MIŠLJENJE EUROPSKE SREDIŠNJE BANKE

od 11. travnja 2022.

o Prijedlogu direktive Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Uvod i pravna osnova

Europska komisija donijela je 16. prosinca 2020. Prijedlog direktive Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148 ([1]) (dalje u tekstu: „predložena direktiva"). Vijeće Europske unije 3. prosinca 2021. utvrdilo je svoj opći stav o predloženoj direktivi ([2]). Nadležnost Europske središnje banke (ESB) za davanje mišljenja temelji se na drugom podstavku članka 127. stavka 4. Ugovora o funkcioniranju Europske unije, s obzirom na to da predložena direktiva sadrži odredbe iz područja nadležnosti ESB-a, a posebno promicanja nesmetanog funkcioniranja platnih sustava, doprinosa nesmetanom vođenju politika koje provode nadležna tijela u vezi sa stabilnošću sustava financijskog tržišta te zadaća ESB-a u vezi s bonitetnim nadzorom kreditnih institucija u skladu s četvrtom alinejom članka 127. stavka 2. te člankom 127. stavcima 5. i 6. Ugovora. Upravno vijeće donijelo je ovo Mišljenje u skladu s prvom rečenicom članka 17. stavka 5. Poslovnika Europske središnje banke.

Opće napomene

ESB snažno podupire ciljeve predložene direktive u pogledu povećanja razine kiberotpornosti u svim relevantnim sektorima, smanjenja nedosljednosti na unutarnjem tržištu i poboljšanja razine informiranosti o stanju i kolektivne sposobnosti za pripremu i odgovor osiguravanjem učinkovite suradnje u Uniji.

ESB prepoznaje važnost održavanja snažnih veza između predložene direktive i financijskog sektora, koje bi trebale ostati dio ekosustava mrežnih i informacijskih sustava (NIS) radi promicanja dosljedne procjene rizika povezanih s informacijskom i komunikacijskom tehnologijom (IKT) širom Unije te poticanja učinkovite međusektorske razmjene informacija i suradnje u rješavanju kiberprijetnji. U tu bi svrhu nadležna tijela na temelju predložene uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor ([3]) (dalje u tekstu „DORA") trebala moći sudjelovati u raspravama o strateškim politikama i tehničkom radu Skupine za suradnju u području mrežne i informacijske sigurnosti te razmjenjivati informacije i dalje surađivati s jedinstvenim kontaktnim točkama i nacionalnim timovima za odgovor na računalne sigurnosne incidente iz predložene direktive ([4]).

1. Područje primjene predložene direktive

1.1 ESB razumije da će se, kad je riječ o subjektima financijskog sektora, DORA smatrati sektorskim zakonodavstvom kojim se uvode zahtjevi za upravljanje kibersigurnosnim rizicima i izvješćivanje o incidentima koji su po učinku barem istovjetni onima utvrđenima u predloženoj direktivi ([5]). Stoga se odredbe predložene direktive koje se odnose na upravljanje kibersigurnosnim rizicima, obveze izvješćivanja, razmjenu informacija te nadzor i provedbu neće primjenjivati na financijske subjekte obuhvaćene DORA-om ([6]). Kako je objašnjeno u uvodnim izjavama predložene direktive, odredbe DORA-e koje se odnose na mjere za upravljanje rizicima u području IKT-a, upravljanje IKT

([1]) COM(2020) 823 konačno.
([2]) Dostupno na mrežnim stranicama Vijeća www.consilium.europa.eu.
([3]) COM(2020) 595 konačno.
([4]) Vidi stavak 1.5 Mišljenja CON/2021/20 Europske središnje banke od 4. lipnja 2021. o Prijedlogu uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor (SL C 343, 26.8.2021., str. 1.). Sva mišljenja ESB-a objavljuju su na EUR-Lexu. Članak 17. stavak 5. i članak 42. DORA-e; članak 11. predložene direktive.
([5]) Članak 2. stavak 6. predložene direktive.
([6]) Uvodna izjava 13. i članak 2. stavak 6. predložene direktive.

incidentima i izvješćivanje o incidentima, testiranje digitalne operativne otpornosti, mehanizme razmjene informacija i IKT rizik treće strane trebale bi se primjenjivati umjesto onih iz predložene direktive ([7]).

1.2 ESB također napominje da Vijeće, u svom općem stavu o predloženoj direktivi, predlaže izmjenu kojom se „subjekti koji obavljaju aktivnosti u području pravosuđa, parlamenata ili središnjih banaka" ([8]) isključuju iz primjene predložene direktive. ESB razumije da bi se predložena izmjena proširila na sve osnovne zadaće i nadležnosti Europskog sustava središnjih banaka (ESSB), kako je utvrđeno u članku 127. stavku 2. Ugovora i članku 3. stavku 1. Statuta Europskog sustava središnjih banaka i Europske središnje banke (dalje u tekstu „Statut ESSB-a"), kao što je promicanje neometanog funkcioniranja platnih sustava. U tom pogledu smatra se da su infrastrukture financijskog tržišta koje su u vlasništvu Eurosustava i kojima on upravlja, kao što su sustav TARGET2 i platforma TARGET2-Securities, obuhvaćene predloženim isključenjem središnjih banaka od primjene predložene direktive koje je predložilo Vijeće.

2. **Nadzorne nadležnosti ESSB-a i Eurosustava**

2.1 Uz primarni cilj ESSB-a, a to je održavanje stabilnosti cijena, i u skladu s člankom 127. stavkom 2. Ugovora, jedna od osnovnih zadaća koju ESSB treba izvršavati jest promicanje neometanog funkcioniranja platnih sustava ([9]). U izvršavanju ove osnovne zadaće, ESB i nacionalne središnje banke mogu stvoriti mogućnosti, a ESB može donositi propise radi osiguranja učinkovitih i pouzdanih sustava poravnanja i platnih sustava u Uniji i s drugim zemljama ([10]). U izvršavanju svoje nadzorne uloge ESB je donio Uredbu Europske središnje banke (EU) br. 795/2014 (ESB/2014/28) ([11]) (dalje u tekstu „Uredba o SIPS-u") kojom se načela CPSS-a i IOSCO-a za infrastrukture financijskih tržišta ([12]) prenose u izravno primjenjivo pravo. Uredbom o SIPS-u utvrđuju se zahtjevi za sustave velikih plaćanja i sustave plaćanja malih vrijednosti od sistemske važnosti, bez obzira na to jesu li u javnom ili privatnom vlasništvu. Zahtjevi iz Uredbe o SIPS-u već uključuju, među ostalim, upravljanje operativnim rizicima i uspostavu okvira za kiberotpornost ([13]).

2.2 Osim sistemski važnih platnih sustava, nadzor Eurosustava obuhvaća platne sustave koji nisu sistemski važni, elektroničke instrumente plaćanja, sheme i aranžmane te druge infrastrukture i pružatelje ključnih usluga, kako je utvrđeno u okviru nadzorne politike Eurosustava ([14]). Platni sustavi i drugi aranžmani koji podliježu nadzoru Eurosustava nisu izričito uključeni u područje primjene predložene direktive ([15]). Istodobno, s obzirom na to da je predložena direktiva instrument za minimalno usklađivanje ([16]), provedbeni propisi koje su donijele države članice u konačnici bi se mogli preklapati s nadzornim ovlastima Eurosustava. Kako bi se to izbjeglo, u uvodnim izjavama predložene direktive trebalo bi izričito navesti nadležnosti ESSB-a na temelju Ugovora i Statuta ESSB-a te nadležnosti Eurosustava na temelju Uredbe o SIPS-u i općenito na temelju okvira nadzorne politike Eurosustava.

([7]) Uvodna izjava 13. predložene direktive.
([8]) Članak 2. stavak 3.a prvi podstavak točka (b) općeg stava Vijeća o predloženoj direktivi.
([9]) Članak 127. stavak 2. UFEU-a, kako je naveden u članku 3. stavku 1. Statuta ESSB-a.
([10]) Članak 22. Statuta ESSB-a.
([11]) Uredba Europske središnje banke (EU) br. 795/2014 od 3. srpnja 2014. o nadzornim zahtjevima za sistemski važne platne sustave (ESB/2014/28) (SL L 217, 23.7.2014., str. 16.).
([12]) Vidi Odbor za platne sustave i sustave namire (CPSS) i Tehnički odbor Međunarodne organizacije komisija za vrijednosne papire (IOSCO), Načela za infrastrukture financijskog tržišta, travanj 2012., dostupno na mrežnim stranicama Banke za međunarodne namire www.bis.org. U njegovoj se odgovornosti D navodi da se „od svih članova CPSS-a i IOSCO-a očekuje da primjenjuju načela na relevantne infrastrukture financijskog tržišta u svojim jurisdikcijama u najvećoj mogućoj mjeri dopuštenoj pravnim okvirom u njihovoj jurisdikciji".
([13]) Članak 15. Uredbe (EU) br. 795/2014 (ESB/2014/28).
([14]) Okvir nadzorne politike Eurosustava, revidirana inačica (srpanj 2016.), dostupno na mrežnim stranicama ESB-a www.ecb.europa.eu.
([15]) Članak 2. predložene direktive i prilozi I. i II. predloženoj direktivi.
([16]) Članak 3. predložene direktive.

3. **IKT rizik treće strane, upravljanje incidentima i krizama velikih razmjera, razmjena informacija i nacionalne strategije za kibersigurnost**

3.1 *Upravljanje IKT rizicima trećih strana*

3.1.1 Predloženom direktivom nadležna tijela ovlašćuju se da pri izvršavanju svojih provedbenih ovlasti u odnosu na ključne subjekte izdaju obvezujuće upute ili nalog kojim se od tih subjekata zahtijeva da uklone utvrđene nedostatke ili povrede obveza iz predložene direktive ([17]). Istodobno, „glavno nadzorno tijelo" imenovano u skladu s DORA-om može trećim stranama pružateljima ključnih IKT usluga uputiti preporuke za upravljanje potencijalnim sistemskim rizicima koji proizlaze iz praksi eksternalizacije i koncentracije IKT rizika treće strane ([18]).

3.1.2 S obzirom na to da bi ključni subjekt u skladu s predloženom direktivom mogao biti imenovan i trećom stranom pružateljem ključnih IKT usluga u skladu s DORA-om, ESB ponavlja ([19]) da bi trebalo izbjegavati izdavanje proturječnih preporuka i obvezujućih uputa. U tom pogledu ESB pozdravlja opći stav Vijeća o predloženoj direktivi. U skladu s tim pristupom nadležna tijela trebaju obavijestiti „Nadzorni forum", uspostavljen u skladu s DORA-om, kada izvršavaju svoje nadzorne i provedbene ovlasti u odnosu na ključni subjekt koji je imenovan kao treća strana pružatelj ključnih IKT usluga u skladu s DORA-om ([20]).

3.2 *Upravljanje incidentima i krizama velikih razmjera*

3.2.1 U skladu s predloženom direktivom ([21]), države članice moraju imenovati jedno ili više nadležnih tijela odgovornih za upravljanje incidentima i krizama velikih razmjera. Kako je objašnjeno u uvodnim izjavama predložene direktive, incident velikih razmjera trebao bi značiti incident sa znatnim učinkom na najmanje dvije države članice ili incident čiji poremećaj premašuje sposobnost države članice da na njega odgovori. Incidenti velikih razmjera mogu postati prave krize, kojima se narušava pravilno funkcioniranje unutarnjeg tržišta ([22]).

3.2.2 Iako su nadležna tijela imenovana u skladu s DORA-om i dalje odgovorna za upravljanje kiberincidentima koji se odnose na financijske subjekte, suradnja sa strukturama i tijelima uspostavljenima u skladu s predloženom direktivom bit će ključna za osiguravanje koordiniranog odgovora u cijeloj Uniji. U tu bi svrhu ESB pozdravio sudjelovanje nadležnih tijela imenovanih u skladu s DORA-om, uključujući ESB, u Europskoj mreži organizacija za vezu za kiberkrize (EU-CyCLONe)(EU-CyCLONe) ([23]) kada kiberincidenti i kiberkrize velikih razmjera utječu na financijski sektor.

3.3 *Razmjena informacija*

3.3.1 Kako je prethodno navedeno, ESB snažno podupire suradnju između nadležnih tijela imenovanih u skladu s DORA-om sa strukturama i tijelima uspostavljenima u skladu s predloženom direktivom. Konkretno, razmjenom informacija među tijelima može se omogućiti međusektorsko učenje, doprinijeti sprečavanju kibernapada i djelotvornom upravljanju njima te promicati dosljedna procjena rizika povezanih s IKT-om širom Unije. Međutim, ESB naglašava da bi se razmjena informacija trebala odvijati tamo gdje postoje jasno utvrđeni mehanizmi klasifikacije i razmjene informacija, zajedno s odgovarajućim zaštitnim mjerama kako bi se osigurala povjerljivost ([24]). ESB pozdravlja opći stav Vijeća o predloženoj direktivi kojim se predlaže redovita razmjena

([17]) Članak 29. stavak 4. točka (b) predložene direktive.
([18]) Članak 31. DORA-e.
([19]) Vidi stavak 1.2 Mišljenja CON/2021/20.
([20]) Članak 29. stavak 10. općeg stava Vijeća o predloženoj direktivi.
([21]) Članak 7. stavak 1. predložene direktive.
([22]) Uvodna izjava 27. predložene direktive.
([23]) Članak 14. predložene direktive.
([24]) Vidi stavak 1.5 Mišljenja CON/2021/20.

relevantnih informacija među tijelima ([25]), uspostava sporazuma o suradnji kojima se utvrđuje mehanizam za razmjenu informacija ([26]) te automatsko i izravno prosljeđivanje obavijesti o incidentima ([27]). U tom bi pogledu trebalo osigurati da se informacije koje su povjerljive u skladu s odredbama o čuvanju poslovne tajne u skladu s DORA-om ([28]) ili relevantnim sektorskim zakonodavstvom ([29]) mogu razmjenjivati s nadležnim tijelima iz predložene direktive samo ako je ta razmjena potrebna nadležnim tijelima za primjenu odredbi predložene direktive ([30]).

3.4 *Nacionalna strategija za kibersigurnost*

3.4.1 U skladu s predloženom direktivom, države članice moraju donijeti nacionalne strategije za kibersigurnost kako bi definirale strateške ciljeve i odgovarajuće mjere politike i regulatorne mjere u cilju postizanja i održavanja visoke razine kibersigurnosti ([31]). Kako je pojašnjeno u uvodnim izjavama predložene direktive, države članice trebale bi nastaviti uključivati financijski sektor u svoje strategije za kibersigurnost ([32]). Indikativno, u okviru svojih nacionalnih strategija za kibersigurnost države članice trebale bi donijeti politike za kibersigurnost u lancu opskrbe IKT proizvodima i uslugama koje subjekti upotrebljavaju za pružanje svojih usluga. Kad je riječ o financijskom sektoru, nacionalne strategije za kibersigurnost trebale bi biti usklađene s regulatornim okvirom koji proizlazi iz DORA-e. U tom pogledu ESB smatra da su potrebna dodatna pojašnjenja kako bi se osigurala usklađenost nacionalnih strategija za kibersigurnost sa sektorskim zakonodavstvom.

Na mjestima gdje ESB preporučuje izmjenu predložene direktive, poseban prijedlog nacrta naveden je u posebnom tehničkom radnom dokumentu uz obrazloženje dano u tu svrhu. Tehnički radni dokument dostupan je na engleskom jeziku na EUR-Lexu.

Sastavljeno u Frankfurtu na Majni 11. travnja 2022.

Predsjednica ESB-a
Christine LAGARDE

([25]) Članak 11. stavak 5. općeg stava Vijeća o predloženoj direktivi.
([26]) Uvodna izjava 23.a općeg stava Vijeća o predloženoj direktivi.
([27]) Uvodna izjava 13. općeg stava Vijeća o predloženoj direktivi.
([28]) Članak 49. DORA-e.
([29]) Članci od 53 do 62. Direktive 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ (SL L 176, 27.6.2013., str. 338.).
([30]) Članak 2. stavak 5 i članak 11. stavak 4. predložene direktive.
([31]) Članak 5. predložene direktive.
([32]) Uvodna izjava 13. predložene direktive.