Europos Sąjungos
oficialusis leidinys

LT
L serija

2024/1772

2024 6 25

KOMISIJOS DELEGUOTASIS REGLAMENTAS (ES) 2024/1772

2024 m. kovo 13 d.

kuriuo Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 papildomas techniniais reguliavimo standartais, kuriais patikslinami su IRT susijusių incidentų ir kibernetinių grėsmių klasifikavimo kriterijai, nustatomos reikšmingumo ribos ir nurodomi pranešimų apie didelius incidentus duomenys

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 ([1]), ypač į jo 18 straipsnio 4 dalies trečią pastraipą,

kadangi:

(1) Reglamentu (ES) 2022/2554 siekiama suderinti ir racionalizuoti pranešimų apie su IRT susijusius incidentus ir su mokėjimais susijusius operacinius arba saugumo incidentus, susijusius su kredito įstaigomis, mokėjimo įstaigomis, informavimo apie sąskaitas paslaugų teikėjais ir elektroninių pinigų įstaigomis (toliau – incidentai), teikimo reikalavimus. Kadangi pranešimų teikimo reikalavimai taikomi 20 skirtingų rūšių finansų sektoriaus subjektams, klasifikavimo kriterijai ir reikšmingumo ribos, pagal kuriuos nustatomi dideli incidentai ir didelės kibernetinės grėsmės, turėtų būti nustatyti paprastai, suderintai ir nuosekliai, atsižvelgiant į visų atitinkamų finansų sektoriaus subjektų paslaugų ir veiklos specifiką;

(2) siekiant užtikrinti proporcingumą, klasifikavimo kriterijai ir reikšmingumo ribos turėtų atspindėti visų finansų sektoriaus subjektų dydį bei bendrą rizikos profilį ir jų paslaugų pobūdį, mastą ir sudėtingumą. Be to, kriterijai ir reikšmingumo ribos turėtų būti nustatyti taip, kad jie būtų nuosekliai taikomi visiems finansų sektoriaus subjektams, nepriklausomai nuo jų dydžio ir rizikos profilio, ir neužkrautų neproporcingos atskaitomybės naštos mažesniems finansų sektoriaus subjektams. Tačiau, siekiant reaguoti į situacijas, kai incidentas, kuris pats neviršija taikomos ribos, paveikia daug klientų, turėtų būti nustatyta absoliuti riba, daugiausia orientuota į didesnius finansų sektoriaus subjektus;

(3) kalbant apie pranešimų apie incidentus teikimo sistemas, veikusias prieš įsigaliojant Reglamentui (ES) 2022/2554, finansų sektoriaus subjektams turėtų būti užtikrintas tęstinumas. Todėl klasifikavimo kriterijai ir reikšmingumo ribos turėtų būti suderinti su EBI gairėmis dėl pranešimų apie didelius incidentus teikimo pagal Europos Parlamento ir Tarybos direktyvą (ES) 2015/2366 ([2]), gairėmis dėl periodinės informacijos ir pranešimų apie reikšmingus pakeitimus, kuriuos ESMA turi teikti sandorių duomenų saugyklos, ECB/BPM pranešimų apie kibernetinius incidentus sistema bei kitomis atitinkamomis gairėmis ir parengti vadovaujantis tomis gairėmis. Klasifikavimo kriterijai ir ribos taip pat turėtų būti tinkami finansų sektoriaus subjektams, kuriems pranešimų apie incidentus teikimo reikalavimai iki Reglamento (ES) 2022/2554 įsigaliojimo nebuvo taikomi;

(4) kalbant apie klasifikavimo kriterijų „paveiktų sandorių suma ir skaičius“, sandorių sąvoka yra plati ir apima įvairią veiklą ir paslaugas pagal įvairius sektorinius teisės aktus, taikomus finansų sektoriaus subjektams. Taikant tą klasifikavimo kriterijų turėtų būti įtrauktos mokėjimo operacijos ir finansinių priemonių, kriptoturto, biržos prekių ar bet kokio kito turto, įskaitant garantinę įmoką, užtikrinimo priemonę arba įkaitą, visų formų iškeitimas tiek į pinigus, tiek į bet kokį kitą turtą. Klasifikuojant reikėtų atsižvelgti į visus sandorius, susijusius su turtu, kurio vertė gali būti išreikšta pinigų suma;

([1]) OL L 333, 2022 12 27, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) 2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 dėl mokėjimo paslaugų vidaus rinkoje, kuria iš dalies keičiamos direktyvos 2002/65/EB, 2009/110/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 ir panaikinama Direktyva 2007/64/EB (OL L 337, 2015 12 23, p. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) turėtų būti užtikrinta, kad klasifikavimo kriterijai apimtų visų svarbių rūšių didelius incidentus. Nedaug klasifikavimo kriterijų apima kibernetinius išpuolius, susijusius su įsibrovimu į tinklų ar informacines sistemas. Tačiau jie yra svarbūs, nes bet koks įsibrovimas į tinklų ir informacines sistemas gali pakenkti finansų sektoriaus subjektui. Todėl klasifikavimo kriterijai „paveiktos ypatingos svarbos paslaugos“ ir „duomenų praradimas“ turėtų būti patikslinti taip, kad apimtų šių rūšių didelius incidentus, visų pirma neteisėtus įsibrovimus, kurie, net jei jų poveikis nėra iš karto žinomas, gali turėti sunkių padarinių, konkrečiai, gali būti padaryta duomenų saugumo pažeidimų ir gali būti nutekinti duomenys;

(6) kadangi kredito įstaigoms taikoma tiek incidentų klasifikavimo sistema pagal Reglamento (ES) 2022/2554 18 straipsnį, tiek operacinės rizikos sistema pagal Komisijos deleguotąjį reglamentą (ES) 2018/959 ([3]), incidento ekonominio poveikio vertinimo metodas, grindžiamas sąnaudų ir nuostolių apskaičiavimu, turėtų būti kuo labiau suderintas abiejose sistemose, kad nebūtų nustatyta nesuderinamų ar prieštaringų reikalavimų;

(7) Reglamento (ES) 2022/2554 18 straipsnio 1 dalies c punkte nustatytu kriterijumi, susijusiu su geografiniu incidento pasiskirstymu, daugiausia dėmesio turėtų būti skiriama tarpvalstybiniam incidento poveikiui, nes incidento poveikį finansų sektoriaus subjekto veiklai viename jurisdikciją turinčiame subjekte apims kiti tame straipsnyje nustatyti kriterijai;

(8) atsižvelgiant į tai, kad klasifikavimo kriterijai yra tarpusavyje priklausomi ir susiję vieni su kitais, didelių incidentų, apie kuriuos reikia pranešti pagal Reglamento (ES) 2022/2554 19 straipsnio 1 dalį, nustatymo metodas turėtų būti grindžiamas kriterijų deriniu, kuriame kai kurie kriterijai, glaudžiai susiję su sąvokų „su IRT susijęs incidentas“ ir „didelis su IRT susijęs incidentas“ apibrėžtimis, nustatytomis Reglamento (ES) 2022/2554 3 straipsnio 8 ir 10 punktuose, turėtų būti svarbesni klasifikuojant didelius incidentus nei kiti kriterijai;

(9) kad pranešimai apie didelius incidentus, kuriuos kompetentingos institucijos gauna pagal Reglamento (ES) 2022/2554 19 straipsnio 1 dalį, ir atitiktų priežiūros tikslus, ir padėtų užkirsti kelią neigiamo poveikio išplitimui visame finansų sektoriuje, reikšmingumo ribos turėtų sudaryti sąlygas apimti didelius incidentus, daugiausia dėmesio skiriant, *inter alia*, poveikiui konkrečių subjektų ypatingos svarbos paslaugoms, konkrečioms absoliučioms ir santykinėms klientų ar finansų partnerių riboms, sandoriams, rodantiems reikšmingą poveikį finansų sektoriaus subjektui, ir poveikio kitose valstybėse narėse dydį;

(10) incidentais, darančiais poveikį finansų sektoriaus subjektų ypatingos svarbos paslaugoms, turėtų būti laikomi incidentai, kurie daro poveikį IRT paslaugoms arba tinklų ir informacinėms sistemoms, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, arba finansinėms paslaugoms, kurioms teikti reikia veiklos leidimo, arba piktavališka neteisėta prieiga prie tinklų ir informacinių sistemų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos. Piktavališka neteisėta prieiga prie tinklų ir informacinių sistemų, kuriomis palaikomos ypatingos svarbos arba svarbios finansų sektoriaus subjektų funkcijos, kelia didelę riziką finansų sektoriaus subjektui ir, kadangi ji gali daryti poveikį kitiems finansų sektoriaus subjektams, visada turėtų būti laikoma dideliu incidentu, apie kurį reikia pranešti;

(11) pasikartojantys incidentai, susiję su panašia akivaizdžia pagrindine priežastimi, kurie atskirai nėra dideli incidentai, gali rodyti didelius finansų sektoriaus subjekto incidentų ir rizikos valdymo procedūrų trūkumus. Todėl pasikartojantys incidentai, kai jie per tam tikrą laikotarpį įvyksta pakartotinai, visi kartu turėtų būti laikomi dideliu incidentu;

(12) atsižvelgiant į tai, kad kibernetinės grėsmės gali turėti neigiamą poveikį finansų sektoriaus subjektui ir sektoriui, didelės kibernetinės grėsmės, apie kurias finansų sektoriaus subjektai gali pranešti, turėtų rodyti pasitvirtinimo tikimybę ir ypatingą galimo poveikio svarbą. Atitinkamai, siekiant užtikrinti aiškų ir nuoseklų kibernetinių grėsmių dydžio vertinimą, kibernetinės grėsmės klasifikavimas kaip didelės turėtų priklausyti nuo tikimybės, kad didelių incidentų klasifikavimo kriterijai ir jų riba būtų atitikti, jei grėsmė pasitvirtintų, nuo kibernetinės grėsmės rūšies ir nuo finansų sektoriaus subjekto turimos informacijos;

([3]) 2018 m. kovo 14 d. Komisijos deleguotasis reglamentas (ES) 2018/959, kuriuo papildomas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 575/2013 ir nustatoma vertinimo metodika, pagal kurią kompetentingos institucijos leidžia įstaigoms taikyti pažangiuosius operacinės rizikos vertinimo metodus (OL L 169, 2018 7 6, p. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) atsižvelgiant į tai, kad kitų valstybių narių kompetentingoms institucijoms turi būti pranešta apie incidentus, kurie daro poveikį jų jurisdikcijai priklausantiems finansų sektoriaus subjektams ir klientams, poveikio kitame jurisdikciją turinčiame subjekte vertinimas pagal Reglamento (ES) 2022/2554 19 straipsnio 7 dalį turėtų būti grindžiamas pagrindine incidento priežastimi, galimu plintančiu neigiamu poveikiu per paslaugas teikiančias trečiąsias šalis ir finansų rinkos infrastruktūroms, taip pat incidento poveikiu svarbioms klientų ar finansų partnerių grupėms;

(14) Reglamento (ES) 2022/2554 19 straipsnio 6 ir 7 dalyse nurodyti pranešimų teikimo savo šalies ir kitų valstybių narių kompetentingoms institucijoms procesai turėtų sudaryti sąlygas atitinkamiems gavėjams įvertinti incidentų poveikį. Todėl perduodama informacija turėtų apimti visus finansų sektoriaus subjekto kompetentingai institucijai pateiktuose pranešimuose apie incidentus pateiktus duomenis;

(15) jei incidentas laikomas asmens duomenų saugumo pažeidimu pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 ([4]) ir Europos Parlamento ir Tarybos direktyvą 2002/58/EB ([5]), šis reglamentas neturėtų daryti poveikio tuose Sąjungos teisės aktuose nustatytoms pareigoms registruoti asmens duomenų saugumo pažeidimus ir apie juos pranešti. Kompetentingos institucijos turėtų bendradarbiauti ir keistis informacija visais svarbiais klausimais su institucijomis, nurodytomis Reglamente (ES) 2016/679 ir Direktyvoje 2002/58/EB;

(16) šis reglamentas grindžiamas techninių reguliavimo standartų projektais, kuriuos Komisijai pateikė Europos priežiūros institucijos, pasikonsultavusios su Europos Sąjungos kibernetinio saugumo agentūra (ENISA) ir Europos Centriniu Banku (ECB);

(17) Europos priežiūros institucijų jungtinis komitetas, nurodytas Europos Parlamento ir Tarybos reglamento (ES) Nr. 1093/2010 ([6]) 54 straipsnyje, Europos Parlamento ir Tarybos reglamento (ES) Nr. 1094/2010 ([7]) 54 straipsnyje ir Europos Parlamento ir Tarybos reglamento (ES) Nr. 1095/2010 ([8]) 54 straipsnyje, surengė atviras viešas konsultacijas dėl techninių reguliavimo standartų projektų, kuriais pagrįstas šis reglamentas, išnagrinėjo galimas siūlomų standartų sąnaudas ir naudą ir paprašė, kad pagal Reglamento (ES) Nr. 1093/2010 37 straipsnį įsteigta Bankininkystės suinteresuotųjų subjektų grupė, pagal Reglamento (ES) Nr. 1094/2010 37 straipsnį įsteigta Draudimo ir perdraudimo suinteresuotųjų subjektų grupė ir Profesinių pensijų suinteresuotųjų subjektų grupė ir pagal Reglamento (ES) Nr. 1095/2010 37 straipsnį įsteigta Vertybinių popierių ir rinkų suinteresuotųjų subjektų grupė pateiktų rekomendacijų;

([4]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1093/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos bankininkystės institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/78/EB (OL L 331, 2010 12 15, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1094/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos draudimo ir profesinių pensijų institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/79/EB (OL L 331, 2010 12 15, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1095/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos vertybinių popierių ir rinkų institucija) ir iš dalies keičiamas Sprendimas Nr. 716/2009/EB bei panaikinamas Komisijos sprendimas 2009/77/EB (OL L 331, 2010 12 15, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([9]) 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis pateikė nuomonę 2024 m. sausio 24 d.,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I SKYRIUS

KLASIFIKAVIMO KRITERIJAI

1 straipsnis

Klientai, finansų partneriai ir sandoriai

1. Reglamento (ES) 2022/2554 18 straipsnio 1 dalies a punkte nurodytas klientų, kurių veikla buvo sutrikdyta dėl incidento, skaičius atspindi visų paveiktų klientų (fizinių ar juridinių asmenų), kurie negali arba incidento metu negalėjo pasinaudoti finansų sektoriaus subjekto teikiama paslauga arba kuriems incidentas padarė neigiamą poveikį, skaičių. Tas skaičius, kaip paveiktos paslaugos gavėjas, taip pat apima trečiąsias šalis, kurioms aiškiai taikomas finansų sektoriaus subjekto ir kliento sutartinis susitarimas.

2. Reglamento (ES) 2022/2554 18 straipsnio 1 dalies a punkte nurodytas finansų partnerių, kurių veikla buvo sutrikdyta dėl incidento, skaičius atspindi visų paveiktų finansų partnerių, kurie su finansų sektoriaus subjektu yra sudarę sutartimi įformintą susitarimą, skaičių.

3. Kalbant apie Reglamento (ES) 2022/2554 18 straipsnio 1 dalies a punkte nurodytą klientų ir finansų partnerių, kurių veikla buvo sutrikdyta dėl incidento, svarbą, finansų sektoriaus subjektas atsižvelgia į tai, kokiu mastu poveikis klientui arba finansų partneriui paveiks finansų sektoriaus subjekto verslo tikslų įgyvendinimą, taip pat į galimą incidento poveikį rinkos efektyvumui.

4. Kalbant apie Reglamento (ES) 2022/2554 18 straipsnio 1 dalies a punkte nurodytą sandorių, kuriuos sutrikdė incidentas, sumą ar skaičių, finansų sektoriaus subjektas atsižvelgia į visus paveiktus sandorius, susijusius su pinigų suma, kai bent viena sandorio dalis vykdoma Sąjungoje.

5. Jei neįmanoma nustatyti faktinio paveiktų klientų ar finansų partnerių skaičiaus arba faktinio paveiktų sandorių skaičiaus ar sumos, finansų sektoriaus subjektas tuos skaičius arba sumas įvertina remdamasis turimais palyginamų ataskaitinių laikotarpių duomenimis.

2 straipsnis

Poveikis reputacijai

1. Siekdami nustatyti Reglamento (ES) 2022/2554 18 straipsnio 1 dalies a punkte nurodytą incidento poveikį reputacijai, finansų sektoriaus subjektai laiko, kad poveikis reputacijai buvo padarytas, jei tenkinamas bent vienas iš šių kriterijų:

a) incidentas aptartas žiniasklaidoje;

b) įvykus incidentui skirtingi klientai arba finansų partneriai pakartotinai skundėsi dėl tiesiogiai klientams teikiamų paslaugų arba ypatingos svarbos verslo santykių;

c) įvykus incidentui finansų sektoriaus subjektas negalės arba greičiausiai negalės įvykdyti reguliavimo reikalavimų;

d) įvykus incidentui finansų sektoriaus subjektas praras arba greičiausiai praras klientų arba finansų partnerių, o tai padarys reikšmingą poveikį jo veiklai.

([9]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. Vertindami incidento poveikį reputacijai, finansų sektoriaus subjektai atsižvelgia į paviešinimo lygį, kurį incidentas pasiekė arba greičiausiai pasieks pagal kiekvieną 1 dalyje nurodytą kriterijų.

3 straipsnis

Trukmė ir laikas, kurį nebuvo teikiamos paslaugos

1. Finansų sektoriaus subjektai Reglamento (ES) 2022/2554 18 straipsnio 1 dalies b punkte nurodytą incidento trukmę matuoja nuo momento, kada incidentas įvyko, iki jo pašalinimo momento.

Jei negali nustatyti momento, kada incidentas įvyko, incidento trukmę finansų sektoriaus subjektai matuoja nuo to momento, kada jis buvo aptiktas. Finansų sektoriaus subjektai, sužinoję, kad incidentas įvyko, prieš jį aptikdami, incidento trukmę matuoja nuo momento, kada incidentas užregistruotas tinklo ar sistemos žurnaluose ar kituose duomenų šaltiniuose.

Jeigu dar nežino, kada incidentas bus pašalintas, arba negali patikrinti įrašų registracijos žurnaluose ar kituose duomenų šaltiniuose, finansų sektoriaus subjektai taiko įverčius.

2. Finansų sektoriaus subjektai Reglamento (ES) 2022/2554 18 straipsnio 1 dalies b punkte nurodytą laiką, kurį dėl incidento nebuvo teikiamos paslaugos, matuoja nuo to momento, kai klientams, finansų partneriams ar kitiems vidaus ar išorės naudotojams paslauga tampa visiškai arba iš dalies neprieinama, iki momento, kai įprasta veikla ar operacijos atkuriamos iki paslaugų lygio, kuris buvo užtikrinamas prieš incidentą. Jei dėl laiko, kurį paslaugos neteikiamos, paslaugos teikimas vėluoja po to, kai buvo atkurta įprasta veikla ar operacijos, laikas, kurį nebuvo teikiamos paslaugos, matuojamas nuo incidento pradžios iki momento, kai ta vėluojanti paslauga yra teikiama visa apimtimi.

Jei negali nustatyti momento, kada prasidėjo laikas, kurį nebuvo teikiamos paslaugos, tą laiką finansų sektoriaus subjektai matuoja nuo to momento, kai aptikta, kad paslauga neteikiama.

4 straipsnis

Geografinis pasiskirstymas

Siekdami nustatyti Reglamento (ES) 2022/2554 18 straipsnio 1 dalies c punkte nurodytą geografinį pasiskirstymą incidento paveiktose vietovėse, finansų sektoriaus subjektai įvertina, ar incidentas daro arba padarė poveikį kitose valstybėse narėse ir visų pirma poveikio bet kuriai iš toliau nurodytų šalių dydį:

a) klientams ir finansų partneriams kitose valstybėse narėse;

b) filialams ar kitiems grupei priklausantiems finansų sektoriaus subjektams, vykdantiems veiklą kitose valstybėse narėse;

c) finansų rinkos infrastruktūroms arba paslaugas teikiančioms trečiosioms šalims, kurios gali paveikti kitose valstybėse narėse esančius finansų sektoriaus subjektus, kuriems jos teikia paslaugas, jei tokia informacija yra prieinama.

5 straipsnis

Duomenų praradimas

Siekdami nustatyti Reglamento (ES) 2022/2554 18 straipsnio 1 dalies d punkte nurodytą duomenų praradimą dėl incidento, finansų sektoriaus subjektai atsižvelgia į šiuos aspektus:

a) kiek tai susiję su duomenų prieinamumu, – ar dėl incidento finansų sektoriaus subjektui, jo klientams ar partneriams reikalingi duomenys laikinai arba visam laikui tapo neprieinami arba netinkami naudoti;

b) kiek tai susiję su duomenų autentiškumu, – ar incidentas pakenkė duomenų šaltinio patikimumui;

c) kiek tai susiję su duomenų vientisumu, – ar incidentas lėmė neteisėtą duomenų pakeitimą, dėl kurio jie tapo netikslūs arba neišsamūs;

d) kiek tai susiję su duomenų konfidencialumu, – ar dėl incidento prieigą prie duomenų gavo tokios teisės neturinti šalis arba sistema arba jie buvo joms atskleisti.

6 straipsnis

Paveiktų paslaugų ypatinga svarba

Siekdami nustatyti Reglamento (ES) 2022/2554 18 straipsnio 1 dalies e punkte nurodytą incidento paveiktų paslaugų ypatingą svarbą, finansų sektoriaus subjektai įvertina, ar incidentas:

a) veikia arba paveikė IRT paslaugas arba tinklų ir informacines sistemas, kuriomis palaikomos ypatingos svarbos ar svarbios finansų sektoriaus subjekto funkcijos;

b) veikia arba paveikė finansų sektoriaus subjekto teikiamas finansines paslaugas, kurioms teikti reikia veiklos leidimo ar registracijos arba kurių priežiūrą vykdo kompetentingos institucijos;

c) sudaro arba sudarė sąlygas sėkmingai gauti piktavališką ir neteisėtą prieigą prie finansų sektoriaus subjekto tinklų ir informacinių sistemų.

7 straipsnis

Ekonominis poveikis

1. Siekdami nustatyti Reglamento (ES) 2022/2554 18 straipsnio 1 dalies f punkte nurodytą ekonominį incidento poveikį, finansų sektoriaus subjektai, neatsižvelgdami į susigrąžintų lėšų sumas, atsižvelgia į toliau nurodytų rūšių tiesiogines ir netiesiogines sąnaudas ir nuostolius, kuriuos jie patyrė dėl incidento:

a) nusavintas lėšas arba finansinį turtą, už kuriuos jie yra atsakingi, įskaitant dėl vagystės prarastą turtą;

b) programinės ar aparatinės įrangos arba infrastruktūros pakeitimo arba perkėlimo išlaidas;

c) personalo išlaidas, įskaitant išlaidas, susijusias su darbuotojų pakeitimu ar perkėlimu, papildomų darbuotojų įdarbinimu, atlygiu už viršvalandžius ir prarastų ar pablogėjusių įgūdžių susigrąžinimu;

d) mokėtinus mokesčius už sutartinių įsipareigojimų nesilaikymą;

e) teisių gynimo ir kompensavimo klientams išlaidas;

f) nuostolius dėl negautų pajamų;

g) išlaidas, susijusias su vidaus ir išorės komunikacija;

h) konsultavimo išlaidas, įskaitant išlaidas, susijusias su teisinėmis konsultacijomis, teismo ekspertizės paslaugomis ir taisomojo pobūdžio paslaugomis.

2. 1 dalyje nurodytos sąnaudos ir nuostoliai neapima išlaidų, kurios yra būtinos kasdienei įmonės veiklai, visų pirma:

a) infrastruktūros, įrangos, aparatinės ir programinės įrangos bendro pobūdžio priežiūros išlaidų ir darbuotojų įgūdžių atnaujinimo išlaidų;

b) vidaus ar išorės sąnaudų veiklai gerinti po incidento, įskaitant atnaujinimus, patobulinimus ir rizikos vertinimo iniciatyvas;

c) draudimo įmokų.

3. Finansų sektoriaus subjektai sąnaudų ir nuostolių sumas apskaičiuoja remdamiesi pranešimų teikimo metu turimais duomenimis. Jei sąnaudų ir nuostolių faktinių sumų nustatyti neįmanoma, finansų sektoriaus subjektai nustato tų sumų įverčius.

4. Vertindami ekonominį incidento poveikį finansų sektoriaus subjektai susumuoja 1 dalyje nurodytas sąnaudas ir nuostolius.

II SKYRIUS

DIDELI INCIDENTAI IR REIKŠMINGUMO RIBOS

8 straipsnis

Dideli incidentai

1. Taikant Reglamento (ES) 2022/2554 19 straipsnio 1 dalį, incidentas laikomas dideliu incidentu, jei jis paveikė 6 straipsnyje nurodytas ypatingos svarbos paslaugas ir jei tenkinama bet kuri iš šių sąlygų:

a) pasiekta 9 straipsnio 5 dalies b punkte nurodyta reikšmingumo riba;

b) pasiektos dvi ar daugiau kitų 9 straipsnio 1–6 dalyse nurodytų reikšmingumo ribų.

2. Pasikartojantys incidentai, kurie atskirai nelaikomi dideliais incidentais pagal 1 dalį, yra laikomi vienu dideliu incidentu, jei jie atitinka visas šias sąlygas:

a) jie įvyko bent du kartus per 6 mėnesius;

b) jų akivaizdi pagrindinė priežastis yra ta pati, kaip nurodyta Reglamento (ES) 2022/2554 20 straipsnio pirmos pastraipos b punkte;

c) jie visi kartu atitinka 1 dalyje nustatytus kriterijus, kad būtų laikomi dideliu incidentu.

Finansų sektoriaus subjektai kas mėnesį vertina, ar yra pasikartojančių incidentų.

Ši dalis netaikoma labai mažoms įmonėms ir finansų sektoriaus subjektams, išvardytiems Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje.

9 straipsnis

Reikšmingumo ribos dideliems incidentams nustatyti

1. Klientų, finansų partnerių ir sandorių kriterijaus reikšmingumo riba yra pasiekta, jei tenkinama kuri nors iš šių sąlygų:

a) paveiktų klientų skaičius yra didesnis nei 10 % visų klientų, kurie naudojasi paveikta paslauga;

b) paveiktų klientų, kurie naudojasi paveikta paslauga, skaičius yra didesnis nei 100 000;

c) paveiktų finansų partnerių skaičius yra didesnis nei 30 % visų finansų partnerių, vykdančių veiklą, susijusią su paveiktos paslaugos teikimu;

d) paveiktų sandorių skaičius yra didesnis nei 10 % finansų sektoriaus subjekto vykdomų sandorių, susijusių su paveikta paslauga, skaičiaus dienos vidurkio;

e) paveiktų sandorių suma yra didesnė nei 10 % finansų sektoriaus subjekto vykdomų sandorių, susijusių su paveikta paslauga, vertės dienos vidurkio;

f) poveikis padarytas klientams arba finansų partneriams, kurie nustatyti kaip svarbūs pagal 1 straipsnio 3 dalį.

Jei neįmanoma nustatyti faktinio paveiktų klientų ar finansų partnerių skaičiaus arba faktinio paveiktų sandorių skaičiaus ar sumos, finansų sektoriaus subjektas tuos skaičius arba sumas įvertina remdamasis turimais palyginamų ataskaitinių laikotarpių duomenimis.

2. Poveikio reputacijai kriterijaus reikšmingumo riba yra pasiekta, jei tenkinama kuri nors iš 2 straipsnio a–d punktuose nustatytų sąlygų.

3. Trukmės ir laiko, kurį nebuvo teikiamos paslaugos, kriterijaus reikšmingumo riba yra pasiekta, jei tenkinama kuri nors iš šių sąlygų:

a) incidentas trunka ilgiau nei 24 valandas;

b) laikas, kurį nebuvo teikiamos IRT paslaugos, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, yra ilgesnis nei 2 valandos.

4. Geografinio pasiskirstymo kriterijaus reikšmingumo riba yra pasiekta, jei incidentas daro poveikį dviejose ar daugiau valstybių narių pagal 4 straipsnį.

5. Duomenų praradimo kriterijaus reikšmingumo riba yra pasiekta, jei tenkinama kuri nors iš šių sąlygų:

a) bet koks 5 straipsnyje nurodytas poveikis duomenų prieinamumui, autentiškumui, vientisumui ar konfidencialumui daro arba darys neigiamą poveikį finansų sektoriaus subjekto verslo tikslų įgyvendinimui arba jo gebėjimui vykdyti reguliavimo reikalavimus;

b) sėkmingai įgyjama bet kokia piktavališka ir neteisėta prieiga prie tinklų ir informacinių sistemų, kuriai netaikomas a punktas, jei dėl tokios prieigos gali būti prarasti duomenys.

6. Ekonominio poveikio kriterijaus reikšmingumo riba yra pasiekta, jei finansų sektoriaus subjekto dėl incidento patirtos sąnaudos ir nuostoliai viršija arba greičiausiai viršys 100 000 EUR.

III SKYRIUS

DIDELĖS KIBERNETINĖS GRĖSMĖS

10 straipsnis

Didelio reikšmingumo ribos didelėms kibernetinėms grėsmėms nustatyti

Taikant Reglamento (ES) 2022/2554 18 straipsnio 2 dalį, kibernetinė grėsmė laikoma didele, jei tenkinamos visos šios sąlygos:

a) pasitvirtinusi kibernetinė grėsmė galėtų paveikti arba galėtų būti paveikusi finansų sektoriaus subjekto ypatingos svarbos ar svarbias funkcijas arba galėtų paveikti kitus finansų sektoriaus subjektus, paslaugas teikiančias trečiąsias šalis, klientus ar finansų partnerius, remiantis finansų sektoriaus subjekto turima informacija;

b) yra didelė tikimybė, kad kibernetinė grėsmė pasitvirtins finansų sektoriaus subjekte arba kituose finansų sektoriaus subjektuose, atsižvelgiant bent į šiuos elementus:

   i) taikytiną riziką, susijusią su a punkte nurodyta kibernetine grėsme, įskaitant galimus finansų sektoriaus subjekto sistemų pažeidžiamumus, kuriais galima pasinaudoti;

   ii) priešiškų subjektų pajėgumus ir ketinimą, kiek tai žinoma finansų sektoriaus subjektui;

   iii) išliekančią grėsmę ir sukauptas žinias apie incidentus, kurie padarė poveikį finansų sektoriaus subjektui arba jo paslaugas teikiančiai trečiajai šaliai, klientams ar finansų partneriams;

c) pasitvirtinusi kibernetinė grėsmė galėtų atitikti kurį nors iš šių aspektų:

   i) Reglamento (ES) 2022/2554 18 straipsnio 1 dalies e punkte nustatytą paslaugų ypatingos svarbos kriterijų, kaip nurodyta šio reglamento 6 straipsnyje;

   ii) 9 straipsnio 1 dalyje nustatytą reikšmingumo ribą;

   iii) 9 straipsnio 4 dalyje nustatytą reikšmingumo ribą.

Jei, priklausomai nuo kibernetinės grėsmės rūšies ir turimos informacijos, finansų sektoriaus subjektas padaro išvadą, kad galėtų būti pasiektos 9 straipsnio 2, 3, 5 ir 6 dalyse nustatytos reikšmingumo ribos, į tas ribas taip pat gali būti atsižvelgiama.

IV SKYRIUS

DIDELIŲ INCIDENTŲ SVARBA KOMPETENTINGOMS INSTITUCIJOMS KITOSE VALSTYBĖSE NARĖSE IR PRANEŠIMŲ DUOMENYS, KURIAIS TURI BŪTI DALIJAMASI SU KITOMIS KOMPETENTINGOMIS INSTITUCIJOMIS

11 straipsnis

Didelių incidentų svarba kompetentingoms institucijoms kitose valstybėse narėse

Reglamento (ES) 2022/2554 19 straipsnio 7 dalyje nurodytas vertinimas, ar didelis incidentas yra svarbus kompetentingoms institucijoms kitose valstybėse narėse, yra grindžiamas tuo, ar incidento pagrindinė priežastis kilo iš kitos valstybės narės arba ar incidentas daro arba darė didelį poveikį kitoje valstybėje narėje bet kuriai iš šių šalių:

a) klientams arba finansų partneriams;

b) finansų sektoriaus subjekto filialams arba kitam grupei priklausančiam finansų sektoriaus subjektui;

c) finansų rinkos infrastruktūrai arba paslaugas teikiančiai trečiajai šaliai, kuri gali paveikti finansų sektoriaus subjektus, kuriems ji teikia paslaugas.

12 straipsnis

Didelių incidentų duomenys, kuriais turi būti dalijamasi su kitomis kompetentingomis institucijomis

Didelių incidentų duomenys, kuriuos kompetentingos institucijos turi pateikti kitoms kompetentingoms institucijoms pagal Reglamento (ES) 2022/2554 19 straipsnio 6 dalį, ir pranešimai, kuriuos EBI, ESMA arba EIOPA ir ECB turi pateikti atitinkamoms kompetentingoms institucijoms kitose valstybėse narėse pagal to reglamento 19 straipsnio 7 dalį, apima tokio paties lygio nenuasmenintą informaciją kaip ir pranešimai apie didelius incidentus, gaunami iš finansų sektoriaus subjektų pagal Reglamento (ES) 2022/2554 19 straipsnio 4 dalį.

V SKYRIUS

BAIGIAMOSIOS NUOSTATOS

13 straipsnis

Įsigaliojimas

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

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2024 m. kovo 13 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN