MNENJE EVROPSKE CENTRALNE BANKE

z dne 11. aprila 2022

o predlogu direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Uvod in pravna podlaga

Evropska komisija je 16. decembra 2020 sprejela predlog direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148 ([1]) (v nadaljnjem besedilu: predlagana direktiva). Svet Evropske unije se je 3. decembra 2021 dogovoril o splošnem pristopu glede predlagane direktive ([2]). Pristojnost Evropske centralne banke (ECB), da poda mnenje, izhaja iz drugega pododstavka člena 127(4) Pogodbe o delovanju Evropske unije, saj predlagana direktiva vsebuje določbe, ki sodijo na področja iz njene pristojnosti, zlasti podpiranje nemotenega delovanja plačilnih sistemov, prispevanje k nemotenemu vodenju politik pristojnih organov glede stabilnosti finančnega sistema ter naloge ECB, ki se nanašajo na bonitetni nadzor kreditnih institucij, v skladu s četrto alineo člena 127(2), členom 127(5) in členom 127(6) Pogodbe. V skladu s prvim stavkom člena 17.5 Poslovnika Evropske centralne banke je to mnenje sprejel Svet ECB.

Splošne pripombe

ECB odločno podpira cilje predlagane direktive, da se zviša raven kibernetske odpornosti v vseh ustreznih sektorjih, zmanjšajo razlike na notranjem trgu ter izboljšata raven situacijskega zavedanja in skupna zmogljivost za pripravo in odzivanje z zagotavljanjem učinkovitega sodelovanja v Uniji.

ECB priznava pomen ohranjanja močnih povezav med predlagano direktivo in finančnim sektorjem, ki bi moral ostati del ekosistema omrežij in informacijskih sistemov, da se spodbuja skladno ocenjevanje tveganj, povezanih z informacijsko in komunikacijsko tehnologijo (IKT), v vsej Uniji ter učinkovita medsektorska izmenjava informacij in sodelovanje pri obravnavanju kibernetskih groženj. V ta namen bi moralo biti omogočeno, da pristojni organi v skladu s predlagano uredbo Evropskega parlamenta in Sveta o digitalni operativni odpornosti za finančni sektor ([3]) (v nadaljnjem besedilu: uredba DORA) sodelujejo v razpravah o strateških politikah in pri tehničnem delu skupine za sodelovanje na področju varnosti omrežij in informacij ter si izmenjujejo informacije in dodatno sodelujejo z enotnimi kontaktnimi točkami in nacionalnimi skupinami za odzivanje na incidente na področju računalniške varnosti iz predlagane direktive ([4]).

1. Področje uporabe predlagane direktive

1.1 ECB razume, da se bo v zvezi s subjekti finančnega sektorja uredba DORA obravnavala kot sektorska zakonodaja, ki uvaja zahteve glede upravljanja tveganj za kibernetsko varnost in priglasitve incidentov, ki so po učinku vsaj enakovredne zahtevam iz predlagane direktive ([5]). Zato se določbe predlagane direktive, ki se nanašajo na obvladovanje tveganj za kibernetsko varnost, obveznosti poročanja, izmenjavo informacij ter nadzor in izvrševanje, za finančne subjekte, zajete z uredbo DORA, ne bodo uporabljale ([6]). Kakor je pojasnjeno v uvodnih izjavah predlagane direktive, bi se morale namesto določb predlagane direktive uporabljati določbe uredbe DORA, ki se

([1]) COM(2020) 823 final.
([2]) Dostopno na spletni strani Sveta na naslovu www.consilium.europa.eu.
([3]) COM(2020) 595 final.
([4]) Glej odstavek 1.5 Mnenja CON/2021/20 Evropske centralne banke z dne 4. junija 2021 o predlogu uredbe Evropskega parlamenta in Sveta o digitalni operativni odpornosti za finančni sektor (UL C 343, 26.8.2021, str. 1). Vsa mnenja ECB so objavljena na spletni strani EUR-Lex. Člena 17(5) in 42 uredbe DORA; člen 11 predlagane direktive.
([5]) Člen 2(6) predlagane direktive.
([6]) Uvodna izjava 13 in člen 2(6) predlagane direktive.

nanašajo na ukrepe za obvladovanje tveganj na področju IKT, upravljanje incidentov, povezanih z IKT, in poročanje o incidentih, testiranje digitalne operativne odpornosti, dogovore o izmenjavi informacij in tveganje tretjih oseb na področju IKT ([7]).

1.2 ECB tudi ugotavlja, da Svet v svojem splošnem pristopu glede predlagane direktive predlaga spremembo, s katero bi iz uporabe predlagane direktive izključili „subjekte, ki izvajajo dejavnosti v sodstvu, parlamentih ali centralnih bankah“ ([8]). ECB razume, da bi predlagana sprememba zajemala vse temeljne naloge in pristojnosti Evropskega sistema centralnih bank (ESCB), kakor so določene v členu 127(2) Pogodbe in členu 3.1 Statuta Evropskega sistema centralnih bank in Evropske centralne banke (v nadaljnjem besedilu: Statut ESCB), kot je podpiranje nemotenega delovanja plačilnih sistemov. V tej zvezi se šteje, da so infrastrukture finančnega trga v lasti in upravljanju Eurosistema, kot sta TARGET2 in TARGET2-Securities, zajete v predlogu Sveta o izključitvi centralnih bank iz uporabe predlagane direktive.

2. **Pristojnosti ESCB in Eurosistema na področju pregleda**

2.1 Poleg poglavitnega cilja ESCB, da ohranja stabilnost cen, in v skladu s členom 127(2) Pogodbe je ena od temeljnih nalog ESCB podpirati nemoteno delovanje plačilnih sistemov ([9]). Pri izvajanju te temeljne naloge lahko ECB in nacionalne centralne banke ustvarijo možnosti in ECB lahko sprejme predpise za zagotovitev učinkovitih in zanesljivih klirinških in plačilnih sistemov znotraj Unije in z drugimi državami ([10]). ECB je pri opravljanju svoje pregledniške vloge sprejela Uredbo Evropske centralne banke (EU) št. 795/2014 (ECB/2014/28) ([11]) (v nadaljnjem besedilu: uredba o SPPS), ki prenaša načela CPSS-IOSCO za infrastrukture finančnega trga ([12]) v pravo, ki se neposredno uporablja. Uredba o SPPS določa zahteve za sistemsko pomembne sisteme za plačila velikih vrednosti in za plačila malih vrednosti, v javni ali zasebni lasti. Zahteve iz uredbe o SPPS med drugim že vključujejo upravljanje operativnega tveganja in vzpostavitev okvira za kibernetsko odpornost ([13]).

2.2 Eurosistemov pregled poleg sistemsko pomembnih plačilnih sistemov zajema tudi plačilne sisteme, ki niso sistemsko pomembni, elektronske plačilne instrumente, sheme in ureditve ter druge infrastrukture in ponudnike kritičnih storitev, kakor je določeno v okviru politike pregleda Eurosistema ([14]). Plačilni sistemi in druge ureditve, ki so predmet pregleda Eurosistema, niso izrecno vključeni v področje uporabe predlagane direktive ([15]). Glede na to, da je predlagana direktiva instrument za minimalno harmonizacijo ([16]), bi se lahko izvedbena zakonodaja, ki jo sprejmejo države članice, na koncu prekrivala s pristojnostjo Eurosistema za pregled. Da bi se temu izognili, bi bilo treba v uvodnih izjavah predlagane direktive izrecno priznati pristojnosti ESCB v skladu s Pogodbo in Statutom ESCB ter pristojnosti Eurosistema v skladu z uredbo o SPPS in na splošno v skladu z okvirom politike pregleda Eurosistema.

([7]) Uvodna izjava 13 predlagane direktive.
([8]) Člen 2(3a), prvi pododstavek, točka (b), splošnega pristopa Sveta glede predlagane direktive.
([9]) Člen 127(2) PDEU, ki se ponovi v členu 3.1 Statuta ESCB.
([10]) Člen 22 Statuta ESCB.
([11]) Uredba Evropske centralne banke (EU) št. 795/2014 z dne 3. julija 2014 o pregledniških zahtevah za sistemsko pomembne plačilne sisteme (ECB/2014/28) (UL L 217, 23.7.2014, str. 16).
([12]) Glej Odbor za plačilne in poravnalne sisteme (CPSS) ter tehnični odbor Mednarodnega združenja nadzornikov trga vrednostnih papirjev (IOSCO), *Principles for financial market infrastructures*, april 2012, dostopno na spletni strani Banke za mednarodne poravnave na naslovu www.bis.org. V odgovornosti D v navedenih načelih je navedeno, da „se od vseh članic CPSS in IOSCO pričakuje, da bodo načela uporabljale za ustrezne infrastrukture finančnega trga v svoji jurisdikciji v največji meri, ki jo omogoča pravni okvir v tej jurisdikciji“.
([13]) Člen 15 Uredbe (EU) št. 795/2014 (ECB/2014/28).
([14]) *Eurosystem oversight policy framework, revised version* (julij 2016), dostopno na spletni strani ECB na naslovu www.ecb.europa.eu.
([15]) Člen 2 predlagane direktive ter prilogi I in II k predlagani direktivi.
([16]) Člen 3 predlagane direktive.

3. **Tveganje tretjih oseb na področju IKT, upravljanje velikih incidentov in kriz, izmenjava informacij in nacionalna strategija za kibernetsko varnost**

3.1 *Upravljanje tveganja tretjih oseb na področju IKT*

3.1.1 Predlagana direktiva pooblašča pristojne organe, da pri izvajanju svojih izvršilnih pooblastil v zvezi z bistvenimi subjekti izdajo zavezujoča navodila ali odredbo, s katero od takih subjektov zahtevajo, da odpravijo ugotovljene pomanjkljivosti ali kršitve obveznosti iz predlagane direktive ([17]). Hkrati lahko „glavni nadzornik“, imenovan na podlagi uredbe DORA, na ključne tretje ponudnike storitev IKT naslovi priporočila za upravljanje možnih sistemskih tveganj, povezanih z oddajanjem del v zunanje izvajanje in koncentracijo odvisnosti od tretjih oseb na področju IKT ([18]).

3.1.2 Glede na to, da je lahko bistveni subjekt v skladu s predlagano direktivo imenovan tudi za ključnega tretjega ponudnika storitev IKT v skladu z uredbo DORA, ECB ponovno poudarja ([19]), da bi se bilo treba izogniti izdajanju nasprotujočih si priporočil in zavezujočih navodil. V tej zvezi ECB pozdravlja splošni pristop Sveta glede predlagane direktive. V skladu s tem pristopom morajo pristojni organi obvestiti „nadzorniški forum“, ustanovljen na podlagi uredbe DORA, kadar izvajajo svoja nadzorna in izvršilna pooblastila v zvezi z bistvenim subjektom, ki je v skladu z uredbo DORA imenovan za ključnega tretjega ponudnika storitev IKT ([20]).

3.2 *Upravljanje velikih incidentov in kriz*

3.2.1 V skladu s predlagano direktivo ([21]) morajo države članice imenovati enega ali več pristojnih organov, odgovornih za upravljanje velikih incidentov in kriz. Kakor je pojasnjeno v uvodnih izjavah predlagane direktive, bi moral velik incident pomeniti incident, ki ima velik vpliv na vsaj dve državi članici ali ki povzroči motnje, ki presegajo zmožnost države članice za odziv nanje. Veliki incidenti se lahko sprevržejo v popolno krizo, ki povzroči motnje pravilnega delovanja notranjega trga ([22]).

3.2.2 Pristojni organi, imenovani na podlagi uredbe DORA, sicer ostajajo odgovorni za upravljanje kibernetskih incidentov v zvezi s finančnimi subjekti, vendar bo sodelovanje s strukturami in organi, vzpostavljenimi v skladu s predlagano direktivo, ključno za zagotovitev usklajenega odziva v vsej Uniji. Zato bi ECB pozdravila to, da bi pristojni organi, imenovani na podlagi uredbe DORA, vključno z ECB, sodelovali v evropski organizacijski mreži za povezovanje v kibernetski krizi (EU-CyCLONe) ([23]), kadar veliki kibernetski incidenti in krize vplivajo na finančni sektor.

3.3 *Izmenjava informacij*

3.3.1 Kakor je navedeno zgoraj, ECB odločno podpira sodelovanje med pristojnimi organi, imenovanimi na podlagi uredbe DORA, s strukturami in organi, vzpostavljenimi v skladu s predlagano direktivo. Izmenjava informacij med organi lahko zlasti omogoči medsektorsko učenje, prispeva k preprečevanju in učinkovitemu upravljanju kibernetskih napadov ter spodbuja skladno ocenjevanje tveganj, povezanih z IKT, v vsej Uniji. Kljub temu ECB poudarja, da bi se morale informacije izmenjavati, kadar obstajajo jasno vzpostavljeni mehanizmi za razvrščanje in izmenjavo informacij v povezavi z ustreznimi zaščitnimi ukrepi za zagotovitev zaupnosti ([24]). ECB pozdravlja splošni pristop Sveta glede predlagane direktive, s katerim se predlaga redna izmenjava relevantnih informacij med

([17]) Člen 29(4), točka (b), predlagane direktive.
([18]) Člen 31 uredbe DORA.
([19]) Glej odstavek 1.2 Mnenja CON/2021/20.
([20]) Člen 29(10) splošnega pristopa Sveta glede predlagane direktive.
([21]) Člen 7(1) predlagane direktive.
([22]) Uvodna izjava 27 predlagane direktive.
([23]) Člen 14 predlagane direktive.
([24]) Glej odstavek 1.5 Mnenja CON/2021/20.

organi ([25]), sklenitev dogovorov o sodelovanju, ki bi določali mehanizem za izmenjavo informacij ([26]), ter samodejno in neposredno posredovanje priglasitev incidentov ([27]). V zvezi s tem bi bilo treba zagotoviti, da se informacije, ki so zaupne v skladu z določbami o poslovni skrivnosti iz uredbe DORA ([28]) ali ustrezne sektorske zakonodaje ([29]), lahko izmenjujejo s pristojnimi organi iz predlagane direktive le, če je ta izmenjava potrebna, da lahko pristojni organi uporabljajo določbe predlagane direktive ([30]).

3.4 *Nacionalna strategija za kibernetsko varnost*

3.4.1 V skladu s predlagano direktivo morajo države članice sprejeti nacionalne strategije za kibernetsko varnost, v katerih opredelijo strateške cilje ter ustrezne ukrepe politike in regulativne ukrepe za doseganje in ohranjanje visoke ravni kibernetske varnosti ([31]). Kakor je pojasnjeno v uvodnih izjavah predlagane direktive, bi morale države članice v svoje strategije za kibernetsko varnost še naprej vključevati finančni sektor ([32]). Države članice bi morale na primer kot del nacionalnih strategij za kibernetsko varnost sprejeti politike za obravnavanje kibernetske varnosti v dobavni verigi proizvodov in storitev IKT, ki jih subjekti uporabljajo za opravljanje svojih storitev. Kar zadeva finančni sektor, bi morale biti nacionalne strategije za kibernetsko varnost skladne z regulativnim okvirom, ki izhaja iz uredbe DORA. V zvezi s tem ECB meni, da so potrebna dodatna pojasnila, da se zagotovi skladnost nacionalnih strategij za kibernetsko varnost s sektorsko zakonodajo.

Kadar ECB priporoča, da se predlagana direktiva spremeni, je konkretni predlog spremembe besedila s pripadajočimi pojasnili naveden v ločenem tehničnem delovnem dokumentu. Tehnični delovni dokument je dostopen v angleščini na spletni strani EUR-Lex.

V Frankfurtu na Majni, 11. aprila 2022

Predsednica ECB
Christine LAGARDE

([25]) Člen 11(5) splošnega pristopa Sveta glede predlagane direktive.
([26]) Uvodna izjava 23a splošnega pristopa Sveta glede predlagane direktive.
([27]) Uvodna izjava 13 splošnega pristopa Sveta glede predlagane direktive.
([28]) Člen 49 uredbe DORA.
([29]) Členi 53 do 62 Direktive 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij, spremembi Direktive 2002/87/ES in razveljavitvi direktiv 2006/48/ES in 2006/49/ES (UL L 176, 27.6.2013, str. 338).
([30]) Člena 2(5) in 11(4) predlagane direktive.
([31]) Člen 5 predlagane direktive.
([32]) Uvodna izjava 13 predlagane direktive.