EIROPAS CENTRĀLĀS BANKAS ATZINUMS

(2022. gada 11. aprīlis)

atzinums par priekšlikumu Eiropas Parlamenta un Padomes direktīvai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Ievads un tiesiskais pamats

Eiropas Komisija 2020. gada 16. decembrī apstiprināja priekšlikumu Eiropas Parlamenta un Padomes direktīvai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148 ([1]) (turpmāk – "ierosinātā direktīva"). Eiropas Savienības Padome 2021. gada 3. decembrī vienojās par vispārīgo pieeju attiecībā uz ierosināto direktīvu ([2]). Eiropas Centrālās bankas (ECB) kompetence sniegt atzinumu pamatojas uz Līguma par Eiropas Savienības darbību 127. panta 4. punkta otro daļu, jo ierosinātā direktīva ietver noteikumus, kas ir ECB kompetences jomās, jo īpaši tādās kā maksājumu sistēmu raitas darbības veicināšana, palīdzība kompetentām iestādēm sekmīgi īstenot politiku, kas attiecas uz finanšu tirgus sistēmas stabilitāti, un ECB uzdevumi attiecībā uz kredītiestāžu prudenciālo uzraudzību saskaņā ar Līguma 127. panta 2. punkta ceturto ievilkumu, 127. panta 5. punktu un 127. panta 6. punktu. ECB Padome šo atzinumu pieņēmusi saskaņā ar Eiropas Centrālās bankas reglamenta 17.5. panta pirmo teikumu.

Vispārīgi apsvērumi

ECB stingri atbalsta ierosinātās direktīvas mērķus palielināt kibernoturības līmeni visās attiecīgajās nozarēs, samazināt neatbilstības iekšējā tirgū un uzlabot situācijas apzināšanos un kolektīvās spējas sagatavoties un reaģēt, nodrošinot efektīvu sadarbību Savienībā.

ECB atzīst, ka ir svarīgi saglabāt ciešu saikni starp ierosināto direktīvu un finanšu sektoru, kam arī turpmāk vajadzētu būt daļai no tīklu un informācijas sistēmu (TIS) ekosistēmas, lai veicinātu ar informācijas un komunikācijas tehnoloģijām (IKT) saistīto risku konsekventu novērtēšanu visā Savienībā un veicinātu efektīvu starpnozaru informācijas apmaiņu un sadarbību kiberdraudu gadījumos. Šajā nolūkā kompetentajām iestādēm saskaņā ar ierosināto Eiropas Parlamenta un Padomes regulu par finanšu sektora digitālās darbības noturību ([3]) (turpmāk – "DORA") vajadzētu būt iespējai piedalīties TIS sadarbības grupas stratēģiskajās politikas diskusijās un tehniskajā darbā, kā arī apmainīties ar informāciju un turpināt sadarbību ar vienotajiem kontaktpunktiem un nacionālajām datordrošības incidentu reaģēšanas vienībām, kas minētas ierosinātajā direktīvā ([4]).

1. Ierosinātās direktīvas darbības joma

1.1 ECB saprot, ka attiecībā uz finanšu sektora vienībām DORA tiks uzskatīta par nozarei specifisku tiesību aktu, ar ko ievieš tādas kiberdrošības riska pārvaldības un incidentu paziņošanas prasības, kuras ir vismaz līdzvērtīgas ierosinātajā direktīvā noteiktajām prasībām ([5]). Tāpēc ierosinātās direktīvas noteikumi, kas attiecas uz kiberdrošības riska pārvaldību, ziņošanas pienākumiem, informācijas apmaiņu un uzraudzību un izpildi, neattieksies uz finanšu vienībām, uz kurām attiecas DORA ([6]). Kā paskaidrots ierosinātās direktīvas apsvērumos, ierosinātās direktīvas vietā

([1]) COM(2020) 823 final.
([2]) Pieejams Padomes interneta vietnē www.consilium.europa.eu
([3]) COM(2020) 595 final.
([4]) Sk. 1.5. punktu Eiropas Centrālās bankas Atzinumā CON/2021/20 (2021. gada 4. jūnijs) par priekšlikumu Eiropas Parlamenta un Padomes regulai par finanšu sektora digitālās darbības noturību (OV C 343, 26.8.2021., 1. lpp.). Visi ECB atzinumi tiek publicēti EUR-Lex. DORA 17. panta 5. punkts un 42. pants; ierosinātās direktīvas 11. pants.
([5]) Ierosinātās direktīvas 2. panta 6. punkts.
([6]) Ierosinātās direktīvas 13) apsvērums un 2. panta 6. punkts.

būtu jāpiemēro DORA noteikumi, kas attiecas uz IKT riska pārvaldības pasākumiem, ar IKT saistītu incidentu pārvaldību un ziņošanu par incidentiem, digitālās darbības noturības testēšanu, informācijas apmaiņas kārtību un trešo personu risku ([7]).

1.2 ECB arī norāda, ka Padome savā vispārīgajā pieejā attiecībā uz ierosināto direktīvu ierosina grozījumu, lai no ierosinātās direktīvas piemērošanas jomas izslēgtu "vienības, kas veic darbības tiesu iestāžu, parlamentu vai centrālo banku jomā" ([8]). ECB saprot, ka ierosinātais grozījums attiektos uz visiem Eiropas Centrālo banku sistēmas (ECBS) pamatuzdevumiem un kompetencēm, kā noteikts Līguma 127. panta 2. punktā un Eiropas Centrālo banku sistēmas un Eiropas Centrālās bankas Statūtu (turpmāk – "ECBS Statūti") 3.1. pantā, piemēram, maksājumu sistēmu raitas darbības veicināšanu. Šajā sakarā tiek uzskatīts, ka uz Eurosistēmai piederošām un pārvaldītām finanšu tirgus infrastruktūrām, piemēram, TARGET2 un TARGET2 vērtspapīriem, attiecas Padomes ierosinājums izslēgt centrālās bankas no ierosinātās direktīvas piemērošanas jomas.

2. **ECBS un Eurosistēmas pārraudzības kompetence**

2.1 Līdztekus ECBS galvenajam mērķim saglabāt cenu stabilitāti un saskaņā ar Līguma 127. panta 2. punktu viens no ECBS pamatuzdevumiem ir veicināt maksājumu sistēmu raitu darbību ([9]). Pildot šo pamatuzdevumu, ECB un nacionālās centrālās bankas var dot iespējas, un ECB var izdot regulas, lai Savienībā un attiecībās ar citām valstīm nodrošinātu efektīvas un stabilas ieskaita un maksājumu sistēmas ([10]). Pildot pārraudzības funkcijas, ECB pieņēma Eiropas Centrālās bankas Regulu (ES) Nr. 795/2014 (ECB/2014/28) ([11]) (turpmāk – "SNMS regula"), ar kuru CPSS-IOSCO finanšu tirgus infrastruktūru principi ([12]) tiek pārvērsti tieši piemērojamos tiesību aktos. SNMS regulā noteiktas prasības gan liela apjoma, gan neliela apjoma maksājumu sistēmām, kurām ir sistēmiska nozīme, neatkarīgi no tā, vai tās ir publiskas vai privātas. SNMS regulas prasības cita starpā jau ietver operacionālā riska pārvaldību un kibernoturības sistēmas izveidi ([13]).

2.2 Papildus sistēmiski nozīmīgām maksājumu sistēmām Eurosistēmas pārraudzība aptver nesistēmiski svarīgas maksājumu sistēmas, elektroniskos maksājumu instrumentus, shēmas un mehānismus, kā arī citas infrastruktūras un kritiski svarīgu pakalpojumu sniedzējus, kā noteikts Eurosistēmas pārraudzības politikas regulējumā ([14]). Maksājumu sistēmas un citi mehānismi, uz kuriem attiecas Eurosistēmas pārraudzība, nav skaidri iekļauti ierosinātās direktīvas darbības jomā ([15]). Tajā pašā laikā, ņemot vērā, ka ierosinātā direktīva ir minimālās saskaņošanas instruments ([16]), iespējams, ka dalībvalstu pieņemtie īstenošanas tiesību akti varētu pārklāties ar Eurosistēmas pārraudzības kompetenci. Lai to novērstu, ierosinātās direktīvas apsvērumos būtu skaidri jāatzīst ECBS kompetence saskaņā ar Līgumu un ECBS Statūtiem, kā arī Eurosistēmas kompetence saskaņā ar SNMS regulu un Eurosistēmas pārraudzības politikas regulējumu kopumā.

([7]) Ierosinātās direktīvas 13) apsvērums.
([8]) Padomes vispārīgās pieejas attiecībā uz ierosināto direktīvu 2. panta 3.a punkta pirmās daļas b) apakšpunkts.
([9]) LESD 127. panta 2. punkts, kas atspoguļots ECBS Statūtu 3.1. pantā.
([10]) ECBS Statūtu 22. pants.
([11]) Eiropas Centrālās bankas Regula (ES)Nr. 795/2014 (2014. gada 3. jūlijs) par sistēmiski nozīmīgu maksājumu sistēmu pārraudzību (ECB/2014/28) (OV L 217, 23.7.2014., 16. lpp.).
([12]) Sk. Starptautiskās Vērtspapīru komisiju organizācijas (IOSCO) Maksājumu un norēķinu sistēmu komitejas (CPSS) un Starptautiskās Vērtspapīru komisiju organizācijas (IOSCO) Tehniskās komitejas Finanšu tirgus infrastruktūru principi (*Principles for Financial Market Infrastructures*), 2012. gada aprīlis, pieejami Starptautisko norēķinu bankas interneta vietnē www.bis.org. Tajos noteiktā D atbildība paredz, ka "no visiem CPSS un IOSCO locekļiem tiek sagaidīts, ka tie attiecīgajām to jurisdikcijā esošajām FTI principus piemēros pēc iespējas lielākajā mērā, ko pieļauj to jurisdikcijas tiesiskais regulējums".
([13]) Regulas (ES) Nr. 795/2014 (ECB/2014/28) 15. pants.
([14]) Eurosistēmas pārraudzības politikas regulējums (*Eurosystem oversight policy framework*), pārskatītā versija (2016. gada jūlijs), pieejama ECB interneta vietnē www.ecb.europa.eu.
([15]) Ierosinātās direktīvas 2. pants un ierosinātās direktīvas I un II pielikums.
([16]) Ierosinātās direktīvas 3. pants.

3. **Trešo personu IKT risks, plaša mēroga incidentu un krīžu pārvaldība, informācijas sniegšana un nacionālā kiberdrošības stratēģija**

3.1 *Trešo personu IKT riska pārvaldība*

3.1.1 Ierosinātā direktīva pilnvaro kompetentās iestādes, īstenojot savas izpildes pilnvaras attiecībā uz būtiskām vienībām, izdot saistošus norādījumus vai rīkojumus, pieprasot minētajām vienībām novērst konstatētos trūkumus vai ierosinātajā direktīvā noteikto pienākumu pārkāpumus ([17]). Tajā pašā laikā saskaņā ar DORA ieceltais "vadošais pārraugs" var sniegt ieteikumus kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, lai pārvaldītu iespējamos sistēmiskos riskus, ko rada ārpakalpojumu prakse un trešo personu koncentrācija IKT jomā ([18]).

3.1.2 Ņemot vērā to, ka būtisku vienību saskaņā ar ierosināto direktīvu var izraudzīties arī par kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, saskaņā ar DORA, ECB atkārtoti uzsver ([19]), ka būtu jāizvairās no pretrunīgu ieteikumu un saistošo norādījumu sniegšanas. Šajā sakarā ECB atzinīgi vērtē Padomes vispārīgo pieeju attiecībā uz ierosināto direktīvu. Saskaņā ar šo pieeju kompetentajām iestādēm jāinformē saskaņā ar DORA izveidotais "Pārraudzības forums" gadījumos, kuros tās īsteno savas uzraudzības un izpildes pilnvaras attiecībā uz būtisku vienību, kura saskaņā ar DORA izraudzīta kā kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus ([20]).

3.2 *Plaša mēroga incidentu un krīžu pārvaldība*

3.2.1 Saskaņā ar ierosināto direktīvu ([21]) dalībvalstīm jāizraugās viena vai vairākas kompetentās iestādes, kas ir atbildīgas par plaša mēroga incidentu un krīžu pārvaldību. Kā paskaidrots ierosinātās direktīvas apsvērumos, plaša mēroga incidentam vajadzētu nozīmēt incidentu, kam ir būtiska ietekme uz vismaz divām dalībvalstīm vai kura izraisītie darbības traucējumi pārsniedz dalībvalsts spēju uz to reaģēt. Plaša mēroga incidenti var kļūt par pilntiesīgām krīzēm, kas traucē iekšējā tirgus pienācīgu darbību ([22]).

3.2.2 Lai gan saskaņā ar DORA izraudzītās kompetentās iestādes joprojām ir atbildīgas par tādu kiberdrošības incidentu pārvaldību, kas attiecas uz finanšu vienībām, sadarbībai ar struktūrām un iestādēm, kas izveidotas saskaņā ar ierosināto direktīvu, būs izšķiroša nozīme, lai nodrošinātu koordinētu reaģēšanu visā Savienībā. Šajā nolūkā ECB atzinīgi vērtētu saskaņā ar DORA izraudzīto kompetento iestāžu, t. sk. ECB, dalību Eiropas Kiberkrīžu sadarbības organizāciju tīklā (EU-CyCLONe) ([23]) gadījumos, kuros liela mēroga kiberdrošības incidenti un krīzes skar finanšu sektoru.

3.3 *Informācijas sniegšana*

3.3.1 Kā norādīts iepriekš, ECB stingri atbalsta saskaņā ar DORA izraudzīto kompetento iestāžu sadarbību ar struktūrām un iestādēm, kas izveidotas saskaņā ar ierosināto direktīvu. Jo īpaši informācijas apmaiņa starp iestādēm var veicināt starpnozaru apmācību, palīdzēt novērst un efektīvi pārvaldīt kiberuzbrukumus un veicināt ar IKT saistīto risku konsekventu novērtēšanu visā Savienībā. Tomēr ECB uzsver, ka informācijas sniegšanai būtu jānotiek, pastāvot skaidri noteiktiem klasifikācijas un informācijas sniegšanas mehānismiem, ko papildina atbilstīgi aizsardzības pasākumi konfidencialitātes nodrošināšanai ([24]) ECB atzinīgi vērtē Padomes vispārīgo pieeju attiecībā uz ierosināto

([17]) Ierosinātās direktīvas 29. panta 4. punkta b) apakšpunkts.
([18]) DORA 31. pants.
([19]) Sk. Atzinuma CON/2021/20 1.2. punktu.
([20]) Padomes vispārīgās pieejas attiecībā uz ierosināto direktīvu 29. panta 10. punkts.
([21]) Ierosinātās direktīvas 7. panta 1. punkts.
([22]) Ierosinātās direktīvas 27) apsvērums.
([23]) Ierosinātās direktīvas 14. pants.
([24]) Sk. Atzinuma CON/2021/20 1.5. punktu.

direktīvu, kurā ierosināta regulāra attiecīgās informācijas apmaiņa starp iestādēm ([25]),sadarbības mehānismu izveide, nosakot informācijas sniegšanas mehānismu ([26]), un automātiska un tieša incidentu paziņojumu nosūtīšana ([27]). Šajā sakarā būtu jānodrošina, ka ar informāciju, kas ir konfidenciāla saskaņā ar DORA ([28]) paredzētajiem noteikumiem par dienesta noslēpumu vai attiecīgajiem nozaru tiesību aktiem ([29]), ar ierosinātajā direktīvā minētajām kompetentajām iestādēm var apmainīties tikai tad, ja šāda apmaiņa ir vajadzīga, lai kompetentās iestādes varētu piemērot ierosinātās direktīvas noteikumus ([30]).

3.4 *Nacionālā kiberdrošības stratēģija*

3.4.1 Saskaņā ar ierosināto direktīvu dalībvalstīm jāpieņem nacionālās kiberdrošības stratēģijas, lai noteiktu stratēģiskos mērķus un piemērotus politikas un regulatīvos pasākumus nolūkā sasniegt un uzturēt augstu kiberdrošības līmeni ([31]). Kā paskaidrots ierosinātās direktīvas apsvērumos, dalībvalstīm būtu jāturpina finanšu sektoru iekļaut savās attiecīgajās kiberdrošības stratēģijās ([32]). Indikatīvi, savas nacionālās kiberdrošības stratēģijas ietvaros dalībvalstīm būtu jāpieņem politikas nostādnes, kas attiecas uz kiberdrošību IKT produktu un pakalpojumu piegādes ķēdē, ko vienības izmanto savu pakalpojumu sniegšanai. Ciktāl tas attiecas uz finanšu sektoru, nacionālajām kiberdrošības stratēģijām vajadzētu būt saskaņotām ar no DORA izrietošo tiesisko regulējumu. Šajā sakarā ECB uzskata, ka vajadzīgi papildu precizējumi, lai nodrošinātu, ka nacionālās kiberdrošības stratēģijas atbilst nozaru tiesību aktiem.

Gadījumā, kuros ECB iesaka grozīt ierosināto direktīvu, konkrētais redakcionālais priekšlikums ir izklāstīts atsevišķā tehniskā darba dokumentā, kuram pievienots attiecīgs paskaidrojuma teksts. Tehniskais darba dokuments angļu valodā ir pieejams *EUR-Lex*.

Frankfurtē pie Mainas, 2022. gada 11. aprīlī

ECB prezidente
Christine LAGARDE

([25]) Padomes vispārīgās pieejas attiecībā uz ierosināto direktīvu 11. panta 5. punkts.
([26]) Padomes vispārīgās pieejas attiecībā uz ierosināto direktīvu 23.a) apsvērums.
([27]) Padomes vispārīgās pieejas attiecībā uz ierosināto direktīvu 13) apsvērums.
([28]) DORA 49. pants.
([29]) 53.–62. pants Eiropas Parlamenta un Padomes Direktīvā 2013/36/ES (2013. gada 26. jūnijs) par piekļuvi kredītiestāžu darbībai un kredītiestāžu prudenciālo uzraudzību, ar ko groza Direktīvu 2002/87/EK un atceļ Direktīvas 2006/48/EK un 2006/49/EK (OV L 176, 27.6.2013., 338. lpp.).
([30]) Ierosinātās direktīvas 2. panta 5. punkts un 11. panta 4. punkts.
([31]) Ierosinātās direktīvas 5. pants.
([32]) Ierosinātās direktīvas 13) apsvērums.