EUROPOS CENTRINIO BANKO NUOMONĖ

2022 m. balandžio 11 d.

dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Įžanga ir teisinis pagrindas

2020 m. gruodžio 16 d. Europos Komisija priėmė pasiūlymą dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148 ([1]) (toliau – pasiūlyta direktyva). 2021 m. gruodžio 3 d. Europos Sąjungos Taryba susitarė dėl bendro požiūrio dėl pasiūlytos direktyvos ([2]). Europos Centrinio Banko (ECB) kompetencija teikti nuomonę grindžiama Sutarties dėl Europos Sąjungos veikimo 127 straipsnio 4 dalies antra pastraipa, nes pasiūlytoje direktyvoje yra nuostatų, priklausančių ECB kompetencijos sritims, visų pirma susijusioms su sklandaus mokėjimo sistemų veikimo skatinimu, indėliu į sklandų kompetentingų institucijų politikos, susijusios su finansų rinkos sistemos stabilumu, vykdymu ir ECB uždaviniais kredito įstaigų prudencinės priežiūros srityje pagal Sutarties 127 straipsnio 2 dalies ketvirtą įtrauką, 127 straipsnio 5 dalį ir 127 straipsnio 6 dalį. Vadovaudamasi Europos Centrinio Banko darbo reglamento 17 straipsnio 5 dalies pirmuoju sakiniu, Valdančioji taryba priėmė šią nuomonę.

Bendrosios pastabos

ECB tvirtai remia pasiūlytos direktyvos tikslus didinti kibernetinio atsparumo lygį visuose atitinkamuose sektoriuose, mažinti neatitikimus vidaus rinkoje ir didinti informuotumą apie padėtį bei bendrus gebėjimus pasirengti ir reaguoti užtikrinant veiksmingą bendradarbiavimą Sąjungoje.

ECB pripažįsta, kad svarbu išlaikyti tvirtus ryšius tarp pasiūlytos direktyvos ir finansų sektoriaus, kuris turėtų išlikti tinklų ir informacinių sistemų (TIS) ekosistemos dalimi, siekiant skatinti nuoseklų su informacinėmis ir ryšių technologijomis (IRT) susijusios rizikos vertinimą visoje Sąjungoje ir skatinti veiksmingą tarpsektorinį keitimąsi informacija ir bendradarbiavimą kovojant su kibernetinėmis grėsmėmis. Tuo tikslu kompetentingos institucijos pagal pasiūlytą Europos Parlamento ir Tarybos reglamentą dėl skaitmeninės veiklos atsparumo finansų sektoriuje ([3]) (DORA) turėtų turėti galimybę dalyvauti strateginėse politinėse diskusijose ir TIS bendradarbiavimo grupės techninėje veikloje, taip pat keistis informacija ir toliau bendradarbiauti su pasiūlytoje direktyvoje nurodytais bendraisiais informaciniais centrais ir nacionalinėmis reagavimo į kompiuterinius saugumo incidentus tarnybomis ([4]).

1. Pasiūlytos direktyvos taikymo sritis

1.1 ECB supranta, kad, kiek tai susiję su finansų sektoriaus subjektais, DORA bus laikomas konkretiems sektoriams skirtu teisės aktu, nustatančiu kibernetinio saugumo rizikos valdymo ir pranešimo apie incidentus reikalavimus, kurių poveikis yra bent lygiavertis nustatytiesiems pasiūlytoje direktyvoje ([5]). Todėl pasiūlytos direktyvos nuostatos, susijusios su kibernetinio saugumo rizikos valdymu, ataskaitų teikimo prievolėmis, keitimusi informacija, priežiūra ir vykdymo užtikrinimu, nebus taikomos jokiems finansų sektoriaus subjektams, kuriems taikomas DORA ([6]). Kaip paaiškinta pasiūlytos direktyvos konstatuojamosiose dalyse, vietoj pasiūlytos direktyvos nuostatų turėtų būti

([1]) COM (2020) 823 final.
([2]) Paskelbta Tarybos interneto svetainėje www.consilium.europa.eu
([3]) COM (2020) 595 final.
([4]) Žr. 2021 m. birželio 4 d. Europos Centrinio Banko nuomonės CON/2021/20 dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl skaitmeninės veiklos atsparumo finansų sektoriuje (OL C 343, 2021 8 26, p. 1) 1.5 dalį. Visos ECB nuomonės skelbiamos EUR-Lex. DORA 17 straipsnio 5 dalis ir 42 straipsnis, pasiūlytos direktyvos 11 straipsnis.
([5]) Pasiūlytos direktyvos 2 straipsnio 6 dalis.
([6]) Pasiūlytos direktyvos 13 konstatuojamoji dalis ir 2 straipsnio 6 dalis.

taikomos DORA nuostatos, susijusios su informacinių ir ryšių technologijų (IRT) rizikos valdymo priemonėmis, IRT incidentų valdymu ir pranešimu apie incidentus, taip pat su skaitmeninės veiklos atsparumo testavimu, dalijimosi informacija tvarka ir trečiosios šalies IRT rizika ([7]).

1.2 ECB taip pat atkreipia dėmesį, kad Taryba savo bendrame požiūryje dėl pasiūlytos direktyvos formuluoja pasiūlymą, kad direktyva nebūtų taikoma subjektams, kurie vykdo veiklą teisminių institucijų, parlamentų arba centrinių bankų veiklos srityse ([8]). ECB supranta, kad pasiūlytas dalinis pakeitimas apimtų visas pagrindines Europos centrinių bankų sistemos užduotis ir kompetencijas, išdėstytas Sutarties 127 straipsnio 2 dalyje ir Europos centrinių bankų sistemos ir Europos Centrinio Banko statuto (ECBS statutas) 3 straipsnio 1 dalyje, kaip antai sklandaus mokėjimo sistemų veikimo skatinimas. Šiuo požiūriu laikoma, kad Eurosistemai priklausančios ir jos eksploatuojamos finansų rinkos infrastruktūros, tokios kaip TARGET2 ir TARGET2-Securities patenka į Tarybos siūlomą centrinių bankų neįtraukimą į pasiūlytos direktyvos taikymo sritį.

2. **ECBS ir Eurosistemos priežiūros kompetencija**

2.1 Greta pagrindinio ECBS tikslo – palaikyti kainų stabilumą, ir vadovaujantis Sutarties 127 straipsnio 2 dalimi, vienas iš pagrindinių uždavinių, kurį turi vykdyti ECBS, yra sklandaus mokėjimo sistemų veikimo skatinimas ([9]). Vykdydami šį pagrindinį uždavinį ECB ir nacionaliniai centriniai bankai gali sudaryti sąlygas, o ECB gali priimti reglamentus, kad būtų užtikrintas tarpuskaitos ir mokėjimo sistemų veiksmingumas ir patikimumas Sąjungoje ir su kitomis šalimis ([10]). Vykdydamas šį priežiūros vaidmenį, ECB priėmė Europos Centrinio Banko reglamentą (ES) Nr. 795/2014 (ECB/2014/28) ([11]) (toliau – SSMS reglamentas), kuriuo CPSS-IOSCO Finansų rinkos infrastruktūrų principai ([12]) perkeliami į tiesiogiai taikytiną teisę. SSMS reglamentas įtvirtina reikalavimus tiek didelės vertės, tiek ir mažmeninėms sisteminės svarbos mokėjimo sistemoms, nepriklausomai nuo to, ar jos priklauso valstybės ar privačiam sektoriui. SSMS reglamento reikalavimai jau apima, be kita ko, operacinės rizikos valdymą ir kibernetinio atsparumo sistemos sukūrimą ([13]).

2.2 Greta sistemiškai svarbių mokėjimo sistemų Eurosistemos priežiūra apima ir ne sisteminės svarbos mokėjimo sistemas, elektroninio mokėjimo priemones, schemas ir susitarimus, taip pat kitas infrastruktūras ir ypatingos svarbos paslaugų teikėjus, kaip nurodyta Eurosistemos priežiūros politikos pagrinduose ([14]). Mokėjimo sistemos ir kiti susitarimai, kuriems taikoma Eurosistemos priežiūra, nėra aiškiai įtraukti į pasiūlytos direktyvos taikymo sritį ([15]). Taip pat, atsižvelgiant į tai, kad pasiūlyta direktyva yra būtino suderinimo priemonė ([16]), valstybių narių priimti įgyvendinimo teisės aktai galiausiai gali dubliuotis su Eurosistemos priežiūros kompetencija. Siekiant to išvengti, pasiūlytos direktyvos konstatuojamosiose dalyse turėtų būti aiškiai pripažinta ECBS kompetencija pagal Sutartį ir ECBS statutą, taip pat Eurosistemos kompetencija pagal SSMS reglamentą ir apskritai pagal Eurosistemos priežiūros politikos sistemą.

([7]) Pasiūlytos direktyvos 13 konstatuojamoji dalis.
([8]) Tarybos bendro požiūrio dėl pasiūlytos direktyvos 2 straipsnio 3a dalies pirmos pastraipos b punktas.
([9]) Sutarties 127 straipsnio 2 dalis, kaip atsispindi ECBS statuto 3 straipsnio 1 dalyje.
([10]) ECBS statuto 22 straipsnis.
([11]) 2014 m. liepos 3 d. Europos Centrinio Banko reglamentas (ES) Nr. 795/2014 dėl priežiūros reikalavimų sistemiškai svarbioms mokėjimo sistemoms (ECB/2014/28) (OL L 217, 2014 7 23, p. 16).
([12]) Žr. 2012 m. balandžio mėn. Tarptautinės vertybinių popierių komisijų organizacijos (IOSCO) Mokėjimo ir atsiskaitymo sistemų komiteto (CPSS) ir Techninio komiteto Finansų rinkos infrastruktūrų principus, paskelbtus Tarptautinių atsiskaitymų banko interneto svetainėje www.bis.org. D atsakomybėje nurodyta, kad „visi CPSS ir IOSCO nariai turėtų kuo plačiau taikyti principus atitinkamoms FRI savo jurisdikcijose, kiek tai leidžiama pagal jų jurisdikcijos teisinę sistemą“.
([13]) Reglamento (ES) Nr. 795/2014 (ECB/2014/28) 15 straipsnis.
([14]) Eurosistemos priežiūros politikos sistema, peržiūrėta redakcija (2016 m. liepos mėn.), paskelbta ECB interneto svetainėje www.ecb.europa.eu.
([15]) Pasiūlytos direktyvos 2 straipsnis ir pasiūlytos direktyvos I ir II priedai.
([16]) Pasiūlytos direktyvos 3 straipsnis.

3. **Trečiosios šalies keliama IRT rizika, didelio masto incidentų ir krizių valdymas, dalijimasis informacija ir nacionalinė kibernetinio saugumo strategija**

3.1 *Trečiosios šalies keliamos IRT rizikos valdymas*

3.1.1 Pasiūlyta direktyva kompetentingoms institucijoms suteikiami įgaliojimai, naudojantis savo vykdymo užtikrinimo įgaliojimais esminių subjektų atžvilgiu, priimti privalomus nurodymus arba įsakymą, kuriuo reikalaujama, kad tie subjektai pašalintų nustatytus trūkumus arba šioje direktyvoje nustatytų pareigų pažeidimus ([17]); Be to, pagal DORA paskirta atsakingoji priežiūros institucija gali teikti rekomendacijas ypatingos svarbos IRT paslaugas teikiančioms trečiosioms šalims, kaip valdyti galimą sisteminę riziką, susijusią su užsakomosiomis paslaugomis ir IRT trečiųjų šalių koncentracija ([18]).

3.1.2 Atsižvelgdamas į tai, kad esminis subjektas pagal pasiūlytą direktyvą taip pat gali būti paskirtas ypatingos svarbos IRT paslaugas teikiančia trečiąja šalimi pagal DORA, ECB pakartoja ([19]), kad reikėtų vengti teikti prieštaringas rekomendacijas ir privalomus nurodymus. Šiuo atžvilgiu ECB palankiai vertina Tarybos bendrą požiūrį į pasiūlytą direktyvą. Pagal šį požiūrį kompetentingos institucijos informuoja pagal DORA įsteigtą priežiūros forumą, kai jos naudojasi priežiūros ir vykdymo užtikrinimo įgaliojimais, susijusiais su esminiu subjektu, pagal DORA paskirtu ypatingos svarbos IRT paslaugas teikiančia trečiąja šalimi ([20]).

3.2 *Didelio masto incidentų ir krizių valdymas*

3.2.1 Pagal pasiūlytą direktyvą ([21]) valstybės narės privalo paskirti vieną arba daugiau kompetentingų institucijų, kurios atsako už didelio masto incidentų ir krizių valdymą. Kaip paaiškinta pasiūlytos direktyvos konstatuojamosiose dalyse, didelio masto incidentas turėtų reikšti incidentą, kuris turi reikšmingą poveikį ne mažiau kaip dviem valstybėms narėms arba į kurio sukeltą sutrikimą valstybė narė nepajėgia reaguoti. Didelio masto incidentai gali stiprėti ir virsti plataus masto krizėmis, dėl kurių vidaus rinka negali tinkamai veikti ([22]).

3.2.2 Nors pagal DORA paskirtos kompetentingos institucijos tebėra atsakingos už finansų sektoriaus subjektų kibernetinio saugumo incidentų valdymą, bendradarbiavimas su pagal pasiūlytą direktyvą įsteigtomis struktūromis ir institucijomis bus labai svarbus siekiant užtikrinti koordinuotą atsaką visoje Sąjungoje. Šiuo tikslu ECB palankiai vertintų pagal DORA paskirtų kompetentingų institucijų, įskaitant ECB, dalyvavimą Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas (EU-CyCLONe) ([23]), kai didelio masto kibernetinio saugumo incidentai ir krizės daro poveikį finansų sektoriui.

3.3 *Dalijimasis informacija*

3.3.1 Kaip nurodyta pirmiau, ECB tvirtai remia pagal DORA paskirtų kompetentingų institucijų bendradarbiavimą su struktūromis ir institucijomis, įsteigtomis pagal pasiūlytą direktyvą. Visų pirma, valdžios institucijoms dalijantis informacija gali būti sudarytos sąlygos tarpsektoriniam mokymuisi, prisidedama prie kibernetinių išpuolių prevencijos ir veiksmingo valdymo ir skatinamas nuoseklus su IRT susijusios rizikos vertinimas visoje Sąjungoje. Vis dėlto ECB pabrėžia, kad informacija turėtų būti dalinamasi tais atvejais, kai yra aiškiai nustatyti klasifikavimo ir dalijimosi informacija mechanizmai, kartu taikant pakankamas konfidencialumo užtikrinimo priemones ([24]). ECB palankiai vertina Tarybos bendrą požiūrį dėl pasiūlytos direktyvos, kuriame siūloma institucijoms reguliariai keistis

([17]) Pasiūlytos direktyvos 29 straipsnio 4 dalies b punktas.
([18]) DORA 31 straipsnis.
([19]) Žr. Nuomonės CON/2021/20 1.2 dalį.
([20]) Tarybos bendro požiūrio dėl pasiūlytos direktyvos 29 straipsnio 10 dalis.
([21]) Pasiūlytos direktyvos 7 straipsnio 1 dalis.
([22]) Pasiūlytos direktyvos 27 konstatuojamoji dalis.
([23]) Pasiūlytos direktyvos 14 straipsnis.
([24]) Žr. Nuomonės CON/2021/20 1.5 dalį.

atitinkama informacija ([25]), sudaryti bendradarbiavimo susitarimus, kuriuose būtų nustatytas keitimosi informacija mechanizmas ([26]), ir automatiškai bei tiesiogiai perduoti pranešimus apie incidentus ([27]). Šiuo atžvilgiu turėtų būti užtikrinta, kad informacija, kuri yra konfidenciali pagal DORA profesinės paslapties nuostatas ([28]) arba atitinkamus konkretiems sektoriams skirtus teisės aktus ([29]), būtų galima keistis su pasiūlytoje direktyvoje nurodytomis kompetentingomis institucijomis tik tais atvejais, kai toks keitimasis būtinas, kad kompetentingos institucijos galėtų taikyti pasiūlytos direktyvos nuostatas ([30]).

3.4 *Nacionalinė kibernetinio saugumo strategija*

3.4.1 Pagal pasiūlytą direktyvą reikalaujama, kad valstybės narės priimtų nacionalines kibernetinio saugumo strategijas, kuriose būtų apibrėžti strateginiai tikslai ir tinkamos politikos bei reguliavimo priemonės, kad būtų pasiektas ir išlaikytas aukštas kibernetinio saugumo lygis ([31]). Kaip paaaiškinta pasiūlytos direktyvos konstatuojamosiose dalyse, valstybės narės į savo kibernetinio saugumo strategijas turėtų ir toliau įtraukti finansų sektorių ([32]). Preliminariai, įgyvendindamos savo nacionalines kibernetinio saugumo strategijas, valstybės narės turėtų nustatyti politiką dėl kibernetinio saugumo klausimų IRT produktų ir paslaugų, kuriuos esminiai ir svarbūs subjektai naudoja teikdami savo paslaugas, tiekimo grandinėje. Kiek tai susiję su finansų sektoriumi, nacionalinės kibernetinio saugumo strategijos turėtų derėti su reguliavimu, siūlomu pasiūlyme dėl reglamento dėl skaitmeninės veiklos atsparumo finansų sektoriuje (DORA). Šiuo atžvilgiu ECB mano, kad reikia papildomų patikslinimų siekiant užtikrinti, kad nacionalinės kibernetinio saugumo strategijos nuosekliai derėtų su konkretiems sektoriams skirtais teisės aktais.

Kai ECB rekomenduoja iš dalies keisti pasiūlytą direktyvą, konkretūs redagavimo pasiūlymai kartu su aiškinamuoju tekstu pateikiami techniniame darbo dokumente. Techninis darbo dokumentas anglų kalba paskelbtas „EUR-Lex“ interneto svetainėje.

Priimta Frankfurte prie Maino 2022 m. balandžio 11 d.

ECB Pirmininkė
Christine LAGARDE

([25]) Tarybos bendro požiūrio dėl pasiūlytos direktyvos 11 straipsnio 5 dalis.
([26]) Tarybos bendro požiūrio dėl pasiūlytos direktyvos 23a konstatuojamoji dalis.
([27]) Tarybos bendro požiūrio dėl pasiūlytos direktyvos 13 konstatuojamoji dalis.
([28]) DORA 49 straipsnis.
([29]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyvos 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų priežiūros, kuria iš dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB (OJ L 176, 27.6.2013, p. 338) 53-62 straipsniai.
([30]) Pasiūlytos direktyvos 2 straipsnio 5 dalis ir 11 straipsnio 4 dalis.
([31]) Pasiūlytos direktyvos 5 straipsnis.
([32]) Pasiūlytos direktyvos 13 konstatuojamoji dalis.