EVROPSKA CENTRALNA BANKA

EUROSISTEM

SL **ECB-PUBLIC**

MNENJE EVROPSKE CENTRALNE BANKE

z dne 8. novembra 2018

o določitvi bistvenih storitev in izvajalcev bistvenih storitev za potrebe varnosti omrežij in informacijskih sistemov

(CON/2018/47)

Uvod in pravna podlaga

Evropska centralna banka (ECB) je 5. oktobra 2018 prejela zahtevo Ministrstva za javno upravo Republike Slovenije za mnenje o predlogu uredbe o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev (v nadaljnjem besedilu: predlog uredbe).

Pristojnost ECB, da poda mnenje, izhaja iz členov 127(4) in 282(5) Pogodbe o delovanju Evropske unije ter iz tretje, pete in šeste alinee člena 2(1) Odločbe Sveta 98/415/ES[1], saj se predlog uredbe nanaša na Banko Slovenije, plačilne in poravnalne sisteme in pravila v zvezi s finančnimi institucijami, kolikor pomembno vplivajo na stabilnost finančnih institucij in trgov, ter na naloge, ki se nanašajo na bonitetni nadzor kreditnih institucij in so prenesene na ECB v skladu s členom 127(6) Pogodbe. V skladu s prvim stavkom člena 17.5 Poslovnika Evropske centralne banke je to mnenje sprejel Svet ECB.

1. Namen predloga uredbe

1.1 Pri predlogu uredbe gre za izvedbeno uredbo, ki jo mora sprejeti Vlada Republike Slovenije na podlagi Zakona o informacijski varnosti[2]. Z navedenim zakonom se je v slovensko zakonodajo prenesla Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta[3]. Zakon določa okvir, katerega cilj je zagotavljanje, da se sprejmejo ustrezni varnostni ukrepi na področju informacijskih sistemov za preprečitev kibernetskih incidentov, njihovo priglasitev in odziv nanje. Zakon o informacijski varnosti določa nacionalni skupini za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij in njune naloge ter vzpostavlja pristojni nacionalni organ za informacijsko varnost (v nadaljnjem besedilu: nacionalni organ za informacijsko varnost), ki deluje tudi kot enotna kontaktna točka za informacijsko varnost. Zakon ureja tudi pristojnosti in naloge nacionalnega organa za informacijsko varnost ter temu organu in njegovim inšpektorjem daje pooblastila in instrumente za nadzor nad izvajalci zadevnih storitev.

1.2 Zakon o informacijski varnosti se uporablja za naslednje izvajalce storitev: (i) izvajalce bistvenih storitev; (ii) ponudnike digitalnih storitev in (iii) organe državne uprave, ki upravljajo informacijske

1 Odločba Sveta 98/415/ES z dne 29. junija 1998 o posvetovanju nacionalnih organov z Evropsko centralno banko glede osnutkov pravnih predpisov (UL L 189, 3.7.1998, str. 42).

2 Zakon o informacijski varnosti (Uradni list RS, št. 30/18).

3 Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

sisteme oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti. Zakon predvideva, da bodo izvajalci bistvenih storitev subjekti, ki delujejo na področjih, ki so določena v navedenem zakonu in med drugim vključujejo bančništvo in infrastrukturo finančnega trga. Zakon pooblašča vlado, da določi posamezne izvajalce bistvenih storitev. Najprej pa mora vlada določiti podrobnejši seznam bistvenih storitev na zadevnih področjih in podrobnejšo metodologijo za določitev izvajalcev teh storitev[4]. Namen predloga uredbe je urediti ti dve vprašanji.

1.3 Kar zadeva podrobni seznam storitev, predlog uredbe določa posamezne storitve na podlagi standardne klasifikacije dejavnosti. Na področju bančništva predlog uredbe določa naslednje storitve[5]: (i) centralno bančništvo (delovanje v vlogi bančnika državnega sektorja, vključno glede podračunov za pokojninsko, zdravstveno in socialno zavarovanje); (ii) drugo denarno posredništvo (sprejemanje depozitov in dajanje kreditov s strani bank, hranilnic in kreditnih zadrug) ter (iii) druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade (dejavnost obdelave finančnih transakcij in dejavnost poravnav, vključno s transakcijami s kreditnimi karticami – plačilni promet). Na področju infrastrukture finančnega trga predlog uredbe določa naslednje storitve: (i) upravljanje finančnih trgov (poslovanje in nadzor finančnih trgov razen tistega, ki ga opravljajo državni organi: zbirna hramba vrednostnih papirjev, ugotavljanje in izpolnjevanje obveznosti iz poslov z vrednostnimi papirji ter vodenje centralnega registra imetnikov nematerializiranih vrednostnih papirjev) ter (ii) posredništvo pri trgovanju z vrednostnimi papirji (trgovanje z vrednostnimi papirji, s katerimi se trguje na mestu trgovanja v skladu z zakonom, ki ureja trg finančnih instrumentov, in s tem povezane dejavnosti, borzno posredništvo vrednostnih papirjev).

1.4 Predlog uredbe izrecno določa, da (i) se ne uporablja za storitve, katerih zagotavljanje je odvisno od informacijskih sistemov, ki jih upravlja Evropski sistem centralnih bank (ESCB); (ii) se ne uporablja za storitve, katerih zagotavljanje je odvisno od informacijskih sistemov v upravljanju Banke Slovenije, ki jih nadzira ESCB, ter (iii) ne posega v nadzor informacijskih sistemov s področja pristojnosti Banke Slovenije ali ESCB, ki ga urejajo predpisi Evropske unije in na njihovi podlagi sprejeti predpisi Republike Slovenije[6]. Predlog uredbe tudi določa, da je pri določitvi posameznih izvajalcev bistvenih storitev s področja bančništva potrebno predhodno soglasje Banke Slovenije, če je zagotavljanje teh storitev odvisno od informacijskih sistemov Banke Slovenije, ki niso informacijski sistemi iz zgornjih točk (i) in (ii), za katere se predlog uredbe ne uporablja, in jih Banka Slovenije uporablja za izvajanje svojih nalog po Zakonu o Banki Slovenije[7], Statutu Evropskega sistema centralnih bank in Evropske centralne banke (v nadaljnjem besedilu: Statut ESCB) in predpisih Evropske unije[8].

4 Glej 5. člen, prvi in drugi odstavek 6. člena ter četrti odstavek 7. člena Zakona o informacijski varnosti.
5 Glej prilogo k predlogu uredbe ter 13. in 14. člen predloga uredbe.
6 Glej 2. člen predloga uredbe.
7 Zakon o Banki Slovenije (Uradni list RS, št. 72/06 – uradno prečiščeno besedilo, 59/11 in 55/17).
8 Glej četrti odstavek 6. člena predloga uredbe.

1.5 Zakon o informacijski varnosti določa, da vlada kot izvajalce bistvenih storitev poleg tistih, ki jih določi na podlagi predloga uredbe, kakor je opisano zgoraj, določi tudi upravljavce kritične infrastrukture, ki so določeni v skladu z Zakonom o kritični infrastrukturi[9,10].

2 Splošne pripombe

2.1 Kakor je bilo že navedeno[11], ECB podpira cilj Direktive (EU) 2016/1148, ki je zagotoviti visoko skupno raven varnosti omrežij in informacij v Uniji ter v poslovnih sektorjih in državah članicah doseči skladen pristop na tem področju. Pomembno je zagotoviti, da je notranji trg varno okolje za poslovanje in da imajo države članice zagotovljeno določeno minimalno raven pripravljenosti na incidente na področju kibernetske varnosti[12].

2.2 V zvezi s posebnimi določbami predloga uredbe, ki se nanašajo na informacijske sisteme, ki jih upravlja ali „nadzira“ Banka Slovenije in/ali ESCB, kakor je opisano v odstavku 1.5, ECB razume, da pojem „nadzor“, kakor se uporablja v predlogu uredbe, obsega „nadzor“ (angleško: *supervision*) in „pregled“ (angleško: *oversight*). Po slovenskem pravu je pojem „nadzor“ mogoče razumeti tako, da se nanaša na oboje, „nadzor“ in „pregled“, kakor se ta dva pojma razume na primer v angleškem jeziku.

3 Vpliv predloga uredbe na sistemsko pomembne plačilne sisteme (SPPS) in TARGET2-Securities

3.1 ECB je v vlogi preglednika na podlagi člena 3.1, člena 22 in prve alinee člena 34.1 Statuta ESCB sprejela Uredbo (EU) št. 795/2014 (ECB/2014/28). Z navedeno uredbo se v pravno zavezujoči obliki izvajajo načela za infrastrukture finančnega trga, ki sta jih izdala Odbor za plačilne in poravnalne sisteme (CPSS) in Mednarodno združenje nadzornikov trga vrednostnih papirjev (IOSCO)[13]. Nedavno se je z njo uvedla vrsta novih zahtev za upravljavce SPPS, ki obravnavajo nova tveganja, vključno s tistimi, ki so povezana z operativnim in varnostnim tveganjem (kot je kibernetska odpornost)[14], pri čemer te zahteve med drugim upoštevajo smernice Odbora za plačila in tržne infrastrukture (CPMI) in IOSCO za kibernetsko odpornost infrastruktur finančnega trga, ki so bile objavljene leta 2016[15]. Med SPPS, za katere velja navedena uredba, ima posebno vlogo

9 Zakon o kritični infrastrukturi (Uradni list RS, št. 75/17). ECB je bila zaprošena za mnenje o navedenem zakonu in je izdala Mnenje CON/2017/31.

10 Glej tretji odstavek 6. člena Zakona o informacijski varnosti.

11 Glej npr. odstavek 2.1 Mnenja CON/2014/58, odstavek 2.1 Mnenja CON/2017/10, odstavek 2.2 Mnenja CON/2018/22, odstavek 2.2 Mnenja CON/2018/27 in odstavek 3.1 Mnenja CON/2018/39. Vsa mnenja ECB so objavljena na spletni strani ECB na naslovu www.ecb.europa.eu.

12 Glej npr. člen 15(4a) Uredbe 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).

13 Dostopno na spletni strani Banke za mednarodne poravnave na naslovu www.bis.org.

14 Glej člen 15, ki zahteva, da upravljavci SPPS: (i) redno in po večjih spremembah pregledajo, revidirajo in preizkusijo sisteme, operativne politike, postopke in kontrole; (ii) vzpostavijo učinkovit okvir za kibernetsko odpornost, ki vsebuje ustrezne upravljavske ukrepe; (iii) določijo svoje ključne dejavnosti in sredstva, ki jih podpirajo, ter vzpostavijo ustrezne ukrepe, s katerimi jih zaščitijo pred kibernetskimi napadi, zaznajo te napade, se odzovejo nanje in si po njih opomorejo; (iv) vzpostavljene ukrepe redno preizkušajo ter (v) imajo ustrezno raven situacijskega zavedanja glede kibernetskih groženj, tudi na podlagi postopka trajnega učenja.

15 Dostopno na spletni strani Banke za mednarodne poravnave.

sistem TARGET2, saj je v lasti in upravljanju Eurosistema ter je predmet stroge ureditve in pregleda.

3.2 Na podlagi prvega in drugega odstavka 2. člena predloga uredbe, ki iz področja uporabe predloga uredbe izvzemata storitve, ki se zagotavljajo z uporabo informacijskih sistemov, ki jih upravlja ESCB ali jih upravlja Banka Slovenije in nadzira ali pregleduje ESCB, ECB razume, da so te storitve posledično izvzete tudi iz področja uporabe Zakona o informacijski varnosti. ECB to pozdravlja, saj bi moralo prispevati k zagotavljanju, da slovenska zakonodaja o informacijski varnosti ne posega v pristojnosti ESCB, skladno z načelom primarnosti prava Unije in načelom neodvisnosti centralnih bank v skladu s členom 130 Pogodbe[16].

3.3 ECB zlasti razume, da bi bile na podlagi prvega odstavka 2. člena predloga uredbe iz področja uporabe zadevne zakonodaje izvzete storitve TARGET2-Securities (T2S), saj v skladu s členom 6 Smernice ECB/2012/13 Evropske centralne banke[17] in členom 7 okvirnega sporazuma o T2S[18] T2S upravlja ESCB. Poleg tega T2S skladno z odločitvijo Sveta ECB v okviru politike pregleda Eurosistema (revidirana različica iz julija 2016) spada v pristojnost Eurosistema za pregled po členu 127(2) Pogodbe in členih 3(1) in 22 Statuta ESCB[19].

3.4 ECB prav tako razume, da je na podlagi drugega odstavka 2. člena predloga uredbe iz področja uporabe predloga uredbe in Zakona o informacijski varnosti izvzeta slovenska komponenta sistema TARGET2, saj je upravljavec te komponente Banka Slovenije. Sistem TARGET2 je bil s Sklepom ECB/2014/35 Evropske centralne banke[20] določen kot SPPS in pregleduje ga ECB kot pristojni organ v skladu z Uredbo (EU) št. 795/2014 (ECB/2014/28).

3.5 ECB razume, da je cilj tretjega odstavka 2. člena predloga uredbe omejiti vpliv predloga uredbe na nadzor ali pregled, ki ga opravlja Banka Slovenije ali centralne banke ESCB na podlagi prava Unije[21], tako da določitev izvajalcev bistvenih storitev v skladu s predlogom uredbe in posledična uporaba Zakona o informacijski varnosti za tako določene izvajalce ne bosta vplivali na opravljanje omenjenega nadzora ali pregleda. Poleg tega, da je iz področja uporabe Zakona o informacijski varnosti izvzeta slovenska komponenta sistema TARGET2, ECB razume, da na podlagi tretjega odstavka 2. člena predloga uredbe zadevna slovenska zakonodaja ne bo posegala v pristojnosti Eurosistema na področju SPPS, tudi ne prek nadzorniških pooblastil nacionalnega organa za informacijsko varnost in njegovih inšpektorjev po Zakonu o informacijski varnosti.

---

16 Glej npr. odstavek 2.2 Mnenja CON/2014/58, odstavek 2.2 Mnenja CON/2017/10, odstavek 3.1.1 Mnenja CON/2018/22 in odstavek 3.2.1 Mnenja CON/2018/39.

17 Smernica ECB/2012/13 Evropske centralne banke z dne 18. julija 2012 o TARGET2-Securities (UL L 215, 11.8.2012, str. 19).

18 Dostopno na spletni strani ECB.

19 Dostopno na spletni strani ECB.

20 Sklep ECB/2014/35 Evropske centralne banke z dne 13. avgusta 2014 o določitvi sistema TARGET2 kot sistemsko pomembnega plačilnega sistema v skladu z Uredbo (EU) št. 795/2014 o pregledniških zahtevah za sistemsko pomembne plačilne sisteme (UL L 245, 20.8.2014, str. 5).

21 Kakor je opisano v odstavku 1.3, seznam bistvenih storitev po predlogu uredbe vključuje „dejavnost obdelave finančnih transakcij in dejavnost poravnav, vključno s transakcijami s kreditnimi karticami – plačilni promet“ in „upravljanje finančnih trgov“ (poslovanje in nadzor finančnih trgov razen tistega, ki ga opravljajo državni organi: zbirna hramba vrednostnih papirjev, ugotavljanje in izpolnjevanje obveznosti iz poslov z vrednostnimi papirji ter vodenje centralnega registra imetnikov nematerializiranih vrednostnih papirjev).

4 Vpliv predloga uredbe na plačilne sisteme, ki niso SPPS

4.1 Plačilni sistemi, ki niso SPPS, obsegajo sisteme za plačila velikih vrednosti, ki niso sistemsko pomembni, in sisteme za plačila malih vrednosti, ki niso sistemsko pomembni. V skladu z revidiranim okvirom za pregled sistemov za plačila malih vrednosti[22] so bili sistemi za plačila malih vrednosti, ki niso sistemsko pomembni, razdeljeni v dve skupini: prominentno pomembni sistemi za plačila malih vrednosti in drugi sistemi za plačila malih vrednosti. Slovenski lokalni klirinški in plačilni sistemi za plačila malih vrednosti so bili razvrščeni kot prominentno pomembni sistemi za plačila malih vrednosti ali drugi sistemi za plačila malih vrednosti[23] in ECB razume, da bi bili glede na sedanje stanje, ker njihove storitve ustrezajo vrstam storitev s seznama bistvenih storitev po predlogu uredbe, upravljavci teh sistemov ali nekateri od njih lahko določeni kot izvajalci bistvenih storitev, s tem pa bi se uvrstili v okvir Zakona o informacijski varnosti in postali predmet nadzorniških ukrepov nacionalnega organa za informacijsko varnost in njegovih inšpektorjev.

4.2 V skladu z Eurosistemovim okvirom politike pregleda morajo sistemi za plačila velikih vrednosti, ki niso sistemsko pomembni, in sistemi za plačila malih vrednosti, ki niso sistemsko pomembni, upoštevati načela za infrastrukture finančnega trga CPSS-IOSCO, sistemi za plačila malih vrednosti, ki niso sistemsko pomembni, pa morajo poleg tega upoštevati tudi pregledniška pričakovanja za povezave med sistemi za plačila malih vrednosti[24]. Navedena načela in pričakovanja so instrumenti mehkega prava, kar pomeni, da za sisteme za plačila velikih vrednosti, ki niso sistemsko pomembni, prominentno pomembne sisteme za plačila malih vrednosti in druge sisteme za plačila malih vrednosti veljajo pregledniški standardi (ki so primerljivi s standardi po Uredbi (EU) št. 795/2014 (ECB/2014/28)), strogo gledano pa pregleda ali nadzora teh sistemov ne ureja noben predpis Unije[25]. Banka Slovenije je pristojna za nadzor in pregled plačilnih sistemov, ki niso SPPS, na podlagi Zakona o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih[26], ki v tem delu ne izvaja „predpisov“ Unije, kakor je opisano v tem odstavku[27].

4.3 Revidirani okvir za pregled sistemov za plačila malih vrednosti določa, da so vsi sistemi za plačila malih vrednosti del področja plačil in poravnave v euroobmočju ter tako sodijo v okvir pregleda. Eurosistem je zato zainteresiran, da se zagotovi, da se z izvajanjem Direktive (EU) 2016/1148 ali pri uvajanju drugih predpisov, povezanih z varnostjo omrežij in informacij, ne poseže v okvir za pregled in standarde, ki veljajo za te sisteme[28].

4.4 Če je predvideno, da se plačilni sistemi, ki niso SPPS, izključijo iz področja uporabe predloga uredbe in Zakona o informacijski varnosti, ECB predlaga, da se zaradi pravne varnosti izrecno pojasni, da zadevna zakonodaja ne posega v pregled Banke Slovenije ali ESCB nad plačilnimi sistemi, ki niso SPPS ter za katere se uporabljajo veljavni okviri, smernice in načela za pregled. Če

22 Glej Eurosistemov revidirani okvir za pregled sistemov za plačila malih vrednosti (*Revised oversight framework for retail payment systems*) (februar 2016), dostopen na spletni strani ECB.

23 Glej Eurosistemov pregled plačilnih sistemov (*Overview of payment systems*), dostopen na spletni strani ECB.

24 Glej Eurosistemova pregledniška pričakovanja za povezave med sistemi za plačila malih vrednosti (*Oversight expectations for links between retail payment systems*), dostopna na spletni strani ECB.

25 Glej odstavek 2.4.4 Mnenja CON/2017/31 in odstavek 3.2.3 Mnenja CON/2018/22.

26 Zakon o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (Uradni list RS, št. 7/18 in 9/18 – popr.).

27 Glej tudi odstavek 2.4.4 Mnenja CON/2017/31.

28 Glej odstavek 3.2.4 Mnenja CON/2018/22.

pa slovenski organi menijo, da je treba plačilne sisteme, ki niso SPPS, vključiti v področje uporabe predloga uredbe in Zakona o informacijski varnosti, ECB izpostavlja, da 5. točka drugega odstavka 27. člena Zakona o informacijski varnosti predvideva, da nacionalni organ za informacijsko varnost sodeluje z regulatorji in nadzorniki področij, na katerih se izvajajo bistvene storitve. ECB predlaga, da se pri uporabi te določbe vzpostavi učinkovita ureditev izmenjave informacij in sodelovanja ter s tem zagotovi, da bo nacionalni organ za informacijsko varnost informacije o dejanskih in potencialnih kibernetskih incidentih in ukrepih, ki jih načrtuje ali jih je sprejel in vplivajo na plačilne sisteme, ki niso SPPS, pravočasno in učinkovito dajal Banki Slovenije, tako da bo ta lahko opravljala naloge, ki jih ima po Pogodbi in slovenskem pravu. V vsakem primeru bi bilo priporočljivo pojasniti, kakšna sta natančno področje uporabe predloga uredbe in Zakona o informacijski varnosti ter obseg nadzorniških pooblastil nacionalnega organa za informacijsko varnost in njegovih inšpektorjev v razmerju do plačilnih sistemov, ki niso SPPS, da bi preprečili morebitne nejasnosti glede veljavnih standardov in pooblastil zadevnih organov[29].

5 Vpliv predloga uredbe na ponudnike kritičnih storitev

Revidirani okvir politike pregleda Eurosistema[30] zajema ponudnike kritičnih storitev. Podobno kot v primeru plačilnih sistemov, ki niso SPPS, ni mogoče izključiti možnosti, da bi predlog uredbe in nadzorniška pooblastila nacionalnega organa za informacijsko varnost zajeli tudi ponudnike kritičnih storitev, za katere veljajo pregledniški ukrepi, ki so instrumenti mehkega prava in se ne bi šteli za predpise Unije v smislu tretjega odstavka 2. člena predloga uredbe. Zato ECB predlaga, da slovenski organi pri uporabi Zakona o informacijski varnosti, če bi to lahko vplivalo na ponudnike kritičnih storitev, upoštevajo obstoječo ureditev pregleda[31].

6 Vpliv predloga uredbe na plačilne storitve ter plačilne instrumente in sheme

6.1 Okvir politike pregleda Eurosistema določa, da so plačilni instrumenti, kot so plačilne kartice, kreditna plačila, direktne obremenitve in elektronski denar, „sestavni del plačilnih sistemov“ in jih tako vključuje v okvir pregleda. Za plačilne instrumente se vloga primarnega preglednika (za Eurosistem) določi glede na nacionalno zasidranost plačilne sheme in glede na to, kje je pravno ustanovljen njen organ upravljanja. Za sheme kreditnih plačil in direktnih obremenitev v enotnem območju plačil v eurih ter nekatere mednarodne kartične sheme ima vlogo primarnega preglednika ECB. Za ponudnike plačilnih storitev velja Direktiva (EU) 2015/2366 Evropskega parlamenta in Sveta[32], ki se uporablja od januarja 2018, kakor je izvedena v nacionalnem pravu. Za ponudnike plačilnih storitev torej veljajo predpisi Unije in predpisi Republike Slovenije (vključno s predpisi, sprejetimi na podlagi predpisov Unije), pregleda mednarodnih in domačih kartičnih shem pa ne urejajo predpisi Unije v pravem pomenu besede[33].

29 Prav tam.

30 Str. 9.

31 Glej odstavek 3.3.1 Mnenja CON/2018/22.

32 Direktiva (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES ter 2013/36/EU in Uredbe (EU) št. 1093/2010 ter razveljavitvi Direktive 2007/64/ES (UL L 337, 23.12.2015, str. 35).

33 Glej odstavek 2.4.3 Mnenja CON/2017/31 in odstavek 3.4.2 Mnenja CON/2018/22.

6.2 ECB meni, da ni povsem jasno, ali so različne plačilne sheme in plačilni instrumenti zajeti v vrsti storitev, ki je v predlogu uredbe navedena kot „druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade“. Zato predlaga, da se v zvezi z organi, pristojnimi za pregled plačilnih shem, instrumentov in storitev, ter za razmerje med njimi in nacionalnim organom za informacijsko varnost zagotovi enako pojasnilo oziroma vzpostavi enak učinkovit okvir izmenjave informacij in sodelovanja, kakor je opisano v odstavku 4.4[34].

7 Vpliv predloga uredbe na centralne depotne družbe

7.1 Centralne depotne družbe so predmet stroge ureditve in nadzora različnih organov v skladu z Uredbo (EU) št. 909/2014 Evropskega parlamenta in Sveta[35], ki določa zahteve v zvezi z operativnim tveganjem. Centralne depotne družbe bi morale upoštevati tudi smernice CPMI-IOSCO za kibernetsko odpornost, ki veljajo za vse infrastrukture finančnega trga.

7.2 Poleg tega, da so pristojni nacionalni organi pristojni za nadzor na podlagi Uredbe (EU) št. 909/2014, je treba izpostaviti, da so lahko nacionalni organi, zlasti članice ESCB, pristojni tudi za pregled centralnih depotnih družb. V tej zvezi uvodna izjava 8 Uredbe (EU) št. 909/2014 pravi, da navedena uredba ne bi smela posegati v pristojnosti ECB in nacionalnih centralnih bank za zagotavljanje učinkovitih in zanesljivih klirinških in plačilnih sistemov v Uniji in v drugih državah ter da navedena uredba članicam ESCB ne bi smela preprečevati dostopa do informacij, ki jih potrebujejo za opravljanje svojih dolžnosti, vključno z nadzorom [*oversight*] centralnih depotnih družb in drugih infrastruktur finančnih trgov.

7.3 Nadzor nad KDD d.d., slovensko centralno depotno družbo, opravljata Banka Slovenije in slovenska Agencija za trg vrednostnih papirjev, pregled pa opravlja Banka Slovenije[36]. Čeprav kaže, da je KDD zajeta v vrstah storitev, določenih v predlogu uredbe, kot so zbirna hramba vrednostnih papirjev, ugotavljanje in izpolnjevanje obveznosti iz poslov z vrednostnimi papirji ter vodenje centralnega registra imetnikov nematerializiranih vrednostnih papirjev, ECB razume, da Zakon o informacijski varnosti ne bi smel posegati v nadzor in pregled KDD, glede na to, da se ta nadzor in pregled opravljata na podlagi predpisov Unije. Vendar pa bi morali predlog uredbe spremeniti, da bi pojasnili, da odgovornosti nacionalnega organa za informacijsko varnost ne posegajo v naloge Banke Slovenije niti Agencije za trg vrednostnih papirjev ter so z njunimi nalogami usklajene.

8 Vpliv predloga uredbe na kreditne institucije

8.1 V skladu s tretjim odstavkom 2. člena predloga uredbe ta ne posega v nadzor informacijskih sistemov s področja pristojnosti Banke Slovenije ali ESCB. Predlog uredbe tako ne bi smel vplivati

34 Glej odstavek 3.4.3 Mnenja CON/2018/22.

35 Uredba (EU) št. 909/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o izboljšanju ureditve poravnav vrednostnih papirjev v Evropski uniji in o centralnih depotnih družbah ter o spremembi direktiv 98/26/ES in 2014/65/EU ter Uredbe (EU) št. 236/2012 (UL L 257, 28.8.2014, str. 1).

36 Nadzor KDD urejata Zakon o trgu finančnih instrumentov (Uradni list RS, št. 108/10 – uradno prečiščeno besedilo, 78/11, 55/12, 105/12 – ZBan-1J, 63/13 – ZS-K, 30/16 in 9/17) ter Uredba o izvajanju Uredbe (EU) o izboljšanju ureditve poravnav vrednostnih papirjev v Evropski uniji in o centralnih depotnih družbah (Uradni list RS, št. 60/16). Agencija za trg vrednostnih papirjev izda KDD dovoljenje za opravljanje notarskih storitev in storitev centralnega vodenja računov in s tem povezanih pomožnih nebančnih storitev ter nadzira opravljanje teh storitev.

na pristojnost ESCB po pravu Unije in nadzor informacijskih sistemov v pristojnosti Banke Slovenije. Vendar pa ECB razume, da bi bile nekatere kreditne institucije s sedežem v Sloveniji lahko določene kot izvajalci bistvenih storitev in bi tako morale izpolnjevati obveznosti po Zakonu o informacijski varnosti. Glede tega je treba izpostaviti naslednje.

8.2 Z Uredbo Sveta (EU) št. 1024/2013[37] se na ECB prenašajo naloge, ki se nanašajo na bonitetni nadzor kreditnih institucij, z namenom prispevati k njihovi varnosti in trdnosti ter zaščititi stabilnost finančnega sistema Unije in posameznih držav članic. ECB je odgovorna za učinkovito in skladno delovanje enotnega mehanizma nadzora (EMN) ter nadzoruje delovanje EMN na podlagi razdelitve odgovornosti med ECB in pristojnimi nacionalnimi organi, vključno z Banko Slovenije. ECB izdaja in odvzema dovoljenja vsem kreditnim institucijam. V zvezi s pomembnimi kreditnimi institucijami je ECB med drugim zadolžena tudi za zagotavljanje skladnosti z upoštevnim pravom Unije, ki kreditnim institucijam nalaga bonitetne zahteve, vključno z zahtevo, da morajo vzpostaviti stabilno ureditev upravljanja, vključno z zanesljivimi postopki obvladovanja tveganj in mehanizmi notranjih kontrol[38]. Zato so ECB podeljena vsa pooblastila za nadzor, ki omogočajo poseg v delovanje kreditnih institucij in so potrebna za opravljanje njenih funkcij[39].

8.3 Bonitetni nadzor kreditnih institucij obsega tudi vprašanja v zvezi s kibernetsko varnostjo in zaščito infrastrukture, ki je pomembna za delovanje kreditnih institucij, in sicer v okviru bonitetnega nadzora nad operativnim tveganjem, ki pomeni tveganje izgube zaradi neprimernega ali neuspešnega izvajanja notranjih procesov, ravnanj ljudi in delovanja sistemov ali zaradi zunanjih dogodkov[40]. V tej zvezi ima ECB med drugim pooblastilo, da omeji poslovanje, dejavnosti ali mrežo institucije ali zahteva odpravo dejavnosti, ki pomenijo preveliko tveganje za stabilnost institucije[41]. Ker je ocenjevanje ustreznosti ureditev notranjega upravljanja ena od temeljnih pristojnosti bonitetnih nadzornikov, predlog uredbe in zahteve po Zakonu o informacijski varnosti ne bi smeli posegati v naloge, ki jih bonitetni nadzorniki v tej zvezi opravljajo[42].

8.4 Nacionalni organ za informacijsko varnost ima po Zakonu o informacijski varnosti vrsto pooblastil za ukrepanje v primeru incidentov na področju kibernetske varnosti. Zlasti lahko v primeru težjega ali kritičnega incidenta oziroma kibernetskega napada ali grožnje zavezancem po zakonu določi takšne ustrezne in sorazmerne ukrepe, kot je potrebno za zaustavitev incidenta, ki že poteka, preprečitev realizacije verjetnega incidenta in odpravo posledic incidenta ter za zmanjšanje pričakovanih škodljivih posledic verjetnega incidenta[43]. Inšpektorji nacionalnega organa za informacijsko varnost lahko pri nadzoru nad izvajanjem zakona izrekajo tudi ukrepe za odpravo

---

37 Uredba Sveta (EU) št. 1024/2013 z dne 15. oktobra 2013 o prenosu posebnih nalog, ki se nanašajo na politike bonitetnega nadzora kreditnih institucij, na Evropsko centralno banko (UL L 287, 29.10.2013, str. 63).

38 Glej člen 4(1)(e) in člen 6(4) Uredbe (EU) št. 1024/2013.

39 Glej člen 64(1) Direktive 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij, spremembi Direktive 2002/87/ES in razveljavitvi direktiv 2006/48/ES in 2006/49/ES (UL L 176, 27.6.2013, str. 338); glej tudi odstavek 4.1 Mnenja CON/2018/22 in odstavek 3.5.1 Mnenja CON/2018/39.

40 Glej člen 4(1)(52) Uredbe (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in investicijska podjetja ter o spremembi Uredbe (EU) št. 648/2012 (UL L 176, 27.6.2013, str. 1).

41 Glej člen 16(2)(e) Uredbe (EU) št. 1024/2013.

42 Glej odstavek 2.12 Mnenja CON/2014/9, odstavek 3.5 Mnenja CON/2014/58, odstavek 4.3 Mnenja CON/2018/22 in odstavek 3.5.2 Mnenja CON/2018/39.

43 Glej 21. in 22. člen Zakona o informacijski varnosti.

ugotovljenih pomanjkljivosti[44]. Prav tako lahko izvajalcem bistvenih storitev prepovejo uporabo njihovega informacijskega sistema, dokler niso ugotovljene pomanjkljivosti odpravljene, vendar le v skrajnem primeru in upoštevaje pomen področja, na katerem delujejo, oziroma njihovega sistema in dejavnosti, če s tem ukrepom ni ogrožena oskrba na posameznem področju oziroma zagotavljanje njihovih storitev[45].

8.5 Res je, da se naloge ECB in Banke Slovenije kot bonitetnih nadzornikov v številnih ključnih elementih razlikujejo od nalog in pristojnosti nacionalnih skupin za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij in nacionalnega organa za informacijsko varnost. Kljub temu bi lahko prišlo do prekrivanja, če bi lahko ukrepi teh skupin ali organa vplivali na bonitetni nadzor kreditnih institucij po pravu Unije in slovenskem pravu. Najočitnejši primer tega bi bil, če bi se nacionalni organ za informacijsko varnost in njegovi inšpektorji odločili, da v skladu s pooblastili po Zakonu o informacijski varnosti prepovejo uporabo informacijskega sistema. Če pomembna kreditna institucija ne bi smela uporabljati informacijskega sistema, ki ga uporablja za opravljanje plačilnih storitev, bi to lahko pomembno vplivalo na njeno nemoteno poslovanje in finančno stanje. Dodatno bi lahko obveščanje prizadetih oseb ali javnosti o kibernetskih incidentih[46] vplivalo na zaupanje javnosti v prizadeto institucijo. ECB in pristojni nacionalni organi v EMN so odgovorni za ocenjevanje načrtov sanacije in sprejemanje ukrepov za zgodnje posredovanje v skladu z Direktivo 2014/59/EU Evropskega parlamenta in Sveta[47]. Poleg tega je ECB primarno odgovorna za ugotovitev, da pomembna kreditna institucija propada ali bo verjetno propadla, kar je pogoj za reševanje[48]. V primeru reševanja je eden od njegovih ciljev zagotoviti kontinuiteto izvajanja kritičnih funkcij[49], kar lahko vključuje kontinuiteto delovanja plačilne funkcije kreditne institucije[50].

8.6 Po Zakonu o informacijski varnosti se lahko izvajalcem storitev izrečejo tudi upravne globe, kadar ne izpolnijo obveznosti iz tega zakona[51].

8.7 Glede na zgoraj navedeno in ker se tretji odstavek 2. člena predloga uredbe trenutno nanaša samo na pristojnosti ESCB po pravu Unije in nadzor informacijskih sistemov (ne pa na nadzor kreditnih institucij), ECB predlaga, da se pojasni, da področje uporabe Zakona o informacijski varnosti in pooblastila pristojnih organov na njegovi podlagi prav tako ne posegajo v pristojnosti, naloge in pooblastila ECB (in Banke Slovenije) po Uredbi (EU) št. 1024/2013 in slovenskem pravu[52]. Da bi ECB in Banka Slovenije lahko opravljali svoje naloge v okviru EMN, ECB tudi priporoča, da se vzpostavi učinkovit okvir, ki bo zagotovil, da bo nacionalni organ za informacijsko varnost dajal informacije o dejanskih in potencialnih kibernetskih incidentih, ki vplivajo na pomembne nadzorovane subjekte, ter o ukrepih, ki jih načrtuje ali jih je sprejel. Kadar to pride v poštev, bi

44 Glej 32. člen Zakona o informacijski varnosti.
45 Glej 35. člen Zakona o informacijski varnosti.
46 Glej deveti odstavek 13. člena in 23. člen Zakona o informacijski varnosti.
47 Glej člene 27 do 30 Direktive 2014/59/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o vzpostavitvi okvira za sanacijo ter reševanje kreditnih institucij in investicijskih podjetij ter o spremembi Šeste direktive Sveta 82/891/EGS ter direktiv 2001/24/ES, 2002/47/ES, 2004/25/ES, 2005/56/ES, 2007/36/ES, 2011/35/EU, 2012/30/EU in 2013/36/EU in uredb (EU) št. 1093/2010 ter (EU) št. 648/2012 Evropskega parlamenta in Sveta (UL L 173, 12.6.2014, str. 190).
48 Glej člen 32(1)(a) Direktive 2014/59/EU.
49 Glej člen 31(2)(a) Direktive 2014/59/EU.
50 Glej odstavka 4.4 in 4.5 Mnenja CON/2018/22.
51 Glej enajsto poglavje Zakona o informacijski varnosti.
52 Glej tudi odstavek 4 Mnenja CON/2018/22 in odstavek 3.5 Mnenja CON/2018/39.

moral nacionalni organ za informacijsko varnost informacije pravočasno in učinkovito dajati Banki Slovenije in prek nje ECB. Slovenski zakonodajalec bi lahko tudi proučil, kakšno je razmerje med pooblastili nacionalnega organa za informacijsko varnost po Zakonu o informacijski varnosti ter postopki in pooblastili ustreznih organov v zvezi z reševanjem[53].

9 Drugi informacijski sistemi Banke Slovenije

Četrti odstavek 6. člena predloga uredbe se nanaša na informacijske sisteme Banke Slovenije, ki je ne upravlja ESCB niti jih ne upravlja Banka Slovenije in nadzira ESCB, jih pa Banka Slovenije uporablja za izvajanje svojih nalog po Zakonu o Banki Slovenije, Statutu ESCB in predpisih Unije. ECB razume, da bi bil primer informacijskega sistema, za katerega bi veljala ta določba, infrastruktura za upravljanje sistema zakladniškega računa, ki jo Banka Slovenije uporablja za vodenje računov državnih organov[54]. Na podlagi obrazložitve predloga uredbe, ki pojasnjuje, da je namen te določbe podoben namenu sorodne določbe o kritični infrastrukturi Banke Slovenije v Zakonu o kritični infrastrukturi, ECB sklepa, da je nameraval zakonodajalec v četrtem odstavku 6. člena zahtevati soglasje Banke Slovenije pred sprejetjem vsake odločitve po Zakonu o informacijski varnosti, ki bi se nanašala na informacijski sistem, ki je zajet s to določbo, zlasti sistem za upravljanje sistema zakladniškega računa. Ker je besedilo četrtega odstavka 6. člena nejasno, bi ga bilo treba zaradi pravne varnosti spremeniti.

10 Razno

Zaradi pravne varnosti bi bilo treba zagotoviti, da bodo izjeme in zaščitni ukrepi, določeni v predlogu uredbe, veljali tudi za upravljavce kritične infrastrukture v vlogi izvajalcev bistvenih storitev.

To mnenje bo objavljeno na spletni strani ECB.

V Frankfurtu na Majni, 8. novembra 2018

[podpis]

Predsednik ECB

Mario DRAGHI

53 Glej odstavek 4.6 Mnenja CON/2018/22.

54 Glej tudi prilogo k predlogu uredbe, ki določa, da je centralno bančništvo, „delovanje v vlogi bančnika državnega sektorja, vključno glede podračunov za pokojninsko, zdravstveno in socialno zavarovanje“, bistvena storitev.