EUROPOS
KOMISIJA

Briuselis, 2020 09 24
COM(2020) 595 final

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)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

AIŠKINAMASIS MEMORANDUMAS

1. PASIŪLYMO APLINKYBĖS

- Pasiūlymo pagrindimas ir tikslai

Šis pasiūlymas įtrauktas į skaitmeninių finansų dokumentų rinkinį, sudarytą iš priemonių, kuriomis siekiama toliau sudaryti sąlygas plėtoti ir remti skaitmeninių finansų potencialą, skatinti inovacijas ir konkurenciją, kartu mažinant dėl to kylančią riziką. Tai atitinka Komisijos prioritetus užtikrinti, kad Europa prisitaikytų prie skaitmeninio amžiaus, ir kurti perspektyvią žmonėms tarnaujančią ekonomiką. Skaitmeninių finansų dokumentų rinkinys apima naują ES finansų sektoriui skirtą skaitmeninių finansų strategiją[1], kuria siekiama užtikrinti, kad ES dalyvautų skaitmeninėje revoliucijoje ir, pasitelkusi pirmaujančias inovatyvias Europos įmones, jai vadovautų, taip vartotojams ir įmonėms sudarydama sąlygas naudotis skaitmeninių finansų privalumais. Be šio pasiūlymo, rinkinys taip pat apima pasiūlymą dėl kriptoturto rinkų reglamento[2], pasiūlymą dėl reglamento dėl paskirstytojo registro technologijos (PRT) rinkos infrastruktūrai skirtos bandomosios tvarkos[3] ir pasiūlymą dėl direktyvos, kuria būtų paaiškintos arba iš dalies pakeistos tam tikros susijusios ES finansinių paslaugų taisyklės[4]. Finansų sektoriuje skaitmeninimas ir veiklos atsparumas yra dvi tos pačios monetos pusės. Dėl skaitmeninių technologijų, arba informacinių ir ryšių technologijų (IRT), atsiranda ne tik galimybių, bet ir rizika. Jas reikia gerai suprasti ir valdyti, ypač susidarius nepalankiausioms sąlygoms.

Todėl politikos formuotojai ir priežiūros institucijos vis daugiau dėmesio skiria rizikai, kylančiai dėl priklausomybės nuo IRT. Jie visų pirma bandė padidinti įmonių atsparumą nustatydami standartus ir koordinuodami reguliavimo ar priežiūros darbą. Šis darbas buvo atliekamas tiek tarptautiniu, tiek europiniu lygmeniu, taip pat tiek visuose sektoriuose, tiek keliuose konkrečiuose sektoriuose, įskaitant finansinių paslaugų sektorių.

Vis dėlto IRT rizika ir toliau kelia grėsmę ES finansų sistemos veiklos atsparumui, efektyvumui ir stabilumui. Po 2008 m. finansų krizės vykdyta reforma visų pirma buvo didinamas ES finansų sektoriaus finansinis atsparumas[5], o taikant priemones, skirtas platesnio masto operacinės rizikos mažinimui, IRT rizika netiesiogiai sumažinta tik kai kuriose srityse..

Nors ES finansinių paslaugų teisės aktų pakeitimais, padarytais po krizės, buvo sukurtas bendras taisyklių sąvadas, reglamentuojantis didelę su finansinėmis paslaugomis susijusios finansinės rizikos dalį, jais nebuvo išsamiai sprendžiami skaitmeninės veiklos atsparumo klausimai. Priemonėms, kurių buvo imtasi pastarųjų atžvilgiu, buvo būdingos savybės, ribojančios jų veiksmingumą. Pavyzdžiui, jos dažnai buvo rengiamos minimalaus derinimo direktyvų arba principais grindžiamų reglamentų forma, paliekant daug erdvės skirtingiems

---

1 2020 m. rugsėjo 23 d. Komisijos komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos Centriniam Bankui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ES skaitmeninių finansų strategijos (COM(2020) 591).

2 Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl kriptoturto rinkų, kuriuo iš dalies keičiama Direktyva (ES) 2019/1937 (COM(2020) 593).

3 Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl paskirstytojo registro technologija grindžiamoms rinkos infrastruktūroms skirtos bandomosios tvarkos (COM(2020) 594).

4 Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos, kuria iš dalies keičiamos direktyvos 2006/43/EB, 2009/65/EB, 2009/138/ES, 2011/61/ES, ES/2013/36, 2014/65/ES, (ES) 2015/2366 ir ES/2016/2341 (COM(2020) 596).

5 Įvairiomis priimtomis priemonėmis iš esmės siekta padidinti finansų sektoriaus subjektų kapitalo išteklius ir likvidumą, taip pat sumažinti rinkos ir kredito riziką.

požiūriams visoje bendrojoje rinkoje. Be to, reglamentuojant operacinę riziką IRT rizikai buvo skirta gan mažai arba nepakankamai dėmesio. Galiausiai šios priemonės finansinių paslaugų sektoriniuose teisės aktuose yra nevienodos. Taigi Sąjungos lygmens intervencija nevisiškai atitiko tai, ko Europos finansų sektoriaus subjektams reikėjo operacinei rizikai valdyti taip, kad nenukentėtų nuo IRT incidentų poveikio, į jį reaguotų ir atkurtų dėl jo sutrikdytą veiklą. Ji taip pat nesuteikė finansų priežiūros institucijoms pakankamų priemonių jų įgaliojimams vykdyti, kad būtų užkirstas kelias finansiniam nestabilumui, atsirandančiam pasireiškus tokiai IRT rizikai.

Kadangi ES lygmeniu nėra detalių ir išsamių skaitmeninės veiklos atsparumo taisyklių, daugėja nacionalinių reguliavimo iniciatyvų (pvz., susijusių su skaitmeninės veiklos atsparumo testavimu) ir priežiūros metodų (pvz., kuriais sprendžiamas priklausomybės nuo IRT paslaugas teikiančių trečiųjų šalių klausimas). Tačiau dėl tarpvalstybinio IRT rizikos pobūdžio valstybių narių lygmens veiksmai turi tik nedidelį poveikį. Be to, dėl nesuderintų nacionalinių iniciatyvų atsirado dubliavimosi, neatitikimų, pasikartojančių reikalavimų, didelių administracinių ir reikalavimų laikymosi išlaidų, visų pirma tenkančių tarpvalstybiniams finansų sektoriaus subjektams, arba IRT rizika neaptinkama, taigi ir nemažinama. Ši padėtis skaido bendrąją rinką, kenkia ES finansų sektoriaus stabilumui bei vientisumui ir kelia pavojų vartotojų ir investuotojų apsaugai.

Todėl būtina nustatyti detalią ir išsamią ES finansų sektoriaus subjektų skaitmeninės veiklos atsparumo sistemą. Ši sistema sustiprins bendro taisyklių sąvado skaitmeninės rizikos valdymo aspektą. Visų pirma, ja bus sustiprintas ir racionalizuotas finansų sektoriaus subjektų atliekamas IRT rizikos valdymas, nustatytas išsamus IRT sistemų testavimas, padidintas priežiūros institucijų informuotumas apie kibernetinę riziką ir su IRT susijusius incidentus, su kuriais susiduria finansų sektoriaus subjektai, be to, finansų priežiūros institucijoms bus suteikti įgaliojimai prižiūrėti riziką, kylančią dėl finansų sektoriaus subjektų priklausomybės nuo IRT paslaugas teikiančių trečiųjų šalių. Pasiūlymu bus sukurtas nuoseklus pranešimo apie įvykius mechanizmas, padėsiantis palengvinti finansų sektoriaus subjektų administracinę naštą ir sustiprinsiantis priežiūros veiksmingumą.

- Suderinamumas su toje pačioje politikos srityje galiojančiomis nuostatomis

Šis pasiūlymas yra dalis platesnio darbo, vykdomo Europos ir tarptautiniu lygmeniu, siekiant sustiprinti finansinių paslaugų kibernetinį saugumą ir sumažinti platesnę operacinę riziką[6].

Pasiūlymu taip pat reaguojama į 2019 m. Bendrą Europos priežiūros institucijų (EPI) techninę rekomendaciją[7], kurioje raginta laikytis nuoseklesnio požiūrio į IRT rizikos mažinimą finansų srityje ir rekomenduojama Komisijai proporcingai stiprinti finansinių paslaugų sektoriaus skaitmeninės veiklos atsparumą įgyvendinant ES konkrečiam sektoriui skirtą iniciatyvą. EPI rekomendaciją parengė reaguodamos į Komisijos 2018 m. „FinTech“ srities veiksmų planą[8].

- Suderinamumas su kitomis Sąjungos politikos sritimis

Komisijos Pirmininkės U. von der Leyen politinėse gairėse[9] ir Komisijos komunikate „Europos skaitmeninės ateities formavimas“[10] pažymima, kad Europai labai svarbu

---

6 Bazelio bankų priežiūros komitetas, „Kibernetinis atsparumas – praktikos įvairovė“ (angl. *Cyber-resilience: Range of practices*), 2018 m. gruodžio mėn., ir „Patikimo operacinės rizikos valdymo principai“ (angl. *Principles for sound management of operational risk (PSMOR)*), 2014 m. spalio mėn.

7 Bendra Europos priežiūros institucijų rekomendacija Europos Komisijai dėl būtinybės sustiprinti teisinius ES finansų sektoriaus IRT rizikos valdymo reikalavimus (JC 2019 26 (2019)).

8 Europos Komisija, „FinTech“ srities veiksmų planas (COM/2018/0109 *final*).

9 Komisijos Pirmininkė U. von der Leyen, 2019–2024 m. kadencijos Europos Komisijos politinės gairės, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_lt.pdf.

pasinaudoti visais skaitmeninio amžiaus privalumais ir sustiprinti savo pramonės bei inovacijų pajėgumą neperžengiant saugumo ir etikos ribų. Europos duomenų strategijoje[11] nustatytos keturi ramsčiai – duomenų apsauga, pagrindinės teisės, sauga ir kibernetinis saugumas – būtinos sąlygos duomenų teikiamomis galimybėmis besinaudojančiai visuomenei. Visai neseniai Europos Parlamentas pradėjo rengti ataskaitą dėl skaitmeninių finansų, kurioje, be kita ko, ragina laikytis bendro požiūrio į finansų sektoriaus kibernetinį atsparumą[12]. Teisinė sistema, kuria stiprinamas ES finansų sektoriaus subjektų skaitmeninės veiklos atsparumas, atitinka šiuos politikos tikslus. Pasiūlymu taip pat būtų remiama politika, kuria siekiama atsigauti po koronaviruso pandemijos, nes juo būtų užtikrinta, kad priklausomybė nuo skaitmeninių finansų augtų kartu su veiklos atsparumu.

Įgyvendinant šią iniciatyvą nebūtų prarasti su horizontaliąja kibernetinio saugumo sistema (pvz., Direktyva dėl tinklų ir informacinių sistemų saugumo, TIS direktyva) susiję privalumai, nes finansų sektorius ir toliau patektų į jos taikymo sritį. Finansų sektorius ir toliau būtų glaudžiai susijęs su TIS bendradarbiavimo įstaiga, o finansų priežiūros institucijos galėtų keistis atitinkama informacija esamoje TIS ekosistemoje. Ši iniciatyva atitiktų Europos ypatingos svarbos infrastruktūros objektų direktyvą, kuri šiuo metu peržiūrima siekiant padidinti ypatingos svarbos infrastruktūros objektų apsaugą ir atsparumą su kibernetine veikla nesusijusioms grėsmėms. Galiausiai šis pasiūlymas visiškai atitinka saugumo sąjungos strategiją[13], kurioje buvo raginama imtis iniciatyvos dėl finansų sektoriaus skaitmeninės veiklos atsparumo, atsižvelgiant į didelę jo priklausomybę nuo IRT paslaugų ir didelį pažeidžiamumą kibernetinių išpuolių atžvilgiu.

2. TEISINIS PAGRINDAS, SUBSIDIARUMO IR PROPORCINGUMO PRINCIPAI

- Teisinis pagrindas

Šis pasiūlymas dėl reglamento grindžiamas SESV 114 straipsniu.

Juo pašalinamos finansinių paslaugų vidaus rinkos kūrimo ir veikimo kliūtys, o patys kūrimo ir veikimo procesai tobulinami suderinant IRT rizikos valdymo, pranešimų teikimo, testavimo ir trečiosios šalies keliamos IRT rizikos srityse taikomas taisykles. Egzistuojantys skirtumai šioje srityje tiek teisės aktų, tiek priežiūros lygmenimis, taip pat nacionaliniu ir ES lygmenimis trukdo veikti bendrajai finansinių paslaugų rinkai, nes tarpvalstybinę veiklą vykdantys finansų sektoriaus subjektai susiduria su skirtingais ar iš dalies sutampančiais reguliavimo reikalavimais ar priežiūros lūkesčiais, galinčiais jiems trukdyti naudotis įsisteigimo laisve ir paslaugų teikimo laisve. Skirtingomis taisyklėmis taip pat iškraipoma tos pačios rūšies finansų sektoriaus subjektų konkurencija skirtingose valstybėse narėse. Be to, tose srityse, kuriose reikalavimai nesuderinti, suderinti iš dalies ar nepakankamai, skirtingos nacionalinės taisyklės ar metodai, kurie jau galioja arba yra priimami ir įgyvendinami nacionaliniu lygmeniu, gali turėti atgrasomąjį poveikį finansinių paslaugų bendrosios rinkos

---

[10] Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos skaitmeninės ateities formavimas“ (COM(2020) 67 *final*).

[11] Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos duomenų strategija“ (COM(2020) 66 *final*).

[12] Ataskaita su rekomendacijomis Komisijai „Skaitmeniniai finansai: dėl kriptoturto kylanti rizika. Reguliavimo ir priežiūros iššūkiai finansinių paslaugų, įstaigų ir rinkų srityje“, (2020/2034(INL)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en

[13] Komisijos komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ES saugumo sąjungos strategijos (COM(2020) 605 *final*).

laisvėms. Tai ypač pasakytina apie skaitmeninės veiklos testavimo sistemas ir ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūrą.

Kadangi pasiūlymas turi poveikį kelioms Europos Parlamento ir Tarybos direktyvoms, priimtoms remiantis SESV 53 straipsnio 1 dalimi, tuo pat metu priimamas ir pasiūlymas dėl direktyvos, siekiant atspindėti būtinus tų direktyvų pakeitimus.

- Subsidiarumo principas

Dėl stiprių finansinių paslaugų tarpusavio sąsajų, reikšmingos tarpvalstybinės finansų sektoriaus subjektų veiklos ir didelės viso finansų sektoriaus priklausomybės nuo IRT paslaugas teikiančių trečiųjų šalių visų bendras interesas siekiant neprarasti ES finansų rinkų patikimumo– sudaryti sąlygas dideliam skaitmeninės veiklos atsparumui. Skirtumai, atsirandantys dėl nevienodos ar dalinės tvarkos, iš dalies sutampančių ar perteklinių reikalavimų, taikomų tiems patiems finansų sektoriaus subjektams, kurie vykdo tarpvalstybinę veiklą arba turi kelis veiklos leidimus[14] bendrojoje rinkoje, gali būti veiksmingai šalinami tik Sąjungos lygmeniu.

Šiuo pasiūlymu suderinamas itin integruoto ir tarpusavyje susijusio sektoriaus, kuriam jau taikomas bendras taisyklių rinkinys ir priežiūra daugelyje kitų pagrindinių sričių, skaitmeninės veiklos komponentas. Kalbant apie tokius klausimus, kaip pranešimas apie su IRT susijusius incidentus, tik suderintomis Sąjungos taisyklėmis būtų galima sumažinti administracinę naštą ir finansines išlaidas, susijusias su pranešimu apie tą patį su IRT susijusį incidentą skirtingoms Sąjungos ir nacionalinėms institucijoms. ES veiksmai taip pat reikalingi siekiant sudaryti palankesnes sąlygas tarpvalstybinę veiklą vykdančių subjektų, kuriems nesant Sąjungos taisyklių skirtingose valstybėse narėse taikomos arba gali būti taikomos skirtingos sistemos, pažangaus skaitmeninės veiklos atsparumo testavimo rezultatų tarpusavio pripažinimui. Tik Sąjungos lygmens veiksmais galima suvienodinti valstybių narių nustatytus testavimo metodus. ES masto veiksmai taip pat reikalingi siekiant suteikti tinkamus priežiūros įgaliojimus, kad būtų galima stebėti riziką, kylančią dėl IRT paslaugas teikiančių trečiųjų šalių, įskaitant ES finansų sektoriaus koncentracijos ir neigiamo poveikio plitimo riziką.

- Proporcingumo principas

Siūlomomis taisyklėmis neviršijama to, kas būtina pasiūlyme nurodytiems tikslams pasiekti. Jos taikomos tik aspektams, kurių valstybės narės negali įgyvendinti pačios, ir atvejus, kai administracinė našta ir išlaidos yra proporcingos konkretiems ir bendriesiems tikslams, kurių siekiama.

Proporcingumas nustatomas pagal taikymo sritį ir intensyvumą, taikant kokybinius ir kiekybinius vertinimo kriterijus. Jais siekiama užtikrinti, kad naujosios taisyklės, kad ir taikomos visiems finansų sektoriaus subjektams, būtų kartu pritaikytos šių subjektų rizikai ir specifikai pagal jų dydį ir veiklos pobūdį. Proporcingumas taip pat įtrauktas į IRT rizikos valdymo, skaitmeninio atsparumo testavimo, pranešimo apie didelius su IRT susijusius incidentus tvarkos ir ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūros taisykles.

- Priemonės pasirinkimas

[14] Tas pats finansų sektoriaus subjektas gali turėti bankininkystės, investicinės įmonės ir mokėjimo įstaigos licenciją, kurių kiekvieną išdavė skirtinga vienos ar kelių valstybių narių priežiūros institucija.

Priemonės, kurių reikia IRT rizikai valdyti, apie su susijusius IRT incidentus pranešti, ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims testuoti ir prižiūrėti, turi būti įtrauktos į reglamentą, siekiant užtikrinti, kad išsamūs reikalavimai būtų veiksmingai ir tiesiogiai taikomi vienodai, nedarant poveikio proporcingumui ir šiame reglamente numatytoms konkrečioms taisyklėms. Nuoseklumas mažinant skaitmeninės veiklos riziką padeda stiprinti pasitikėjimą finansų sistema ir išlaikyti jos stabilumą. Kadangi priimant reglamentą padedama mažinti reglamentavimo sudėtingumą, skatinama priežiūros konvergencija ir didinamas teisinis tikrumas, šiuo reglamentu taip pat prisidedama prie finansų sektoriaus subjektų, visų pirma vykdančių tarpvalstybinę veiklą, reikalavimų laikymosi išlaidų mažinimo, o tai savo ruožtu padėtų šalinti konkurencijos iškraipymą.

Šiuo reglamentu taip pat panaikinami teisės aktų skirtumai ir nevienodi nacionaliniai reguliavimo ar priežiūros metodai, susiję su IRT rizika, ir taip pašalinamos bendrosios finansinių paslaugų rinkos veikimo kliūtys, visų pirma trukdančios finansų sektoriaus subjektams, kurie vykdo tarpvalstybinę veiklą, sklandžiai naudotis įsisteigimo ir paslaugų teikimo laisve.

Galiausiai bendras taisyklių sąvadas daugiausia buvo rengiamas priimant reglamentus, tad jo atnaujinimas įtraukiant skaitmeninės veiklos atsparumo komponentą turėtų būti atliekamas pasitelkiant tokią pačią teisinę priemonę.

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

- Galiojančių teisės aktų *ex post* vertinimas / tinkamumo patikrinimas

Iki šiol nė viename Sąjungos finansinių paslaugų teisės akte pagrindinis dėmesys nebuvo skiriamas veiklos atsparumui ir nė viename iš jų, net ir tuose, kurių taisyklėmis apskritai reguliuojamas operacinės rizikos aspektas, kurio viena iš sudedamųjų dalių yra IRT rizika, nebuvo visapusiškai nagrinėjama dėl skaitmeninimo kylanti rizika. Sąjungos intervencija iki šiol padėjo tenkinti poreikius ir spręsti problemas, kilusias po 2008 m. finansų krizės: kredito įstaigos nebuvo pakankamai kapitalizuotos, finansų rinkos nebuvo pakankamai integruotos, o suderinimas iki tol buvo minimalus. Tada IRT rizika nebuvo laikoma prioritetu, todėl įvairių finansinių pasektorių teisinės sistemos plėtotos nekoordinuotai. Vis dėlto Sąjungos veiksmais pasiekti užsibrėžti tikslai užtikrinti finansinį stabilumą ir parengti bendrą suderintų prudencinių ir elgesio rinkoje taisyklių, taikomų finansų sektoriaus subjektams visoje ES, rinkinį. Kadangi Sąjungos intervenciją priimant teisės aktus lemiantys veiksniai praeityje nesudarė sąlygų specialioms ar visapusiškoms taisyklėms, skirtoms plačiai paplitusio skaitmeninių technologijų naudojimo ir su tuo susijusios finansų sektoriaus rizikos problemai spręsti, regis, būtų sudėtinga atlikti aiškų vertinimą. Numanomas vertinimas ir su juo susiję teisės aktų pakeitimai atspindėti kiekviename šio reglamento ramstyje.

- Konsultacijos su suinteresuotosiomis šalimis

Rengdama šį pasiūlymą Komisija konsultavosi su suinteresuotosiomis šalimis, visų pirma:

i) Komisija surengė specialias atviras viešas konsultacijas (2019 m. gruodžio 19 d.–2020 m. kovo 19 d.)[15];

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

ii) Komisija konsultavosi su visuomene atlikdama įžanginį poveikio vertinimą (2019 m. gruodžio 19 d.–2020 m. sausio 16 d.)[16];

iii) Komisijos tarnybos du kartus konsultavosi su valstybių narių ekspertais, dirbančiais Bankininkystės, mokėjimų ir draudimo ekspertų grupėje (2020 m. gegužės 18 d. ir 2020 m. liepos 16 d.)[17];

iv) Komisijos tarnybos surengė specialų internetinį seminarą skaitmeninės veiklos atsparumo klausimais, kuris buvo vienas iš 2020 m. vykusių informacinių skaitmeninių finansų renginių (2020 m. gegužės 19 d.).

Per viešas konsultacijas Komisija siekė gauti informacijos, aktualios plėtojant galimą ES tarpsektorinės skaitmeninės veiklos atsparumo sistemą finansinių paslaugų srityje. Iš atsakymų matyti platus pritarimas naujos specialios sistemos, pagal kurią būtų imtasi veiksmų keturiose srityse, dėl kurių vyko konsultacijos, nustatymui, bet kartu pabrėžiamas poreikis užtikrinti proporcingumą ir atidžiai spręsti sąveikos su TIS direktyvos horizontaliosiomis taisyklėmis problemą ir šią sąveiką paaiškinti. Komisija gavo du atsakymus dėl įžanginio poveikio vertinimo, kuriuose respondentai aptarė konkrečius aspektus, susijusius su jų veiklos sritimi.

2020 m. gegužės 18 d. surengtame Komisijos bankininkystės, mokėjimų ir draudimo ekspertų grupės posėdyje valstybės narės išreiškė didelę paramą finansų sektoriaus skaitmeninės veiklos atsparumo stiprinimui imantis veiksmų, numatytų kartu su keturiais Komisijos pristatytais elementais. Valstybės narės taip pat pabrėžė būtinybę aiškiai suderinti naujas taisykles su operacinės rizikos taisyklėmis (ES finansinių paslaugų teisės aktuose) ir horizontaliosiomis kibernetinio saugumo taisyklėmis (TIS direktyva). Antrame posėdyje kai kurios valstybės narės pabrėžė būtinybę užtikrinti proporcingumą ir atsižvelgti į ypatingą mažųjų įmonių ar didesnių grupių patronuojamųjų įmonių padėtį, taip pat būtinybę suteikti tvirtus įgaliojimus už priežiūrą atsakingoms nacionalinėms kompetentingoms institucijoms.

Į pasiūlymą taip pat įtraukta grįžtamoji informacija, gauta per susitikimus su suinteresuotosiomis šalimis ir ES institucijomis bei įstaigomis. Suinteresuotosios šalys, įskaitant IRT paslaugas teikiančias trečiąsias šalis, apskritai pritarė pasiūlymui. Iš gautos grįžtamosios informacijos analizės matyti, kad raginama rengiant taisykles išsaugoti proporcingumą ir laikytis principais ir rizika grindžiamo požiūrio. Daugiausia informacijos pateikė tokios institucijos, kaip Europos sisteminės rizikos valdyba (ESRV), EPI, Europos Sąjungos kibernetinio saugumo agentūra (ENISA) ir Europos Centrinis Bankas (ECB), taip pat valstybių narių kompetentingos institucijos.

- Tiriamųjų duomenų rinkimas ir naudojimas

Rengdama šį pasiūlymą Komisija rėmėsi iš pripažintų šaltinių, įskaitant dvi bendras EPI technines rekomendacijas, surinktais kokybiniais ir kiekybiniais įrodymais. Juos papildė konfidencialūs duomenys ir viešai skelbiamos priežiūros institucijų, tarptautinių standartus nustatančių įstaigų ir pirmaujančių mokslinių tyrimų institutų ataskaitos, taip pat nustatytų suinteresuotųjų šalių iš viso pasaulio finansų sektoriaus pateikti kiekybiniai ir kokybiniai duomenys.

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

- Poveikio vertinimas

Prie šio pasiūlymo pridedamas poveikio vertinimas[18], kuris Reglamentavimo patikros valdybai buvo pateiktas 2020 m. balandžio 29 d. ir jos patvirtintas 2020 m. gegužės 29 d. Reglamentavimo patikros valdyba rekomendavo pasiūlymą tam tikrose srityse patobulinti siekiant: i) pateikti daugiau informacijos apie tai, kaip būtų užtikrintas proporcingumas; ii) geriau pabrėžti, kokiu mastu tinkamiausia galimybė skiriasi nuo bendros EPI techninės rekomendacijos ir kodėl ši galimybė yra optimali, ir iii) papildomai pabrėžti pasiūlymo ir galiojančių ES teisės aktų, įskaitant šiuo metu peržiūrimas taisykles, sąveiką. Poveikio vertinimas buvo pakoreguotas siekiant atsižvelgti į šiuos aspektus, taip pat išsamesnes Reglamentavimo patikros valdybos pastabas.

Rengdama skaitmeninės veiklos atsparumo sistemą, Komisija nagrinėjo keletą galimų politikos priemonių:

- „nieko nekeisti“: veiklos atsparumo taisyklės ir toliau būtų nustatomos pagal dabartines skirtingas ES finansinių paslaugų nuostatas, iš dalies TIS direktyvą ir galiojančias ar būsimas nacionalines taisykles;
- 1 galimybė: kapitalo rezervų stiprinimas – būtų nustatyti papildomi kapitalo rezervai siekiant padidinti finansų sektoriaus subjektų gebėjimą padengti nuostolius, galinčius atsirasti dėl nepakankamo skaitmeninės veiklos atsparumo;
- 2 galimybė: finansinių paslaugų skaitmeninės veiklos atsparumo akto priėmimas – sudaryti sąlygas ES lygmeniu sukurti išsamią sistemą, kurioje būtų nustatytos nuoseklios taisyklės, atitinkančios visų reguliuojamų finansų sektoriaus subjektų skaitmeninės veiklos atsparumo poreikius, ir nustatyti ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūros sistemą;
- 3 galimybė: finansinių paslaugų skaitmeninės veiklos atsparumo aktas kartu su centralizuota ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūra – be skaitmeninės veiklos atsparumo akto (2 galimybė), būtų įsteigta nauja institucija, kuri prižiūrėtų, kaip IRT paslaugas teikiančios trečiosios šalys teikia paslaugas.

Buvo pasirinkta antra galimybė, nes ja veiksmingai, produktyviai ir derinant veiksmus su kitomis Sąjungos politikos sritimis pasiekiama dauguma numatytų tikslų. Dauguma suinteresuotųjų šalių šiai galimybei taip pat teikia pirmenybę.

Dėl pasirinktos galimybės atsirastų ir vienkartinių, ir pasikartojančių išlaidų[19]. Vienkartines išlaidas daugiausia lemia investicijos į IT sistemas, todėl jas sunku kiekybiškai įvertinti atsižvelgiant į nevienodą įmonių sudėtingą IT aplinką, ypač senąsias IT sistemas. Nepaisant to, didelių įmonių atveju šios išlaidos gali būti nedidelės, nes jos jau yra daug investavusios į IRT. Tikimasi, kad mažesnių įmonių išlaidos taip pat nebus didelės, nes būtų taikomos proporcingos priemonės atsižvelgiant į mažesnę jų riziką.

[18] 2020 m. rugsėjo 24 d. Komisijos tarnybų darbinis dokumentas „Poveikio vertinimo ataskaita“, pridedamas prie Europos Parlamento ir Tarybos reglamento 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 (SWD(2020) 198).

[19] *Ten pat, p. 89–94.*

Pasirinkta galimybė turėtų teigiamą poveikį finansinių paslaugų sektoriuje veikiančioms MVĮ ekonominiu, socialiniu ir poveikio aplinkai požiūriu. Pasiūlymu bus paaiškinta MVĮ, kokios taisyklės taikomos, o tai sumažins reikalavimų laikymosi išlaidas.

Pagrindinį pasirinktos politikos galimybės socialinį poveikį pajustų vartotojai ir investuotojai. Didesnis ES finansų sistemos skaitmeninės veiklos atsparumas sumažintų incidentų skaičių ir vidutines kiekvieno incidento išlaidas. Visai visuomenei būtų naudingas didesnis pasitikėjimas finansinių paslaugų sektoriumi.

Galiausiai, kalbant apie poveikį aplinkai, pasirinkta politikos galimybė paskatintų aktyviau naudoti naujausios kartos IRT infrastruktūras ir paslaugas, kurios turėtų tapti tvaresnėmis aplinkos apsaugos požiūriu.

- Reglamentavimo tinkamumas ir supaprastinimas

Panaikinus iš dalies sutampančius pranešimo apie su IRT susijusius incidentus tvarkos reikalavimus sumažėtų administracinė našta ir susijusios išlaidos. Be to, suderintas skaitmeninės veiklos atsparumo testavimas, abipusiai pripažįstamas visoje bendrojoje rinkoje, sumažins išlaidas, ypač tenkančias tarpvalstybinėms įmonėms, kurioms kitu atveju galėtų tekti atlikti testavimą keliose valstybėse narėse[20].

- Pagrindinės teisės

ES yra įsipareigojusi užtikrinti, kad būtų laikomasi pagrindinių teisių apsaugos aukštų standartų. Visi finansų sektoriaus subjektų savanoriško dalijimosi informacija schemos, kuriomis naudotis skatinama šiuo reglamentu, būtų įgyvendinamos patikimoje aplinkoje visapusiškai laikantis Sąjungos duomenų apsaugos taisyklių, visų pirma Europos Parlamento ir Tarybos reglamento (ES) 2016/679[21], ypač tais atvejais, kai siekiant teisėto duomenų valdytojo intereso būtina tvarkyti asmens duomenis.

4. POVEIKIS BIUDŽETUI

Kalbant apie poveikį biudžetui, kadangi dabartiniame reglamente numatoma stiprinti EPI vaidmenį suteikiant joms įgaliojimus tinkamai prižiūrėti ypatingos svarbos IRT paslaugas teikiančias trečiąsias šalis, pasiūlyme būtų numatyta skirti daugiau išteklių, visų pirma priežiūros užduotims vykdyti (pavyzdžiui, patikrinimams vietoje ir elektroniniu būdu, taip pat auditui), ir pasitelkti specialių IRT saugumo žinių turinčius darbuotojus.

Šių išlaidų mastas ir paskirstymas priklausys nuo naujų priežiūros įgaliojimų masto ir (tikslių) užduočių, kurias turės atlikti EPI. Kalbant apie naujus personalo išteklius, įsigaliojus skirtingoms pasiūlymo nuostatoms EBI, ESMA ir EIOPA iš viso reikės 18 visą darbo dieną dirbančių darbuotojų (etato ekvivalentų) – po 6 etato ekvivalentus kiekvienai institucijai (skaičiuojama, kad 2022–2027 m. šios išlaidos sudarys 15,71 mln. EUR). Be to, EPI patirs papildomų IT išlaidų, patikrinimų vietoje komandiruočių ir vertimo raštu išlaidų (skaičiuojama, kad 2022–2027 m. jos sudarys 12 mln. EUR), taip pat kitų administracinių išlaidų (skaičiuojama, kad 2022–2027 m. jos sudarys 2,48 mln. EUR). Todėl skaičiuojama, kad 2022–2027 m. bendros išlaidos sudarys maždaug 30,19 mln. EUR.

---

[20] Ten pat.

[21] 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).

Taip pat reikėtų pažymėti, kad nors darbuotojų skaičius (pvz., nauji darbuotojai ir kitos išlaidos, susijusios su naujomis užduotimis), būtinas tiesioginei priežiūrai, ilgainiui priklausys nuo ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių, kurių priežiūra bus vykdoma, skaičiaus ir dydžio pokyčių, atitinkamos išlaidos bus visiškai finansuojamos iš tų rinkos dalyvių mokamų mokesčių. Todėl poveikis ES biudžeto asignavimams nenumatomas (išskyrus papildomus darbuotojus), nes šios išlaidos bus visiškai finansuojamos iš mokesčių.

Šio pasiūlymo finansinis poveikis ir poveikis biudžetui išsamiai paaiškintas prie šio pasiūlymo pridedamoje finansinėje teisės akto pasiūlymo pažymoje.

5. KITI ELEMENTAI

- Įgyvendinimo planai ir stebėsena, vertinimas ir ataskaitų teikimo tvarka

Į pasiūlymą įtrauktas bendras poveikio konkretiems tikslams stebėsenos ir vertinimo planas, pagal kurį Komisija praėjus ne daugiau kaip trejiems metams nuo įsigaliojimo datos turi atlikti peržiūrą ir pateikti pagrindinių išvadų ataskaitą Europos Parlamentui ir Tarybai.

Peržiūra turi būti atliekama vadovaujantis Komisijos geresnio reglamentavimo gairėmis.

- Išsamus konkrečių pasiūlymo nuostatų paaiškinimas

Pasiūlymo struktūra atitinka kelias pagrindines politikos sritis, t. y. pagrindinius tarpusavyje susijusius ramsčius, bendru sutarimu įtrauktus į Europos ir tarptautines rekomendacijas ir geriausią praktiką, kuriomis siekiama didinti finansų sektoriaus kibernetinį ir veiklos atsparumą.

Reglamento taikymo sritis ir proporcingas reikalingų priemonių taikymas (2 straipsnis)

Siekiant užtikrinti, kad finansų sektoriui taikomi IRT rizikos valdymo reikalavimai būtų nuoseklūs, reglamentas taikomas įvairiems Sąjungos lygmeniu reguliuojamiems finansų sektoriaus subjektams, t. y. kredito įstaigoms, mokėjimo įstaigoms, elektroninių pinigų įstaigoms, investicinėms įmonėms, kriptoturto paslaugų teikėjams, centriniams vertybinių popierių depozitoriumams, pagrindinėms sandorio šalims, prekybos vietoms, sandorių duomenų saugykloms, alternatyvaus investavimo fondų valdytojams ir valdymo įmonėms, duomenų teikimo paslaugų teikėjams, draudimo ir perdraudimo įmonėms, draudimo tarpininkams, perdraudimo tarpininkams ir papildomos draudimo veiklos tarpininkams, profesinių pensijų įstaigoms, kredito reitingų agentūroms, teisės aktų nustatytą auditą atliekantiems auditoriams ir audito įmonėms, ypatingos svarbos lyginamųjų indeksų administratoriams ir sutelktinio finansavimo paslaugų teikėjams.

Tokia taikymo sritis padeda vienodai ir nuosekliai taikyti visus rizikos valdymo komponentus su IRT susijusiose srityse, kartu užtikrinant vienodas sąlygas finansų sektoriaus subjektams vykdyti savo reguliavimo pareigas, susijusias su IRT rizika. Be to, reglamente pripažįstama, kad finansų sektoriaus subjektai gerokai skiriasi savo dydžiu, veiklos pobūdžiu arba jiems gresiančia skaitmenine rizika. Kadangi didesni finansų sektoriaus subjektai turi daugiau išteklių, tik finansų sektoriaus subjektai, nelaikomi labai mažomis įmonėmis, yra įpareigoti, pavyzdžiui, nustatyti sudėtingą valdymo tvarką, specialias valdymo funkcijas, atlikti išsamų vertinimą po tinklų ir informacinės sistemos infrastruktūros svarbių pakeitimų, reguliariai atlikti senųjų IRT sistemų rizikos analizę, išplėsti veiklos tęstinumo ir reagavimo bei veiklos atkūrimo planų testavimą, kad būtų galima nustatyti jų pirminės IRT infrastruktūros pakeitimo atsarginiais įrenginiais scenarijus. Be to, tik finansų sektoriaus subjektai, kurie

laikomi reikšmingais atliekant pažangų skaitmeninio atsparumo testavimą, bus įpareigoti atlikti grėsmėmis grindžiamą skverbimosi (TLPT) testavimą.

Nepaisant šios plačios taikymo srities, ji nėra išsami. Visų pirma, šis reglamentas netaikomas sistemos operatoriams, kaip apibrėžta Direktyvos 98/26/EB[22] dėl atsiskaitymų baigtinumo mokėjimų ir vertybinių popierių atsiskaitymų sistemose 2 straipsnio p punkte, taip pat sistemos dalyviams, nebent toks dalyvis pats yra Sąjungos lygmeniu reguliuojamas finansų sektoriaus subjektas, todėl šis reglamentas jam būtų teisėtai taikomas (t. y. kredito įstaiga, investicinė įmonė, pagrindinė sandorio šalis). Be to, į taikymo sritį nepatenka ir Sąjungos apyvartinių taršos leidimų registras, kuris prižiūrint Europos Komisijai tvarkomas pagal Direktyvą 2003/87/EB[23].

Taikant tokias Atsiskaitymų baigtinumo direktyvos išimtis atsižvelgiama į poreikį papildomai peržiūrėti teisinius ir politinius klausimus, susijusius su Atsiskaitymų baigtinumo direktyvos sistemos operatoriais ir dalyviais, kartu tinkamai atsižvelgiant į šiuo metu centrinių bankų valdomoms mokėjimo sistemoms taikomų sistemų[24] poveikį. Kadangi šie klausimai gali būti susiję su aspektais, kurie yra nesusiję su klausimais, kuriems taikomas šis reglamentas, Komisija toliau vertins, ar į šio reglamento taikymo sritį būtina įtraukti ir subjektus bei IRT infrastruktūras, kurie šiuo metu į ją neįtraukti, ir kokį poveikį tai turėtų.

Su valdymu susiję reikalavimai (4 straipsnis)

Šiuo reglamentu siekiama geriau suderinti finansų sektoriaus subjektų verslo strategijas ir IRT rizikos valdymo vykdymą. Tuo tikslu valdymo organas turės atlikti ypatingos svarbos aktyvų vaidmenį taikant IRT rizikos valdymo sistemą ir laikytis griežtos kibernetinės higienos. Visiška valdymo organo atsakomybė valdant finansų sektoriaus subjekto IRT riziką taps bendruoju principu, kurio pagrindu bus parengti konkretūs reikalavimai, pavyzdžiui, taikomi aiškių pareigų ir atsakomybės už visas su IRT susijusias funkcijas priskyrimui, nuolatiniam dalyvavimui kontroliuojant IRT rizikos valdymo stebėseną, visuose įvairiausiuose patvirtinimo bei kontrolės procesuose ir tinkamai paskirstant IRT investicijas ir mokymo poreikius.

IRT rizikos valdymo reikalavimai (5–14 straipsniai)

Pagal bendrą EPI techninę rekomendaciją skaitmeninės veiklos atsparumas grindžiamas pagrindiniais IRT rizikos valdymo sistemos principais ir reikalavimais. Šie reikalavimai, grindžiami atitinkamais tarptautiniais, nacionaliniais ir sektoriaus standartais, gairėmis ir rekomendacijomis, yra orientuoti į konkrečias IRT rizikos valdymo funkcijas (identifikavimą, apsaugą ir prevenciją, aptikimą, reagavimą ir atkūrimą, mokymąsi, tobulinimąsi bei komunikaciją). Kad neatsiliktų nuo sparčiai kintančios kibernetinių grėsmių aplinkos, finansų sektoriaus subjektai yra įpareigoti diegti ir prižiūrėti atsparias IRT sistemas ir priemones, kuriomis būtų mažinamas IRT rizikos poveikis, nuolat identifikuoti visus IRT rizikos šaltinius, diegti apsaugos ir prevencijos priemones, skubiai aptikti neįprastą veiklą, įgyvendinti specialią ir visapusišką veiklos tęstinumo politiką ir veiklos atkūrimo po

[22] 1998 m. gegužės 19 d. Europos Parlamento ir Tarybos direktyva 98/26/EB dėl atsiskaitymų baigtinumo mokėjimų ir vertybinių popierių atsiskaitymų sistemose (OL L 166, 1998 6 11, p. 45).

[23] 2003 m. spalio 13 d. Europos Parlamento ir Tarybos direktyva 2003/87/EB, nustatanti šiltnamio efektą sukeliančių dujų emisijos leidimų sistemą Bendrijoje ir iš dalies keičianti Tarybos direktyvą 96/61/EB (OL L 275, 2003 10 25, p. 32).

[24] Visų pirma, 2014 m. liepos 3 d. Europos Centrinio Banko reglamento (ES) Nr. 795/2014 dėl priežiūros reikalavimų sistemiškai svarbioms mokėjimo sistemoms.

ekstremaliųjų įvykių planus, kurie yra neatsiejama einamosios veiklos tęstinumo politikos dalis. Pastarieji komponentai reikalingi skubiam veiklos atkūrimui po su IRT susijusių incidentų, visų pirma kibernetinių išpuolių, ribojant žalą ir teikiant pirmenybę saugiam veiklos atnaujinimui. Pačiu reglamentu specialus standartizavimas nenustatomas, tačiau reglamentas grindžiamas Europos ir tarptautiniu mastu pripažintais techniniais standartais arba geriausia sektoriaus praktika, kai jie visiškai atitinka priežiūros nurodymus dėl tokių tarptautinių standartų taikymo ir įtraukimo. Šis reglamentas taip pat taikomas fizinės infrastruktūros ir įrangos, palaikančių technologijų naudojimą, atitinkamus IRT srities procesus ir darbuotojus, iš dalies atsakingus už finansų sektoriaus subjekto veiklos skaitmeninį pėdsaką, vientisumui, saugai ir atsparumui.

Pranešimai apie su IRT susijusius incidentus (15–20 straipsniai)

Pranešimo apie su IRT susijusius incidentus tvarkos suderinimas ir racionalizavimas pasiekiamas, pirma, nustatant bendrą reikalavimą finansų sektoriaus subjektams nustatyti ir įgyvendinti valdymo procesą, skirtą su IRT susijusiems incidentams stebėti ir registruoti, kartu nustatant pareigą juos klasifikuoti remiantis reglamente nustatytais kriterijais, kuriuos toliau plėtoja EPI nustatydamos reikšmingumo ribas. Antra, kompetentingoms institucijoms turi būti pranešta tik apie su IRT susijusius incidentus, kurie laikomi dideliais. Pranešimai turėtų būti teikiami naudojant bendrą šabloną ir laikantis EPI parengtos suderintos procedūros. Finansų sektoriaus subjektai turėtų teikti pradinius, tarpinius ir galutinius pranešimus ir informuoti savo naudotojus ir klientus, kai incidentas daro arba gali daryti poveikį jų finansiniams interesams. Kompetentingos institucijos turėtų pateikti aktualią informaciją apie incidentus kitoms įstaigoms ar institucijoms: EPI, ECB ir pagal Direktyvą (ES) 2016/1148 paskirtiems bendriesiems informaciniams centrams.

Siekiant užmegzti finansų sektoriaus subjektų ir kompetentingų institucijų dialogą, padėsiantį sumažinti poveikį ir identifikuoti tinkamas taisomąsias priemones, pranešimas apie didelius su IRT susijusius incidentus turėtų būti papildytas priežiūros grįžtamąją informaciją ir rekomendacijomis.

Galiausiai EPI, ECB ir ENISA bendroje ataskaitoje turėtų būti toliau nagrinėjama galimybė Sąjungos lygmeniu centralizuoti pranešimų apie su IRT susijusius incidentus teikimą ir įvertintos galimybės įsteigti vieną bendrą ES centrą, kuriam finansų sektoriaus subjektai teiktų pranešimus apie didelius su IRT susijusius incidentus.

Skaitmeninės veiklos atsparumo testavimas (21–24 straipsniai)

IRT rizikos valdymo sistemą sudarantys pajėgumai ir funkcijos turi būti periodiškai testuojami siekiant patikrinti jų parengtį ir identifikuoti silpnąsias vietas, trūkumus ar spragas, taip pat greitai įgyvendinti taisomąsias priemones. Šiuo reglamentu sudaromos sąlygos proporcingai taikyti skaitmeninės veiklos atsparumo testavimo reikalavimus atsižvelgiant į finansų sektoriaus subjektų dydį, veiklos ir rizikos pobūdį: nors testuoti IRT priemones ir sistemas turėtų visi subjektai, pažangų TLPT testavimą reikėtų įpareigoti atlikti tik tuos subjektus, kuriuos kompetentingos institucijos (remdamosi šiame reglamente nustatytais ir EPI toliau išplėtotais kriterijais) yra priskyrusios svarbiems ir kibernetiniu atžvilgiu brandiems subjektams. Šiame reglamente taip pat nustatomi reikalavimai, taikomi testuotojams ir keliose valstybėse narėse veiklą vykdančių finansų sektoriaus subjektų TLPT testavimo rezultatų pripažinimui visoje Sąjungoje.

Trečiosios šalies keliama IRT rizika (25–39 straipsniai)

Reglamentu siekiama užtikrinti patikimą trečiosios šalies keliamos IRT rizikos stebėseną. Šis tikslas bus pasiektas pirmiausia laikantis principinių taisyklių, taikomų finansų sektoriaus subjektų vykdomai rizikos, kylančios dėl IRT paslaugas teikiančių trečiųjų šalių, stebėsenai.

Antra, šiuo reglamentu suderinami pagrindiniai paslaugų ir santykių su IRT paslaugas teikiančiomis trečiosiomis šalimis elementai. Šie elementai apima būtiniausius aspektus, kurie laikomi ypatingai svarbiais, kad finansų sektoriaus subjektas galėtų vykdyti visapusišką trečiosios šalies keliamos IRT rizikos stebėseną visą sutarties sudarymo, vykdymo ir nutraukimo laikotarpį bei po jos nutraukimo.

Visų pirma, sutartyse, kuriomis reglamentuojami tokie santykiai, turės būti išsamiai aprašytos paslaugos, nurodytos vietos, kuriose turi būti tvarkomi duomenys, pateikiamas išsamus paslaugų lygio aprašymas kartu su kiekybiniais ir kokybiniais tiksliniais veiklos rezultatų rodikliais, nurodomos atitinkamos nuostatos dėl asmens duomenų pasiekiamumo, prieinamumo, vientisumo, saugumo ir apsaugos, taip pat prieigos, veiklos atkūrimo ir grąžinimo garantijos IRT paslaugas teikiančioms trečiosioms šalims žlugus, IRT paslaugas teikiančių trečiųjų šalių įspėjimo terminai ir pareigos pranešti, finansų sektoriaus subjekto arba paskirtos trečiosios šalies prieigos, patikrinimo ir audito teisės, aiškios sutarties nutraukimo teisės ir specialios pasitraukimo strategijos. Be to, kadangi kai kuriuos iš šių sutartinių elementų galima standartizuoti, reglamentu skatinama savanoriškai naudoti standartines sutarčių sąlygas, kurias Komisija turi parengti debesijos paslaugai.

Galiausiai reglamentu siekiama skatinti priežiūros metodų, taikomų trečiosios šalies keliamai IRT rizikai finansų sektoriuje, konvergenciją, ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims nustatant Sąjungos priežiūros sistemą. Taikant naują suderintą teisinę sistemą, EPI, paskirtai kiekvienos tokios ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies atsakingąja priežiūros institucija, suteikiami įgaliojimai užtikrinti, kad technologijų paslaugų teikėjai, kurie yra ypatingai svarbūs finansų sektoriaus veikimui, būtų tinkamai stebimi visos Europos mastu. Šiame reglamente numatyta priežiūros sistema yra grindžiama esama finansinių paslaugų srities institucine struktūra, kurioje EPI jungtinis komitetas užtikrina tarpsektorinį visų IRT rizikos klausimų koordinavimą pagal savo kibernetinio saugumo užduotis, padedamas atitinkamo pakomitečio (Priežiūros forumo), atliekančio parengiamąjį darbą, susijusį su atskirais sprendimais ir bendromis rekomendacijomis, skirtomis ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims.

Dalijimasis informacija (40 straipsnis)

Siekiant didinti informuotumą apie IRT riziką, mažinti jos plitimą, remti finansų sektoriaus subjektų gynybos pajėgumus ir grėsmių aptikimo metodus, reglamentu finansų sektoriaus subjektams leidžiama sudaryti susitarimus dėl keitimosi informacija ir žvalgybos informacija apie kibernetines grėsmes.

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,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

atsižvelgdami į Europos Centrinio Banko nuomonę[25],

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę[26],

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, draudimo veiklą, žalų administravimą ir netiesioginio aptarnavimo operacijas. 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;

---

25 [*įrašyti nuorodą*] OL C , , p. .

26 [*įrašyti nuorodą*] OL C , , p. .

(3) 2020 m. ataskaitoje dėl sisteminės kibernetinės rizikos[27] 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[28] į visą finansų sistemą. Sunkūs IRT pažeidimai finansų srityje daro poveikį ne tik finansų sektoriaus subjektams. Jie taip pat sudaro sąlygas vienoje vietoje atsiradusiems pažeidžiamumams plisti finansiniais perdavimo kanalais ir gali turėti neigiamų padarinių Sąjungos finansų sistemos stabilumui, 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;

(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[29] 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;

---

27 2020 m. vasario mėn. ESRV ataskaita „Sisteminė kibernetinė rizika“, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

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

29 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.

(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 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, išplečiant finansų priežiūros institucijų, kurioms pavesta stebėti ir saugoti finansinį stabilumą ir rinkos vientisumą, įgaliojimus;

(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;

(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 visos 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;

(13) finansų sektoriaus subjektai, mažindami IRT riziką, turėtų laikytis to paties požiūrio ir tų pačių principinių taisyklių. Nuoseklumas padeda didinti pasitikėjimą finansų sistema ir išsaugoti jos stabilumą, ypač esant pertekliniam IRT sistemų, platformų ir infrastruktūrų naudojimui, dėl kurio 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;

(15) be finansinių paslaugų teisės aktų, Europos Parlamento ir Tarybos direktyva (ES) 2016/1148[30] 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,

[30] 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).

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 šis reglamentas yra *lex specialis* Direktyvos (ES) 2016/1148 atžvilgiu.

Labai svarbu išlaikyti tvirtą finansų sektoriaus ir Sąjungos horizontaliosios kibernetinio saugumo sistemos sąryšį, nes taip būtų užtikrintas suderinamumas su valstybių narių jau priimtomis kibernetinio saugumo strategijomis, o finansų priežiūros institucijos galėtų būti informuotos 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 kompetentingos institucijos taip pat turėtų konsultuotis ir bendradarbiauti su nacionalinėmis CSIRT, paskirtomis pagal Direktyvos (ES) 2016/1148 9 straipsnį;

(18) taip pat svarbu užtikrinti suderinamumą 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, o tai gali turėti įtakos finansų sektoriui[31];

(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. 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

[31] 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).

sistemų testavimo, kontrolės priemonių ir procesų, taip pat trečiosios šalies keliamos IRT rizikos valdymo mechanizmus ir politiką. Reikėtų didinti finansų sistemos skaitmeninės veiklos atsparumo kartelę, kartu sudarant sąlygas proporcingai taikyti reikalavimus finansų sektoriaus subjektams, kurie yra labai mažos įmonės, kaip apibrėžta Komisijos rekomendacijoje 2003/361/EB[32];

(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)[33] 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;

(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 pranešimo apie su IRT susijusius incidentus tvarka būtų papildyta reikalavimais, kurių šiuo metu trūksta finansų pasektorių teisės aktuose, ir pašalinti 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 tik savo kompetentingoms institucijoms. 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 nekoordinuojamas nacionalines sistemas, tas pačias problemas sprendžiant skirtingai. Dėl to tarpvalstybiniai finansų sektoriaus subjektai patiria dvigubų išlaidų, o abipusis rezultatų pripažinimas yra sudėtingas. Todėl dėl nekoordinuojamo testavimo gali būti skaidoma bendroji rinka;

(24) be to, tais atvejais, kai testavimas neprivalomas, pažeidžiamumai 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 pažeidžiamumų ir rizikos, netestuotų apsaugos pajėgumų ir veiklos tęstinumo ir neįgytų didesnio klientų, tiekėjų ir verslo

---

[32] 2003 m. gegužės 6 d. Komisijos rekomendacija dėl labai mažų, mažųjų ir vidutinio dydžio įmonių sampratos (OL L 124, 2003 5 20, p. 36).

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

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[34], 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 apsunkina tai, kad nėra konkrečių įgaliojimų ir priemonių, leidžiančių nacionalinėms priežiūros institucijoms gerai suprasti priklausomybę nuo IRT paslaugas teikiančių trečiųjų šalių ir tinkamai stebėti riziką,

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

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 yra ypatingai svarbūs finansų sektoriaus subjektų paslaugų teikėjai, veiklą;

(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 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;

(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), 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;

(32) todėl finansų sektoriaus subjektai 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 suvaržant IRT rizikos plitimą ir neleidžiant neigiamam poveikiui plisti finansiniais kanalais. Tokie mechanizmai turėtų būti įgyvendinami visiškai laikantis galiojančių Sąjungos konkurencijos teisės taisyklių[35] ir tokiu būdu, kad būtų visiškai laikomasi Sąjungos duomenų apsaugos taisyklių, iš esmės Europos Parlamento ir Tarybos reglamento (ES) 2016/679[36], 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 turėtų būti taikomos atsižvelgiant į didelius finansų sektoriaus

---

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

36 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).

subjektų dydžio, veiklos pobūdžio ar skaitmeninės rizikos skirtumus. Paprastai finansų sektoriaus subjektai, skirdami išteklius ir pajėgumus IRT rizikos valdymo sistemai įgyvendinti, turėtų tinkamai nustatyti su IRT susijusius poreikius atsižvelgdami į savo dydį ir veiklos pobūdį, 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 išlaidas ir nuostolius, patirtus dėl IRT sutrikimų, ir po 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[37], 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, 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.

---

[37] CPSS-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 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 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 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 pažeidžiamumus, siekdamos prisidėti prie platesnio masto kolektyvinės gynybos;

(43) reikėtų papildomai apsvarstyti galimybę centralizuoti pranešimų apie su IRT susijusius incidentus teikimą vienam pagrindiniam 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 turėtų reguliariai testuoti savo IRT sistemų ir darbuotojų prevencinių, aptikimo, reagavimo ir veiklos atkūrimo pajėgumų veiksmingumą, kad atskleistų ir pašalintų galimus IRT pažeidžiamumus. 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;

(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, 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 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;

(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 sutarčių nutraukimą turėtų lemti bent kelios aplinkybės, iš kurių būtų matyti 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, visų pirma, kai jie sudaromi su trečiojoje valstybėje įsisteigusiomis IRT paslaugas teikiančiomis trečiosiomis šalimis. Šiame etape ir siekiant užtikrinti tinkamą pusiausvyrą tarp būtinybės išsaugoti laisvę sudaryti sutartis ir užtikrinti finansinį stabilumą, manoma, kad nustatyti griežtas IRT paslaugas teikiančių trečiųjų šalių rizikos pozicijų viršutines ribas ir apribojimus yra netikslinga. EPI, paskirta vykdyti kiekvienos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies priežiūrą (toliau – atsakingoji priežiūros institucija), vykdydama 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[38];

(50) siekiant, kad būtų galima reguliariai vertinti ir stebėti IRT paslaugas teikiančios trečiosios šalies gebėjimą saugiai teikti paslaugas finansų sektoriaus subjektui

[38] 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.

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 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 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;

(53) 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 finansų sektoriaus subjekto kompetentinga institucija turėtų turėti teisę, pateikusi įspėjimą ir laikydamasi konfidencialumo principo, patikrinti ir audituoti IRT paslaugas teikiančią trečiąją šalį;

(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 pastarajam veiksmingai pakeisti IRT paslaugas teikiančias trečiąsias šalis arba pasinaudoti vietoje taikomais sprendimais, atitinkančiais teikiamos paslaugos sudėtingumą;

(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, kuriuo Komisija paskelbė apie ketinimą skatinti ir palengvinti standartinių sutarčių sąlygų dėl finansų sektoriaus subjektų debesijos paslaugų veiklos rangos parengimą, remiantis tarpsektorinių debesijos paslaugų suinteresuotųjų šalių indėliu, kurį Komisija užtikrino bendradarbiaudama su finansų sektoriumi;

(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 Eurosistemos lygmeniu nustatytos priežiūros mechanizmų sistemos, kuriomis siekiama padėti vykdyti Sutarties dėl Europos Sąjungos veikimo 127 straipsnio 2 dalyje nurodytas užduotis, turėtų būti taikoma išimtis;

(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;

(59) šia 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, padedamas naujo pakomitečio (Priežiūros forumo), atliksiančio parengiamąjį darbą, susijusį tiek su atskirais sprendimais, skirtais ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, tiek su kolektyvinėms rekomendacijoms, visų pirma dėl ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūros programų lyginamosios analizės, ir nustatysiančio 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, viena iš EPI turėtų būti paskirta kiekvienos iš ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių atsakingąja priežiūros institucija;

(62) atsakingosioms priežiūros institucijoms turėtų būti suteikti reikiami įgaliojimai atlikti ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių tyrimus, patikrinimus vietoje ir ne 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.

Pagrindinės priežiūros pavedimas EPI 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 arba visai nekoordinuodamos savo darbo, 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) be to, atsakingosios priežiūros institucijos 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 atsakingųjų priežiūros institucijų nustatytų tokių esminių rekomendacijų laikymąsi;

(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) siekdami pasinaudoti kompetentingų institucijų ekspertų techninėmis žiniomis operacinės ir IRT rizikos valdymo srityje, atsakingosios priežiūros institucijos turėtų remtis nacionaline priežiūros patirtimi ir sukurti specialias kiekvienai ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai skirtas tyrimo grupes, jose suburdami 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[39] jam pavestais specialiais uždaviniais), bendradarbiavimą ir konsultavimąsi su EPI, tarpusavyje keičiantis informacija ir teikiant pagalbą, susijusią su priežiūros veikla;

(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 vyktų vadovaujantis 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros[40] nustatytais principais. Visų pirma, siekiant užtikrinti vienodas galimybes dalyvauti atliekant su deleguotaisiais aktais susijusį parengiamąjį darbą, Europos Parlamentas ir Taryba visus dokumentus turėtų gauti tuo pačiu metu kaip ir valstybių narių ekspertai, o jų ekspertams turėtų būti 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[41] konsoliduojamos IRT rizikos valdymo nuostatos, nustatytos įvairiuose Sąjungos finansinių paslaugų *acquis* reglamentuose ir direktyvose, įskaitant reglamentus (EB) 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.

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;

(70) ypač svarbu, kad atlikdama parengiamąjį darbą Komisija tinkamai konsultuotųsi, taip pat ir su ekspertais. Komisija ir EPI turėtų užtikrinti, kad tuos standartus ir

---

39 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).

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

41 [*Prašom įrašyti visą nuorodą*]

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 dydį ir sudėtingumą, 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;

– skaitmeninės veiklos atsparumo testavimu;

– keitimusi informacija ir žvalgybos informacija apie kibernetines grėsmes ir pažeidžiamumus;

– 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.

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, su turtu susietų žetonų emitentams ir reikšmingų su turtu susietų žetonų emitentams,

(f) centriniams vertybinių popierių depozitoriumams,

(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,

(o) profesinių pensijų įstaigoms,

(p) kredito reitingų agentūroms,

(q) teisės aktų nustatytą auditą atliekantiems auditoriams ir audito įmonėms,

(r) ypatingos svarbos lyginamųjų indeksų administratoriams,

(s) sutelktinio finansavimo paslaugų teikėjams,

(t) pakeitimo vertybiniais popieriais duomenų saugykloms,

(u) IRT paslaugas teikiančioms trečiosioms šalims.

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

3 straipsnis

Apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

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

(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, įskaitant triktį, perkrovą, gedimą, sutrikimą, sugadinimą, netinkamą naudojimą, praradimą ar kitokios rūšies piktavališką ar nepiktavališką įvykį, kuriai susiklosčius gali būti pakenkta tinklų ir informacinių sistemų, bet kokios nuo technologijų priklausančios priemonės ar proceso, operacijos ir proceso eigos arba paslaugų teikimo saugumui, taip sukeliant pavojų duomenų, programinės įrangos ar bet kurio kito IRT paslaugų ir infrastruktūros komponento vientisumui ar prieinamumui arba pažeidžiant konfidencialumą, sukeliant žalą fizinei IRT infrastruktūrai ar kitą neigiamą poveikį;

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

(6) su IRT susijęs incidentas – nenumatytas nustatytas įvykis tinklų ir informacinėse sistemose dėl kenkėjiškos arba kitos veiklos, dėl kurio kyla pavojus tinklų ir informacinių sistemų ir jose tvarkomos, saugomos arba perduodamos informacijos saugumui arba daromas neigiamas poveikis finansų sektoriaus subjekto teikiamų finansinių paslaugų prieinamumui, konfidencialumui, tęstinumui ar autentiškumui;

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

(8) kibernetinė grėsmė – kibernetinė grėsmė, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/881[42] 2 straipsnio 8 punkte;

(9) kibernetinis išpuolis – su IRT susijęs piktavališkas incidentas, kai priešiškas subjektas bando sunaikinti, atskleisti, pakeisti, išjungti, pavogti ar įgyti neteisėtą prieigą prie bet 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 yda, kuriais gali būti pasinaudota 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 – skaitmenines ir duomenų paslaugas teikianti įmonė, įskaitant debesijos paslaugų, programinės įrangos, duomenų analizės ir duomenų centrų paslaugų teikėjus, 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[43] 2 straipsnio 4 punkte;

(16) IRT paslaugos – skaitmeninės ir duomenų paslaugos, teikiamos naudojantis IRT sistemomis vienam ar keliems vidaus ar išorės naudotojams, įskaitant duomenų teikimo, duomenų įvedimo, duomenų saugojimo, duomenų tvarkymo ir duomenų teikimo paslaugas, duomenų stebėsenos, duomenimis grindžiamo verslo ir sprendimų priėmimo palaikymo paslaugas;

(17) ypatingos svarbos arba svarbi funkcija – funkcija, 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, jo finansinės veiklos rezultatams arba jo paslaugų ir veiklos patikimumui ar tęstinumui;

---

[42] 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).

[43] 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 29 straipsnį paskirta IRT paslaugas teikianti trečioji šalis, kuriai taikoma 30–37 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, neįkūręs įmonės ar nevykdantis veiklos Sąjungoje ir 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, neįkūręs įmonės ar nevykdantis veiklos Sąjungoje ir 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, kad finansų sektoriaus subjektas, o galiausiai ir visos Sąjungos finansų sistema, nebegalės vykdyti ypatingos svarbos funkcijų arba patirs 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[44] 3 straipsnio 1 dalies 20 punkte, Europos Parlamento ir Tarybos reglamento (ES) 20xx/xx[45] [MICA] 3 straipsnio 1 dalies u 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[46] 4 straipsnio 1 dalies 1 punkte;

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

(25) mokėjimo įstaiga – mokėjimo įstaiga, kaip apibrėžta Direktyvos (ES) 2015/2366 1 straipsnio 1 dalies d punkte;

(26) elektroninių pinigų įstaiga – elektroninių pinigų įstaiga, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/110/EB[47] 2 straipsnio 1 punkte;

---

44 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).

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

46 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).

47 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).

(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 3 punkte;

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

(38) perdraudimo tarpininkas – perdraudimo tarpininkas, kaip apibrėžta Direktyvos (ES) 2016/97 2 straipsnio 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;

(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 n punkte [*LB: įrašyti MICA reglamento nuorodą*];

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

(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 j punkte;

(47) ypatingos svarbos lyginamųjų indeksų administratorius – ypatingos svarbos lyginamųjų indeksų administratorius, kaip apibrėžta Reglamento xx/202x [*OL: įrašyti Lyginamųjų indeksų reglamento nuorodą*] x straipsnio x punkte;

(48) sutelktinio finansavimo paslaugų teikėjas – sutelktinio finansavimo paslaugų teikėjas, kaip apibrėžta Reglamento (ES) 202x/xx [*LB: įrašyti Sutelktinio finansavimo reglamento nuorodą*] x straipsnio x 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 įmonė – finansų sektoriaus subjektas, kaip apibrėžta Rekomendacijos 2003/361/EB priedo 2 straipsnio 3 dalyje.

II SKYRIUS

IRT RIZIKOS VALDYMAS

I SKIRSNIS

4 straipsnis

Valdymas ir organizavimas

1. Finansų sektoriaus subjektai įdiegia vidaus valdymo ir kontrolės sistemas, kuriomis užtikrinamas veiksmingas ir prudencinis visos IRT rizikos valdymas.

2. Finansų sektoriaus subjekto valdymo organas nustato, tvirtina, prižiūri ir atsako už visų priemonių, susijusių su 5 straipsnio 1 dalyje nurodyta IRT rizikos valdymo sistema, įgyvendinimą.

Taikant pirmą pastraipą, valdymo organas:

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

(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, 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 visų atitinkamų 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 naudojimo;

(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 tinkamai informuotas apie su IRT susijusius incidentus ir jų poveikį, taip pat reagavimo, veiklos atkūrimo ir taisomąsias priemones.

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

4. Valdymo organo nariai reguliariai dalyvauja specialiuose mokymuose, kad įgytų ir turėtų naujausių pakankamų žinių ir gūdžių IRT rizikai ir jos poveikiui finansų sektoriaus subjekto veiklai suprasti ir įvertinti.

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, atitinkantį jų verslo poreikius, dydį ir sudėtingumą.

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, 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, bei reguliariai ją peržiūri.

5. Finansų sektoriaus subjektai, išskyrus labai mažas įmones, užtikrina tinkamą IRT valdymo funkcijų, kontrolės funkcijų ir vidaus audito funkcijų atskyrimą 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.

7. 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 kurią laiku tikrinami ir taisomi esminiai IRT audito nustatyti faktai, atsižvelgiant į audito peržiūros išvadas, kartu tinkamai atsižvelgiant į finansų sektoriaus subjektų paslaugų ir veiklos pobūdį, mastą ir sudėtingumą.

9. Į 1 dalyje nurodytą IRT rizikos valdymo sistemą įtraukiama skaitmeninio 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 bazinė 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 visapusė IRT kelių pardavėjų strategija subjekto lygmeniu, parodant pagrindinę priklausomybę nuo IRT paslaugas teikiančių trečiųjų šalių ir pateikiant pirkimo iš įvairių paslaugas teikiančių trečiųjų šalių loginį pagrindimą;

   (h) įgyvendinamas skaitmeninės veiklos atsparumo testavimas;

   (i) nurodoma komunikacijos strategiją su IRT susijusių incidentų atveju.

10. Gavę kompetentingų institucijų sutikimą, finansų sektoriaus subjektai gali pavesti grupės vidaus arba išorės įmonėms tikrinti atitiktį IRT rizikos valdymo reikalavimams.

6 straipsnis

IRT sistemos, protokolai ir priemonės

1. 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, pobūdį, įvairovę, sudėtingumą ir 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 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 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 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 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 IRT turto konfigūraciją ir skirtingo IRT turto sąsajas ir tarpusavio priklausomybę.

5. Finansų sektoriaus subjektai identifikuoja ir dokumentais pagrindžia visus procesus, kurie priklauso nuo IRT paslaugas teikiančių trečiųjų šalių, ir nustato tarpusavio sąsajas su IRT paslaugas teikiančiomis trečiosiomis šalimis.

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, ypač iki senųjų ir naujųjų 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 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 pažangiausias IRT technologijas ir procesus, kuriais:

   (a) užtikrinamas 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 netinkamo administravimo ar tvarkymo, įskaitant netinkamą apskaitą, rizikos.

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

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

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

   (c) įgyvendina politiką, kuria fizinė ir virtualioji prieiga prie IRT sistemos išteklių ir duomenų suteikiama tik tiek, kiek tai reikalinga teisėtoms ir patvirtintoms funkcijoms ir veiklai, ir tuo tikslu parengia politikos, procedūrų ir kontrolės priemonių rinkinį, skirtą prieigos teisėms ir patikimam jų administravimui;

   (d) įgyvendina griežtų tapatumo nustatymo mechanizmų politiką ir protokolus, pagrįstus atitinkamais standartais ir specialiomis kontrolės sistemomis, kad būtų užkirstas kelias prieigai prie kriptografinių raktų, kuriais duomenys užšifruojami remiantis patvirtintų duomenų klasifikavimo ir rizikos vertinimo procesų rezultatais;

   (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 skubiai 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 visiems galimiems reikšmingiems bendriems gedimo taškams identifikuoti.

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

2. 1 dalyje nurodytais aptikimo mechanizmais sudaromos sąlygos keliems kontrolės lygmenims, nustatomos įspėjimo ribos ir kriterijai, pagal kuriuos būtų galima pradėti su IRT susijusių incidentų aptikimo ir reagavimo į su IRT susijusius incidentus procesus, ir įdiegiami automatiniai įspėjimo mechanizmai atitinkamiems darbuotojams, atsakingiems už reagavimą į su IRT susijusius incidentus.

3. Finansų sektoriaus subjektai skiria pakankamai išteklių ir pajėgumų, deramai atsižvelgdami į savo dydį, veiklos ir rizikos pobūdį, naudotojų veiklai, neįprastai IRT veiklai ir su IRT susijusiems incidentams, visų pirma kibernetiniams išpuoliams, stebėti.

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 specialią ir išsamią IRT veiklos tęstinumo politiką, kuri yra neatsiejama finansų sektoriaus subjekto veiklos tęstinumo politikos dalis.

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:

   (a) registruoti visus su IRT susijusius incidentus;

   (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 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, pagal kurią, 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 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 išlaidas ir nuostolius, patirtus dėl IRT sutrikimo ir su IRT susijusių incidentų.

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. 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, kurių operacinė aplinka skiriasi nuo pagrindinės sistemos, nėra tiesiogiai sujungta su pastarąja ir yra patikimai apsaugota 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 turi atsarginius IRT pajėgumus, kurių išteklių pajėgumai ir funkcijos yra pakankami ir tinkami veiklos poreikiams tenkinti.

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 iš karto prieinama finansų sektoriaus subjekto darbuotojams, kad būtų užtikrintas ypatingos svarbos paslaugų tęstinumas, jei pirminė duomenų tvarkymo vieta taptų neprieinama.

6. Nustatydami kiekvienos funkcijos atkūrimo laiko ir taško tikslus, finansų sektoriaus subjektai atsižvelgia 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 atlieka daug patikrinimų, įskaitant sutikrinimą, siekdami užtikrinti, kad duomenų vientisumas būtų aukščiausio lygio. Šie 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, tinkamų jų dydžiui, veiklos ir rizikos pobūdžiui, 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 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, finansų sektoriaus subjektai, išskyrus labai mažas įmones, apie tuos pakeitimus praneša kompetentingoms institucijoms.

   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, 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. Jie taikomi visiems darbuotojams ir vyresniosios vadovybės nariams.

Finansų sektoriaus subjektai 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 apie su IRT susijusius incidentus arba didelius pažeidžiamumus.

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 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;

(b) nurodyti, kaip 8 straipsnio 2 dalyje nurodyta IRT saugumo politika, procedūromis ir priemonėmis saugumo kontrolės priemonės įtraukiamos į sistemas nuo pat projektavimo (pritaikytasis saugumas), numatomas pritaikymas prie kintančios grėsmių aplinkos ir numatoma galimybė naudoti pakopinės apsaugos technologiją;

(c) patikslinti 8 straipsnio 4 dalies b punkte nurodytus tinkamus būdus, metodus ir protokolus;

(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: įrašyti datą – 1 metai nuo 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.

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 atitinkamus 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 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 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 ir tai, ar su IRT susijęs incidentas turėjo poveikį reputacijai;

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

(c) geografinis pasiskirstymas su IRT susijusio incidento paveiktose vietovėse, ypač jei poveikis 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 pasikonsultavusios 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 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 tuos bendrų techninių reguliavimo standartų projektus pateikia Komisijai iki [*LB: įrašyti datą – 1 metai nuo 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.

2. Kai didelis su IRT susijęs incidentas daro arba gali daryti poveikį paslaugų naudotojų ir klientų finansiniams interesams, finansų sektoriaus subjektai nepagrįstai nedelsdami informuoja savo paslaugų naudotojus ir klientus apie didelį su IRT susijusį incidentą ir kuo greičiau juos informuoja apie visas priemones, kurių imtasi tokio incidento neigiamam poveikiui sumažinti.

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

(a) pradinį pranešimą nedelsiant, bet ne vėliau kaip iki darbo dienos pabaigos, arba, dideliam su IRT susijusiam incidentui įvykus iki darbo dienos pabaigos likus mažiau nei 2 valandoms, ne vėliau kaip per 4 valandas nuo kitos darbo dienos pradžios, arba, jei nėra galimybės pasinaudoti pranešimų teikimo kanalais, kai tik tokia galimybė atsiranda;

(b) tarpinį pranešimą ne vėliau kaip per vieną savaitę nuo 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.

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.

5. Gavusi 1 dalyje nurodytą pranešimą, kompetentinga institucija nepagrįstai nedelsdama pateikia išsamią informaciją apie incidentą:

(a) atitinkamai EBI, ESMA arba EIOPA;

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

(c) pagal Direktyvos (ES) 2016/1148 8 straipsnį paskirtam bendrajam informaciniam punktui.

6. EBI, ESMA arba EIOPA ir ECB 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;

(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 punkte nurodytus bendrų techninių reguliavimo standartų projektus ir 1 dalies b punkte nurodytus bendrų techninių įgyvendinimo standartų projektus iki 202x xx mėn. [*LB: įrašyti datą – 1 metai nuo įsigaliojimo dienos]*.

Komisijai suteikiami įgaliojimai papildyti šį reglamentą priimant šio straipsnio 1 dalies a punkte 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 punkte nurodytus bendrus techninius įgyvendinimo standartus atitinkamai pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1095/2010 ir (ES) Nr. 1094/2010 15 straipsnį.

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 ES centro įsteigimo sąlygos;

(b) nauda, apribojimai ir galima rizika;

(c) operacijų valdymo elementai;

(d) narystės sąlygos;

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

(f) preliminarus finansinių išlaidų, susijusių su 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: įrašyti datą – 3 metai nuo įsigaliojimo dienos]*.

20 straipsnis

Priežiūros grįžtamoji informacija

1. Gavusi 17 straipsnio 1 dalyje nurodytą ataskaitą, 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.

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

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

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, deramai atsižvelgdami į savo dydį, veiklos ir rizikos pobūdį, 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.

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 visų ypatingos svarbos IRT sistemų ir programų testavimą atlieka bent kartą per metus.

22 straipsnis

IRT priemonių ir sistemų testavimas

1. 21 straipsnyje nurodytoje skaitmeninės veiklos atsparumo testavimo programoje numatoma atlikti visus atitinkamus testus, įskaitant pažeidžiamumo vertinimą ir skenavimą, atvirojo kodo analizę, tinklo saugumo vertinimus, spragų analizavimą, fizinio saugumo patikrinimus, klausimynus ir skenavimo programinės įrangos sprendimus, pirminio kodo patikrinimus, jei įmanoma; scenarijais grindžiamus testus, suderinamumo testavimą, veiklos efektyvumo testavimą, ištisinio srauto (angl. *end-to-end*) testavimą arba skverbimosi testavimą.

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 4 dalį, bent kas trejus metus atlieka pažangų testavimą, taikydami grėsmėmis grindžiamą skverbimosi testavimą.

2. Grėsmėmis grindžiamas skverbimosi testavimas apima bent finansų sektoriaus subjekto ypatingos svarbos funkcijas bei paslaugas ir yra taikomas tokias funkcijas palaikančioms tikralaikėms produkcijos sistemoms. Tikslią grėsmėmis grindžiamo skverbimosi testavimo apimtį nustato finansų sektoriaus subjektai, atsižvelgdami į

ypatingos svarbos funkcijų ir paslaugų vertinimą, ir tvirtina kompetentingos institucijos.

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

Kai grėsmėmis grindžiamas skverbimosi testavimas apima IRT paslaugas teikiančias trečiąsias šalis, finansų sektoriaus subjektas imasi priemonių, būtinų šių paslaugų teikėjų dalyvavimui užtikrinti.

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 paslaugų ar operacijų sutrikdymo riziką.

Testavimo pabaigoje, susitarus dėl ataskaitų ir koregavimo planų, finansų sektoriaus subjektas ir išorės testuotojai pateikia kompetentingai institucijai dokumentus, patvirtinančius, kad grėsmėmis grindžiamas skverbimosi testavimas buvo atliktas laikantis reikalavimų. Kompetentingos institucijos patvirtina dokumentus ir išduoda pažymą.

3. Finansų sektoriaus subjektai pagal 24 straipsnį sudaro sutartis su testuotojais dėl grėsmėmis grindžiamo skverbimosi testavimo atlikimo.

Kompetentingos institucijos identifikuoja finansų sektoriaus subjektus, turinčius atlikti grėsmėmis grindžiamą skverbimosi testavimą, proporcingai finansų sektoriaus subjekto dydžiui, mastui, veiklai ir bendram rizikos pobūdžiui, 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.

4. EBI, ESMA ir EIOPA, pasikonsultavusios su ECB ir atsižvelgdamos į atitinkamas Sąjungos sistemas, taikomas žvalgybos informacija grindžiamiems skverbimosi testams, parengia techninių reguliavimo standartų projektus, kuriuose patikslinami:

(a) kriterijai, naudojami taikant šio straipsnio 6 dalį;

(b) reikalavimai, taikomi:

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

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

(c) testavimo rezultatams, užbaigimui ir koregavimo etapams;

(c) kokios rūšies bendradarbiavimas priežiūros srityje yra reikalingas atliekant finansų sektoriaus subjektų, vykdančių veiklą daugiau nei vienoje valstybėje narėje, grėsmėmis grindžiamą skverbimosi testavimą, 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: įrašyti datą – 2 mėnesiai iki įsigaliojimo dienos*].

Komisijai suteikiami įgaliojimai papildyti šį reglamentą priimant šio straipsnio 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 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;

   (d) išorės testuotojų atveju 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) išorės testuotojų atveju yra tinkamai ir visiškai apdrausti atitinkamu profesinės civilinės atsakomybės draudimu, įskaitant draudimą nuo netinkamo elgesio ir aplaidumo rizikos.

2. Finansų sektoriaus subjektai 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 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.

3. Taikydami IRT rizikos valdymo sistemą, finansų sektoriaus subjektai priima ir reguliariai peržiūri trečiosios šalies keliamos IRT rizikos strategiją, atsižvelgdami į 5 straipsnio 9 dalies g punkte nurodytą kelių pardavėjų 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 IRT paslaugas teikiančių trečiųjų šalių teikiamų IRT paslaugų naudojimo.

   Pirmoje pastraipoje nurodyti sutartimi įforminti susitarimai tinkamai pagrindžiami dokumentais, atskiriant tuos, kurie apima ypatingos svarbos ar svarbias funkcijas, ir susitarimus, kurie jų neapima.

   Finansų sektoriaus subjektai ne rečiau kaip kartą per metus kompetentingoms institucijoms pateikia informaciją apie naujų susitarimų dėl 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 naujausių informacijos saugumo standartų.

7. Naudodamiesi prieigos, patikrinimo ir audito teisėmis IRT paslaugas 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 didelis 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 sutartimi įforminti susitarimai dėl IRT paslaugų naudojimo būtų nutraukti bent toliau nurodytomis aplinkybėmis:

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

(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, 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 nebegali veiksmingai prižiūrėti finansų sektoriaus subjekto dėl atitinkamo sutartimi įforminto susitarimo.

9. Finansų sektoriaus subjektai nustato pasitraukimo strategijas, 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.

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: [įrašyti datą – 1 metai nuo 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: įrašyti datą – 1 metai nuo įsigaliojimo dienos]*.

Komisijai suteikiami įgaliojimai papildyti šį reglamentą priimant šio straipsnio 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 IRT paslaugų:

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

   (b) atsirastų keli sutartimi įforminti susitarimai dėl 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 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, visų pirma tuo atveju, kai IRT subrangovas yra įsisteigęs trečiojoje valstybėje.

   Kai sutartimi įforminti susitarimai dėl IRT paslaugų naudojimo sudaromi su trečiojoje valstybėje įsisteigusia IRT paslaugas teikiančia trečiąja šalimi, finansų sektoriaus subjektai laiko svarbiais bent šiuos veiksnius:

   (a) duomenų apsaugos reikalavimų laikymąsi;

   (b) veiksmingą teisės aktų vykdymo užtikrinimą;

   (c) nemokumo teisės nuostatas, taikytinas IRT paslaugas teikiančios trečiosios šalies bankroto atveju;

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

   Finansų sektoriaus subjektai įvertina, ar ir kaip galimai ilgos ar sudėtingos subrangos grandinės gali turėti įtakos jų gebėjimui visapusiškai 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 viename rašytiniame dokumente, kurį šalys gali gauti popierine arba atsisiunčiama ir prieinama forma.

2. Sutartimi įformintuose IRT paslaugų naudojimo susitarimuose turi būti 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, kuriose turi būti teikiamos pagal sutartį arba subrangos sutartį vykdomos funkcijos ir paslaugos ir kuriose turi būti tvarkomi duomenys, nurodant saugojimo vietą, ir reikalavimas, kad IRT paslaugas teikianti trečioji šalis praneštų finansų sektoriaus subjektui, jeigu ji ketina keisti tokias vietas;

(c) nuostatos dėl asmens duomenų pasiekiamumo, prieinamumo, vientisumo, saugumo ir apsaugos bei 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;

(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) IRT paslaugas teikiančios trečiosios šalies įspėjimo terminai ir pareigos pranešti finansų sektoriaus subjektui, įskaitant pranešimą apie bet kokius pokyčius, kurie gali turėti reikšmingos įtakos IRT paslaugas teikiančios trečiosios šalies gebėjimui veiksmingai atlikti ypatingos svarbos ar svarbias funkcijas pagal sutartus paslaugų lygius;

(f) IRT paslaugas teikiančios trečiosios šalies pareiga teikti 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 tinkamai užtikrinama, kad finansų sektoriaus subjektas saugiai teiktų paslaugas, laikydamasis taikytinos reguliavimo sistemos;

(h) teisė 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 daryti atitinkamų dokumentų kopijas, kai veiksmingai naudotis šiomis teisėmis netrukdo arba nevaržo kiti sutartimi įforminti susitarimai arba įgyvendinimo politika;

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

iii) įsipareigojimą visapusiškai bendradarbiauti finansų sektoriaus subjektui atliekant patikrinimus vietoje ir išsamią informaciją apie nuotolinio audito apimtį, sąlygas ir dažnumą;

(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 institucijų lūkesčius;

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

(a) kurį IRT paslaugas teikianti trečioji šalis toliau vykdys atitinkamas funkcijas ar teiks paslaugas, kad būtų sumažinta finansų sektoriaus subjekto veiklos sutrikimų rizika;

(b) per kurį finansų sektoriaus subjektas gali pakeisti IRT paslaugas teikiančią trečiąją šalį arba pasirinkti vietoje taikomus sprendimus, atitinkančius teikiamos paslaugos sudėtingumą.

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

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.

EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai iki [*OL: įrašyti datą – 1 metai nuo 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 forumo, įsteigto pagal 29 straipsnio 1 dalį, rekomendacija:

(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.

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.

3. Komisijai pagal 50 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais papildomi 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. EPI per jungtinį komitetą sudaro, skelbia ir kasmet 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 Priežiūros forumui, įsteigtam pagal 29 straipsnį. Priežiūros forumas 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.

9. Finansų sektoriaus subjektai nesinaudoja trečiojoje valstybėje įsisteigusios IRT paslaugas teikiančios trečiosios šalies, kuri, jei būtų įsisteigusi Sąjungoje, būtų paskirta ypatingos svarbos paslaugų teikėju pagal 1 dalies a punktą, paslaugomis.

29 straipsnis

Priežiūros sistemos struktūra

1. Pagal reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 57 straipsnį jungtinis komitetas įsteigia Priežiūros forumą, kuris veikia kaip pakomitetis, padedantis jungtiniam komitetui ir 28 straipsnio 1 dalies b punkte nurodytai atsakingajai priežiūros institucijai dirbti trečiosios šalies keliamos IRT rizikos finansų sektoriuose srityje. Priežiūros forumas rengia jungtinio komiteto bendrų pozicijų ir bendrų aktų projektus toje srityje.

   Priežiūros forumas reguliariai aptaria atitinkamus pokyčius, susijusius su IRT rizika ir pažeidžiamumais, ir skatina nuoseklų požiūrį į trečiosios šalies keliamos IRT rizikos stebėseną Sąjungos mastu.

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

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

4. Priežiūros forumą sudaro EPI pirmininkai ir vienas kiekvienos valstybės narės atitinkamos kompetentingos institucijos esamo personalo aukšto lygio atstovas. Visų

EPI vykdomieji direktoriai ir po vieną Europos Komisijos, ESRV, ECB ir ENISA atstovą dalyvauja Priežiūros forume stebėtojų teisėmis.

5. Vadovaujantis reglamentų (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 ir (ES) Nr. 1095/2010 16 straipsniu, EPI parengia EPI ir kompetentingų institucijų taikant šį skirsnį vykdomo bendradarbiavimo gaires dėl išsamių procedūrų ir sąlygų, susijusių su kompetentingų institucijų ir EPI 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 atsakingosios priežiūros institucijos teikia ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims.

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

7. EPI, pasitarusios jungtiniame komitete ir remdamosi Priežiūros forumo atliktu parengiamuoju darbu, kasmet pateikia Europos Parlamentui, Tarybai ir Komisijai šio skirsnio taikymo ataskaitą.

30 straipsnis

Atsakingosios priežiūros institucijos užduotys

1. 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.

2. 1 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) 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. Remdamasi 1 dalyje nurodytu vertinimu, atsakingoji priežiūros institucija kiekvienai ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai patvirtina aiškų, išsamų ir pagrįstą individualų priežiūros planą. Tas planas kiekvienais metais pateikiamas ypatingos svarbos IRT paslaugas teikiančiai trečiajai šaliai.

4. Suderinusios 3 dalyje nurodytus metinius priežiūros planus ir juos pateikusios ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, kompetentingos institucijos gali imtis priemonių dėl ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių tik gavusios atsakingosios priežiūros institucijos pritarimą.

31 straipsnis

Atsakingosios priežiūros institucijos įgaliojimai

1. Vykdydama šiame skirsnyje nustatytas pareigas atsakingoji priežiūros institucija turi šiuos įgaliojimus:

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

(b) atlikti bendruosius tyrimus ir patikrinimus 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 šios dalies d punkte nurodytas rekomendacijas;

(d) 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 atsakingoji priežiūros institucija 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 atsakingoji priežiūros institucija 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 atsakingoji priežiūros institucija 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 IRT paslaugas teikianti trečioji šalis arba trečiojoje valstybėje įsisteigęs IRT subrangovas;

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

2. Prieš naudodamasi 1 dalyje nurodytais įgaliojimais atsakingoji priežiūros institucija konsultuojasi su Priežiūros forumu.

3. Ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys sąžiningai bendradarbiauja su atsakingąja priežiūros institucija ir padeda jai atlikti jos užduotis.

4. Atsakingoji priežiūros institucija gali skirti periodinę baudą, kad priverstų ypatingos svarbos IRT paslaugas teikiančią trečiąją šalį laikytis 1 dalies a, b ir c punktų.

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 1 proc. ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies vidutinės dienos pasaulinės apyvartos 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.

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. 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 informacijos pateikimo terminą;

(e) nurodo 31 straipsnio 4 dalyje numatytas periodines baudas, jei pateikiama ne visa reikalaujama informacija;

(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 34 straipsnio 1 dalyje nurodytos tyrimo grupės, gali atlikti būtinus IRT paslaugas teikiančių trečiųjų šalių tyrimus:

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) daryti ar gauti 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.

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, 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 paslaugų teikėją 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 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: įrašyti datą – 1 metai nuo 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 atsakingoji priežiūros institucija, pasikonsultavusi su Priežiūros forumu, 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 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 atsakingųjų priežiūros institucijų rekomendacijomis pagal 37 straipsnio 2 dalį, vertinimą.

2. EPI tuos techninių reguliavimo standartų projektus pateikia Komisijai iki 20xx m. sausio 1 d. [*OL: įrašyti datą – 1 metai nuo 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 nuo atsakingųjų priežiūros institucijų rekomendacijų, pateiktų pagal 31 straipsnio 1 dalies d punktą, gavimo ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys atsakingajai priežiūros institucijai praneša, ar ketina tų rekomendacijų laikytis. Atsakingosios priežiūros institucijos nedelsdamos šią informaciją perduoda kompetentingoms institucijoms.

2. Kompetentingos institucijos stebi, ar finansų sektoriaus subjektai atsižvelgia į riziką, identifikuotą atsakingosios priežiūros institucijos rekomendacijose, skirtose ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims pagal 31 straipsnio 1 dalies d punktą.

3. Pagal 44 straipsnį kompetentingos institucijos gali reikalauti, kad finansų sektoriaus subjektai laikinai iš dalies arba visiškai sustabdytų ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies teikiamos paslaugos naudojimą ar diegimą, kol bus imtasi veiksmų dėl rizikos, identifikuotos ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims skirtose rekomendacijose. Prireikus jos gali

reikalauti, kad finansų sektoriaus subjektai iš dalies arba visiškai nutrauktų atitinkamus sutartimi įformintus susitarimus, sudarytus su ypatingos svarbos IRT paslaugas teikiančiomis trečiosiomis šalimis.

4. Priimdamos 3 dalyje nurodytus sprendimus kompetentingos institucijos 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.

5. Kompetentingos institucijos reguliariai informuoja atsakingąsias priežiūros institucijas apie metodus ir priemones, kurių ėmėsi vykdydamos finansų sektoriaus subjektų priežiūros užduotis, taip pat apie sutartines priemones, kurių ėmėsi pastarieji, kai ypatingos svarbos IRT paslaugas teikiančios trečiosios šalys iš dalies ar visiškai nesutiko su atsakingųjų priežiūros institucijų rekomendacijomis.

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 administracines išlaidas ir yra proporcingas jos apyvartai.

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 gali tarpusavyje 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 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 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[48] reikalavimų ir konkurencijos politikos gairių[49].

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.

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

[48] 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).

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

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, su turtu susietų žetonų emitentų 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 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 xx/202x* 40 ir 41 straipsnius;

(r) sutelktinio finansavimo paslaugų teikėjų atveju – kompetentinga institucija, paskirta pagal *Reglamento xx/202x x 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 gali prašyti būti pakviestos dalyvauti Bendradarbiavimo grupės darbe.

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.

43 straipsnis

Finansinės tarpsektorinės užduotys, komunikacija ir bendradarbiavimas

1. EPI, pasitarusios jungtiniame komitete ir bendradarbiaudamos su kompetentingomis institucijomis, ECB ir ESRV, gali nustatyti mechanizmus, kurie sudarytų sąlygas dalytis veiksminga praktika skirtinguose finansų sektoriuose, kad būtų didinamas informuotumas apie padėtį ir identifikuojami bendri kibernetiniai pažeidžiamumai 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 susijusios 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 ir ECB 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, kompetentingos institucijos nuomone, prieštaraujančius 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 – 1 metai 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, atsakingų asmenų tapatybė ir skirtos nuobaudos.

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].

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 du mėnesius nuo pranešimo Europos Parlamentui ir Tarybai apie šį aktą dienos nei Europos Parlamentas, nei Taryba nepareiškia prieštaravimų arba jeigu dar nepasibaigus šiam laikotarpiui ir Europos Parlamentas, ir Taryba praneša Komisijai, kad prieštaravimų nereikš. Europos Parlamento arba Tarybos iniciatyva šis laikotarpis pratęsiamas dviem mėnesiais.

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 28 straipsnio 2 dalyje nustatytus ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių skyrimo kriterijus ir Europos Parlamentui ir Tarybai pateikia ataskaitą, prie kurios prireikus prideda pasiūlymą dėl teisėkūros procedūra priimamų aktų.

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, EVPRI, pasikonsultavusi su ECBS nariais, parengia techninių reguliavimo standartų projektus, kuriuose nurodomas minimalus veiklos tęstinumo politikos ir veiklos atkūrimo po ekstremaliųjų įvykių plano, išskyrus IRT veiklos tęstinumo ir veiklos atkūrimo po ekstremaliųjų įvykių planus, turinys ir reikalavimai.“;

(3) 56 straipsnio 3 dalies pirma pastraipa pakeičiama taip:

„3. Siekiant užtikrinti nuoseklų šio straipsnio taikymą, EVPRI parengia techninių reguliavimo standartų, kuriuose išsamiai nustatomi 1 dalyje nurodytos registracijos paraiškos duomenys, išskyrus reikalavimus, susijusius su IRT rizikos valdymu, projektus.“;

(4) 79 straipsnio 1 ir 2 dalys pakeičiamos taip:

„1. Sandorių duomenų saugykla nustato galimus veiklos rizikos šaltinius ir juos sumažina sukurdama tinkamas sistemas, kontrolės priemones ir procedūras, įskaitant IRT sistemas, valdomas vadovaujantis Reglamentu (ES) 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.“;

(4) 6 dalies pirma pastraipa pakeičiama taip:

„CVPD nustato, stebi ir valdo riziką, kurią jo operacijoms galėtų kelti pagrindiniai jo valdomų vertybinių popierių atsiskaitymo sistemų dalyviai, taip pat paslaugų ir komunalinių paslaugų teikėjai ir kiti CVPD ar kitos rinkos infrastruktūros. Gavęs prašymą jis pateikia kompetentingoms ir atitinkamoms institucijoms informaciją apie bet kokią tokią nustatytą riziką. Jis taip pat nedelsdamas informuoja kompetentingą instituciją ir atitinkamas institucijas apie visus dėl tokios rizikos, išskyrus IRT riziką, įvykusius operacinius incidentus.“;

(5) 7 dalies pirma pastraipa pakeičiama taip:

„ESMA, glaudžiai bendradarbiaudama su ECBS nariais, parengia techninių reguliavimo standartų projektus, kuriuose tiksliai nurodoma 1 ir 6 dalyse nurodyta operacinė rizika, išskyrus IRT riziką, bei tos rizikos testavimo, valdymo ar kuo didesnio sumažinimo metodai, įskaitant 3 ir 4 dalyse nurodytą veiklos tęstinumo politiką bei veiklos atkūrimo po ekstremaliųjų įvykių planus ir jų vertinimo metodus.“.

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 – 12 mėnesių 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.

Priimta Briuselyje

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas	*Pirmininkas*

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

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

1.3. Pasiūlymo (iniciatyvos) pobūdis

1.4. Tikslas (-ai)

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.6. Pasiūlymo (iniciatyvos) trukmė ir finansinis poveikis

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

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir atskaitomybės taisyklės

2.2. Valdymo ir kontrolės sistema (-os)

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės), kurioms daromas poveikis

3.2. Numatomas poveikis išlaidoms

3.2.1. Numatomo poveikio išlaidoms santrauka

3.2.2. Numatomas poveikis asignavimams

3.2.3. Numatomas poveikis žmogiškiesiems ištekliams

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

3.2.5. Trečiųjų šalių įnašai

3.3. Numatomas poveikis pajamoms

Priedas

Bendrosios prielaidos

Priežiūros įgaliojimai

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA „AGENTŪROS“

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl skaitmeninės veiklos atsparumo finansų sektoriuje.

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

Politikos sritis: finansinis stabilumas, finansinės paslaugos ir kapitalo rinkų sąjunga Veikla: skaitmeninės veiklos atsparumas

1.3. Pasiūlymas susijęs su:

☑ **nauja priemone**

☐ **nauja priemone, kuri bus priimta įgyvendinus bandomąjį projektą ir (arba) atlikus parengiamuosius veiksmus**[50]

☐ **esamos priemonės galiojimo pratęsimu**

☐ **vieno ar daugiau veiksmų sujungimu su kitu / nauju veiksmu**

1.4. Tikslas (-ai)

1.4.1. Bendras (-i) tikslas (-ai)

Bendras iniciatyvos tikslas – didinti ES finansų sektoriaus subjektų skaitmeninės veiklos atsparumą racionalizuojant ir atnaujinant esamas taisykles ir nustatant naujus reikalavimus tose srityse, kuriose yra spragų. Tai taip pat sustiprintų bendro taisyklių sąvado skaitmeninį aspektą. Bendrą tikslą galima suskirstyti į tris bendruosius tikslus: 1) sumažinti finansų sektoriaus sutrikdymo ir nestabilumo riziką, 2) sumažinti administracinę naštą ir padidinti priežiūros veiksmingumą bei 3) sustiprinti vartotojų ir investuotojų apsaugą.

1.4.2. Konkretus (-ūs) tikslas (-ai)

Konkretūs pasiūlymo tikslai: visapusiškiau mažinti informacinių ir ryšių technologijų (IRT) riziką ir padidinti bendrą finansų sektoriaus skaitmeninį atsparumą; racionalizuoti pranešimus apie su IRT susijusius incidentus ir šalinti iš dalies sutampančius pranešimų teikimo reikalavimus; sudaryti sąlygas finansų priežiūros institucijoms susipažinti su informacija apie su IRT susijusius incidentus;

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

užtikrinti, kad finansų sektoriaus subjektai, kuriems taikomas šis pasiūlymas, įvertintų savo prevencinių ir atsparumo priemonių veiksmingumą ir identifikuotų su IRT susijusius pažeidžiamumus;

mažinti bendrosios rinkos susiskaidymą ir sudaryti sąlygas tarpvalstybiniam testavimo rezultatų pripažinimui;

stiprinti sutartines finansų sektoriaus subjektų apsaugos priemones šioms naudojantis IRT paslaugomis, įskaitant veiklos rangos taisykles (reglamentuojančias IRT paslaugas teikiančių trečiųjų šalių stebėseną);

sudaryti sąlygas ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių veiklos priežiūrai;

skatinti keitimąsi žvalgybos informacija apie grėsmes finansų sektoriuje.

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

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

Finansų sektoriaus skaitmeninės veiklos atsparumo aktu būtų užtikrinta visapusiška sistema, apimanti visus skaitmeninės veiklos atsparumo aspektus, ir veiksmingai gerinamas bendras finansų sektoriaus veiklos atsparumas. Juo būtų užtikrintas bendro taisyklių sąvado aiškumas ir nuoseklumas.

Be to, juo būtų užtikrinta aiškesnė ir nuoseklesnė sąveika su TIS direktyva ir jos peržiūra. Šiuo aktu finansų sektoriaus subjektams būtų suteikta aiškumo dėl skirtingų skaitmeninės veiklos atsparumo taisyklių, kurių jiems reikia laikytis, visų pirma tiems finansų sektoriaus subjektams, kurie turi kelis veiklos leidimus ir vykdo veiklą skirtingose ES rinkose.

1.4.4. Veiklos rezultatų rodikliai

Nurodyti pažangos ir pasiekimų stebėsenos rodiklius.

Galimi rodikliai:

Su IRT susijusių incidentų ES finansų sektoriuje skaičius ir jų poveikis

Didelių su IRT susijusių incidentų, apie kuriuos pranešta prudencinės priežiūros institucijoms, skaičius

Finansų sektoriaus subjektų, kurie būtų įpareigoti atlikti grėsmėmis grindžiamą skverbimosi (TLPT) testavimą, skaičius

Finansų sektoriaus subjektų, kurie taiko standartines sutarčių sąlygas sudarydami sutartimi įformintus susitarimus su IRT paslaugas teikiančiomis trečiosiomis šalimis, skaičius

EPI / prudencinių priežiūros institucijų prižiūrimų ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių skaičius

Finansų sektoriaus subjektų, dalyvaujančių dalijimosi žvalgybos informacija apie grėsmes schemose, skaičius

Institucijų, kurios gautų pranešimus apie tą patį su IRT susijusį incidentą, skaičius

Tarpvalstybinių TLPT testų skaičius

1.5. Pasiūlymo (iniciatyvos) pagrindas

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

Finansų sektorius yra labai priklausomas nuo informacinių ir ryšių technologijų (IRT). Nepaisant didelės pažangos, padarytos įgyvendinant nacionalines ir Europos tikslines politikos ir teisėkūros iniciatyvas, IRT rizika ir toliau kelia sunkumų ES finansų sistemos veiklos atsparumui, veiklos efektyvumui ir stabilumui. Po 2008 m. finansų krizės vykdyta reforma visų pirma buvo didinamas ES finansų sektoriaus finansinis atsparumas ir siekta apsaugoti ES konkurencingumą ir stabilumą ekonominiu, prudenciniu ir elgesio rinkoje požiūriu. IRT saugumas ir bendras skaitmeninės veiklos atsparumas yra operacinės rizikos dalis, tačiau jiems teko mažiau dėmesio po krizės įgyvendinamoje reguliavimo darbotvarkėje ir jie buvo plėtoti tik kai kuriose ES finansų rinkos politikos ir reglamentavimo srityse arba tik keliose valstybėse narėse. Dėl to kyla toliau nurodytų problemų, kurios turėtų būti sprendžiamos šiuo pasiūlymu:

ES teisinė sistema, taikoma IRT rizikai ir veiklos atsparumui finansų sektoriuje, yra suskaidyta ir nevisiškai nuosekli.

Dėl to, kad nėra pranešimo apie su IRT susijusius incidentus nuoseklių reikalavimų, priežiūros institucijos negali susidaryti išsamaus incidentų pobūdžio, dažnumo, svarbos ir poveikio vaizdo.

Kai kuriems finansų sektoriaus subjektams taikomi sudėtingi, iš dalies sutampantys ir galbūt nenuoseklūs pranešimo apie tą patį su IRT susijusį incidentą reikalavimai.

Dėl nepakankamo dalijimosi informacija ir bendradarbiavimo žvalgybos informacijos apie kibernetines grėsmes srityje strateginiu, taktiniu ir veiklos lygmeniu atskiri finansų sektoriaus subjektai negali tinkamai įvertinti ir stebėti kibernetinių grėsmių, nuo jų apsisaugoti ir reaguoti į jas.

Kai kuriuose finansų pasektoriuose gali būti taikomos kelios nekoordinuojamos skverbimosi ir atsparumo testavimo sistemos, be to, rezultatai nėra pripažįstami tarpvalstybiniu mastu, o kituose pasektoriuose tokių testavimo sistemų iš viso nėra.

Kadangi priežiūros institucijos neanalizuoja finansų sektoriaus subjektų, kuriems IRT paslaugas teikia trečiosios šalys, veiklos, pavieniai finansų sektoriaus subjektai ir visa finansų sistema susiduria su operacine rizika.

Finansų priežiūros institucijos neturi pakankamai įgaliojimų ar priemonių, kad galėtų stebėti ir valdyti koncentracijos ir sisteminę riziką, kylančią dėl finansų sektoriaus subjektų priklausomybės nuo IRT paslaugas teikiančių trečiųjų šalių.

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

Priežastys imtis veiksmų Europos lygmeniu (*ex ante*):

Skaitmeninės veiklos atsparumas yra bendrasis ES finansų rinkų interesas. ES lygmens veiksmai suteiktų daugiau naudos ir didesnę vertę nei veiksmai, kurių būtų imamasi atskirai nacionaliniu lygmeniu. Neįtraukus šių veiklos nuostatų dėl IRT rizikos, bendrame taisyklių sąvade būtų numatytos priemonės visų kitų rūšių rizikai mažinti Europos lygmeniu, tačiau nebūtų skaitmeninės veiklos atsparumo aspektų arba jiems būtų taikomos fragmentiškos ir nekoordinuojamos nacionalinio lygmens iniciatyvos. Pasiūlymu būtų užtikrintas teisinis aiškumas dėl to, ar ir kaip taikomos skaitmeninės veiklos nuostatos, ypač tarpvalstybiniams finansų sektoriaus subjektams, ir būtų panaikintas poreikis valstybėms narėms individualiai tobulinti taisykles, standartus ir lūkesčius, susijusius su veiklos atsparumu ir kibernetiniu saugumu reaguojant į dabartinę ribotą ES taisyklių taikymo sritį ir bendrą TIS direktyvos pobūdį.

Numatoma sukurti Sąjungos pridėtinė vertė (*ex post*):

Sąjungos intervencija būtų gerokai padidintas politikos veiksmingumas, kartu sumažinant painumą bei finansinę ir administracinę naštą, tenkančią visiems finansų sektoriaus subjektams. Ja būtų suderinta itin tampriai tarpusavyje susijusi ir integruota ekonomikos sritis, kuriai jau sėkmingai taikomos bendros taisyklės ir priežiūra. Pasiūlymu būtų sumažinta pranešimo apie su IRT susijusius incidentus našta ir numanomos išlaidos, susijusios su pranešimu apie tą patį su IRT susijusį incidentą skirtingoms ES ir (arba) nacionalinėms valdžios institucijoms. Juo taip pat bus sudarytos palankesnės sąlygos tarpvalstybinę veiklą

vykdančių subjektų, kuriems skirtingose valstybėse narėse taikomos skirtingos testavimo sistemos, testavimo rezultatų abipusiam pripažinimui ir (arba) patvirtinimui.

1.5.3. Panašios patirties išvados

Nauja iniciatyva

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

Šio pasiūlymo tikslas atitinka daugelį kitų ES politikos sričių ir įgyvendinamų iniciatyvų, visų pirma Tinklų ir informacijos saugumo (TIS) direktyvą ir Europos ypatingos svarbos infrastruktūros objektų direktyvą. Pasiūlymu būtų užtikrinta nauda, susijusi su horizontaliąja kibernetinio saugumo sistema, nes trys finansų pasektoriai būtų ir toliau įtraukti į TIS direktyvos taikymo sritį. Išlaikydamos sąsajas su TIS ekosistema, finansų priežiūros institucijos galėtų keistis aktualia informacija su TIS institucijomis ir dalyvauti TIS bendradarbiavimo grupės darbe. Pasiūlymas neturėtų poveikio TIS direktyvai, greičiau ją papildytų ir pašalintų iš dalies sutampančių taisyklių problemą taikant *lex specialis* išimtį. Finansinių paslaugų reglamento ir TIS direktyvos sąveika ir toliau būtų grindžiama *lex specialis* išlyga, tad finansų sektoriaus subjektams nebūtų taikomi esminiai TIS direktyvos reikalavimai ir būtų išvengta iš dalies sutampančių šių dviejų aktų nuostatų problemos. Be to, pasiūlymas atitinka Europos ypatingos svarbos infrastruktūros objektų direktyvą, kuri šiuo metu peržiūrima siekiant sustiprinti ypatingos svarbos infrastruktūros objektų apsaugą ir atsparumą nekibernetinėms grėsmėms.

Šis pasiūlymas neturėtų poveikio daugiametei finansinei programai (DFP). Pirma, ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūros sistema bus visiškai finansuojama iš šių paslaugų teikėjų mokamų mokesčių; antra, papildomos reguliavimo užduotys, susijusios su EPI pavesta skaitmeninės veiklos atsparumo priežiūra, bus užtikrintos perskirstant jau dirbančius darbuotojus.

Todėl per būsimą metinę biudžeto procedūrą bus pateiktas pasiūlymas didinti agentūros įgaliotų darbuotojų skaičių. Agentūra toliau sieks kuo labiau didinti sąveiką ir našumą (be kita ko, pasitelkdama IT sistemas) ir atidžiai stebės su šio pasiūlymo įgyvendinimu susijusį papildomą darbo krūvį, kurį turėtų atitikti per būsimą metinę biudžeto procedūrą agentūros prašysimas įgaliotų darbuotojų skaičius.

1.5.5. Įvairių turimų finansavimo galimybių vertinimas, įskaitant perskirstymo mastą

Svarstytos kelios finansavimo galimybės:

Pirma, papildomos išlaidos galėtų būti finansuojamos pagal įprastą EPI finansavimo mechanizmą. Tačiau dėl to labai padidėtų ES įnašas į EPI finansinius išteklius.

Ši galimybė pasirenkama išlaidoms, susijusioms su šiuo pasiūlymu nustatomomis reguliavimo užduotimis. Iš tiesų EPI bus paprašytos perskirstyti esamus darbuotojus ir parengti keletą techninių standartų. Tačiau papildomų išlaidų, susijusių su ypatingos svarbos paslaugas teikiančių trečiųjų šalių priežiūra, nebūtų įmanoma padengti perskirstant EPI išteklius, nes, be šiame pasiūlyme numatytų užduočių, jos turi ir kitų užduočių, taip pat užduočių pagal kitus Sąjungos teisės aktus. Be to, priežiūros užduotims, susijusioms su skaitmeninės veiklos atsparumu, reikalingos specialios techninės žinios ir kompetencija. Kadangi dabartinis tokių išteklių lygis EPI nepakankamas, reikia papildomų išteklių.

Galiausiai, remiantis pasiūlymu, mokesčiai bus renkami iš ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių, kurių priežiūra bus vykdoma. Iš tų mokesčių planuojama padengti visus papildomus išteklius, kurių EPI reikia naujoms užduotims ir įgaliojimams vykdyti.

1.6. Pasiūlymo (iniciatyvos) trukmė ir finansinis poveikis

☐ **trukmė ribota**

☐ pasiūlymas (iniciatyva) galioja nuo MMMM [MM DD] iki MMMM [MM DD]

☐ finansinis poveikis nuo MMMM iki MMMM

☑ **trukmė neribota**

Įgyvendinimo pradinis laikotarpis – nuo 2021 m.,

vėliau – visuotinis taikymas.

1.7. Numatytas (-i) valdymo būdas (-ai)[51]

Tiesioginis valdymas, vykdomas Komisijos:

☐ vykdomųjų įstaigų

☐ **Pasidalijamasis valdymas** kartu su valstybėmis narėmis

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

☐ tarptautinėms organizacijoms ir jų agentūroms (nurodyti);

☐ EIB ir Europos investicijų fondui;

☑ 70 ir 71 straipsniuose nurodytoms įstaigoms;

☐ viešosios teisės subjektams;

☐ privatinės teisės reglamentuojamoms įstaigoms, kurioms pavesta teikti viešąsias paslaugas, jeigu jos pateikia pakankamas finansines garantijas;

☐ valstybės narės privatinės teisės reglamentuojamoms įstaigoms, kurioms pavesta įgyvendinti viešojo ir privačiojo sektorių partnerystę ir kurios pateikia pakankamas finansines garantijas;

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

Pastabos

nėra duomenų

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

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir atskaitomybės taisyklės

Nurodyti dažnumą ir sąlygas.

Pagal jau taikomą tvarką EPI reguliariai rengia savo veiklos ataskaitas (įskaitant vidaus ataskaitas vyresniajai vadovybei, ataskaitas valdybai ir metines ataskaitas). Be to, Audito Rūmai ir Komisijos Vidaus audito tarnyba atlieka jų išteklių naudojimo ir veiklos efektyvumo auditą. Į pasiūlymą įtrauktų veiksmų stebėsena ir atsiskaitymas už juos atitiks jau taikomus ir naujus dėl šio pasiūlymo atsiradusius reikalavimus.

2.2. Valdymo ir kontrolės sistema (-os)

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

Valdymas bus netiesioginis ir jį vykdys EPI. Finansavimo mechanizmas būtų įgyvendinamas iš mokesčių, taikomų atitinkamoms ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims.

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

Siekiant teisiškai, ekonomiškai, efektyviai ir veiksmingai naudoti pasiūlymui įgyvendinti skirtus asignavimus, tikimasi, kad įgyvendinant pasiūlymą nebus sudarytos sąlygos atsirasti naujai didelei rizikai, kuri esamoje vidaus kontrolės sistemoje dar nenumatyta. Tačiau nauja problema gali kilti užtikrinant, kad ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių mokesčiai būtų surenkami laiku.

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

EPI reglamentuose numatytos valdymo ir kontrolės sistemos jau įdiegtos. EPI glaudžiai bendradarbiauja su Komisijos Vidaus audito tarnyba, siekdamos užtikrinti, kad visose vidaus kontrolės sistemos srityse būtų laikomasi tinkamų standartų. Tokia tvarka taip pat galios EPI atliekant savo vaidmenį pagal šį pasiūlymą. Be to, kiekvienais finansiniais metais Europos Parlamentas, vadovaudamasis Tarybos rekomendacija, tvirtina EPI biudžeto vykdymo rezultatus.

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

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

Siekiant kovoti su sukčiavimu, korupcija ir visa kita neteisėta veikla, EPI be jokių apribojimų taikomos 2013 m. rugsėjo 11 d. Europos Parlamento ir Tarybos reglamento (ES, Euratomas) Nr. 883/2013 dėl Europos kovos su sukčiavimu tarnybos (OLAF) atliekamų tyrimų nuostatos.

EPI turi specialią kovos su sukčiavimu strategiją ir pagal ją parengtą veiksmų planą. Aktyvesni EPI veiksmai kovos su sukčiavimu srityje atitiks Finansinio reglamento taisykles ir rekomendacijas (taikyti kovos su sukčiavimu priemones vykdant patikimą finansų valdymą), OLAF sukčiavimo prevencijos politiką, Komisijos kovos su sukčiavimu strategijos (COM(2011) 376) ir bendro požiūrio į ES decentralizuotas agentūras (2012 m. liepos mėn.) nuostatas ir su tuo susijusias veiksmų gaires.

Be to, EPI steigimo reglamentuose ir EPI finansiniuose reglamentuose išdėstytos EPI biudžetų vykdymo ir kontrolės nuostatos ir taikytinos finansinės taisyklės, įskaitant sukčiavimo ir pažeidimų prevencijos taisykles.

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės), kurioms daromas poveikis

Dabartinės biudžeto eilutės

Daugiametės finansinės programos išlaidų kategorijas ir biudžeto eilutes nurodyti eilės tvarka.

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Numeris	DA / NDA [52]	ELPA šalių [53]	valstybių kandidačių [54]	trečiųjų valstybių	pagal Finansinio reglamento 21 straipsnio 2 dalies b punktą

Prašomos sukurti naujos biudžeto eilutės

Daugiametės finansinės programos išlaidų kategorijas ir biudžeto eilutes nurodyti eilės tvarka.

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Numeris	DA / NDA	ELPA šalių	valstybių kandidačių	trečiųjų valstybių	pagal Finansinio reglamento 21 straipsnio 2 dalies b punktą

[52] DA – diferencijuotieji asignavimai, NDA – nediferencijuotieji asignavimai.

[53] ELPA – Europos laisvosios prekybos asociacija.

[54] Valstybių kandidačių ir, kai taikoma, Vakarų Balkanų potencialių kandidačių.

3.2. Numatomas poveikis išlaidoms

3.3. Numatomo poveikio išlaidoms santrauka

mln. EUR (tūkstantųjų tikslumu)

Daugiametės finansinės programos išlaidų kategorija	Numeris	Išlaidų kategorija

GD: <..>			2020 m.	2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	**IŠ VISO**
	Įsipareigojimai	(1)									
	Mokėjimai	(2)									
IŠ VISO asignavimų <> GD	Įsipareigojimai										
	Mokėjimai										

Daugiametės finansinės programos išlaidų kategorija		

mln. EUR (tūkstantųjų tikslumu)

		2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	**IŠ VISO**
GD:								
• Žmogiškieji ištekliai								
• Kitos administracinės išlaidos <>								
IŠ VISO GD	Asignavimai							

IŠ VISO asignavimų pagal daugiametės finansinės programos **IŠLAIDŲ KATEGORIJĄ**	(Iš viso įsipareigojimų = Iš viso mokėjimų)							

mln. EUR (tūkstantųjų tikslumu) palyginamosiomis kainomis

		2022 m.	**2023 m.**	**2024 m.**	**2025 m.**	**2026 m.**	**2027 m.**	**IŠ VISO**
IŠ VISO asignavimų pagal 1 IŠLAIDŲ KATEGORIJĄ daugiametės finansinės programos	Įsipareigojimai							
	Mokėjimai							

3.3.1. Numatomas poveikis asignavimams

☑ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai nenaudojami

☐ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai naudojami taip:

Įsipareigojimų asignavimai mln. EUR (tūkstantųjų tikslumu) palyginamosiomis kainomis

Nurodyti tikslus ir atliktus darbus ⇩			2022 m.		2023 m.		2024 m.		2025 m.		2026 m.		2027 m.		**IŠ VISO**	
	ATLIKTI DARBAI															
	Rūšis[55]	Vidutinės sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Bendras skaičius	Iš viso sąnaudų
1 KONKRETUS TIKSLAS[56] …																
- Atlikti																
1 konkretaus tikslo tarpinė suma																
2 KONKRETUS TIKSLAS...																
- Atlikti																
2 konkretaus tikslo tarpinė suma																
IŠ VISO SĄNAUDŲ																

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

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

3.3.2. Numatomas poveikis žmogiškiesiems ištekliams

3.3.2.1. Santrauka

☐ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimų nenaudojama

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

mln. EUR (tūkstantųjų tikslumu) palyginamosiomis kainomis

EBI, EIOPA, ESMA	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	**IŠ VISO**
Laikinieji darbuotojai (AD lygio)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Laikinieji darbuotojai (AST lygio)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Sutartininkai							
Deleguotieji nacionaliniai ekspertai							
IŠ VISO	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Personalo poreikiai (etatų vienetais):

EBI, EIOPA, ESMA ir EEA	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	**IŠ VISO**
Laikinieji darbuotojai (AD lygio) EBI = 5, EIOPA = 5, ESMA = 5	15	15	15	15	15	15	15
Laikinieji darbuotojai (AST lygio) EBI = 1, EIOPA = 1, EEA = 1	3	3	3	3	3	3	3
Sutartininkai							
Deleguotieji nacionaliniai ekspertai							
IŠ VISO	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Numatomi (pagrindinio) GD žmogiškųjų išteklių poreikiai

☑ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškųjų išteklių nenaudojama.

☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai naudojami taip:

Sąmatą nurodyti sveikaisiais skaičiais (arba ne smulkiau nei dešimtųjų tikslumu)

		2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.
• **Etatų plano pareigybės (pareigūnai ir laikinieji darbuotojai)**							
• **Išorės darbuotojai (etatų vienetais)**[57]							
XX 01 02 01 (AC, END, INT finansuojami iš bendrojo biudžeto)							
XX 01 02 02 (CA, LA, SNE, INT ir JPD delegacijose)							
XX 01 04 *yy*[58]	– būstinėje[59]						
	– delegacijose						
XX 01 05 02 (CA, SNE, INT – netiesioginiai moksliniai tyrimai)							
10 01 05 02 (CA, INT, SNE – tiesioginiai moksliniai tyrimai)							
Kitos biudžeto eilutės (nurodyti)							
IŠ VISO							

XX yra atitinkama politikos sritis arba biudžeto antraštinė dalis.

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

Vykdytinų užduočių aprašymas:

Pareigūnai ir laikinieji darbuotojai	
Išorės darbuotojai	

V priedo 3 skirsnyje turėtų būti pateiktas etato ekvivalentų išlaidų apskaičiavimo aprašymas.

[57] CA – sutartininkas („Contract Staff“), LA – vietinis darbuotojas („Local Staff“), SNE – deleguotasis nacionalinis ekspertas („Seconded National Expert“), INT – per agentūrą įdarbintas darbuotojas („agency staff“), JPD – jaunesnysis delegacijos specialistas („Junior Professionals in Delegations“).

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

[59] Paprastai struktūrinių fondų, Europos žemės ūkio fondo kaimo plėtrai (EŽŪFKP) ir Europos žuvininkystės fondo (EŽF) atveju.

3.3.3. Suderinamumas su dabartine daugiamete finansine programa

☑ Pasiūlymas (iniciatyva) atitinka dabartinę daugiametę finansinę programą.

☐ Atsižvelgiant į pasiūlymą (iniciatyvą), reikės pakeisti daugiametės finansinės programos atitinkamos išlaidų kategorijos programavimą.

☐ Įgyvendinant pasiūlymą (iniciatyvą) būtina taikyti lankstumo priemonę arba patikslinti daugiametę finansinę programą[60].

Paaiškinti, ką reikia atlikti, ir nurodyti atitinkamas išlaidų kategorijas, biudžeto eilutes ir sumas. […]

3.3.4. Trečiųjų šalių įnašai

☐ Pasiūlyme (iniciatyvoje) nenumatyta bendro su trečiosiomis šalimis finansavimo.

☑ Pasiūlyme (iniciatyvoje) numatytas bendras finansavimas apskaičiuojamas taip:

mln. EUR (tūkstantųjų tikslumu)

EBI

	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	Iš viso
100 % sąnaudų padengiama iš mokesčių, surinktų iš prižiūrimų subjektų[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
IŠ VISO bendrai finansuojamų asignavimų	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	Iš viso
100 % sąnaudų padengiama iš mokesčių, surinktų iš prižiūrimų subjektų[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
IŠ VISO bendrai finansuojamų asignavimų	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	Iš viso

[60] Žr. Tarybos reglamento (ES, Euratomas) Nr. 1311/2013, kuriuo nustatoma 2014–2020 m. daugiametė finansinė programa, 11 ir 17 straipsnius.

[61] 100 % visų numatomų sąnaudų pridėjus visas darbdavio pensijų įmokas

[62] 100 % visų numatomų sąnaudų pridėjus visas darbdavio pensijų įmokas

100 % sąnaudų padengiama iš mokesčių, surinktų iš prižiūrimų subjektų[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
IŠ VISO bendrai finansuojamų asignavimų	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Numatomas poveikis pajamoms

☑ Pasiūlymas (iniciatyva) neturi finansinio poveikio pajamoms.

☐ Pasiūlymas (iniciatyva) turi finansinį poveikį:

- ☐ nuosaviems ištekliams
- ☐ kitoms pajamoms
- ☐ nurodyti, jei pajamos priskirtos išlaidų eilutėms

mln. EUR (tūkstantųjų tikslumu)

Biudžeto pajamų eilutė:	Einamųjų finansinių metų asignavimai	Pasiūlymo (iniciatyvos) poveikis[64]						
		N metai	**N+1** metai	**N+2** metai	**N+3** metai	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)		
……. straipsnis								

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

[…]

Nurodyti poveikio pajamoms apskaičiavimo metodą.

[…]

63 100 % visų numatomų sąnaudų pridėjus visas darbdavio pensijų įmokas

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

PRIEDAS

Bendrosios prielaidos

I antraštinė dalis. Išlaidos personalui

Apskaičiuojant išlaidas personalui buvo taikomos šios konkrečios prielaidos remiantis toliau paaiškintais nustatytais personalo poreikiais:

- išlaidos papildomam personalui, priimsimam į darbą 2022 m., apskaičiuotos šešiems mėnesiams, atsižvelgiant į numatomą laiką, reikalingą papildomam personalui įdarbinti;
- vidutinės metinės laikinojo darbuotojo išlaidos yra 150 000 EUR, į kurias įskaičiuota 25 000 EUR „darbuotojų išlaikymo“ išlaidų (pastatai, IT ir pan.);
- Paryžiaus (EBI ir ESMA) ir Frankfurto (EIOPA) darbuotojų atlyginimams taikomi korekcijos koeficientai atitinkamai yra 117,7 ir 99,4;
- darbdavio pensijų įmokos už laikinuosius darbuotojus nustatytos pagal standartinius bazinius atlyginimus, įskaičiuotus į standartines vidutines metines išlaidas, t. y. 95 660 EUR;
- papildomi laikinieji darbuotojai yra AD5 ir AST darbuotojai.

II antraštinė dalis. Infrastruktūros ir veiklos išlaidos

Išlaidos apskaičiuotos darbuotojų skaičių padauginus iš dirbtos metų dalies ir standartinių „darbuotojų išlaikymo“ išlaidų, t. y. 25 000 EUR.

III antraštinė dalis. Veiklos išlaidos

Išlaidos apskaičiuotos remiantis šiomis prielaidomis:

- kiekvienos EPI vertimo raštu išlaidos sudaro 350 000 EUR per metus;
- daroma prielaida, kad vienkartinės 500 000 EUR IT išlaidos, tenkančios vienai EPI, lygiomis dalimis patiriamos per dvejus metus – 2022 ir 2023 m.; skaičiuojama, kad 2024 m. vienos EPI metinės priežiūros išlaidos sudarys 50 000 EUR;
- skaičiuojama, kad vienos EPI priežiūros vietoje išlaidos sudarys 200 000 EUR.

Remiantis pateiktais įverčiais, metinės išlaidos sudaro:

Daugiametės finansinės programos išlaidų kategorija	Numeris	

Palyginamosios kainos

EBI:			2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	**IŠ VISO**
1 antraštinė dalis	Įsipareigojimai	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Mokėjimai	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
2 antraštinė dalis	Įsipareigojimai	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Mokėjimai	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
3 antraštinė dalis	Įsipareigojimai	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Mokėjimai	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
IŠ VISO asignavimų EBI	Įsipareigojimai	=1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Mokėjimai	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	**IŠ VISO**
1 antraštinė dalis	Įsipareigojimai	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Mokėjimai	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
2 antraštinė dalis	Įsipareigojimai	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Mokėjimai	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
3 antraštinė dalis	Įsipareigojimai	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Mokėjimai	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
IŠ VISO asignavimų	Įsipareigojimai	=1+1a+3a	1 305	1 811	1 611	1 611	1 611	1 611	9 560

EIOPA	Mokėjimai	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	**IŠ VISO**
1 antraštinė dalis	Įsipareigojimai	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Mokėjimai	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
2 antraštinė dalis	Įsipareigojimai	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Mokėjimai	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
3 antraštinė dalis	Įsipareigojimai	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Mokėjimai	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
IŠ VISO asignavimų ESMA	Įsipareigojimai	=1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Mokėjimai	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Pasiūlymui įgyvendinti veiklos asignavimai naudojami taip:

Įsipareigojimų asignavimai mln. EUR (tūkstantųjų tikslumu) palyginamosiomis kainomis

EBI

Nurodyti tikslus ir atliktus darbus ⇩			2022 m.		2023 m.		2024 m.		2025 m.		2026 m.		2027 m.			
	ATLIKTI DARBAI															
	Rūšis[65]	Vidutinės sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Bendras skaičius	Iš viso sąnaudų
KONKRETUS TIKSLAS Nr. 1[66] Tiesioginė ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūra																
- Atlikti				0,800		0,800		0,600		0,600		0,600		0,600		4,000
1 konkretaus tikslo tarpinė suma																
2 KONKRETUS TIKSLAS...																
- Atlikti																
2 konkretaus tikslo tarpinė suma																
IŠ VISO SĄNAUDŲ				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Nurodyti tikslus ir atliktus darbus ⇩			2022 m.		2023 m.		2024 m.		2025 m.		2026 m.		2027 m.			
	ATLIKTI DARBAI															
	Rūšis[67]	Vidutinės sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Bendras skaičius	Iš viso sąnaudų
KONKRETUS TIKSLAS Nr. 1[68] Tiesioginė ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūra																

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

[66] Kaip apibūdinta 1.4.2 skirsnyje „Konkretus (-ūs) tikslas (-ai)...“.

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

[68] Kaip apibūdinta 1.4.2 skirsnyje „Konkretus (-ūs) tikslas (-ai)...“.

- Atlikti				0,800		0,800		0,600		0,600		0,600		0,600		4,000
1 konkretaus tikslo tarpinė suma																
2 KONKRETUS TIKSLAS...																
- Atlikti																
2 konkretaus tikslo tarpinė suma																
IŠ VISO SĄNAUDŲ				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Nurodyti tikslus ir atliktus darbus ⇩			2022 m.		2023 m.		2024 m.		2025 m.		2026 m.		2027 m.			
	ATLIKTI DARBAI															
	Rūšis[69]	Vidutinės sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Bendras skaičius	Iš viso sąnaudų
KONKRETUS TIKSLAS Nr. 1[70] Tiesioginė ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių priežiūra																
- Atlikti				0,800		0,800		0,600		0,600		0,600		0,600		4,000
1 konkretaus tikslo tarpinė suma																
2 KONKRETUS TIKSLAS...																
- Atlikti																
2 konkretaus tikslo tarpinė suma																
IŠ VISO SĄNAUDŲ				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

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

[70] Kaip apibūdinta 1.4.2 skirsnyje „Konkretus (-ūs) tikslas (-ai)...“.

Priežiūros veikla visiškai finansuojama iš prižiūrimiems subjektams taikomų mokesčių:

EBI

	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	Iš viso
100 % sąnaudų padengiama iš mokesčių, surinktų iš prižiūrimų subjektų[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
IŠ VISO bendrai finansuojamų asignavimų	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	Iš viso
100 % sąnaudų padengiama iš mokesčių, surinktų iš prižiūrimų subjektų[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
IŠ VISO bendrai finansuojamų asignavimų	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	Iš viso
100 % sąnaudų padengiama iš mokesčių, surinktų iš prižiūrimų subjektų[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
IŠ VISO bendrai finansuojamų asignavimų	1,373	1,948	1,748	1,748	1,748	1,748	10,313

SPECIALIOJI INFORMACIJA

Tiesioginės priežiūros įgaliojimai

[71] 100 % visų numatomų sąnaudų pridėjus visas darbdavio pensijų įmokas
[72] 100 % visų numatomų sąnaudų pridėjus visas darbdavio pensijų įmokas
[73] 100 % visų numatomų sąnaudų pridėjus visas darbdavio pensijų įmokas

Pirmiausia reikėtų priminti, kad tiesiogiai ESMA prižiūrimi subjektai turėtų mokėti ESMA mokesčius (vienkartinius registravimo mokesčius ir reguliarius mokesčius už nuolatinę priežiūrą). Tokius mokesčius turi mokėti kredito reitingų agentūros (žr. Komisijos deleguotąjį reglamentą (ES) Nr. 272/2012) ir sandorių duomenų saugyklos (Komisijos deleguotasis reglamentas (ES) Nr. 1003/2013).

Pagal šį pasiūlymą dėl teisėkūros procedūra priimamo akto EPI bus patikėtos naujos užduotys, kuriomis siekiama skatinti priežiūros metodų, taikomų trečiosios šalies keliamai IRT rizika finansų sektoriuje, konvergenciją, ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims taikant Sąjungos priežiūros sistemą.

Šiame pasiūlyme numatyta priežiūros sistema yra grindžiama esama finansinių paslaugų srities institucine struktūra, pagal kurią EPI jungtinis komitetas užtikrina tarpsektorinį visų IRT rizikos klausimų koordinavimą pagal savo kibernetinio saugumo užduotis, o jam padeda atitinkamas pakomitetis (Priežiūros forumas), atliekantis parengiamąjį darbą, susijusį su atskirais sprendimais ir bendromis rekomendacijomis, skirtomis ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims.

Pagal šią sistemą EPI, paskirtoms kiekvienos ypatingos svarbos IRT paslaugas teikiančios trečiosios šalies atsakingosiomis priežiūros institucijomis, suteikiami įgaliojimai užtikrinti, kad technologijų paslaugų teikėjai, atliekantys ypatingos svarbos vaidmenį finansų sektoriaus veikloje, būtų tinkamai stebimi visos Europos mastu. Priežiūros pareigos yra išdėstytos pasiūlyme ir išsamiau paaiškintos aiškinamajame memorandume. Jos apima teises prašyti pateikti visą susijusią informaciją ir dokumentus, kad būtų galima atlikti bendruosius tyrimus ir patikrinimus, pateikti rekomendacijas ir vėliau pateikti ataskaitas dėl veiksmų, kurių imtasi, ar priemonių, kurios įgyvendintos pagal šias rekomendacijas.

Todėl, kad galėtų atlikti naujas šiame pasiūlyme numatytas užduotis, EPI turi pasamdyti papildomus darbuotojus, kurie specializuojasi IRT rizikos srityje ir daugiausia dėmesio skiria priklausomybės nuo trečiųjų šalių vertinimui.

Galima vertinti, kad kiekvienos institucijos žmogiškųjų išteklių poreikis sudaro 6 etatų vienetus (5 AD darbuotojai ir 1 AST darbuotojas, padedantis AD darbuotojui). EPI taip pat patirs papildomų IT išlaidų, kurios sudarys 500 000 EUR (vienkartinės išlaidos), o kiekviena iš trijų EPI patirs 50 000 EUR priežiūros išlaidų per metus. Svarbus elementas vykdant naujas užduotis yra patikrinimai vietoje ir auditas, dėl kurių kiekviena EPI patirs apytikriai 200 000 EUR per metus. Įvairių dokumentų, kuriuos EPI gautų iš ypatingos svarbos IRT paslaugas teikiančių trečiųjų šalių, vertimo išlaidos taip pat įtrauktos į veiklos išlaidų eilutę ir sudaro 350 000 EUR per metus.

Visos minėtos administracinės išlaidos bus visiškai finansuojamos iš metinių mokesčių, kuriuos EPI taikys prižiūrimoms ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims (poveikio ES biudžetui nebus).