotojų ir išorės suinteresuotųjų šalių komunikacijos politiką. 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 subjekto darbuotojui pavedama įgyvendinti ***bent didelių*** su IRT susijusių incidentų komunikacijos strategiją ir tuo tikslu eiti atstovo visuomenei ir žiniasklaidai pareigas.

14 straipsnis

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

Europos bankininkystės institucija (EBI), Europos vertybinių popierių ir rinkų institucija (ESMA) ir Europos draudimo ir profesinių pensijų institucija (EIOPA), pasikonsultavusios su Europos Sąjungos kibernetinio saugumo agentūra (ENISA), parengia techninių reguliavimo standartų projektus, siekdamos:

a) išsamiau nurodyti elementus, kurie turi būti įtraukti į 8 straipsnio 2 dalyje nurodytą IRT saugumo politiką, procedūras, protokolus ir priemones, siekiant užtikrinti tinklų saugumą, taikyti tinkamas apsaugos nuo įsibrovimo ir netinkamo duomenų naudojimo priemones, išsaugoti duomenų autentiškumą ir vientisumą, įskaitant kriptografinius metodus, ir užtikrinti tikslų ir greitą duomenų perdavimą be didelių sutrikimų ***ir nepagrįstų vėlavimų;***

d) plėtoti papildomus 8 straipsnio 4 dalies c punkte nurodytos 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;

e) toliau plėtoti 9 straipsnio 1 dalyje nurodytus elementus, suteikiant galimybę greitai aptikti neįprastą veiklą, ir 9 straipsnio 2 dalyje nurodytus kriterijus, kuriuos įvykdžius inicijuojami su IRT susijusių incidentų aptikimo ir reagavimo procesai;

f) patikslinti 10 straipsnio 1 dalyje nurodytos IRT veiklos tęstinumo politikos komponentus;

g) patikslinti 10 straipsnio 5 dalyje nurodytų IRT veiklos tęstinumo planų testavimą siekiant užtikrinti, kad testuojant būtų tinkamai atsižvelgiama į scenarijus, pagal kuriuos ypatingos svarbos ar 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 tinkama, politinę riziką atitinkamų paslaugų teikėjų jurisdikcijose;

h) patikslinti 10 straipsnio 3 dalyje nurodyto IRT veiklos atkūrimo po ekstremaliųjų įvykių plano komponentus.

EBI, ESMA ir EIOPA tuos techninių reguliavimo standartų projektus pateikia Komisijai iki [OL: prašom įrašyti datą – 1 metai po įsigaliojimo dienos].

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

14a straipsnis

IRT rizikos valdymo sistema, skirta mažiems, tarpusavyje nesusijusiems ir išimtiniams subjektams

1. Pagal 3a straipsnį mažos ir tarpusavyje nesusijusios investicinės įmonės, mokėjimo įstaigos, kurioms taikoma išimtis pagal Direktyvą (ES) 2015/2366, kredito įstaigos, kurioms taikoma išimtis pagal Direktyvą 2013/36/ES, elektroninių pinigų įstaigos, kurioms taikoma išimtis pagal Direktyvą 2009/110/EB, ir mažos profesinių pensijų įstaigos taiko ir administruoja patikimą ir dokumentuotą IRT rizikos valdymo sistemą:

a) joje išsamiai nustatomi mechanizmai ir priemonės, kuriais siekiama sparčiai, veiksmingai ir visapusiškai valdyti visų rūšių IRT riziką, įskaitant atitinkamų fizinių komponentų ir infrastruktūros apsaugą;

b) pagal ją nuolat stebimas visų IRT sistemų saugumas ir veikimas;

c) ji kuo labiau sumažina IRT rizikos poveikį, naudojant patikimas, atsparias ir atnaujintas IRT sistemas, protokolus ir priemones, kurie yra tinkami jų veiklai palaikyti ir paslaugoms teikti;

d) ji tinkamai apsaugo duomenų tinklo ir informacinių sistemų konfidencialumą, vientisumą ir prieinamumą;

e) ji sudaro sąlygas operatyviai nustatyti ir aptikti tinklo ir informacinių sistemų rizikos šaltinius ir anomalijas bei skubiai pašalinti IRT incidentus.

2. 1 dalyje nurodyta IRT rizikos valdymo sistema pagrindžiama dokumentais ir peržiūrima ne rečiau kaip kartą per metus, taip pat įvykus dideliems su IRT susijusiems incidentams ir laikantis priežiūros nurodymų ar išvadų, padarytų atlikus atitinkamą skaitmeninės veiklos atsparumo testavimą arba auditą. Ji nuolat tobulinama remiantis įgyvendinimo ir stebėsenos patirtimi.

Kompetentingai institucijai kasmet pateikiama IRT rizikos valdymo sistemos peržiūros ataskaita.

III SKYRIUS

SU IRT SUSIJĘ INCIDENTAI

VALDYMAS, KLASIFIKAVIMAS IR PRANEŠIMŲ TEIKIMAS

15 straipsnis

Su IRT susijusių incidentų valdymo procesas

1. Finansų sektoriaus subjektai nustato ir įgyvendina su IRT susijusių incidentų valdymo procesą, skirtą su IRT susijusiems incidentams aptikti, valdyti ir apie juos pranešti, ir kaip perspėjimus taiko išankstinio įspėjimo rodiklius.

2. Finansų sektoriaus subjektai nustato ***atitinkamas procedūras ir*** procesus, kad užtikrintų nuoseklią ir integruotą su IRT susijusių incidentų stebėseną, tvarkymą ir tolesnius veiksmus ir taip galėtų identifikuoti ir pašalinti pagrindines priežastis siekdami užkirsti kelią tokiems incidentams.

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

   a) nustatomos su IRT susijusių incidentų identifikavimo, sekimo, registravimo, grupavimo ir klasifikavimo procedūros pagal šių incidentų prioritetą ir rimtumą bei paslaugų, kurioms daromas poveikis, ypatingą svarbą, remiantis 16 straipsnio 1 dalyje nurodytais kriterijais;

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

   c) nustatomi komunikacijos su darbuotojais, išorės suinteresuotosiomis šalimis ir žiniasklaida planai pagal 13 straipsnį ir pranešimo klientams, vidaus problemų sprendimo procedūros, įskaitant su IRT susijusių klientų skundų nagrinėjimą, taip pat informacijos teikimo finansų sektoriaus subjektams, kurie atitinkamais atvejais veikia kaip sandorio šalys, procedūros;

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

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

16 straipsnis

Su IRT susijusių incidentų klasifikavimas

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

   a) naudotojų arba finansų sandorio šalių, kurių veikla buvo sutrikdyta dėl su IRT

susijusio incidento, skaičius ;

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

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

d) duomenų nuostoliai dėl su IRT susijusio incidento, pavyzdžiui, vientisumo praradimas, konfidencialumo praradimas arba prieinamumo praradimas;

e) su IRT susijusio incidento poveikio finansų sektoriaus subjekto IRT sistemoms rimtumas;

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

g) su IRT susijusio incidento ekonominis poveikis absoliučiąja ir santykine verte.

2. EPI, pasitarusios EPI Jungtiniame komitete (toliau – Jungtinis komitetas) ir ***suderinusios*** su Europos Centriniu Banku (ECB) bei ENISA, parengia bendrų techninių reguliavimo standartų projektus, kuriais patikslinami:

a) 1 dalyje nustatyti kriterijai, įskaitant didelių su IRT susijusių incidentų, kuriems taikoma 17 straipsnio 1 dalyje nustatyta pareiga pranešti, nustatymo reikšmingumo ribas;

b) kriterijai, kuriuos turi taikyti kompetentingos institucijos vertindamos didelių su IRT susijusių incidentų svarbą kitų valstybių narių jurisdikcijoms, ir pranešimų apie ***didelius*** su IRT susijusius incidentus duomenys, kuriais turi būti dalijamasi su kitomis kompetentingomis institucijomis pagal 17 straipsnio 5 ir 6 dalis.

3. Rengdamos 2 dalyje nurodytus bendrų techninių reguliavimo standartų projektus, EPI atsižvelgia į tarptautinius standartus, taip pat ENISA parengtas ir paskelbtas specifikacijas, įskaitant, kai tinkama, kitiems ekonomikos sektoriams skirtas specifikacijas. ***EPI taip pat atsižvelgia į tai, jog reikėtų, kad mažųjų ir labai mažų įmonių pastangų laiku ir veiksmingai valdyti incidentą neribotų būtinybė laikytis šiame straipsnyje nustatytų klasifikavimo reikalavimų. EPI taip pat atsižvelgia į finansų sektoriaus subjektų dydį, jų paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą bei jų bendrą rizikos pobūdį.***

EPI tuos bendrų techninių reguliavimo standartų projektus pateikia Komisijai iki [LB: prašom įrašyti datą – ***2 metai*** po įsigaliojimo dienos].

Komisijai suteikiami įgaliojimai papildyti šį reglamentą priimant šio straipsnio 2 dalyje nurodytus techninius reguliavimo standartus laikantis atitinkamų reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsnių.

17 straipsnis

Pranešimas apie didelius su IRT susijusius incidentus

1. Finansų sektoriaus subjektai praneša apie didelius su IRT susijusius incidentus atitinkamai 41 straipsnyje nurodytai kompetentingai institucijai per 3 dalyje nustatytus terminus.

Taikant pirmą pastraipą, finansų sektoriaus subjektai, surinkę ir išanalizavę visą

susijusią informaciją, parengia pranešimą apie incidentą naudodami 18 straipsnyje nurodytą šabloną ir pateikia jį kompetentingai institucijai.

Pranešime pateikiama visa informacija, būtina kompetentingai institucijai, kad ji galėtų nustatyti didelio su IRT susijusio incidento reikšmingumą ir įvertinti galimą tarpvalstybinį poveikį.

1a. Finansų sektoriaus subjektai gali savanoriškai pranešti atitinkamai kompetentingai institucijai apie dideles kibernetines grėsmes, kai mano, kad grėsmė yra svarbi finansų sistemai, paslaugų naudotojams ar klientams. Atitinkama kompetentinga institucija gali pateikti tokią informaciją kitoms atitinkamoms institucijoms pagal 5 dalį.

2. Kai ***įvyksta*** didelis su IRT susijęs incidentas ***ir jis turi reikšmingos įtakos*** paslaugų naudotojų ir klientų finansiniams interesams, finansų sektoriaus subjektai***, kai tik apie jį sužino,*** nepagrįstai nedelsdami informuoja savo paslaugų naudotojus ir klientus apie didelį su IRT susijusį incidentą ir ▌juos informuoja apie ***susijusias*** priemones, kurių imtasi tokio incidento neigiamam poveikiui sumažinti. ***Kai dėl finansų sektoriaus subjektų taikomų atsakomųjų priemonių žala paslaugų naudotojams ir klientams nepadaroma, reikalavimas informuoti paslaugų naudotojus ir klientus netaikomas.***

3. Finansų sektoriaus subjektai pateikia 41 straipsnyje nurodytai kompetentingai institucijai:

a) pradinį pranešimą ***apie didelį*** su IRT ***susijusį incidentą, kuriame pateikiama informacija, kurią dėdamas visas pastangas gali gauti pranešantysis subjektas, tokia tvarka:***

i) įvykus incidentui, kuris reikšmingai sutrikdo finansų sektoriaus subjekto teikiamų paslaugų prieinamumą, kompetentingai institucijai apie jį turi būti pranešama nedelsiant ir bet kuriuo atveju ne vėliau kaip per 24 valandas nuo tada, kai sužinoma apie incidentą;

ii) įvykus incidentui, kuris daro kitokį reikšmingą poveikį subjektui, tačiau ne to subjekto teikiamų paslaugų prieinamumui, kompetentingai institucijai apie jį turi būti pranešama nepagrįstai nedelsiant ir bet kuriuo atveju ne vėliau kaip per 72 valandas nuo tada, kai sužinoma apie incidentą;

iii) įvykus incidentui, kuris daro poveikį to finansų sektoriaus subjekto turimų asmens duomenų vientisumui, konfidencialumui ar saugumui, kompetentingai institucijai apie jį turi būti pranešama nedelsiant ir bet kuriuo atveju ne vėliau kaip per 24 valandas nuo tada, kai sužinoma apie incidentą;

b) tarpinį pranešimą***, kai pirminio incidento statusas reikšmingai pasikeičia arba paaiškėja nauja informacija, kuri galėtų turėti didelį poveikį tam, kaip kompetentinga institucija reaguos į su IRT susijusį incidentą***, po a punkte nurodyto pradinio pranešimo, vėliau, kai tinkama, teikiant atnaujintus pranešimus kiekvieną kartą, kai įvykdomas aktualus būklės atnaujinimas, 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

gaunama faktinių poveikio duomenų, kuriais galima pakeisti įverčius, bet ne vėliau kaip per vieną mėnesį nuo pradinio pranešimo išsiuntimo ***dienos;***

ca) jei c punkte nurodyto galutinio pranešimo pateikimo metu incidentas tebevyksta, galutinis pranešimas pateikiamas praėjus mėnesiui po to, kai incidentas pašalinamas.

41 straipsnyje nurodyta atitinkama kompetentinga institucija numato, kad tinkamai pagrįstais atvejais finansų sektoriaus subjektui leidžiama nukrypti nuo šios dalies a, b, c ir ca punktuose nustatytų terminų, tinkamai atsižvelgiant į finansų sektoriaus subjektų pajėgumą pateikti tikslią ir prasmingą informaciją apie didelius su IRT susijusius incidentus.

4. Finansų sektoriaus subjektai gali perduoti pareigas pranešti pagal šį straipsnį paslaugas teikiančiai trečiajai šaliai tik gavę 41 straipsnyje nurodytos atitinkamos kompetentingos institucijos leidimą šias pareigas perduoti. ***Tokio perdavimo atvejais finansų sektoriaus subjektas ir toliau lieka visiškai atskaitingas už pranešimo apie incidentus reikalavimų vykdymą.***

5. Gavusi 1 dalyje nurodytą pranešimą, kompetentinga institucija nepagrįstai nedelsdama pateikia išsamią informaciją apie ***didelį su IRT susijusį*** incidentą:

a) atitinkamai EBI, ESMA arba EIOPA;

b) atitinkamai ECB 2 straipsnio 1 dalies a, b ir c punktuose nurodytų finansų sektoriaus subjektų atveju; taip pat

c) pagal Direktyvos (ES) 2016/1148 8 straipsnį paskirtam bendrajam informaciniam punktui ***arba CSIRT, paskirtai pagal Direktyvos (ES) 2016/1149 9 straipsnį;***

ca) pertvarkymo institucijai, atsakingai už atitinkamą finansų sektoriaus subjektą, Bendrai pertvarkymo valdybai (BPV), jei subjektas priskiriamas prie Reglamento (ES) Nr. 806/2014 7 straipsnio 2 dalyje nurodytų subjektų arba Reglamento (ES) Nr. 806/2014 7 straipsnio 4 dalies b punkte ir 5 dalyje nurodytų subjektų ir grupių, kai tenkinamos tų dalių taikymo sąlygos;

cb) nacionalinėms pertvarkymo institucijoms, jei subjektas priskiriamas prie Reglamento (ES) Nr. 806/2014 7 straipsnio 3 dalyje nurodytų subjektų ir grupių. Nacionalinės pertvarkymo institucijos kas ketvirtį teikia BPV pagal šį punktą gautų pranešimų, susijusių su Reglamento (ES) Nr. 806/2014 7 straipsnio 3 dalyje nurodytais subjektais ir grupėmis, santrauką;

cc) kitoms atitinkamoms valdžios institucijoms, įskaitant kitų valstybių narių valdžios institucijas.

6. EBI, ESMA arba EIOPA ir ECB***, bendradarbiaudami su ENISA,*** įvertina didelio su IRT susijusio incidento svarbą kitoms atitinkamoms valdžios institucijoms ir apie tai kuo greičiau jas informuoja. ECB informuoja Europos centrinių bankų sistemos narius apie su mokėjimo sistema susijusias problemas. Remdamosi tuo pranešimu, kompetentingos institucijos atitinkamais atvejais nedelsdamos imasi visų būtinų priemonių, kad nebūtų sutrikdytas finansų sistemos stabilumas.

18 straipsnis

Pranešimų turinio ir šablonų derinimas

1. EPI, pasitarusios Jungtiniame komitete ir pasikonsultavusios su ENISA ir ECB, parengia:

   a) bendrų techninių reguliavimo standartų projektus, kad būtų:

      1) nustatytas pranešimų apie didelius su IRT susijusius incidentus turinys;

      2) patikslintos sąlygos, kuriomis finansų sektoriaus subjektai, gavę išankstinį kompetentingos institucijos patvirtinimą, gali pavesti paslaugas teikiančiai trečiajai šaliai šiame skyriuje nustatytas pareigas pranešti;

      3) išsamiau patikslinti kriterijai, pagal kuriuos nustatomas didelio su IRT susijusio incidento poveikis finansų sektoriaus subjektui, kai taikomas 17 straipsnio 3 dalies a punktas;

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

   EPI pateikia Komisijai 1 dalies a ***punkto pirmoje pastraipoje*** nurodytus bendrų techninių reguliavimo standartų projektus ir 1 dalies b ***punkto pirmoje pastraipoje*** nurodytus bendrų techninių įgyvendinimo standartų projektus iki 202x xx mėn. [LB: prašom įrašyti datą – ***2 metai*** po įsigaliojimo dienos].

   Komisijai suteikiami įgaliojimai papildyti šį reglamentą priimant šio straipsnio 1 dalies a ***punkto pirmoje pastraipoje*** nurodytus bendrus techninius reguliavimo standartus laikantis atitinkamų reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1095/2010 ir (ES) Nr. 1094/2010 10–14 straipsnių.

   Komisijai suteikiami įgaliojimai priimti šio straipsnio 1 dalies b ***punkto pirmoje pastraipoje*** nurodytus bendrus techninius įgyvendinimo standartus atitinkamai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1095/2010 ir (ES) Nr. 1094/2010 15 straipsnį.

2. Kol bus gautos 19 straipsnyje nurodytos galimybių ataskaitos dėl tolesnio pranešimų apie incidentus centralizavimo išvados, EPI, pasinaudodamos Jungtiniu komitetu ir bendradarbiaudamos su kompetentingomis institucijomis, ECB, BPV ir ENISA, parengia keitimosi informacija apie didelių su IRT susijusių incidentų pranešimus pagal 17 straipsnio 5 dalį gaires.

Pirmoje pastraipoje nurodytos gairės apima bent:

a) veiksmingiausias ryšių linijas;

b) duomenų, kuriais keičiamasi, saugumo, konfidencialumo ir vientisumo užtikrinimą;

c) galimą finansų sektoriaus subjektų dalyvavimą siekiant papildyti 40 straipsnyje nurodytą keitimąsi informacija.

19 straipsnis

Pranešimo apie didelius su IRT susijusius incidentus centralizavimas

1. EPI, pasitarusios Jungtiniame komitete ir 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. Ataskaitoje nagrinėjami būdai, kaip supaprastinti pranešimų apie su IRT susijusius incidentus, srautą, sumažinti susijusias išlaidas ir prisidėti prie teminės analizės, siekiant didinti priežiūros konvergenciją.

2. 1 dalyje nurodytą ataskaitą sudaro bent šie elementai:

   a) išankstinės tokio ***bendrojo*** ES centro įsteigimo sąlygos;

   b) nauda, apribojimai ir galima rizika;

   ba) galimybės užtikrinti sąveikumą ir įvertinti jo pridėtinę vertę, atsižvelgiant į kitas atitinkamas pranešimų teikimo sistemas, numatytas, pvz., Direktyvoje (ES) 2016/1148;

   c) operacijų valdymo elementai;

   d) narystės sąlygos;

   e) finansų sektoriaus subjektų ir nacionalinių kompetentingų institucijų prieigos prie ***bendrojo*** ES centro sąlygos;

   f) preliminarus finansinių išlaidų, susijusių su ***bendrojo*** ES centro veiklos platformos sukūrimu, įskaitant būtiną kompetenciją, įvertinimas.

3. EPI pateikia 1 dalyje nurodytą ataskaitą Komisijai, Europos Parlamentui ir Tarybai iki 202x m. xx mėn. [OL: prašom įrašyti datą – 3 metai po įsigaliojimo dienos].

20 straipsnis

Priežiūros grįžtamoji informacija

1. Gavusi 17 straipsnio 1 dalyje nurodytą pranešimą, kompetentinga institucija patvirtina, kad pranešimą gavo, ir kuo skubiau pateikia finansų sektoriaus subjektui visą būtiną grįžtamąją informaciją arba rekomendacijas, kad visų pirma būtų aptartos taisomosios priemonės subjekto lygmeniu arba būdai sumažinti neigiamą poveikį įvairiuose sektoriuose, ***taip pat teikia atitinkamai anonimizuotus atsiliepimus, įžvalgas ir žvalgybos informaciją visiems atitinkamiems finansų sektoriaus subjektams, kai tai gali būti naudinga, remdamasi bet kokiais gautais pranešimais apie didelius su IRT susijusius incidentus***.

2. EPI per Jungtinį komitetą kasmet teikia anonimišką ir apibendrintą informaciją apie iš kompetentingų institucijų gautus pranešimus apie ***didelius*** su IRT susijusius incidentus, nurodydamos bent su IRT susijusių didelių incidentų skaičių, pobūdį, poveikį finansų sektoriaus subjektų ar klientų veiklai, ***apskaičiuotas*** išlaidas ir taisomuosius veiksmus, kurių buvo imtasi.

   EPI skelbia įspėjimus ir rengia aukšto lygio statistinius duomenis, kurie naudojami vertinant IRT grėsmes ir pažeidžiamumą.

20a straipsnis

Mokėjimų veiklos arba saugumo incidentai, susiję su tam tikrais finansų sektoriaus subjektais

Šiame skyriuje nustatyti reikalavimai taikomi mokėjimų veiklos ar saugumo incidentams ir dideliems mokėjimų veiklos ar saugumo incidentams, kai jie yra susiję su 2 straipsnio 1 dalies a, b ir c punktuose nurodytais finansų sektoriaus subjektais.

IV SKYRIUS

SKAITMENINĖS VEIKLOS ATSPARUMO TESTAVIMAS

21 straipsnis

Bendrieji skaitmeninės veiklos atsparumo testavimo reikalavimai

1. Siekdami įvertinti pasirengimą su IRT susijusiems incidentams, identifikuoti skaitmeninės veiklos atsparumo silpnąsias vietas, trūkumus ar spragas ir skubiai imtis taisomųjų priemonių, finansų sektoriaus subjektai***, išskyrus labai mažas įmones,*** parengia, taiko ir atnaujina patikimą ir išsamią skaitmeninės veiklos atsparumo testavimo programą, kaip neatsiejamą 5 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 22 ir 23 straipsnių nuostatas.

3. Finansų sektoriaus subjektai, vykdydami 1 dalyje nurodytą skaitmeninės veiklos atsparumo testavimo programą, vadovaujasi rizika grindžiamu metodu, atsižvelgdami į besikeičiančią IRT rizikos aplinką, bet kokią konkrečią riziką, gresiančią ar galinčią grėsti finansų sektoriaus subjektui, informacinio turto ir teikiamų paslaugų ypatingą svarbą, taip pat visus kitus veiksnius, kuriuos finansų sektoriaus subjektas laiko tinkamais.

4. Finansų sektoriaus subjektai užtikrina, kad testavimą atliktų nepriklausomos vidaus ar išorės šalys. ***Kai testavimą atlieka vidaus testuotojas, finansų sektoriaus subjektai skiria pakankamai išteklių ir užtikrina, kad per visą testavimo rengimo ir vykdymo etapų laikotarpį būtų išvengta interesų konfliktų.***

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

6. Finansų sektoriaus subjektai ***užtikrina, kad tinkamas*** visų ypatingos svarbos IRT sistemų ir programų ***testavimas būtų atliktas*** bent kartą per metus.

22 straipsnis

IRT priemonių ir sistemų testavimas

1. 21 straipsnyje nurodytoje skaitmeninės veiklos atsparumo testavimo programoje numatoma atlikti visus tinkamus testus.

Tie testai gali būti pažeidžiamumo vertinimas ir skenavimas, atvirojo kodo analizė, tinklo saugumo vertinimai, spragų analizavimas, fizinio saugumo patikrinimai, klausimynai ir skenavimo programinės įrangos sprendimai, pirminio kodo patikrinimai, jei įmanoma, scenarijais grindžiami testai, suderinamumo testavimas, veiklos efektyvumo testavimas, ištisinio srauto (angl. *end-to-end*) testavimas arba skverbimosi testavimas.

2. 2 straipsnio 1 dalies f ir g punktuose nurodyti finansų sektoriaus subjektai atlieka pažeidžiamumo vertinimą prieš įdiegdami ar pakartotinai įdiegdami naujas ar esamas

paslaugas, palaikančias finansų sektoriaus subjekto ypatingos svarbos funkcijas, programas ir infrastruktūros komponentus.

23 straipsnis

Pažangus IRT priemonių, sistemų ir procesų testavimas, taikant grėsmėmis grindžiamą skverbimosi testavimą

1. Finansų sektoriaus subjektai, nustatyti pagal 3 ***dalies antrą pastraipą***, bent kas trejus metus atlieka pažangų testavimą, taikydami grėsmėmis grindžiamą skverbimosi testavimą.

2. Grėsmėmis grindžiamas skverbimosi testavimas apima bent finansų sektoriaus subjekto ypatingos svarbos ***ir svarbias*** funkcijas bei paslaugas ir yra taikomas tokias funkcijas palaikančioms tikralaikėms produkcijos sistemoms, ***kai įmanoma, arba tokios pačios saugumo konfigūracijos parengiamosios veiksenos sistemoms***. Tikslią grėsmėmis grindžiamo skverbimosi testavimo apimtį nustato finansų sektoriaus subjektai, atsižvelgdami į ypatingos svarbos ***ir svarbių*** funkcijų ir paslaugų vertinimą, ir tvirtina kompetentingos institucijos. ***Nereikalaujama, kad vienas*** grėsmėmis grindžiamas skverbimosi testavimas ***apimtų visas ypatingos svarbos ar svarbias funkcijas.***

   Taikant pirmą pastraipą, finansų sektoriaus subjektai identifikuoja visus atitinkamus pagrindinius IRT procesus, sistemas ir technologijas, kuriais palaikomos ypatingos svarbos ***ar svarbios*** funkcijos ir paslaugos, įskaitant ***ypatingos svarbos ir svarbias*** funkcijas ir paslaugas, kurios perduotos arba pagal susitarimus patikėtos vykdyti IRT paslaugas teikiančioms trečiosioms šalims.

   Kai grėsmėmis grindžiamas skverbimosi testavimas apima ***ypatingos svarbos*** IRT paslaugas teikiančias trečiąsias šalis ***ir, kai būtina, ne ypatingos svarbos IRT paslaugas teikiančias trečiąsias šalis***, finansų sektoriaus subjektas imasi priemonių, būtinų šių paslaugų teikėjų dalyvavimui užtikrinti. ***Tos IRT paslaugas teikiančios trečiosios šalys neprivalo perduoti informacijos ar pateikti išsamios informacijos apie elementus, kurie nėra susiję su atitinkamų finansų sektoriaus subjektų atitinkamų ypatingos svarbos ar svarbių funkcijų rizikos valdymo kontrolės priemonėmis. Toks testavimas nedaro neigiamos įtakos kitiems IRT paslaugas teikiančių trečiųjų šalių klientams.***

   Kai IRT paslaugas teikiančios trečiosios šalies dalyvavimas grėsmėmis grindžiamame skverbimosi testavime galėtų turėti įtakos IRT paslaugas teikiančios trečiosios šalies paslaugų kitiems klientams, kuriems netaikomas šis reglamentas, kokybei, konfidencialumui ar saugumui ar bendram IRT paslaugas teikiančios trečiosios šalies operacijų vientisumui, finansų sektoriaus subjektas ir IRT paslaugas teikianti trečioji šalis gali sutartimi įformindami susitarimą susitarti, kad IRT paslaugas teikiančiai trečiajai šaliai leidžiama tiesiogiai sudaryti sutartimi įformintą susitarimą su išorės testuotoju. IRT paslaugas teikiančios trečiosios šalys gali sudaryti tokius susitarimus visų savo klientų, kurie yra finansų sektoriaus subjektai, vardu, kad būtų galima atlikti bendrą testavimą.

   Finansų sektoriaus subjektai taiko veiksmingas rizikos valdymo kontrolės priemones, kad sumažintų bet kokio galimo poveikio paties finansų sektoriaus subjekto, jo sandorio šalių ar finansų sektoriaus duomenims riziką, žalą jų turtui ir ypatingos svarbos ***ar svarbių funkcijų*** ar operacijų sutrikdymo riziką.

   Testavimo pabaigoje, susitarus dėl ataskaitų ir koregavimo planų, finansų sektoriaus

subjektas ir išorės testuotojai pateikia ***bendrai viešojo sektoriaus valdžios institucijai, paskirtai pagal 3a dalį, arba, jei IRT paslaugas teikiančios trečiosios šalys sudaro sutartimi įformintus susitarimus su išorės testuotojais tiesiogiai, ENISA konfidencialią testavimo rezultatų santrauką ir*** dokumentus, patvirtinančius, kad grėsmėmis grindžiamas skverbimosi testavimas buvo atliktas laikantis reikalavimų. ***Atitinkamai bendra viešojo sektoriaus valdžios institucija arba ENISA*** išduoda pažymą***, kuria patvirtinama, kad testavimas buvo atliktas laikantis dokumentuose pateiktų reikalavimų, kad kompetentingos institucijos galėtų abipusiai pripažinti grėsmėmis grindžiamus skverbimosi testus***. ***Pažymomis dalijamasi su finansų sektoriaus subjekto kompetentinga institucija ir, kai tikslinga, su ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies atsakingąja priežiūros institucija.***

3. Finansų sektoriaus subjektai ***arba IRT paslaugas teikiančios trečiosios šalys, kurioms leidžiama tiesiogiai sudaryti sutartimi įformintus susitarimus su išorės testuotoju pagal šio straipsnio 2 dalį,*** sudaro sutartis su testuotojais pagal 24 straipsnį, kad būtų galima atlikti grėsme grindžiamą skverbimosi testavimą.

Nedarant poveikio jų galimybei perduoti užduotis ir kompetenciją pagal šį straipsnį kitoms kompetentingoms institucijoms, atsakingoms už grėsmėmis grindžiamą skverbimosi testavimą, kompetentingos institucijos ***proporcingai*** identifikuoja finansų sektoriaus subjektus, turinčius atlikti grėsmėmis grindžiamą skverbimosi testavimą, ▌įvertinusios:

a) su poveikiu susijusius veiksnius, visų pirma, finansų sektoriaus subjekto teikiamų paslaugų ir vykdomos veiklos ypatingą svarbą;

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

c) finansų sektoriaus subjekto konkretų IRT rizikos pobūdį ir IRT brandą arba susijusias technologijų ypatybes.

3a. Valstybės narės paskiria bendrą viešojo sektoriaus valdžios instituciją, atsakingą už grėsme grindžiamą skverbimosi testavimą finansų sektoriuje nacionaliniu lygmeniu, išskyrus finansų sektoriaus subjektų identifikavimą pagal 3 dalį, bet įskaitant grėsmėmis grindžiamą skverbimosi testavimą, kurį atlieka finansų sektoriaus subjektai ir IRT paslaugas teikiančios trečiosios šalys, tiesiogiai sudariusios sutartimi įformintus susitarimus su išorės testuotojais. Paskirtai bendrai viešojo sektoriaus valdžios institucijai šiuo tikslu pavedama visa kompetencija ir užduotys.

4. ***EPI, koordinuodamos savo veiksmus su ENISA,*** pasikonsultavusios su ECB ir atsižvelgdamos į atitinkamas Sąjungos sistemas, taikomas žvalgybos informacija ***ir grėsmėmis*** grindžiamiems skverbimosi testams***, įskaitant TIBER-EU sistemą***, parengia ***vieną*** techninių reguliavimo standartų projektų ***rinkinį***, ***kuriame*** patikslinami:

a) kriterijai, naudojami taikant šio straipsnio ***3 dalies antrą pastraipą***;

b) reikalavimai, taikomi:

i) šio straipsnio 2 dalyje nurodyto grėsmėmis grindžiamo skverbimosi testavimo apimčiai;

ii) testavimo metodikai ir metodui, kurį reikia taikyti kiekvienu konkrečiu testavimo proceso etapu;

iii) testavimo rezultatams, užbaigimui ir koregavimo etapams;

c) kokios rūšies bendradarbiavimas priežiūros srityje yra reikalingas įgyvendinant finansų sektoriaus subjektų, vykdančių veiklą daugiau nei vienoje valstybėje narėje, grėsmėmis grindžiamą skverbimosi testavimą ***ir išorės testuotojų, kurie sudaro tiesioginius sutartimi įformintus susitarimus su IRT paslaugas teikiančiomis trečiosiomis šalimis pagal šio straipsnio 2 dalį, atliekamą testavimą ir siekiant palengvinti visapusišką abipusį pripažinimą,*** kad būtų sudarytos sąlygos tinkamo lygio priežiūros institucijų dalyvavimui ir lanksčiam įgyvendinimui, siekiant atsižvelgti į finansų pasektorių arba vietos finansų rinkų specifiką.

EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai iki [OL: prašom įrašyti datą – ***6 mėnesiai*** iki įsigaliojimo dienos].

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

24 straipsnis

Reikalavimai testuotojams

1. Finansų sektoriaus subjektai ***ir IRT paslaugas teikiančios trečiosios šalys, kurioms leidžiama tiesiogiai sudaryti sutartimi įformintus susitarimus su išorės testuotoju pagal 23 straipsnio 2 dalį,*** grėsmėmis grindžiamam skverbimosi testavimui atlikti pasitelkia tik tuos testuotojus, kurie:

a) yra patys tinkamiausi ir geriausios reputacijos;

b) turi techninių ir organizacinių pajėgumų ir įrodo turintys specialios patirties žvalgybos informacijos apie grėsmes, skverbimosi testavimo ar raudonosios komandos testavimo srityje;

c) yra valstybėje narėje sertifikuoti akreditavimo įstaigos arba laikosi oficialių elgesio kodeksų ar etikos sistemų ***nepriklausomai nuo to, ar testuotojai yra iš Sąjungos ar trečiosios valstybės***;

d) ▌pateikia nepriklausomą patikinimą arba audito ataskaitą dėl patikimo rizikos, susijusios su grėsmėmis grindžiamo skverbimosi testavimo vykdymu, 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***;***

ea) jei naudojamasi vidaus testuotojų paslaugomis, jas patvirtino atitinkama kompetentinga institucija ir bendra viešojo sektoriaus valdžios institucija, paskirta pagal 23 straipsnio 3a dalį, ir tos institucijos patikrino, ar finansų sektoriaus subjektas skyrė pakankamai išteklių ir užtikrino, kad visu testavimo rengimo ir vykdymo etapų laikotarpiu būtų išvengta interesų konfliktų.

2. Finansų sektoriaus subjektai ***ir IRT paslaugas teikiančios trečiosios šalys, kurioms leidžiama tiesiogiai sudaryti sutartimi įformintus susitarimus su išorės testuotoju pagal 23 straipsnio 2 dalį,*** užtikrina, kad su išorės testuotojais sudarytuose

susitarimuose būtų reikalaujama patikimai valdyti grėsmėmis grindžiamo skverbimosi testavimo rezultatus ir juos tvarkant, įskaitant bet kokį sukūrimą, projektą, saugojimą, apibendrinimą, ataskaitą, pranešimą ar sunaikinimą, nekelti rizikos finansų sektoriaus subjektui.

V SKYRIUS

TREČIOSIOS ŠALIES KELIAMOS IRT RIZIKOS VALDYMAS

I SKIRSNIS

PAGRINDINIAI PATIKIMO TREČIOSIOS ŠALIES KELIAMOS IRT RIZIKOS VALDYMO PRINCIPAI

25 straipsnis

Bendrieji principai

Finansų sektoriaus subjektai valdo trečiosios šalies keliamą IRT riziką kaip neatsiejamą savo IRT rizikos valdymo sistemos IRT rizikos komponentą, laikydamiesi šių principų:

1. Finansų sektoriaus subjektai, kurie yra sudarę sutartimi įformintus susitarimus dėl IRT paslaugų naudojimo savo verslo operacijoms vykdyti, visada išlieka visiškai atsakingi už visų šiame reglamente ir galiojančiuose finansinių paslaugų srities teisės aktuose nustatytų pareigų laikymąsi ir vykdymą.

2. Finansų sektoriaus subjektų trečiosios šalies keliamos IRT rizikos valdymas atliekamas taikant proporcingumo principą, atsižvelgiant į:

   a) priklausomybės nuo IRT ***pobūdį,*** mastą, sudėtingumą ir svarbą,

   b) 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 ar svarbumą, taip pat į galimą poveikį finansinių paslaugų ir veiklos tęstinumui ir kokybei individualiu ir grupės lygmeniu***;***

   ba) tai, ar IRT paslaugų teikėjas yra IRT paslaugų grupės viduje teikėjas.

3. Taikydami IRT rizikos valdymo sistemą, finansų sektoriaus subjektai***, išskyrus labai mažas įmones,*** priima ir reguliariai peržiūri trečiosios šalies keliamos IRT rizikos strategiją . Ta strategija apima IRT paslaugas teikiančių trečiųjų šalių teikiamų IRT paslaugų naudojimo politiką ir taikoma individualiu ir atitinkamai iš dalies konsoliduotu ir konsoliduotu pagrindu. Valdymo organas reguliariai peržiūri nustatytą riziką, susijusią su ypatingos svarbos ar svarbių funkcijų ranga.

4. Taikydami IRT rizikos valdymo sistemą, finansų sektoriaus subjektai tvarko ir atnaujina subjektų lygmeniu ir iš dalies konsoliduotu bei konsoliduotu lygmenimis informacijos registrą, skirtą visiems sutartimi įformintiems susitarimams dėl ***ypatingos svarbos ar svarbias funkcijas palaikančias*** IRT paslaugas teikiančių trečiųjų šalių teikiamų IRT paslaugų naudojimo.

   Pirmoje pastraipoje nurodyti sutartimi įforminti susitarimai tinkamai dokumentuojami .

   Jei įmanoma, finansų sektoriaus subjektai vadovaujasi EPI ir kompetentingų institucijų paskelbtomis gairėmis ir kitomis priemonėmis, kol įsigalios 10 dalyje nurodyti techniniai įgyvendinimo standartai.

   Finansų sektoriaus subjektai ne rečiau kaip kartą per metus kompetentingoms

institucijoms pateikia informaciją apie naujų susitarimų dėl ***ypatingos svarbos ar svarbias funkcijas palaikančių*** IRT paslaugų naudojimo skaičių, 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 planuojamą sutarčių dėl ypatingos svarbos ar svarbių funkcijų sudarymą ir apie tai, kada funkcija tampa ypatingos svarbos ar svarbi.

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

   a) įvertina, ar sutartimi įformintas susitarimas taikomas ypatingos svarbos ar svarbiai funkcijai;

   b) įvertina, ar įvykdytos sutarčių sudarymo priežiūros sąlygos;

   c) identifikuoja ir įvertina visą atitinkamą riziką, susijusią su sutartimi įformintu susitarimu, įskaitant galimybę, kad tokiais sutartimi įformintais susitarimais gali būti prisidedama prie IRT koncentracijos rizikos padidinimo;

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

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

6. Finansų sektoriaus subjektai gali sudaryti sutartimi įformintus susitarimus tik su tomis IRT paslaugas teikiančiomis trečiosiomis šalimis, kurios laikosi aukštų, tinkamų ir ***atnaujintų*** informacijos saugumo standartų. ***Nustatant, ar taikomi saugumo standartai yra tinkami, taip pat atsižvelgiama į naujausius standartus.***

7. Naudodamiesi prieigos, patikrinimo ir audito teisėmis IRT paslaugas***, susijusias su ypatingos svarbios ar svarbiomis funkcijomis,*** teikiančios trečiosios šalies atžvilgiu, finansų sektoriaus subjektai, taikydami rizika grindžiamą metodą, iš anksto nustato audito ir patikrinimų dažnumą bei audituotinas sritis pagal visuotinai pripažintus audito standartus, atitinkančius priežiūros institucijų nurodymus dėl tokių audito standartų naudojimo ir integravimo.

   Sutartimi įformintų susitarimų, kuriems būdingas ***detalizuotas*** technologinis sudėtingumas, atveju finansų sektoriaus subjektas patikrina, ar auditoriai (vidaus auditoriai, auditorių grupė ar išorės auditoriai) turi tinkamų įgūdžių ir žinių, kad galėtų veiksmingai atlikti atitinkamą auditą ir vertinimą.

8. Finansų sektoriaus subjektai užtikrina, kad pagal sutartimi įformintus susitarimus dėl IRT paslaugų naudojimo ***finansų sektoriaus subjektai galėtų imtis tinkamų taisomųjų ar koregavimo priemonių, kurios galėtų apimti visišką susitarimų nutraukimą, jei jų pakeisti neįmanoma, arba dalinį susitarimų nutraukimą, jei juos galima pakeisti, pagal taikytiną teisę*** bent šiomis aplinkybėmis:

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

aa) bendras priežiūros organas pateikia rekomendaciją pagal 37 straipsnį ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai;

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

c) jei įrodoma, kad bendras IRT paslaugas teikiančios trečiosios šalies IRT rizikos valdymas turi trūkumų, ***būdingų jo sutarčiai su finansų sektoriaus subjektu ir*** visų pirma susijusių su tuo, kaip užtikrinamas konfidencialių, asmens ar kitų neskelbtinų duomenų ar ne asmens duomenų saugumas ir vientisumas;

d) aplinkybėmis, kai kompetentinga institucija ***įrodo, kad ji*** nebegali veiksmingai prižiūrėti finansų sektoriaus subjekto dėl atitinkamo sutartimi įforminto susitarimo.

8a. Siekdami sumažinti sutrikimų riziką finansų sektoriaus subjekto lygmeniu, tinkamai pagrįstomis aplinkybėmis ir susitarę su savo kompetentingomis institucijomis, finansų sektoriaus subjektai gali nuspręsti nenutraukti sutartimi įforminto susitarimo su IRT paslaugas teikiančia trečiąja šalimi, kol jie negali pakeisti IRT paslaugas teikiančios trečiosios šalies arba pasinaudoti subjekto vidaus sprendimais, atitinkančiais teikiamos paslaugos sudėtingumą, laikydamiesi 9 dalyje nurodytos pasitraukimo strategijos.

8b. Tais atvejais, kai sutartimi įforminti susitarimai su IRT paslaugas teikiančiomis trečiosiomis šalimis nutraukiami dėl kurios nors iš 8 dalies a–d punktuose išvardytų aplinkybių, finansų sektoriaus subjektai nepadengia IRT paslaugas teikiančios trečiosios šalies duomenų perkėlimo išlaidų, jei toks perkėlimas viršija pirminėje sutartyje numatytas duomenų perkėlimo išlaidas.

9. ***IRT paslaugų, susijusių su ypatingos svarbos arba svarbiomis funkcijomis, atveju*** finansų sektoriaus subjektai nustato pasitraukimo strategijas***, kurios periodiškai peržiūrimos***. ***Pasitraukimo strategijos nustatomos taip***, kad būtų atsižvelgta į riziką, kuri gali kilti IRT paslaugas teikiančios trečiosios šalies lygmeniu, visų pirma į galimą pastarosios žlugimą, vykdomų funkcijų kokybės pablogėjimą, bet kokį verslo sutrikdymą dėl netinkamo paslaugų teikimo ar jų neteikimo arba reikšmingos rizikos, gresiančios tinkamam ir nuolatiniam funkcijos vykdymui***, arba nutraukus sutartimi įformintą susitarimą su IRT paslaugas teikiančia trečiąja šalimi, kai atsiranda kuri nors iš 8 dalies a–d punktuose 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 yra išsamūs, pagrįsti dokumentais ir prireikus pakankamai išbandyti.

Finansų sektoriaus subjektai identifikuoja alternatyvius sprendimus ir parengia pereinamojo laikotarpio planus, kad galėtų perimti sutartimi perduotas funkcijas 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 imasi tinkamų nenumatytų atvejų priemonių, kad užtikrintų veiklos tęstinumą visomis pirmoje pastraipoje nurodytomis aplinkybėmis.

10. EPI Jungtiniame komitete parengia techninių įgyvendinimo standartų projektus, pagal kuriuos nustatomi standartiniai šablonai, skirti 4 dalyje nurodytam informacijos registrui.

EPI tuos techninių įgyvendinimo standartų projektus pateikia Komisijai iki [OL: prašom įrašyti datą – 1 metai po šio reglamento įsigaliojimo dienos].

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

11. EPI Jungtiniame komitete parengia reguliavimo standartų projektus, kuriuose patikslina:

a) 3 dalyje nurodytos politikos, taikomos sutartimi įformintiems susitarimais dėl IRT paslaugas teikiančių trečiųjų šalių teikiamų IRT paslaugų naudojimo, išsamų turinį, pateikiant nuorodas į pagrindinius atitinkamų susitarimų dėl IRT paslaugų naudojimo gyvavimo ciklo etapus;

b) informacijos, kurią reikia įtraukti į 4 dalyje nurodytą informacijos registrą, rūšis.

EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai iki [LB: prašom įrašyti datą – ***18 mėnesių*** po įsigaliojimo dienos].

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

26 straipsnis

Išankstinis IRT koncentracijos rizikos ir papildomų subrangos susitarimų vertinimas

1. Identifikuodami ir vertindami IRT koncentracijos riziką, kaip nurodyta 25 straipsnio 5 dalies c punkte, finansų sektoriaus subjektai atsižvelgia į tai, ar sudarius sutartimi įformintą susitarimą dėl ***ypatingos svarbos ar svarbias funkcijas palaikančių*** IRT paslaugų:

a) būtų sudarytas susitarimas su IRT paslaugas teikiančia trečiąja šalimi, kuri nėra lengvai pakeičiama, arba

b) atsirastų keli sutartimi įforminti susitarimai dėl ***ypatingos svarbos ar svarbias funkcijas palaikančių*** IRT paslaugų 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, susitarimo su skirtingomis IRT paslaugas teikiančiomis trečiosiomis šalimis, naudą ir išlaidas, atsižvelgdami į tai, ar ir kaip numatyti sprendimai atitinka jų skaitmeninio atsparumo strategijoje nustatytus verslo poreikius ir tikslus.

2. Kai sutartimi įformintame susitarime dėl ***ypatingos svarbos ar svarbias funkcijas***

palaikančių IRT paslaugų naudojimo yra numatyta galimybė IRT paslaugas teikiančiai trečiajai šaliai papildomai sudaryti subrangos sutartis dėl ypatingos svarbos arba svarbios funkcijos su kitomis IRT paslaugas teikiančiomis trečiosiomis šalimis, finansų sektoriaus subjektai įvertina naudą ir riziką, galinčias atsirasti dėl tokių galimų subrangos sutarčių ▌.

Kai sutartimi įforminti susitarimai dėl ***ypatingos svarbos ar svarbias funkcijas palaikančių*** IRT paslaugų naudojimo sudaromi su ▌IRT paslaugas teikiančia trečiąja šalimi, finansų sektoriaus subjektai laiko svarbiais bent šiuos veiksnius:

a) ▌

b) ▌

c) nemokumo teisės nuostatas, taikytinas IRT paslaugas teikiančios trečiosios šalies bankroto atveju; ***taip pat***

d) bet kokius suvaržymus, galinčius atsirasti skubaus finansų sektoriaus subjekto duomenų atkūrimo atveju.

Kai sutartimi įforminti susitarimai dėl ypatingos svarbos ar svarbias funkcijas palaikančių IRT paslaugų naudojimo sudaromi su trečiojoje valstybėje įsisteigusia IRT paslaugas teikiančia trečiąja šalimi, finansų sektoriaus subjektai, be pirmoje ir antroje pastraipose paminėtų veiksnių, taip pat laiko svarbiais šiuos veiksnius:

i) Sąjungos duomenų apsaugos taisyklių laikymąsi ir

ii) veiksmingą šiame reglamente nustatytų taisyklių vykdymo užtikrinimą.

Kai tokie sutartimi įforminti susitarimai apima ypatingos svarbos arba svarbių funkcijų subrangą, finansų sektoriaus subjektai įvertina, ar ir kaip galimai ilgos ar sudėtingos subrangos grandinės gali turėti įtakos jų gebėjimui visapusiškai ***įvertinti antroje ir trečioje pastraipose išvardytus veiksnius, siekiant*** stebėti pagal sutartį perduotas funkcijas***,*** ir kompetentingos institucijos gebėjimui šiuo atžvilgiu veiksmingai prižiūrėti finansų sektoriaus subjektą.

27 straipsnis

Pagrindinės sutartinės nuostatos

1. Finansų sektoriaus subjekto ir IRT paslaugas teikiančios trečiosios šalies teisės ir pareigos aiškiai paskirstomos ir išdėstomos raštu. Visa sutartis, apimanti paslaugų lygio susitarimus, išdėstoma ***raštu*** dokumente, kurį šalys gali gauti popierine arba atsisiunčiama ir prieinama forma.

2. ***Finansų sektoriaus subjektai ir IRT paslaugas teikiančios trečiosios šalys užtikrina, kad*** sutartimi įformintuose IRT paslaugų naudojimo susitarimuose ***būtų*** nurodyta bent::

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

b) vietos, ***konkrečiai regionai ar valstybės***, kuriose turi būti teikiamos pagal sutartį arba subrangos sutartį vykdomos ***IRT*** funkcijos ir paslaugos ir kuriose 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***, įskaitant asmens duomenis,*** pasiekiamumo, prieinamumo, vientisumo, saugumo***, konfidencialumo*** ir apsaugos;

ca) 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 nutraukimo atveju ***arba sutartimi įforminto susitarimo nutraukimo atveju***;

d) 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 atlikti veiksmingą stebėseną ir nepagrįstai nedelsdamas imtis tinkamų taisomųjų veiksmų, kai sutartas paslaugų lygis neužtikrinamas;

e) ▌

f) IRT paslaugas teikiančios trečiosios šalies pareiga teikti ***su teikiama paslauga susijusią*** pagalbą IRT incidento atveju be papildomo mokesčio arba už iš anksto nustatytą mokestį;

g) reikalavimai IRT paslaugas teikiančiai trečiajai šaliai įgyvendinti ir išbandyti nenumatytų veiklos atvejų planus ir taikyti IRT saugumo priemones ir politiką, kuriomis ▌užtikrinama, kad finansų sektoriaus subjektas ***pakankamai*** saugiai teiktų paslaugas, laikydamasis taikytinos reguliavimo sistemos;

h) ▌

i) IRT paslaugas teikiančios trečiosios šalies pareiga visapusiškai bendradarbiauti su finansų sektoriaus subjekto kompetentingomis institucijomis ir pertvarkymo institucijomis, įskaitant jų paskirtus asmenis;

j) sutarties nutraukimo teisės ir susijęs minimalus įspėjimo apie sutarties nutraukimą terminas, atsižvelgiant į kompetentingų ***ir pertvarkymo*** institucijų lūkesčius ***ir, kai tas sutartimi įformintas susitarimas daro poveikį tos pačios grupės vidaus IRT paslaugų teikėjui, analizę pagal rizika grindžiamą metodą;***

k) pasitraukimo strategijos, visų pirma nustatytą privalomą pakankamos trukmės pereinamąjį laikotarpį:

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

ii) per kurį finansų sektoriaus subjektas gali pakeisti IRT paslaugas teikiančią trečiąją šalį arba pasirinkti vietoje taikomus sprendimus, atitinkančius teikiamos paslaugos sudėtingumą***;***

iia) jeigu sutartimi įformintas susitarimas daro poveikį tos pačios grupės vidaus IRT paslaugų teikėjui, jis analizuojamas taikant rizika grindžiamą metodą;

ka) nuostata dėl IRT paslaugas teikiančios trečiosios šalies atliekamo asmens duomenų tvarkymo, kuris turi atitikti Reglamentą (ES) 2016/679.

2a. Be 2 dalyje išdėstytų nuostatų, sutartimi įforminti susitarimai dėl ypatingos svarbos

arba svarbių funkcijų vykdymo apima bent:

a) IRT paslaugas teikiančios trečiosios šalies įspėjimo terminus ir pareigas pranešti finansų sektoriaus subjektui, įskaitant pranešimą apie bet kokius pokyčius, kurie gali turėti reikšmingos įtakos IRT paslaugas teikiančios trečiosios šalies gebėjimui veiksmingai vykdyti ypatingos svarbos arba svarbias funkcijas užtikrinant sutartą paslaugų lygį;

b) teisę nuolat stebėti IRT paslaugas teikiančios trečiosios šalies veiklos efektyvumą, įskaitant:

i) finansų sektoriaus subjekto arba paskirtos trečiosios šalies prieigos, patikrinimo ir audito teises bei teisę peržiūrėti atitinkamų dokumentų kopijas vietoje, jeigu jie turi ypatingą svarbą IRT paslaugas teikiančios trečiosios šalies operacijoms, – veiksmingai naudotis šiomis teisėmis netrukdo ir 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 įsipareigojimą visapusiškai bendradarbiauti kompetentingoms institucijoms, atsakingajai priežiūros institucijai, finansų sektoriaus subjektui arba paskirtai trečiajai šaliai atliekant patikrinimus ir auditą vietoje ir išsamią informaciją apie tokių patikrinimų ir audito apimtį, sąlygas ir dažnumą.

Nukrypstant nuo b punkto, IRT paslaugas teikianti trečioji šalis ir finansų sektoriaus subjektas gali susitarti, kad prieigos, patikrinimo ir audito teisės gali būti perduotos IRT paslaugas teikiančios trečiosios šalies paskirtam nepriklausomam trečiajam asmeniui ir kad finansų sektoriaus subjektas bet kuriuo metu gali prašyti to trečiojo asmens pateikti informaciją ir patikinimą apie IRT paslaugas teikiančios trečiosios šalies veiklos efektyvumą.

2b. Be šio straipsnio 2 ir 2a dalyse išdėstytų nuostatų, sutartimi įforminti susitarimai dėl trečiojoje valstybėje įsisteigusios ir paskirtos ypatingos svarbos paslaugų teikėju pagal 28 straipsnio 9 dalį IRT paslaugas teikiančios trečiosios šalies IRT paslaugų teikimo:

a) nustato, kad sutarčiai taikoma valstybės narės teisė; taip pat

b) užtikrina, kad bendras priežiūros organas ir atsakingoji priežiūros institucija galėtų vykdyti savo pareigas, nurodytas 30 straipsnyje, pagal savo kompetenciją, nustatytą 31 straipsnyje.

Nereikalaujama, kad paslaugas, dėl kurių sudaromi sutartimi įforminti susitarimai, teiktų įmonė, Sąjungoje įsisteigusi pagal valstybės narės teisę.

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

3a. Kompetentingos institucijos turi turėti galimybę susipažinti su šiame straipsnyje nurodytais sutartimi įformintais susitarimais. Tų sutartimi įformintų susitarimų šalys, prieš suteikdamos tokią prieigą kompetentingoms institucijoms, gali susitarti pašalinti neskelbtiną komercinę informaciją arba konfidencialią informaciją, jei

kompetentingos institucijos visapusiškai informuojamos apie pašalinimo mastą ir pobūdį.

4. EPI Jungtiniame komitete parengia techninių reguliavimo standartų projektus, kuriuose patikslinami elementai, kuriuos turi nustatyti ir įvertinti finansų sektoriaus subjektas, sudarydamas subrangos sutartis dėl ypatingos svarbos ar svarbių funkcijų, kad būtų tinkamai įgyvendinamos 2 dalies a punkto nuostatos. ***Rengdamos tų techninių reguliavimo standartų projektus, EPI atsižvelgia į finansų sektoriaus subjektų dydį, jų paslaugų, veiklos ir operacijų pobūdį, mastą ir sudėtingumą bei jų bendrą rizikos profilį.***

   EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai iki [OL: prašom įrašyti datą – ***18 mėnesių*** po įsigaliojimo dienos].

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

II SKIRSNIS

YPATINGOS SVARBOS IRT PASLAUGAS TEIKIANČIŲ TREČIŲJŲ ŠALIŲ PRIEŽIŪROS SISTEMA

28 straipsnis

Ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių paskyrimas

1. EPI, pasitarusios Jungtiniame komitete ir remdamosi priežiūros ***organo***, įsteigto pagal 29 straipsnio 1 dalį, rekomendacija***, pasikonsultavusios su ENISA***:

   a) paskiria IRT paslaugas teikiančias trečiąsias šalis, kurios yra ypatingai svarbios finansų sektoriaus subjektams, atsižvelgdamos į 2 dalyje nurodytus kriterijus;

   b) paskiria EBI, ESMA arba EIOPA kiekvienos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies atsakingąja priežiūros institucija, atsižvelgdamos į tai, ar finansų sektoriaus subjektų, kurie naudojasi tos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies paslaugomis ir kuriems atitinkamai taikomas vienas iš reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 arba (ES) Nr. 1095/2010, bendra turto vertė sudaro daugiau kaip pusę visų finansų sektoriaus subjektų, kurie naudojasi ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies paslaugomis, viso turto vertės, sprendžiant pagal tų finansų sektoriaus subjektų konsoliduotuosius balansus arba atskirus balansus, kai balansai nekonsoliduojami.

   Pagal pirmos pastraipos b punktą paskirta atsakingoji priežiūros institucija yra atsakinga už kasdienę ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies priežiūrą.

2. 1 dalies a punkte nurodytas paskyrimas grindžiamas visais šiais kriterijais:

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

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

      i) pasaulinės sisteminės svarbos įstaigų (G-SII) ar kitų sisteminės svarbos įstaigų (O-SII), kurios priklauso 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 ar svarbiomis funkcijomis, kurios galiausiai yra siejamos su ta pačia IRT paslaugas teikiančią trečiąja šalimi, neatsižvelgiant į tai, ar finansų sektoriaus subjektams tokios paslaugos teikiamos tiesiogiai ar netiesiogiai, sudarius subrangos susitarimus ar pagal juos;

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 rafinuotumo, 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 kitai trečiajai šaliai dėl didelių finansinių išlaidų, laiko ar kitokio pobūdžio išteklių, kurių gali prireikti perkėlimui, arba padidėjusios IRT rizikos ar kitos operacinės rizikos, su kuria finansų sektoriaus subjektas gali susidurti tokio perkėlimo metu;

e) valstybių narių, kuriose atitinkama IRT paslaugas teikianti trečioji šalis teikia paslaugas, skaičiumi;

f) valstybių narių, kuriose veiklą vykdo finansų sektoriaus subjektai, besinaudojantys atitinkamos IRT paslaugas teikiančios trečiosios šalies paslaugomis, skaičiumi***;***

fa) atitinkamų IRT paslaugas teikiančios trečiosios šalies teikiamų paslaugų reikšmingumu ir svarba.

2a. Prieš pradėdamas vertinimą 1 dalies a punkte nurodyto paskyrimo tikslais, bendras priežiūros organas praneša apie tai IRT paslaugas teikiančiai trečiajai šaliai.

Bendras priežiūros organas praneša IRT paslaugas teikiančiai trečiajai šaliai apie pirmoje pastraipoje nurodyto vertinimo rezultatus, pateikdamas rekomendacijos dėl ypatingos svarbos projektą. Per šešias savaites nuo to rekomendacijos projekto gavimo dienos IRT paslaugas teikianti trečioji šalis gali pateikti bendram priežiūros organui pagrįstą pareiškimą dėl vertinimo. Pareiškime dėl vertinimo pateikiama visa susijusi papildoma informacija, kurią IRT paslaugas teikianti trečioji šalis laiko derama pateikti, kad padėtų užtikrinti paskyrimo procedūros išbaigtumą ir tikslumą arba užginčytų rekomendacijos dėl ypatingos svarbos projektą. EPI Jungtinis komitetas tinkamai atsižvelgia į pagrįstą pareiškimą ir, prieš priimdamas sprendimą dėl paskyrimo, gali prašyti, kad IRT paslaugas teikianti trečioji šalis pateiktų papildomos informacijos ar įrodymų.

EPI Jungtinis komitetas praneša IRT paslaugas teikiančiai trečiajai šaliai apie jos paskyrimą ypatingos svarbos paslaugų teikėju. IRT paslaugas teikiančiai trečiajai šaliai suteikiami bent trys mėnesiai, per kuriuos ji turi atlikti būtinus pakeitimus, kad bendras priežiūros organas galėtų vykdyti savo pareigas pagal 30 straipsnį, ir informuoti savo finansų sektoriaus klientus, kuriems ta IRT paslaugas teikianti trečioji šalis teikia paslaugas. Bendras priežiūros organas gali leisti pratęsti prisitaikymo laikotarpį ne daugiau kaip trims mėnesiams, jei to prašo paskirtoji IRT paslaugas teikianti trečioji šalis ir jei tai yra tinkamai pagrįsta.

3. Komisijai pagal 50 straipsnį suteikiami įgaliojimai priimti ***deleguotąjį aktą***, kuriuo ***išsamiau apibūdinami*** 2 dalyje nurodyti kriterijai.

4. 1 dalies a punkte nurodytas paskyrimo mechanizmas netaikomas tol, kol Komisija

nepriims deleguotojo akto pagal 3 dalį.

5. 1 dalies a punkte nurodytas paskyrimo mechanizmas netaikomas IRT paslaugas teikiančioms trečiosioms šalims, kurioms taikomos priežiūros sistemos, sukurtos siekiant padėti atlikti užduotis, nurodytas Sutarties dėl Europos Sąjungos veikimo 127 straipsnio 2 dalyje.

6. ***Bendras priežiūros organas, pasikonsultavęs su ENISA,*** skelbia ir ***reguliariai*** atnaujina Sąjungos lygmens ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių sąrašą.

7. Taikant 1 dalies a punktą, kompetentingos institucijos kasmet apibendrina ir perduoda 25 straipsnio 4 dalyje nurodytus pranešimus ***bendram priežiūros organui***, įsteigtam pagal 29 straipsnį. ***Bendras priežiūros organas*** įvertina finansų sektoriaus subjektų priklausomybę nuo IRT paslaugas teikiančių trečiųjų šalių, remdamasis iš kompetentingų institucijų gauta informacija.

8. IRT paslaugas teikiančios trečiosios šalys, neįtrauktos į 6 dalyje nurodytą sąrašą, gali prašyti, kad jas į tą sąrašą įtrauktų.

Taikant pirmą pastraipą, IRT paslaugas teikianti trečioji šalis pateikia pagrįstą prašymą EBI, ESMA arba EIOPA, kurios pasitarusios Jungtiniame komitete nusprendžia, ar įtraukti tokią IRT paslaugas teikiančią trečiąją šalį į tą sąrašą pagal 1 dalies a punktą.

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

8a. EPI Jungtinis komitetas, remdamasis bendro priežiūros organo rekomendacija, paskiria trečiojoje valstybėje įsisteigusias IRT paslaugas teikiančias trečiąsias šalis, kurios yra ypatingos svarbos finansų sektoriaus subjektams, pagal 1 dalies a punktą.

Šios dalies pirmoje pastraipoje nurodyto paskyrimo procese EPI ir bendras priežiūros organas atlieka 2a dalyje nustatytus procedūrinius veiksmus.

9. Finansų sektoriaus subjektai nesinaudoja trečiojoje valstybėje įsisteigusios ***ypatingos svarbos*** IRT paslaugas teikiančios trečiosios šalies paslaugomis***, nebent ta IRT paslaugas teikianti trečioji šalis turi įmonę, įsteigtą Sąjungoje pagal valstybės narės teisę, ir yra sudariusi sutartimi įformintus susitarimus pagal 27 straipsnio 2b dalį.***

29 straipsnis

Priežiūros sistemos struktūra

1. ***Bendras priežiūros organas įsteigiamas*** siekiant ***prižiūrėti*** IRT paslaugas teikiančių trečiųjų šalių riziką, keliamą visuose finansų sektoriuose, ***ir vykdyti tiesioginę IRT paslaugas teikiančių trečiųjų šalių, paskirtų ypatingos svarbos paslaugų teikėjais pagal 28 straipsnį, priežiūrą***.

Bendro priežiūros organo vaidmuo apsiriboja priežiūros įgaliojimais, susijusiais su IRT rizika, būdinga IRT paslaugoms, kurias ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys teikia finansų sektoriaus subjektams.

Bendras priežiūros ***organas*** reguliariai aptaria atitinkamus pokyčius, susijusius su IRT rizika ir pažeidžiamumais, ir skatina nuoseklų požiūrį į trečiosios šalies keliamos IRT rizikos stebėseną Sąjungos mastu.

2. ***Bendras*** priežiūros ***organas*** kasmet atlieka kolektyvinį visų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūros veiklos rezultatų ir nustatytų faktų

vertinimą ir skatina taikyti koordinavimo priemones, padidinsiančias finansų sektoriaus subjektų skaitmeninės veiklos atsparumą, puoselėja geriausią IRT koncentracijos rizikos mažinimo praktiką ir tiria tarpsektorinio rizikos perleidimo mažinimo priemones.

Bendras priežiūros ***organas*** 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.

3. Į ***bendro*** priežiūros ***organo*** sudėtį įeina EPI ***vykdomieji direktoriai***, po vieną ***kiekvienos EPI*** esamo personalo aukšto lygio atstovą ***ir po vieną bent aštuonių nacionalinių kompetentingų institucijų aukšto lygio atstovą***. Vienas Europos Komisijos, vienas ESRV, vienas ECB ir vienas ENISA atstovas ***ir bent vienas nepriklausomas ekspertas, paskirtas pagal šio straipsnio 3a dalį,*** dalyvauja ▌ kaip stebėtojai.

Kasmet, kai IRT paslaugas teikiančios trečiosios šalys paskiriamos ypatingos svarbos paslaugų teikėjais pagal 28 straipsnio 1 dalies a punktą, EPI Jungtinis komitetas nusprendžia, kurios nacionalinės kompetentingos institucijos turi būti bendro priežiūros organo narėmis, atsižvelgdamas į šiuos veiksnius:

a) ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių, įsisteigusių ar teikiančių paslaugas valstybėje narėje, skaičių;

b) valstybės narės finansų sektoriaus subjektų priklausomybę nuo ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių;

c) nacionalinės kompetentingos institucijos santykinę patirtį;

d) nacionalinės kompetentingos institucijos turimus išteklius ir pajėgumą;

e) poreikį, kad bendro priežiūros organo veikla ir sprendimų priėmimas būtų racionalūs, sklandūs ir veiksmingi.

Bendras priežiūros organas dalijasi dokumentais ir sprendimais su visomis nacionalinėmis kompetentingomis institucijomis, kurios nėra bendro priežiūros organo narės.

Bendro priežiūros organo veiklą remia ir jam padeda paskirti visų EPI darbuotojai.

3a. Šio straipsnio 3 dalyje nurodytą nepriklausomą ekspertą stebėtoju skiria bendras priežiūros organas po viešo ir skaidraus paraiškų teikimo proceso.

Nepriklausomas ekspertas skiriamas dvejų metų kadencijai, atsižvelgiant į jo kompetenciją finansinio stabilumo, skaitmeninės veiklos atsparumo ir IRT saugumo klausimais.

Paskirtas nepriklausomas ekspertas neina jokių pareigų nacionaliniu, Sąjungos ar tarptautiniu lygmenimis. Nepriklausomas ekspertas veikia nepriklausomai ir objektyviai, vadovaudamasis vien tik visos Sąjungos interesais, ir neprašo Sąjungos institucijų ar įstaigų, kurios nors valstybės narės vyriausybės ar bet kurios kitos viešosios ar privačiosios įstaigos nurodymų ir jais nesivadovauja.

Bendras priežiūros organas gali nuspręsti paskirti daugiau nei vieną nepriklausomą ekspertą stebėtoją.

4. Vadovaujantis reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 16 straipsniu, EPI ***iki [OL: prašom įrašyti datą – 18 mėnesių po šio***

reglamento įsigaliojimo dienos] parengia ***bendro priežiūros organo, atsakingosios priežiūros institucijos*** ir kompetentingų institucijų taikant šį skirsnį vykdomo bendradarbiavimo gaires dėl išsamių procedūrų ir sąlygų, susijusių su kompetentingų institucijų ir ***bendro priežiūros organo*** užduočių vykdymu, ir išsamios informacijos apie keitimąsi informacija, kurios reikia kompetentingoms institucijoms siekiant užtikrinti, kad būtų imtasi tolesnių veiksmų dėl rekomendacijų, kurias pagal 31 straipsnio 1 dalies d punktą ***bendras priežiūros organas*** teikia ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims.

5. Šiame skirsnyje nustatytais reikalavimais nedaromas poveikis Direktyvos (ES) 2016/1148 ir kitų Sąjungos priežiūros taisyklių, taikomų debesijos paslaugų teikėjams, taikymui.

6. ***Bendras*** priežiūros ***organas*** kasmet pateikia Europos Parlamentui, Tarybai ir Komisijai šio skirsnio taikymo ataskaitą.

30 straipsnis

Atsakingosios priežiūros institucijos užduotys

1. Atsakingoji priežiūros institucija***, paskirta pagal 28 straipsnio 1 dalies b punktą, vadovauja kasdienei ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūrai ir ją koordinuoja ir yra pagrindinis kontaktinis punktas toms ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims.***

1a. ***Atsakingoji priežiūros institucija*** įvertina, ar kiekviena ypatingos svarbos IRT paslaugas teikianti trečioji šalis taiko išsamias, patikimas ir veiksmingas taisykles, procedūras, mechanizmus ir susitarimus, skirtus IRT rizikai, kurią ji gali kelti finansų sektoriaus subjektams, valdyti. ***Atliekant tą vertinimą daugiausia dėmesio visų pirma skiriama ypatingos svarbos arba svarbias funkcijas palaikančioms IRT paslaugoms, kurias finansų sektoriaus subjektams teikia ypatingos svarbos IRT paslaugas teikianti trečioji šalis, tačiau vertinimas taip pat gali būti platesnis, jei tai tikslinga vertinant su tomis funkcijomis susijusią riziką.***

2. ***1a*** dalyje nurodytą vertinimą sudaro:

   a) IRT reikalavimai, kuriais visų pirma užtikrinamas paslaugų, kurias ypatingos svarbos IRT paslaugas teikianti trečioji šalis teikia finansų sektoriaus subjektams, saugumas, prieinamumas, tęstinumas, masto keičiamumas ir kokybė, taip pat gebėjimas visada laikytis aukštų duomenų saugumo, konfidencialumo ir vientisumo standartų;

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

   c) rizikos valdymo procesai, įskaitant IRT rizikos valdymo politiką, IRT veiklos tęstinumą ir IRT veiklos atkūrimo po ekstremaliųjų įvykių planus;

   d) valdymo priemonės, įskaitant organizacinę struktūrą, kuriai taikomos aiškios, skaidrios ir nuoseklios atsakomybės ir atskaitomybės taisyklės, leidžiančios veiksmingai valdyti IRT riziką;

   e) ***didelių*** su IRT susijusių incidentų identifikavimas, stebėsena ir skubus pranešimas apie juos finansų sektoriaus subjektams, tų incidentų, visų pirma kibernetinių išpuolių, valdymas ir sprendimas;

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

g) IRT sistemų, infrastruktūros ir kontrolės priemonių testavimas;

h) IRT auditas;

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

3. ***Remdamasis 1a*** dalyje nurodytu ***atsakingosios priežiūros institucijos atliktu*** vertinimu, ***bendras priežiūros organas, vadovaujamas ir koordinuojamas atsakingosios priežiūros institucijos, parengia ir pasiūlo*** kiekvienai ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai ▌aiškų, išsamų ir pagrįstą individualų priežiūros planą.

Rengdamas priežiūros plano projektą, bendras priežiūros organas konsultuojasi su visomis atitinkamomis kompetentingomis institucijomis ir bendraisiais informaciniais centrais, nurodytais Direktyvos (ES) 2016/1148 8 straipsnyje, siekdamas užtikrinti, kad nebūtų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių pareigų pagal tą direktyvą neatitikimų ar dubliavimosi.

Priežiūros planą kasmet tvirtina atsakingosios priežiūros institucijos valdyba.

Prieš patvirtinant priežiūros plano projektą, jis pateikiamas ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai.

Gavusi priežiūros plano projektą, ypatingos svarbos IRT paslaugas teikianti trečioji šalis per šešias savaites jį peržiūri ir pateikia pagrįstą pareiškimą dėl priežiūros plano projekto. Toks pagrįstas pareiškimas gali būti pateikiamas tik tuo atveju, jei ypatingos svarbos IRT paslaugas teikianti trečioji šalis gali pateikti įrodymų, kad priežiūros plano vykdymas padarytų neproporcingą poveikį klientams, kuriems šis reglamentas netaikomas, arba sutrikdytų jų veiklą, arba kad yra veiksmingesnis arba efektyvesnis nustatytos IRT rizikos valdymo sprendimas. Jei toks pareiškimas pateikiamas, ypatingos svarbos IRT paslaugas teikianti trečioji šalis bendram priežiūros organui pasiūlo veiksmingesnį arba efektyvesnį sprendimą priežiūros plano projekto tikslams pasiekti.

Prieš patvirtindama priežiūros planą, atsakingosios priežiūros institucijos valdyba tinkamai atsižvelgia į pagrįstą pareiškimą ir gali paprašyti papildomos informacijos ar įrodymų iš IRT paslaugas teikiančios trečiosios šalies.

4. ***Patvirtinus*** 3 dalyje nurodytus metinius priežiūros planus ir juos ***pateikus*** ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, kompetentingos institucijos gali imtis priemonių dėl ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių tik gavusios ***bendro*** priežiūros ***organo*** pritarimą.

31 straipsnis

Priežiūros įgaliojimai

1. Vykdydama šiame skirsnyje nustatytas pareigas atsakingoji priežiūros institucija turi šiuos įgaliojimus***, susijusius su ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių teikiamomis paslaugomis finansų sektoriaus subjektams***:

a) prašyti visos susijusios informacijos ir dokumentų pagal 32 straipsnį;

b) atlikti bendruosius tyrimus ir patikrinimus ***vietoje*** pagal 33 ir 34 straipsnius;

c) prašyti ataskaitų, kai užbaigiama priežiūros veikla, kuriose būtų nurodyti veiksmai, kurių imtasi, arba taisomosios priemonės, kurias ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys įgyvendino atsižvelgdamos į ***1a dalyje*** nurodytas rekomendacijas***.***

1a. Kad galėtų vykdyti šiame skirsnyje nustatytas pareigas, remdamasis atsakingosios priežiūros institucijos gauta informacija ir atsakingosios priežiūros institucijos atliktų tyrimų rezultatais, bendras priežiūros organas turi įgaliojimus: imtis veiksmų atsižvelgiant į rekomendacijas dėl 30 straipsnio 2 dalyje nurodytų sričių, visų pirma dėl:

i) konkrečių IRT saugumo ir kokybės reikalavimų ar procesų, visų pirma susijusių su pataisų, naujinių, šifravimo ir kitų saugumo priemonių, kuriuos ***bendras*** priežiūros ***organas*** laiko svarbiomis 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 ***bendras*** priežiūros ***organas*** laiko svarbiomis užkertant kelią bendrų gedimo taškų atsiradimui ar jų plitimui arba siekiant kuo labiau sumažinti galimą sisteminį poveikį visame Sąjungos finansų sektoriuje IRT koncentracijos rizikos atveju;

iii) pagal 32 ir 33 straipsnius atlikus subrangos susitarimų, įskaitant subrangos susitarimus, kuriuos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys ketina sudaryti su kitomis IRT paslaugas teikiančiomis trečiosiomis šalimis arba trečiojoje valstybėje įsisteigusiais IRT subrangovais, – bet kokių planuojamų subrangos sutarčių, įskaitant veiklos subrangą, kai ***bendras*** priežiūros ***organas*** mano, kad papildomų subrangos sutarčių sudarymas gali kelti riziką finansų sektoriaus subjekto teikiamoms paslaugoms arba riziką finansiniam stabilumui;

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

– numatomas subrangovas yra trečiojoje valstybėje įsisteigę IRT paslaugas teikianti trečioji šalis arba IRT subrangovas, ***neturintys Sąjungoje pagal valstybės narės teisę įsteigtos įmonės***;

– subrangos sutartis sudaroma dėl ypatingos svarbos arba svarbios finansų sektoriaus subjekto funkcijos***;***

– ***dėl subrangos kils didelė ir aiški rizika finansų sektoriaus subjektui arba Sąjungos finansų sistemos finansiniam stabilumui.***

1b. 1 ir 1a dalyse nurodytais įgaliojimais prireikus naudojamasi ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies teikiamų IRT paslaugų, kuriomis remiamos ne ypatingos svarbos arba svarbios funkcijos, atžvilgiu.

1c. Naudodamiesi 1 ir 1a dalyse nurodytais įgaliojimais, atsakingoji priežiūros institucija ir bendras priežiūros organas tinkamai atsižvelgia į Direktyvoje (ES) 2016/1148 nustatytą sistemą ir, kai tikslinga, konsultuojasi su atitinkamomis pagal tą direktyvą įsteigtomis kompetentingomis institucijomis, kad būtų išvengta

nereikalingo techninių ir organizacinių priemonių, kurios galėtų būti taikomos ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims pagal tą direktyvą, dubliavimo.

2. ***Prieš baigdamas rengti ir teikdamas rekomendacijas pagal 1a dalį, bendras priežiūros organas informuoja ypatingos svarbos IRT paslaugas teikiančią trečiąją šalį apie savo ketinimus ir suteikia galimybę IRT paslaugas teikiančiai trečiajai šaliai pateikti informaciją, į kurią, jos nuomone, turėtų būti atsižvelgta prieš baigiant rengti rekomendaciją arba siekiant užginčyti planuojamas rekomendacijas. Rekomendacijos užginčijimo priežastis gali būti, be kita ko, neproporcingas poveikis klientams, kuriems šis reglamentas netaikomas, arba jiems skirtų paslaugų sutrikdymas, arba faktas, kad yra veiksmingesnis ar efektyvesnis sprendimas siekiant valdyti nustatytą IRT riziką.***

3. Ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys sąžiningai bendradarbiauja su atsakingąja priežiūros institucija ***ir bendru priežiūros organu ir*** padeda ***jiems*** atlikti ***jų*** užduotis.

4. ***Tais atvejais, kai visiškai arba iš dalies nesilaikoma priemonių, kurių reikalaujama imtis pagal 1 dalies a, b arba c punktus, ir pasibaigus ne mažiau kaip 60 kalendorinių dienų laikotarpiui nuo tos dienos, kurią ypatingos svarbos IRT paslaugas teikianti trečioji šalis gavo pranešimą apie priemonę,*** atsakingoji priežiūros institucija gali ***nuspręsti*** skirti periodinę baudą, kad priverstų ypatingos svarbos IRT paslaugas teikiančią trečiąją šalį laikytis ***reikalavimų***.

4a. ***4 dalyje nurodytą periodinę baudą atsakingoji priežiūros institucija skiria tik kraštutiniu atveju ir tais atvejais, kai ypatingos svarbos IRT paslaugas teikianti trečioji šalis nesiima priemonių, kurių reikalaujama imtis pagal 1 dalies a, b arba c punktus.***

5. 4 dalyje nurodyta periodinė bauda skiriama kasdien, kol bus pradėta laikytis reikalavimų, ir ne ilgiau kaip šešis mėnesius nuo pranešimo ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai.

6. Periodinės baudos dydis, apskaičiuojamas nuo sprendime dėl periodinės baudos skyrimo nustatytos dienos, sudaro ***iki*** 1 proc. ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies vidutinės dienos pasaulinės apyvartos***, susijusios su finansų sektoriaus subjektams, kuriems taikomas šis reglamentas, teikiamomis paslaugomis,*** praėjusiais finansiniais metais.

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

8. EPI viešai paskelbia apie kiekvieną skirtą periodinę baudą, išskyrus atvejus, kai toks viešas paskelbimas sukeltų rimtą pavojų finansų rinkoms arba pernelyg pakenktų susijusioms šalims.

9. Prieš skirdama periodinę baudą pagal 4 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. Jiems suteikiama galimybė 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.

32 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 dokumentus, 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 rangos būdu perdavė veiklos funkcijas ar veiklą.

Ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys privalo pateikti pirmoje pastraipoje nurodytą informaciją tik apie finansų sektoriaus subjektams, kuriems taikomas šis reglamentas ir kurie naudojasi ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių paslaugomis ypatingos svarbos arba svarbioms funkcijoms vykdyti, teikiamas paslaugas. Ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys praneša atitinkamam finansų sektoriaus subjektui apie konkrečius su tuo finansų sektoriaus subjektu susijusius prašymus.

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 informacijos, atstovą, kad jis neprivalo pateikti informacijos, tačiau, jeigu jis savanoriškai atsakys į gautą prašymą, pateikta informacija privalo būti teisinga arba neklaidinanti.

3. ***Sprendimu*** įpareigodama 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 ***pagrįstą*** informacijos pateikimo terminą;

   e) nurodo 31 straipsnio 4 dalyje numatytas periodines baudas, jei pateikiama ne visa reikalaujama informacija ***arba tokia informacija nepateikiama iki***

d punkte nurodyto termino;

f) nurodo teisę apskųsti sprendimą EPI apeliacinei tarybai ir prašyti, kad jis būtų peržiūrėtas Europos Sąjungos Teisingumo Teismo (toliau – Teisingumo Teismas) pagal atitinkamų 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. Tinkamai įgalioti teisininkai gali pateikti informaciją savo klientų vardu. Visa atsakomybė už informacijos išsamumą, teisingumą ir neklaidingumą tenka ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai.

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

33 straipsnis

Bendrieji tyrimai

1. Siekdama vykdyti šiame reglamente nustatytas pareigas atsakingoji priežiūros institucija, padedama ***35 straipsnio*** 1 dalyje nurodytos tyrimo grupės, gali atlikti būtinus IRT paslaugas teikiančių trečiųjų šalių tyrimus***, laikydamasi proporcingumo principo***. ***Atlikdama tyrimą atsakingoji priežiūros institucija turi imtis atsargumo priemonių ir užtikrinti, kad būtų apsaugotos ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių klientų, kuriems netaikomas šis reglamentas, teisės, įskaitant priemones, susijusias su poveikiu paslaugų lygiui, duomenų prieinamumui ir konfidencialumui.***

2. Atsakingoji priežiūros institucija turi įgaliojimus:

a) nagrinėti įrašus, duomenis, procedūras ir kitą medžiagą, susijusią su jo užduočių vykdymu, neatsižvelgiant į laikmenas, kuriose jie saugomi;

b) ***saugiu būdu peržiūrėti*** šių įrašų, duomenų, procedūrų ir kitos medžiagos patvirtintas kopijas ar jų išrašus;

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

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

e) reikalauti telefono ir duomenų srauto duomenų.

3. Pareigūnai ir kiti asmenys, kuriuos atsakingoji priežiūros institucija įgaliojo atlikti 1 dalyje nurodytą tyrimą, savo įgaliojimais naudojasi pateikę raštišką įgaliojimą, kuriame nurodomas tyrimo dalykas ir tikslas.

Tame įgaliojime taip pat nurodomos 31 straipsnio 4 dalyje nustatytos periodinės baudos, taikomos tais atvejais, jei nepateikti visi reikalaujami įrašai, duomenys, procedūros ar bet kokia kita medžiaga arba nepateikti ar yra neišsamūs atsakymai į klausimus, užduotus IRT paslaugas teikiančios trečiosios šalies atstovams.

4. IRT paslaugas teikiančios trečiosios šalies atstovai turi bendradarbiauti su atsakingosios priežiūros institucijos sprendimu pradėtų tyrimų vykdytojais. Sprendime nurodomas

tyrimo dalykas ir tikslas, 31 straipsnio 4 dalyje nustatytos 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, atsakingosios priežiūros institucijos praneša finansų sektoriaus subjektų, kurie naudojasi tos IRT paslaugas teikiančios trečiosios šalies paslaugomis, kompetentingoms institucijoms apie tyrimą ir nurodo įgaliotų asmenų tapatybę.

34 straipsnis

Patikrinimai vietoje

1. Siekdama vykdyti šiame reglamente nustatytas pareigas, atsakingoji priežiūros institucija, padedama 35 straipsnio 1 dalyje nurodytų 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 neelektroninius patikrinimus.

   Pirmoje pastraipoje nurodyti įgaliojimai atlikti patikrinimus vietoje taikomi ne tik Sąjungos teritorijose, jei trečiojoje valstybėje esančios teritorijos patikrinimas atitinka visus šiuos reikalavimus:

   - ***jis yra būtinas, kad atsakingoji priežiūros institucija galėtų vykdyti savo pareigas pagal šį reglamentą;***
   - ***jis yra tiesiogiai susijęs su IRT paslaugų teikimu Sąjungos finansų sektoriaus subjektams;***
   - ***tai svarbu vykstančiam tyrimui.***

1a. Atlikdama patikrinimą vietoje atsakingoji priežiūros institucija turi imtis atsargumo priemonių ir užtikrinti, kad būtų apsaugotos ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių klientų, kuriems netaikomas šis reglamentas, teisės, įskaitant priemones, susijusias su poveikiu paslaugų lygiui, duomenų prieinamumui ir konfidencialumui.

2. Pareigūnai ir kiti asmenys, kuriuos atsakingoji priežiūros institucija įgaliojo atlikti patikrinimą vietoje, gali patekti į bet kurias šias verslo patalpas, teritoriją arba valdą ir turi visus įgaliojimus užplombuoti bet kurias verslo patalpas ir apskaitos knygas arba įrašus tokiam laikotarpiui ir tokia apimtimi, kokie būtini patikrinimui atlikti.

   Jie naudojasi savo įgaliojimais pateikę raštišką įgaliojimą, kuriame nurodomas patikrinimo dalykas bei tikslas ir 31 straipsnio 4 dalyje nustatytos periodinės baudos, taikomos, jei atitinkamų IRT paslaugas teikiančių trečiųjų šalių atstovai neleidžia atlikti patikrinimo.

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

4. Patikrinimai apima visas susijusias IRT sistemas, tinklus, įtaisus, informaciją ir duomenis***, kuriuos atsakingoji priežiūros institucija laiko tinkamais ir technologijų požiūriu svarbiais,*** naudojamus paslaugoms finansų sektoriaus subjektams teikti arba padedančius jas teikti.

5. Prieš bet kurį planuojamą patikrinimą vietoje atsakingosios priežiūros institucijos pateikia pagrįstą įspėjimą ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, 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 jis turi prasidėti, ir nurodomos 31 straipsnio 4 dalyje nustatytos 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 Teismo.

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 skirtas patikrinimas, atsakingoji priežiūros institucija informuoja ypatingos svarbos IRT ***paslaugas teikiančią trečiąją šalį*** apie tokio nesutikimo padarinius, įskaitant galimybę atitinkamų finansų sektoriaus subjektų kompetentingoms institucijoms nutraukti su ypatingos svarbos IRT paslaugas teikiančia trečiąja šalimi sudarytus sutartimi įformintus susitarimus.

35 straipsnis

Nuolatinė priežiūra

1. Atliekant bendruosius tyrimus arba patikrinimus vietoje atsakingosioms priežiūros institucijoms padeda tyrimo grupė, suburta kiekvienai ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai.

2. 1 dalyje nurodytą jungtinę tyrimo grupę sudaro ne daugiau kaip 10 atsakingosios priežiūros institucijos***, kitų EPI*** ir atitinkamų kompetentingų institucijų, prižiūrinčių finansų sektoriaus subjektus, kuriems ypatingos svarbos IRT paslaugas teikia trečioji šalis, darbuotojų, kurie dalyvaus rengiantis priežiūros veiklai ir ją vykdant. Visi jungtinės tyrimo grupės nariai turi patirties IRT ir operacinės rizikos srityse. Jungtinės tyrimo grupės darbą koordinuoja paskirtas EPI darbuotojas (toliau – atsakingosios priežiūros institucijos koordinatorius).

3. EPI Jungtiniame komitete parengia bendrų techninių reguliavimo standartų projektus, kuriuose patikslinama, kaip atitinkamų kompetentingų institucijų darbuotojai skiriami jungtinės tyrimo grupės nariais, taip pat tyrimo grupės užduotys ir darbo tvarka. EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai iki [OL: prašom įrašyti datą – 1 metai po įsigaliojimo dienos].

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

4. Per tris mėnesius nuo tyrimo arba patikrinimo vietoje pabaigos ***bendras*** priežiūros ***organas*** pagal 31 straipsnyje nurodytus įgaliojimus priima rekomendacijas, adresuotas ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai.

5. 4 dalyje nurodytos rekomendacijos nedelsiant perduodamos ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai ir finansų sektoriaus subjektų, kuriems ji teikia paslaugas, kompetentingoms institucijoms.

   Vykdydamos priežiūros veiklą atsakingosios priežiūros institucijos ***ir bendras***

priežiūros organas gali atsižvelgti į visus atitinkamus trečiųjų šalių sertifikatus ir IRT paslaugas teikiančių trečiųjų šalių vidaus ar išorės audito ataskaitas, kurias pateikia ypatingos svarbos IRT paslaugas teikianti trečioji šalis.

36 straipsnis

Sąlygų, kuriomis galima vykdyti priežiūros veiklą, suderinimas

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

   a) informacija, kurią ypatingos svarbos IRT paslaugas teikianti trečioji šalis turi pateikti, kai sutinka savanoriškai atsakyti į prašymą, kaip nurodyta 28 straipsnio 8 dalyje;

   b) ataskaitų, kurių gali būti prašoma taikant 31 straipsnio 1 dalies c punktą, turinys ir forma;

   c) informacijos, kurią ypatingos svarbos IRT paslaugas teikianti trečioji šalis įpareigojama pateikti, atskleisti arba pranešti pagal 31 straipsnio 1 dalį, pateikimas, įskaitant struktūrą, formas ir metodus;

   d) išsami informacija apie kompetentingų institucijų atliekamą ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priemonių, taikytų remiantis ***bendro*** priežiūros ***organo*** rekomendacijomis pagal 37 straipsnio 2 dalį, vertinimą.

2. EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai iki 20xx m. sausio 1 d. [OL: prašom įrašyti datą – 1 metai po įsigaliojimo dienos].

   Komisijai suteikiami įgaliojimai papildyti šį reglamentą priimant šio straipsnio pirmoje pastraipoje nurodytus techninius reguliavimo standartus laikantis atitinkamų reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 10–14 straipsniuose nustatytos tvarkos.

37 straipsnis

Kompetentingų institucijų tolesni veiksmai

1. Per 30 kalendorinių dienų po ***bendro*** priežiūros ***organo*** rekomendacijų, pateiktų pagal 31 straipsnio ***1a dalį***, gavimo ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys ***bendram*** priežiūros ***organui*** praneša, ar ketina tų rekomendacijų laikytis. ***Bendras*** priežiūros ***organas nedelsdamas*** šią informaciją perduoda kompetentingoms ***atitinkamų finansų sektoriaus subjektų*** institucijoms.

2. Kompetentingos institucijos ***informuoja finansų sektoriaus subjektus, sudariusius sutartimi įformintus susitarimus su ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis, apie riziką, identifikuotą bendro priežiūros organo rekomendacijose, skirtose toms ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims pagal 31 straipsnio 1a dalį, ir*** stebi, ar finansų sektoriaus subjektai atsižvelgia į nustatytą riziką. ***Bendras priežiūros organas stebi, ar ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys ėmėsi priemonių dėl tose rekomendacijose identifikuotos rizikos.***

3. ***Kai reguliavimo tikslų negalima įgyvendinti kitomis priemonėmis ir nacionalinės valdžios institucijos, remdamosi bendro priežiūros organo pateikta informacija, pateikė įspėjimus atitinkamiems finansų sektoriaus subjektams, atsakingosios***

priežiūros institucijos valdyba, remdamasi bendro priežiūros organo rekomendacija ir pasikonsultavusi su kompetentingomis atitinkamų finansų sektoriaus subjektų institucijomis, gali ▌ laikinai iš dalies arba visiškai ***sustabdyti*** ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies teikiamos paslaugos naudojimą ar diegimą ***atitinkamuose finansų sektoriaus subjektuose, patiriančiuose riziką, identifikuotą*** ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims skirtose rekomendacijose***, kol ta rizika nebus pašalinta***. Prireikus ***kraštutiniu atveju*** jos gali reikalauti, kad ***ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys*** iš dalies arba visiškai nutrauktų atitinkamus sutartimi įformintus susitarimus, sudarytus su ***finansų sektoriaus subjektais, kuriems kyla identifikuota rizika***.

4. Priimdama 3 dalyje nurodytus sprendimus ***atsakingosios priežiūros*** institucijos ***valdyba*** atsižvelgia į rizikos, kurios ypatingos svarbos IRT paslaugas teikianti trečioji šalis nemažina, 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 kitaip sietinas su reikalavimų nesilaikymu;

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

da) tai, ar sustabdymas ar nutraukimas kelia riziką ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies paslaugų naudotojo verslo operacijų tęstinumui.

4a. 3 dalyje numatyti sprendimai įgyvendinami tik po to, kai apie tai tinkamai informuojami visi su juo susiję finansų sektoriaus subjektai. Atitinkamiems finansų sektoriaus subjektams suteikiamas laikotarpis, neviršijantis to, kas tikrai būtina, kad jie galėtų pakoreguoti savo užsakomųjų paslaugų ir sutartimi įformintus susitarimus su ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis taip, kad nekiltų pavojus skaitmeninės veiklos atsparumui, ir įgyvendinti savo pasitraukimo strategijas ir pereinamojo laikotarpio planus, nurodytus 25 straipsnyje.

Ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys, kurioms taikomi 3 dalyje numatyti sprendimai, visapusiškai bendradarbiauja su atitinkamais finansų sektoriaus subjektais.

5. Kompetentingos institucijos reguliariai informuoja ***bendrą*** priežiūros ***organą*** apie metodus ir priemones, kurių ėmėsi vykdydamos finansų sektoriaus subjektų priežiūros užduotis.

38 straipsnis

Priežiūros mokesčiai

1. EPI ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims taiko mokesčius, kurie visiškai padengia būtinas EPI išlaidas, susijusias su priežiūros užduočių vykdymu pagal šį reglamentą, ir, be kita ko, kompensuoja visas išlaidas, kurios gali būti patirtos dėl kompetentingų institucijų darbo, atlikto įsitraukus į priežiūros veiklą pagal 35

straipsnį.

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.

1a. Jei sudarytas administracinis susitarimas su trečiosios valstybės reguliavimo ir priežiūros institucija pagal šio straipsnio 1 dalį, ta institucija gali būti 35 straipsnio 1 dalyje nurodytos tyrimo grupės narė.

2. Komisijai pagal 50 straipsnį suteikiami įgaliojimai priimti deleguotąjį aktą, kuriuo šis reglamentas būtų papildytas nustatant mokesčių dydį ir jų mokėjimo būdą.

39 straipsnis

Tarptautinis bendradarbiavimas

1. Vadovaudamosi atitinkamų reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 33 straipsniu, EBI, ESMA ir EIOPA gali sudaryti administracinius susitarimus su trečiųjų valstybių reguliavimo ir priežiūros institucijomis, kad būtų skatinamas tarptautinis bendradarbiavimas dėl trečiųjų šalių keliamos IRT rizikos įvairiuose finansų sektoriuose, visų pirma plėtojama geriausia praktika, susijusi 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 skirdamos trečiųjų šalių keliamos IRT rizikos raidai ir jos poveikiui finansiniam stabilumui, rinkos vientisumui, investuotojų apsaugai ar bendrosios rinkos veikimui.

VI SKYRIUS

DALIJIMOSI INFORMACIJA SCHEMOS

40 straipsnis

Dalijimosi informacija ir žvalgybos informacija apie kibernetines grėsmes schemos

1. Finansų sektoriaus subjektai ***deda pastangas*** tarpusavyje ***ir su IRT paslaugas teikiančiomis trečiosiomis šalimis*** keistis informacija ir žvalgybos informacija apie kibernetines grėsmes, įskaitant užvaldymo rodiklius, taktiką, metodus ir procedūras, kibernetinio saugumo įspėjimus ir konfigūravimo priemones, jei toks dalijamasis informacija ir žvalgybos duomenimis:

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

   b) vyksta patikimose finansų sektoriaus subjektų ***ir IRT paslaugas teikiančių trečiųjų šalių*** bendruomenėse;

   c) yra įgyvendinamas pagal dalijimosi informacija schemas, kuriomis apsaugoma galimai neskelbtina informacija, kuria dalijamasi, ir kurioms taikomos elgesio taisyklės, visapusiškai laikantis verslo konfidencialumo, asmens duomenų apsaugos[1] reikalavimų ir konkurencijos politikos gairių[2].

2. Taikant 1 dalies c punktą, dalijimosi informacija schemose apibrėžiamos dalyvavimo sąlygos ir, kai tinkama, išsamiai išdėstomos valdžios institucijų dalyvavimo sąlygos ir kompetencija, pagal kurią pastarosios gali būti įtrauktos į dalijimosi informacija schemas, taip pat operaciniai elementai, įskaitant specialių IT platformų naudojimą.

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

---

1 Vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (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).

2 Komisijos komunikatas „Sutarties dėl Europos Sąjungos veikimo 101 straipsnio taikymo horizontaliesiems bendradarbiavimo susitarimams gairės“ (2011/C 11/01).

VII SKYRIUS

KOMPETENTINGOS INSTITUCIJOS

41 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 užtikrina toliau nurodytos kompetentingos institucijos pagal atitinkamais teisės aktais suteiktus įgaliojimus:

a) kredito įstaigų atveju – kompetentinga institucija, paskirta pagal Direktyvos 2013/36/ES 4 straipsnį, nedarant poveikio konkrečioms užduotims, ECB suteiktoms Reglamentu (ES) Nr. 1024/2013;

b) mokėjimo paslaugų teikėjų atveju – kompetentinga institucija, paskirta pagal Direktyvos (ES) 2015/2366 22 straipsnį;

c) elektroninių mokėjimų įstaigų atveju – kompetentinga institucija, paskirta pagal Direktyvos 2009/110/EB 37 straipsnį;

d) investicinių įmonių atveju – kompetentinga institucija, paskirta pagal Direktyvos (ES) 2019/2034 4 straipsnį;

e) kriptoturto paslaugų teikėjų, kriptoturto emitentų ***ir siūlytojų***, su turtu susietų žetonų emitentų ***ir siūlytojų*** ir reikšmingų su turtu susietų žetonų emitentų atveju – kompetentinga institucija, paskirta pagal [20xx m. Reglamento (ES) (MICA reglamento)] 3 straipsnio 1 dalies ee punkto pirmą įtrauką;

f) centrinių vertybinių popierių depozitoriumų ***ir vertybinių popierių atsiskaitymų sistemų operatorių*** atveju – kompetentinga institucija, paskirta pagal Reglamento (ES) Nr. 909/2014 11 straipsnį;

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

h) prekybos vietų ir duomenų teikimo paslaugų teikėjų atveju – kompetentinga institucija, paskirta pagal Direktyvos 2014/65/ES 67 straipsnį;

i) sandorių duomenų saugyklų atveju – kompetentinga institucija, paskirta pagal Reglamento (ES) Nr. 648/2012 55 straipsnį;

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

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

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

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

n) profesinių pensijų įstaigų atveju – kompetentinga institucija, paskirta pagal

Direktyvos 2016/2341 47 straipsnį;

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

p) teisės aktų nustatytą auditą atliekančių auditorių ir audito įmonių atveju – kompetentinga institucija, paskirta pagal Direktyvos 2006/43/EB 3 straipsnio 2 dalį ir 32 straipsnį;

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

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

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

42 straipsnis

Bendradarbiavimas su struktūromis ir institucijomis, įsteigtomis Direktyva (ES) 2016/1148

1. Siekiant skatinti pagal šį reglamentą paskirtų kompetentingų institucijų ir pagal Direktyvos (ES) 2016/1148 11 straipsnį įsteigtos Bendradarbiavimo grupės bendradarbiavimą ir sudaryti sąlygas keistis priežiūros informacija, EPI ir kompetentingos institucijos ***kviečiamos*** dalyvauti Bendradarbiavimo grupės darbe***, kiek tas darbas yra atitinkamai susijęs su priežiūros ir kontrolės veikla, susijusia su subjektais, išvardytais Direktyvos (ES) 2016/1148 II priedo 7 punkte, kurie taip pat yra paskirti ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis pagal šio reglamento 28 straipsnį***.

2. Kompetentingos institucijos gali konsultuotis, kai tinka, su bendruoju informaciniu centru ir nacionalinėmis reagavimo į kompiuterių saugumo incidentus tarnybomis, atitinkamai nurodytomis Direktyvos (ES) 2016/1148 8 ir 9 straipsniuose.

2a. Prieš vykdydama bendruosius tyrimus ir patikrinimus vietoje pagal šio reglamento 33 ir 34 straipsnius, atsakingoji priežiūros institucija informuoja atitinkamas kompetentingas institucijas, paskirtas pagal Direktyvą (ES) 2016/1148, ir su jomis bendradarbiauja.

43 straipsnis

Finansinės tarpsektorinės užduotys, komunikacija ir bendradarbiavimas

1. EPI, pasitarusios jungtiniame komitete ir bendradarbiaudamos su kompetentingomis institucijomis, ECB, ***Bendra pertvarkymo valdyba (jei informacija susijusi su subjektais, kuriems taikomas Reglamentas (ES) Nr. 806/2014)*** ir ESRV, gali nustatyti mechanizmus, kurie sudarytų sąlygas dalytis veiksminga praktika skirtinguose finansų sektoriuose, kad būtų didinamas informuotumas apie padėtį ir identifikuojami bendri kibernetiniai pažeidžiamumo atvejai ir rizika įvairiuose sektoriuose.

   Jos gali parengti krizių valdymo ir nenumatytų atvejų užduotis, apimančias kibernetinių išpuolių scenarijus, siekdamos sukurti komunikacijos kanalus ir palaipsniui sudaryti

sąlygas veiksmingam ES lygmens koordinuotam atsakui didelio tarpvalstybinio IRT incidento ar ***didelės kibernetinės*** grėsmės, turinčios sisteminį poveikį visam Sąjungos finansų sektoriui, atveju.

Atitinkamais atvejais šios užduotys gali padėti patikrinti finansų sektoriaus priklausomybę nuo kitų ekonomikos sektorių.

2. Kompetentingos institucijos, EBI, ESMA arba EIOPA, ECB, ***nacionalinės pertvarkymo institucijos ir Bendra pertvarkymo valdyba (jei informacija susijusi su subjektais, kuriems taikomas Reglamentas (ES) Nr. 806/2014)*** glaudžiai bendradarbiauja tarpusavyje ir keičiasi informacija, kad galėtų vykdyti savo pareigas pagal 42–48 straipsnius. Jos glaudžiai koordinuoja savo atliekamą priežiūros veiklą, kad būtų identifikuoti ir ištaisyti šio reglamento pažeidimai, plėtojama ir skatinama geriausia praktika, palengvinamas bendradarbiavimas, nesutarimų atveju padedama užtikrinti nuoseklų aiškinimą ir teikiami įvairias jurisdikcijas apimantys vertinimai.

44 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. Šio straipsnio 1 dalyje nurodyti įgaliojimai apima bent įgaliojimus:

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

   b) atlikti patikrinimus vietoje arba tyrimus;

   c) reikalauti taikyti korekcines ir taisomąsias priemones už šio reglamento reikalavimų pažeidimus.

3. Nedarant poveikio valstybių narių teisei taikyti baudžiamąsias sankcijas pagal 46 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 įgaliojimus kompetentingoms institucijoms taikyti bent šias administracines nuobaudas arba taisomąsias priemones už šio reglamento reikalavimų pažeidimus:

   a) paskelbti įsakymą fiziniam arba juridiniam asmeniui nutraukti pažeidimą ir vengti pakartotinio pažeidimo;

   b) reikalauti laikinai arba visam laikui nutraukti bet kokią praktiką ar elgesį, ***kurie laikomi prieštaraujančiais*** šio reglamento nuostatoms, ir užkirsti kelią tos praktikos ar elgesio pasikartojimui;

   c) patvirtinti bet kokios 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 punkte ir 4 dalyje nurodytos nuostatos taikomos juridiniams asmenims, valstybės narės įgalioja kompetentingas institucijas skirti administracines nuobaudas ir taisomąsias priemones, laikantis nacionalinėje teisėje numatytų sąlygų, 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 nurodytos administracinės nuobaudos ar taisomosios priemonės, būtų tinkamai motyvuoti ir galėtų būti apskųsti.

45 straipsnis

Naudojimasis įgaliojimu skirti administracines nuobaudas ir taisomąsias priemones

1. Kompetentingos institucijos savo įgaliojimais skirti 44 straipsnyje nurodytas administracines nuobaudas ir taisomąsias priemones naudojasi pagal savo nacionalines teisines sistemas, kai tinkama:

a) tiesiogiai;

b) bendradarbiaudamos su kitomis valdžios institucijomis;

c) savo atsakomybe perduodamos įgaliojimus kitoms institucijoms;

d) kreipdamosi į kompetentingas teismines institucijas.

2. Priimdamos sprendimą dėl administracinių nuobaudų ar taisomųjų priemonių, skiriamų pagal 44 straipsnį, rūšies ir dydžio, kompetentingos institucijos atsižvelgia į tai, kiek pažeidimas yra tyčinis ar padarytas dėl aplaidumo, ir į visas kitas atitinkamas aplinkybes, įskaitant tam tikrais atvejais į:

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) trečiųjų šalių dėl pažeidimo patirtus nuostolius, jei juos galima nustatyti;

f) atsakingo fizinio ar juridinio asmens bendradarbiavimo su kompetentinga institucija lygį, nedarant poveikio poreikiui užtikrinti, kad tas asmuo grąžintų neteisėtai gautą pelną ar išvengtus nuostolius;

g) atsakingo fizinio ar juridinio asmens anksčiau padarytus pažeidimus.

46 straipsnis

Baudžiamosios sankcijos

1. Valstybės narės gali priimti sprendimą nenustatyti taisyklių dėl administracinių nuobaudų ar taisomųjų priemonių už pažeidimus, už kuriuos skiriamos baudžiamosios sankcijos pagal jų nacionalinę teisę.

2. Jeigu valstybės narės yra nusprendusios už šio reglamento pažeidimus nustatyti baudžiamąsias sankcijas, jos užtikrina, kad būtų nustatytos tinkamos priemonės, kad kompetentingos institucijos turėtų visus būtinus įgaliojimus palaikyti ryšius su savo jurisdikcijos teisminėmis, baudžiamojo persekiojimo ar baudžiamosios teisenos institucijomis, kad galėtų gauti konkrečią su nusikalstamų veikų tyrimais arba procesais, pradėtais dėl šio reglamento pažeidimų, susijusią informaciją, ir tą pačią informaciją teikti kitoms kompetentingoms institucijoms ir EBI, ESMA ir EIOPA, ir taip galėtų įvykdyti pareigas bendradarbiauti šio reglamento tikslais.

47 straipsnis

Pareiga pranešti

Valstybės narės pateikia Komisijai, ESMA, EBI ir EIOPA visus įstatymus ir kitus teisės aktus, kuriais įgyvendinamas šis skyrius, įskaitant visas atitinkamas baudžiamosios teisės nuostatas iki [OL: įrašyti datą – ***12 mėnesių*** nuo įsigaliojimo dienos]. Valstybės narės nepagrįstai nedelsdamos praneša Komisijai, ESMA, EBI ir EIOPA apie visus vėlesnius jų pakeitimus.

48 straipsnis

Administracinių nuobaudų skelbimas

1. Kompetentingos institucijos nepagrįstai nedelsdamos savo oficialiose interneto svetainėse skelbia visus sprendimus skirti administracinę nuobaudą, 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, ***skirtos nuobaudos ir išimtiniu atveju*** atsakingų asmenų tapatybė.

3. Jeigu kompetentinga institucija, atlikusi įvertinimą kiekvienu konkrečiu atveju, mano, kad juridinių asmenų tapatybės arba fizinių asmenų tapatybės ir asmens duomenų paskelbimas būtų neproporcingas, keltų grėsmę finansų rinkų stabilumui ar vykdomam baudžiamajam tyrimui arba padarytų neproporcingą žalą atitinkamam asmeniui, kiek ją galima nustatyti, ji dėl sprendimo skirti administracinę nuobaudą priima bet kurį 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 nurodytas galimybes būtų nepakankamai užtikrinta, jog finansų rinkų stabilumui nekils pavojus arba toks paskelbimas nebūtų proporcingas 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. Kai kompetentinga institucija paskelbia sprendimą skirti administracinę nuobaudą, dėl kurios pateiktas skundas atitinkamoms teisminėms institucijoms, kompetentinga institucija nedelsdama savo oficialioje interneto svetainėje paskelbia šią informaciją, o

vėliau – visą paskesnę susijusią informaciją apie tokio skundo nagrinėjimo rezultatus. Taip pat paskelbiami visi teisminės institucijos sprendimai panaikinti sprendimą skirti administracinę nuobaudą.

6. Kompetentingos institucijos užtikrina, kad bet kokia pagal 1–4 dalis paskelbta informacija jų oficialioje interneto svetainėje būtų prieinama bent penkerius metus po jos paskelbimo. Į paskelbtą informaciją įtraukti asmens duomenys kompetentingos institucijos oficialioje interneto svetainėje skelbiami tokį laikotarpį, koks būtinas vadovaujantis taikytinomis duomenų apsaugos taisyklėmis.

49 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 nuostatos.

2. Pareiga saugoti profesinę paslaptį taikoma visiems asmenims, kurie dirba ar dirbo kompetentingose institucijose pagal šį reglamentą arba bet kokioje kitoje institucijoje, rinkos subjekte arba fiziniam arba juridiniam asmeniui, kuriems tos kompetentingos institucijos delegavo savo įgaliojimus, įskaitant jų samdomus auditorius ir ekspertus.

3. Profesine paslaptimi laikoma informacija negali būti atskleista jokiam kitam asmeniui ar institucijai, išskyrus Sąjungos arba nacionalinės teisės aktų nuostatose nurodytus atvejus.

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.

VIII SKYRIUS

DELEGUOTIEJI AKTAI

50 straipsnis

Įgaliojimų delegavimas

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

2. 28 straipsnio 3 dalyje ir 38 straipsnio 2 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo [LB: įrašyti datą – 5 metai nuo šio reglamento įsigaliojimo dienos]. ***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 28 straipsnio 3 dalyje ir 38 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 28 straipsnio 3 dalį ir 38 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

51 straipsnis

Nuostata dėl peržiūros

Komisija iki [LB: įrašyti datą – 5 metai nuo šio reglamento įsigaliojimo dienos], atitinkamai pasikonsultavusi su EBI, ESMA, EIOPA ir ESRV, peržiūri skyrimo kriterijus ir Europos Parlamentui ir Tarybai pateikia ataskaitą, prie kurios prireikus prideda pasiūlymą dėl teisėkūros procedūra priimamų aktų. ***Ataskaitoje įvertinama bent ši informacija:***

a) ***galimybė išplėsti šio reglamento taikymo sritį įtraukiant mokėjimo sistemų operatorius;***

b) ***savanoriškas pranešimo apie dideles kibernetines grėsmes pobūdis;***

c) 28 straipsnio 2 dalyje nustatytų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių skyrimo kriterijai; ***taip pat***

d) ***bendros priežiūros institucijos sprendimų priėmimo veiksmingumas ir bendros priežiūros institucijos ir ES nepriklausančių valstybių kompetentingų institucijų informacijos mainai.***

II SKIRSNIS

PAKEITIMAI

52 straipsnis

Reglamento (EB) Nr. 1060/2009 pakeitimai

Reglamento (EB) Nr. 1060/2009 I priedo A skirsnio 4 punkto pirma pastraipa pakeičiama taip:

„Kredito reitingų agentūra taiko patikimas administracines ir apskaitos procedūras, vidaus kontrolės mechanizmus, veiksmingas rizikos vertinimo procedūras ir veiksmingas IRT sistemų valdymo kontrolės ir apsaugos priemones pagal Europos Parlamento ir Tarybos reglamentą (ES) 2021/xx* [DORA].

* Europos Parlamento ir Tarybos reglamentas (ES) 2021/xx […] (OL L XX, MMMM M D, p. X).“.

53 straipsnis

Reglamento (ES) Nr. 648/2012 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) 2021/xx* [DORA].

* Europos Parlamento ir Tarybos reglamentas (ES) 2021/xx […] (OL L XX, MMMM M D, p. X).“;

b) 6 dalis išbraukiama;

2) 34 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. Pagrindinė sandorio šalis parengia, įdiegia ir taiko tinkamą veiklos tęstinumo politiką ir veiklos atkūrimo po ekstremaliųjų įvykių planą, apimantį IRT veiklos tęstinumo ir veiklos atkūrimo po ekstremaliųjų įvykių planus, parengtus vadovaujantis Reglamentu (ES) 2021/xx [DORA], 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:

„Siekiant užtikrinti nuoseklų šio straipsnio taikymą, ESMA, 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 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, ESMA 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) 2021/xx [DORA].

2. Sandorių duomenų saugykla parengia, įdiegia ir palaiko tinkamą veiklos tęstinumo politiką ir veiklos atkūrimo po ekstremaliųjų įvykių planą, įskaitant IRT veiklos tęstinumo ir veiklos atkūrimo po ekstremaliųjų įvykių planus, parengtus vadovaujantis Reglamentu (ES) 2021/xx [DORA], kad būtų palaikomos jos funkcijos, būtų laiku atkurta veikla ir kad būtų vykdomi sandorių duomenų saugyklos įsipareigojimai.“;

5) 80 straipsnio 1 dalis išbraukiama.

54 straipsnis

Reglamento (ES) Nr. 909/2014 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) 2021/xx* [DORA], 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.

* Europos Parlamento ir Tarybos reglamentas (ES) 2021/xx […] (OL L XX, MMMM M D, p. X).“;

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 parengia, įdiegia ir taiko tinkamą veiklos tęstinumo ir veiklos atkūrimo po ekstremaliųjų įvykių planą, įskaitant IRT veiklos tęstinumo ir veiklos atkūrimo po ekstremaliųjų įvykių planus, parengtus vadovaujantis Reglamentu (ES) 2021/xx [DORA], kuriais siekiama 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) 2021/xx [DORA] 11 straipsnio 5 ir 7 punktuose.“;

55 straipsnis

Reglamento (ES) Nr. 600/2014 pakeitimai

Reglamentas (ES) Nr. 600/2014 iš dalies keičiamas taip:

1) 27g straipsnis iš dalies keičiamas taip:

   a) 4 dalis išbraukiama;

   b) 8 dalies c punktas pakeičiamas taip:

   c) „c) 3 ir 5 dalyse nustatyti konkretūs organizaciniai reikalavimai.“;

2) 27h straipsnis iš dalies keičiamas taip:

   a) 5 dalis išbraukiama;

   b) 8 dalies e punktas pakeičiamas taip:

   „e) 4 dalyje nustatyti konkretūs organizaciniai reikalavimai.“;

3) 27i straipsnis iš dalies keičiamas taip:

   a) 3 dalis išbraukiama;

   b) 5 dalies b punktas pakeičiamas taip:

   „b) 2 ir 4 dalyse nustatyti konkretūs organizaciniai reikalavimai.“.

56 straipsnis

Įsigaliojimas ir taikymas

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

Jis taikomas nuo [LB: įrašyti datą – ***24 mėnesiai*** nuo įsigaliojimo dienos].

Tačiau 23 ir 24 straipsniai taikomi nuo [LB: įrašyti datą – 36 mėnesiai nuo šio reglamento įsigaliojimo dienos].

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkė	*Pirmininkas*