III

(Pripravljalni akti)

EVROPSKA CENTRALNA BANKA

MNENJE EVROPSKE CENTRALNE BANKE

z dne 4. junija 2021

o predlogu uredbe Evropskega parlamenta in Sveta o digitalni operativni odpornosti za finančni sektor

(CON/2021/20)

(2021/C 343/01)

Uvod in pravna podlaga

Evropska centralna banka (ECB) je 22., 23. in 29. decembra 2020 prejela zahteve Sveta Evropske unije oziroma Evropskega parlamenta za mnenje o predlogu uredbe Evropskega parlamenta in Sveta o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014 in (EU) št. 909/2014 ([1]) (v nadaljnjem besedilu: predlagana uredba) ter predlogu direktive o spremembi direktiv 2006/43/ES, 2009/65/ES, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 in (EU) 2016/2341 ([2]) (v nadaljnjem besedilu: predlagana direktiva o spremembi; skupaj s predlagano uredbo: predlagana akta).

Pristojnost ECB, da poda mnenje, izhaja iz členov 127(4) in 282(5) Pogodbe o delovanju Evropske unije, saj predlagana akta vsebujeta določbe, ki sodijo na področja iz njene pristojnosti, zlasti opredelitev in izvajanje denarne politike, 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 prvo in 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.

1. Splošne pripombe

1.1 ECB pozdravlja predlagano uredbo, katere cilj je okrepiti kibernetsko varnost in operativno odpornost finančnega sektorja. ECB zlasti pozdravlja cilj predlagane uredbe, da se odpravijo ovire za vzpostavitev in delovanje notranjega trga za finančne storitve ter da se ju okrepi s harmonizacijo pravil, ki se uporabljajo pri upravljanju tveganj na področju informacijske in komunikacijske tehnologije (IKT), poročanju, testiranju in tveganjih tretjih oseb na področju IKT. ECB poleg tega pozdravlja cilj predlagane uredbe, da se poenostavijo in harmonizirajo prekrivajoče se regulativne zahteve ali pričakovanja glede nadzora, ki trenutno veljajo za finančne subjekte v skladu s pravom Unije.

1.2 ECB razume, da je predlagana uredba v zvezi s finančnimi subjekti, ki so opredeljeni kot izvajalci bistvenih storitev ([3]), sektorski pravni akt (*lex specialis*) v smislu člena 1(7) Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta ([4]) (v nadaljnjem besedilu: direktiva NIS); to pomeni, da bi zahteve iz predlagane uredbe načeloma prevladale nad direktivo NIS. V praksi bi finančni subjekti, ki so opredeljeni kot izvajalci bistvenih storitev ([5]), med drugim poročali o incidentih v skladu s predlagano uredbo in ne direktivo NIS. Čeprav ECB pozdravlja zmanjšanje možnih prekrivajočih se zahtev za finančne subjekte na področju poročanja

([1]) COM (2020) 595 final.
([2]) COM (2020) 596 final.
([3]) Glej člen 1(2) predlagane uredbe.
([4]) 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).
([5]) Glej člen 5 direktive NIS.

o incidentih, bi bilo treba medsebojno vplivanje predlagane uredbe in direktive NIS dodatno proučiti. V skladu s predlagano uredbo bi lahko na primer za tretjega ponudnika storitev IKT ([6]) veljala priporočila, ki jih izda glavni nadzornik ([7]). Hkrati pa je lahko prav ta tretji ponudnik storitev IKT v skladu z direktivo NIS opredeljen kot izvajalec bistvenih storitev in zanj veljajo zavezujoča navodila, ki jih izda pristojni organ ([8]). V takem primeru bi lahko za tretjega ponudnika storitev IKT veljala nasprotujoča si priporočila, izdana v skladu s predlagano uredbo, in zavezujoča navodila, izdana v skladu z direktivo NIS. ECB zakonodajnima organoma Unije predlaga dodatno proučitev možnih neskladij med predlagano uredbo in direktivo NIS, ki bi lahko ovirala harmonizacijo in zmanjšanje prekrivajočih se in nasprotujočih si zahtev za finančne subjekte.

1.3 ECB tudi razume, da bodo v skladu s predlogom direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148 ([9]) (v nadaljnjem besedilu: predlagana direktiva NIS2) za „skorajšnje dogodke“ ([10]) veljale obveznosti poročanja ([11]). Čeprav je v uvodni izjavi 39 predlagane direktive NIS2 omenjen pomen pojma „skorajšnji dogodek“, pa ni jasno, ali je namen zahtevati, da finančni subjekti iz člena 2 predlagane uredbe poročajo o skorajšnjih dogodkih. V zvezi s tem in ker je mogoče skorajšnje dogodke prepoznati kot take šele po tem, ko se zgodijo, bi ECB želela pravočasno prejemati obvestila o pomembnih skorajšnjih dogodkih, kakor to zdaj velja za kibernetske incidente. ECB predlaga večjo usklajenost med predlagano uredbo in predlagano direktivo NIS2, da se razjasni natančen obseg poročanja, ki bi veljal za vsak posamezen finančni subjekt v skladu s tema ločenima, a povezanima zakonodajnima aktoma Unije. Obenem bi bilo treba „skorajšnje dogodke“ opredeliti in oblikovati določbe za razjasnitev njihove pomembnosti.

1.4 ECB pozdravlja spodbujanje finančnih subjektov k prostovoljni izmenjavi obveščevalnih podatkov o kibernetskih grožnjah, da bi izboljšali in okrepili svoj položaj glede kibernetske odpornosti. ECB je sama pomagala pri tržno vodeni pobudi za izmenjavo obveščevalnih podatkov o kibernetskih incidentih (CIISI-EU) in dala na voljo načrte, na podlagi katerih lahko vsakdo razvija in spodbuja tako pobudo ([12]).

1.5 ECB podpira sodelovanje med pristojnimi organi za namene predlagane uredbe, evropskimi nadzornimi organi in skupinami za odzivanje na incidente na področju računalniške varnosti (CSIRT) ([13]). Izmenjava informacij je bistvena za zagotovitev operativne odpornosti Unije, saj lahko izmenjava informacij in sodelovanje med organi prispevata k preprečevanju kibernetskih napadov in pomagata zmanjšati širjenje groženj na področju IKT. Treba bi bilo spodbujati skupno razumevanje tveganj, povezanih z IKT, in zagotoviti dosledno ocenjevanje takih tveganj po vsej Uniji. Izredno pomembno je, da informacije z enotno kontaktno točko ([14]) in nacionalnimi sistemi CSIRT izmenjujejo pristojni organi ([15]) samo takrat, kadar obstajajo jasno vzpostavljeni mehanizmi za razvrščanje in izmenjavo informacij v povezavi z ustreznimi zaščitnimi ukrepi za zagotovitev zaupnosti.

1.6 Nazadnje, ECB bi v okviru predlagane uredbe pozdravila uvedbo pravil o osebnih podatkih in hrambi podatkov. Pri dolžini obdobja hrambe bi bilo treba upoštevati morebitne preiskave, inšpekcijske preglede, zahteve po predložitvi informacij, sporočanje, objavo, vrednotenje, preverjanje, ocenjevanje in pripravo načrtov pregleda ali nadzora, ki bi jih pristojni organi morali izvesti v okviru svojih obveznosti in dolžnosti v skladu s predlagano uredbo. V zvezi s tem bi bilo ustrezno 15-letno obdobje hrambe. Navedeno obdobje

([6]) Glej člen 3(15) predlagane uredbe.
([7]) Glej člen 31(1)(d) predlagane uredbe.
([8]) Glej člen 15(3) direktive NIS.
([9]) COM (2020) 823 final.
([10]) Dogodki, ki bi lahko povzročili škodo, vendar se je uspešno preprečilo, da bi se v celoti uresničili; glej uvodno izjavo 39 direktive NIS2.
([11]) Glej člen 11 direktive NIS2.
([12]) *Cyber threat Intelligence Information Sharing Initiative* (CIISI-EU), dostopno na spletni strani ECB na naslovu www.ecb.europa.eu.
([13]) Glej člen 42 predlagane uredbe.
([14]) Glej člen 8(3) direktive NIS.
([15]) Glej tudi člene 11, 26 in 27 direktive NIS2.

hrambe podatkov bi se lahko skrajšalo ali podaljšalo glede na potrebe v posebnih primerih. ECB v zvezi s tem predlaga, naj zakonodajna organa Unije pri oblikovanju ustrezne določbe o osebnih podatkih in hrambi podatkov upoštevajo tudi načelo najmanjšega obsega podatkov in nadaljnjo obdelavo za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene ([16]).

2. **Posebne pripombe o pregledu ter kliringu in poravnavi vrednostnih papirjev**

2.1 *Pristojnosti ESCB in Eurosistema na področju pregleda*

2.1.1 Pogodba ter Statut Evropskega sistema centralnih bank in Evropske centralne banke (v nadaljnjem besedilu: Statut ESCB) določata, da Eurosistem izvaja pregled nad klirinškimi in plačilnimi sistemi, kar je tesno povezano z njegovimi temeljnimi nalogami na področju denarne politike. V skladu s četrto alineo člena 127(2) Pogodbe, ki se ponovi v členu 3.1 Statuta ESCB, je ena od temeljnih nalog Evropskega sistema centralnih bank (ESCB) podpirati nemoteno delovanje plačilnih sistemov. 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 ([17]). ECB je v skladu s svojo pregledniško vlogo sprejela Uredbo Evropske centralne banke (EU) št. 795/2014 (ECB/2014/28) (v nadaljnjem besedilu: uredba o SPPS) ([18]). Z uredbo o SPPS se v normativni obliki izvajajo načela za infrastrukture finančnega trga iz aprila 2012, ki sta jih izdala Odbor za plačilne in poravnalne sisteme in Mednarodno združenje nadzornikov trga vrednostnih papirjev ([19]), ki so pravno zavezujoča ter zajemajo sistemsko pomembne sisteme za plačila velikih vrednosti in za plačila malih vrednosti, ki jih upravlja centralna banka Eurosistema ali zasebni subjekt. V okviru politike pregleda Eurosistema ([20]) so plačilni instrumenti opredeljeni kot „sestavni del plačilnih sistemov“ in zato vključeni v okvir pregleda. Okvir za pregled plačilnih instrumentov se trenutno pregleduje ([21]). V tem okviru je plačilni instrument (npr. kartica, kreditno plačilo, direktna obremenitev, prenos elektronskega denarja in digitalni plačilni žeton ([22])) opredeljen kot osebna naprava (ali več naprav) in/ali niz postopkov, ki so dogovorjeni med uporabnikom plačilnih storitev in ponudnikom plačilnih storitev, ki se uporabljajo za odreditev prenosa vrednosti ([23]).

2.1.2 Zato ECB pozdravlja to, da so upravljavci sistemov, kakor so opredeljeni v točki (p) člena 2 Direktive 98/26/ES Evropskega parlamenta in Sveta ([24]), plačilni sistemi (vključno s tistimi, ki jih upravljajo centralne banke), plačilne sheme in plačilne ureditve izvzeti iz člena o področju uporabe predlagane uredbe, in sicer glede na

([16]) Glej člena 4(b) in 13 Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

([17]) Glej člen 22 Statuta ESCB.

([18]) 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).

([19]) Dostopno na spletni strani Banke za mednarodne poravnave na naslovu www.bis.org.

([20]) *Eurosystem oversight policy framework, Revised version* (julij 2016), dostopno na spletni strani ECB na naslovu www.ecb.europa.eu.

([21]) Glej revidirani in konsolidirani okvir *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements* iz oktobra 2020 (okvir PISA), ki je dostopen na spletni strani ECB na naslovu www.ecb.europa.eu.

([22]) Digitalni plačilni žeton je digitalna oblika vrednosti, zavarovana s terjatvami ali sredstvi, knjiženimi drugje, ki omogoča prenos vrednosti med končnimi uporabniki. Digitalni plačilni žetoni lahko, odvisno od temeljne zasnove, predvidevajo prenos vrednosti, ki ne vključuje nujno osrednje tretje osebe in/ali uporabe plačilnih računov.

([23]) „Prenos vrednosti“: „Dejanje, ki ga odredi plačnik ali se odredi v imenu plačnika ali ga odredi prejemnik plačila, za prenos sredstev ali digitalnih plačilnih žetonov ali polog ali dvig gotovine na račun uporabnika ali z njega neodvisno od osnovnih obveznosti med plačnikom in prejemnikom plačila. Prenos lahko vključuje enega ali več ponudnikov plačilnih storitev.“ Navedena opredelitev „prenosa vrednosti“ v okviru PISA odstopa od opredelitve prenosa „denarnih sredstev“ v Direktivi (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). „Prenos vrednosti“ v kontekstu „plačilnega instrumenta“, kakor je opredeljen v navedeni direktivi, se lahko nanaša samo na prenos „denarnih sredstev“. V skladu z navedeno direktivo „denarna sredstva“ ne vključujejo digitalnih plačilnih žetonov, razen če se žetoni lahko razvrstijo kot elektronski denar (ali bolj hipotetično kot knjižni denar).

([24]) Direktiva 98/26/ES Evropskega parlamenta in Sveta z dne 19. maja 1998 o dokončnosti poravnave pri plačilih in sistemih poravnave vrednostnih papirjev (UL L 166, 11.6.1998, str. 45).

uporabo zgoraj navedenih okvirov pregleda. Iz navedenih razlogov bi bilo treba v uvodnih izjavah predlagane uredbe jasno izraziti pristojnosti ESCB v skladu s Pogodbo in pristojnosti Eurosistema v skladu z uredbo o SPPS.

2.1.3 ECB prav tako pozdravlja to, da se iz uporabe okvira pregleda, določenega v predlagani uredbi, izvzamejo tretji ponudniki storitev IKT, za katere veljajo okviri pregleda, vzpostavljeni za podpiranje nalog iz člena 127(2) Pogodbe ([25]). V zvezi s tem želi ECB poudariti, da za centralne banke ESCB, ki delujejo kot monetarni organi ([26]), in Eurosistem pri opravljanju storitev prek sistema TARGET2, TARGET2-Securites (T2S) ([27]) in poravnave takojšnjih plačil v sistemu TARGET (TIPS) ([28]) člen predlagane uredbe o področju uporabe ne velja, niti se ti ne obravnavajo kot tretji ponudniki storitev IKT, ki bi lahko bili uvrščeni med ključne tretje ponudnike storitev IKT za namene predlagane uredbe. Eurosistem pregleduje T2S v povezavi s svojim mandatom za zagotavljanje učinkovitih in zanesljivih klirinških in plačilnih sistemov. Poleg tega je organ ESMA pojasnil, da T2S ni izvajalec ključnih storitev ([29]) v smislu Uredbe (EU) št. 909/2014 Evropskega parlamenta in Sveta ([30]) (v nadaljnjem besedilu: uredba o CDD). Zato se organizacijska in operativna varnost, učinkovitost in odpornost T2S zagotavljajo z veljavnim pravnim, regulativnim in operativnim okvirom in dogovorjenimi ureditvami upravljanja T2S in ne z uredbo o CDD.

2.1.4 Okvir politike pregleda Eurosistema ([31]) poleg tega zajema ponudnike kritičnih storitev, kot je Združenje za svetovne finančne telekomunikacije med bankami (Society for Worldwide Interbank Financial Telecommunication – SWIFT). SWIFT je družba z omejeno odgovornostjo s sedežem v Belgiji, ki zagotavlja storitve varnega sporočanja na mednarodni ravni. Glavni preglednik SWIFT je centralna banka Nationale Bank van België/Banque Nationale de Belgique, ki na podlagi ureditve skupnega pregleda izvaja preglede SWIFT v sodelovanju z drugimi centralnimi bankami iz skupine G10, vključno z ECB. Pregledniki iz skupine G10 potrjujejo, da se pri pregledovanju osredotočajo zlasti na operativno tveganje SWIFT, saj se šteje za primarno kategorijo tveganja, zaradi katerega bi lahko SWIFT pomenil sistemsko tveganje za finančni sistem Unije. V zvezi s tem je skupina za skupno pregledovanje SWIFT (*SWIFT Cooperative Oversight Group*) razvila poseben sklop načel in pričakovanj na visoki ravni, ki veljajo za SWIFT, na primer prepoznavanje in upravljanje tveganj, informacijska varnost, zanesljivost in odpornost, tehnološko načrtovanje in komunikacija z uporabniki. Pregledniki iz skupine G10 pričakujejo, da bo SWIFT upošteval smernice Odbora za plačila in tržne infrastrukture (CPMI) in Mednarodnega združenja nadzornikov trga vrednostnih papirjev (IOSCO) za kibernetsko odpornost (*Guidance on cyber resilience*) ([32]) ter druge mednarodne standarde na področju varnosti IKT, ki kot celota presegajo zahteve iz predlagane uredbe.

2.1.5 Ni mogoče z gotovostjo trditi, da bi predlagana uredba za SWIFT in morda druge ponudnike storitev, za katere velja okvir politike pregleda Eurosistema, lahko veljala kot za tretje ponudnike storitev IKT, če bi zagotavljali storitve, ki niso zajete v členu 127(2) Pogodbe. ECB zato močno pozdravlja dejstvo, da so ponudniki storitev, za katere že velja okvir politike pregleda Eurosistema, med drugim tudi SWIFT, izključeni iz področja uporabe okvira za pregled, določenega v predlagani uredbi.

([25]) Glej člen 28(5) predlagane uredbe.

([26]) Glej odstavek 1.3 mnenja Evropske centralne banke z dne 19. februarja 2021 o predlogu uredbe o trgih kriptoimetij in spremembi Direktive (EU) 2019/1937 (CON/2021/4). Vsa mnenja ECB so objavljena na spletni strani EUR-Lex.

([27]) Glej Prilogo IIa k Smernici ECB/2012/27 Evropske centralne banke z dne 5. decembra 2012 o transevropskem sistemu bruto poravnave v realnem času (TARGET2) (UL L 30, 30.1.2013, str. 1). Smernica ECB/2012/13 Evropske centralne banke z dne 18. julija 2012 o TARGET2-Securities (UL L 215, 11.8.2012, str. 19), Sklep Evropske centralne banke ECB/2011/20 z dne 16. novembra 2011 o določitvi podrobnih pravil in postopkov za izvajanje meril primernosti centralnih depotnih družb za dostop do storitev TARGET2-Securities (UL L 319, 2.12.2011, str. 117). Glej tudi okvirni sporazum o T2S in kolektivni sporazum.

([28]) Glej Prilogo IIb k Smernici ECB/2012/27.

([29]) Glej člen 30(5) Uredbe (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) in člen 68 Delegirane uredbe Komisije (EU) 2017/392 z dne 11. novembra 2016 o dopolnitvi Uredbe (EU) št. 909/2014 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi o zahtevah glede izdaje dovoljenj, nadzora in poslovanja za centralne depotne družbe (UL L 65, 10.3.2017, str. 48).

([30]) 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).

([31]) *Eurosystem oversight policy framework, Revised version* (julij 2016), dostopno na spletni strani ECB na naslovu www.ecb.europa.eu.

([32]) Dostopno na spletni strani Banke za mednarodne poravnave na naslovu www.bis.org.

2.2 *Pristojnosti ESCB na področju poravnave vrednostnih papirjev*

2.2.1 Centralne depotne družbe (CDD) so infrastrukture finančnega trga, ki so strogo regulirane in jih različni organi strogo nadzirajo v skladu z uredbo o CDD, v kateri so določene zahteve v zvezi s poravnavo finančnih instrumentov ter pravila o organizaciji in vodenju CDD. CDD bi morale poleg tega upoštevati tudi Smernice CPMI-IOSCO za kibernetsko odpornost, ki so operacionalizirane s pregledniškimi pričakovanji glede kibernetske odpornosti infrastruktur finančnega trga (*Cyber resilience oversight expectations for financial market infrastructures*) (december 2018) ([33]). Poleg nadzornih pristojnosti, ki so v skladu z uredbo o CDD zaupane pristojnim nacionalnim organom, delujejo članice ESCB kot „zadevni organi" v vlogi preglednikov sistemov poravnave vrednostnih papirjev, ki jih upravljajo CDD, centralnih bank, ki izdajajo najpomembnejše valute, v katerih se opravlja poravnava, in centralnih bank, v poslovnih knjigah katerih se poravna denarni del poslov ([34]). V zvezi s tem je v uvodni izjavi 8 uredbe o CDD navedeno, da bi se morala navedena uredba uporabljati brez poseganja v pristojnosti ECB in nacionalnih centralnih bank za zagotavljanje učinkovitih in zanesljivih klirinških in plačilnih sistemov v Uniji in v drugih državah. V uvodni izjavi 8 je navedeno tudi, da uredba o CDD članicam ESCB ne bi smela preprečevati dostopa do informacij, ki jih potrebujejo za opravljanje svojih dolžnosti ([35]), vključno s pregledom CDD in drugih infrastruktur finančnega trga ([36]).

2.2.2 Poleg tega članice ESCB pogosto delujejo kot posredniki za poravnavo denarnega dela poslov z vrednostnimi papirji, Eurosistem pa CDD ponuja storitve poravnave prek T2S. Pregled Eurosistema nad T2S je povezan z njegovo nalogo zagotavljanja učinkovitih in zanesljivih klirinških in plačilnih sistemov, medtem ko si pristojni in zadevni organi CDD prizadevajo zagotoviti njihovo nemoteno delovanje, varnost in učinkovitost poravnave ter pravilno delovanje finančnih trgov v svojih jurisdikcijah.

2.2.3 Centralne banke ESCB v skladu s predlagano uredbo ([37]) ne sodelujejo pri pripravi tehničnih standardov v zvezi s specifikacijo tveganj na področju IKT. Podobno zadevni organi v skladu s predlagano uredbo ([38]) niso obveščeni o incidentih, povezanih z IKT. Centralna banka ESCB bi morala ohraniti enako raven sodelovanja, kot je trenutno določena v uredbi o CDD, zadevne organe pa bi bilo treba obveščati o incidentih, povezanih z IKT. Eurosistem je zadevni organ za vse CDD euroobmočja in za več drugih CDD v EU. Centralne banke ESCB bi morale biti obveščene o incidentih, povezanih z IKT, ki so pomembni za opravljanje njihovih nalog, vključno s pregledom CDD in drugih infrastruktur finančnega trga. Tveganja, ki so jim izpostavljene CDD, vključno s tveganji na področju IKT, lahko ogrozijo ustrezno delovanje CDD. Zato so tveganja na področju IKT pomembna za zadevne organe, ki bi jim bilo treba zagotoviti celovit in podroben pregled teh tveganj, da bi jih ocenili in vplivali na pristop CDD k upravljanju tveganj. Predlagana uredba ne bi smela določati manj omejevalnih zahtev v zvezi s tveganji na področju IKT v primerjavi s tistimi iz uredbe o CDD in povezanih veljavnih regulativnih tehničnih standardov.

2.2.4 Poleg tega bi morala zakonodajna organa Unije pojasniti medsebojni vpliv predlagane uredbe ([39]) in regulativnih tehničnih standardov, ki dopolnjujejo uredbo o CDD. Še posebej ni jasno, ali naj bi bila CDD izvzeta iz obveznosti zagotavljanja lastne sekundarne lokacije, če tako lokacijo zagotavlja njen tretji ponudnik storitev IKT ([40]). Če bi bila CDD izvzeta iz te obveznosti zagotavljanja sekundarne lokacije, pa ni jasno, kakšna

([33]) Dostopno na spletni strani ECB na naslovu www.ecb.europa.eu.

([34]) Glej člen 12 Uredbe (EU) št. 909/2014.

([35]) Glej tudi člen 13 ter člena 17(4) in 22(6) Uredbe (EU) št. 909/2014.

([36]) Glej odstavek 7.3 Mnenja Evropske centralne banke z dne 6. aprila 2017 o identifikaciji kritične infrastrukture zaradi varnosti informacijske tehnologije (CON/2017/10); odstavek 7.2 Mnenja 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); odstavek 3.5.2 Mnenja Evropske centralne banke z dne 2. maja 2019 o varnosti omrežij in informacijskih sistemov (CON/2019/17) ter odstavek 3.5.2 Mnenja Evropske centralne banke z dne 11. novembra 2019 o varnosti omrežij in informacijskih sistemov (CON/2019/38).

([37]) Glej člen 54(5) predlagane uredbe in člen 45(7) Uredbe (EU) št. 909/2014.

([38]) Glej člen 54(4) predlagane uredbe in člen 45(6) Uredbe (EU) št. 909/2014.

([39]) Glej člen 11(5) predlagane uredbe.

([40]) Glej člen 78(3) Delegirane uredbe Komisije (EU) 2017/392 z dne 11. novembra 2016 o dopolnitvi Uredbe (EU) št. 909/2014 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi o zahtevah glede dovoljenj, nadzora in poslovanja za centralne depotne družbe (UL L 65, 10.3.2017, str. 48).

bi bila pravna veljavnost te zahteve. Prav tako se predlagana uredba ([41]) sklicuje na cilj glede časa za obnovitev oziroma ponovno vzpostavitev delovanja in cilje glede točke obnovitve za vsako funkcijo ([42]), medtem ko zadevni regulativni tehnični standard v zvezi s časom do ponovne vzpostavitve delovanja, določenim za kritične dejavnosti CDD, razlikuje med kritičnimi dejavnostmi ([43]) in kritičnimi operacijami ([44]). Zakonodajna organa Unije morata zaradi preprečitve tveganja nasprotujočih si zahtev dodatno pojasniti in razmisliti o medsebojnem vplivu predlagane uredbe in regulativnih tehničnih standardov, ki dopolnjujejo uredbo o CDD. Nazadnje bi bilo treba pojasniti, da se izjeme, ki v skladu z uredbo o CDD ([45]) veljajo za CDD, ki jih upravljajo nekateri javni subjekti, s predlagano uredbo razširjajo.

2.3 *Pristojnosti ESCB na področju kliringa vrednostnih papirjev*

2.3.1 Centralnim bankam ESCB so zaupane pristojnosti na področju pregleda centralnih nasprotnih strank (CNS). V zvezi s tem nacionalne centralne banke Eurosistema pogosto sodelujejo z ustreznimi pristojnimi nacionalnimi organi pri pregledniških in nadzornih funkcijah glede CNS ter sodelujejo v kolegiju CNS, ustanovljenem na podlagi Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta ([46]) (v nadaljnjem besedilu: uredba EMIR). Ustrezne članice Eurosistema ([47]) kot pregledniki oziroma nadzorniki sodelujejo v kolegijih EMIR ter zastopajo Eurosistem kot centralno banko izdajateljico za CNS, pri katerih je euro ena najpomembnejših valut za finančne instrumente, pri katerih se opravi kliring (in za eksteritorialne CNS, ki kliring znatnega dela finančnih instrumentov opravljajo v eurih). ECB je centralna banka izdajateljica za CNS zunaj euroobmočja.

2.3.2 Centralne banke ESCB v skladu s predlagano uredbo ([48]) ne sodelujejo pri pripravi tehničnih standardov v zvezi s specifikacijo tveganj na področju IKT. Poleg tega v predlagani uredbi ([49]) nikjer niso omenjene zahteve v zvezi s ciljem glede časa do ponovne vzpostavitve delovanja niti v zvezi s ciljem glede točke ponovne vzpostavitve delovanja v skladu z uredbo EMIR ([50]). Predlagana regulativna ureditev ne bi smela določati manj omejevalnih zahtev v zvezi s tveganji na področju IKT, kot že obstajajo. Zato je bistveno, da se določijo jasni cilji glede časa do ponovne vzpostavitve delovanja in točke ponovne vzpostavitve delovanja, da se vzpostavi trden okvir za upravljanje neprekinjenega poslovanja. Ohranjanje konkretnih ciljev glede časa do ponovne vzpostavitve delovanja in točke ponovne vzpostavitve delovanja je tudi del načel CPMI-IOSCO za infrastrukture finančnega trga ([51]). Sedanjo določbo iz uredbe EMIR bi bilo treba ohraniti, predlagano uredbo pa bi bilo treba ustrezno prilagoditi. Centralne banke ESCB bi morale sodelovati pri pripravi zakonodaje na sekundarni ravni ter nadaljnji razjasnitvi medsebojnega vpliva predlagane uredbe in dopolnilnih regulativnih tehničnih standardov in razmisleku o tem s strani zakonodajnih organov Unije, da se prepreči tveganje nasprotujočih si ali prekrivajočih se zahtev.

3. **Posebne pripombe o vidikih bonitetnega nadzora**

3.1 Uredba Sveta (EU) št. 1024/2013 ([52]) (v nadaljnjem besedilu: uredba o EMN) na ECB prenaša posebne naloge v zvezi z bonitetnim nadzorom kreditnih institucij v euroobmočju in določa, da je ECB odgovorna za učinkovito in skladno delovanje enotnega mehanizma nadzora (EMN), v okviru katerega se med ECB in sodelujočimi pristojnimi nacionalnimi organi razdelijo posebne nadzorne pristojnosti. ECB ima zlasti nalogo, da izdaja in odvzema dovoljenja vsem kreditnim institucijam. ECB je med drugim zadolžena tudi za zagotavljanje skladnosti z upoštevnimi predpisi Unije, ki kreditnim institucijam nalagajo bonitetne zahteve, vključno z zahtevo, da morajo vzpostaviti stabilno ureditev upravljanja, na primer zanesljive postopke obvladovanja tveganj in mehanizme notranjih kontrol ([53]). ECB ima zato vsa pooblastila za nadzor, ki omogočajo poseganje v dejavnost kreditnih

([41]) Glej člen 11(6) predlagane uredbe.
([42]) Glej člen 3(17) predlagane uredbe.
([43]) Glej člen 76(2)(d) in (e) Delegirane uredbe Komisije (EU) 2017/392.
([44]) Glej člen 78(2) in (3) Delegirane uredbe Komisije (EU) 2017/392.
([45]) Glej člen 1(4) Uredbe (EU) št. 909/2014.
([46]) Uredba (EU) št. 648/2012 Evropskega parlamenta in Sveta z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov (UL L 201, 27.7.2012, str. 1).
([47]) Glej člen 18(2)(g) in (h) uredbe EMIR.
([48]) Glej člen 53(2)(b) in (3) predlagane uredbe ter člen 34(3) uredbe EMIR.
([49]) Glej člen 53(2)(a) predlagane uredbe.
([50]) Glej člen 34 uredbe EMIR.
([51]) Glej dokument CPMI-IOSCO *Principles for Financial Market Infrastructures*, ki je dostopen na spletni strani Banke za mednarodne poravnave na naslovu www.bis.org.
([52]) 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).
([53]) Glej člena 4(1)(e) in 6(4) Uredbe (EU) št. 1024/2013.

institucij in so potrebna za opravljanje njenih funkcij. ECB in ustrezni pristojni nacionalni organi so torej tisti pristojni organi, ki izvajajo določena pooblastila bonitetnega nadzora v skladu z Uredbo 2013/575/EU Evropskega parlamenta in Sveta ([54]) (v nadaljnjem besedilu: uredba o kapitalskih zahtevah) in Direktivo 2013/36/EU Evropskega parlamenta in Sveta ([55]) (v nadaljnjem besedilu: direktiva o kapitalskih zahtevah).

3.2 V predlagani uredbi je navedeno, da bi bilo treba enotna pravila in sistem nadzora dodatno oblikovati tako, da bi vključevala digitalno operativno odpornost in varnost IKT, in sicer z razširitvijo pooblastil finančnih nadzornikov, ki so odgovorni za spremljanje in varstvo finančne stabilnosti in celovitosti trga ([56]). Cilj je spodbuditi vzpostavitev celovitega okvira za IKT ali operativno tveganje s harmonizacijo ključnih zahtev glede digitalne operativne odpornosti za vse finančne subjekte ([57]). Cilj predlagane uredbe je zlasti utrditi in nadgraditi zahteve glede tveganj na področju IKT, ki so bile doslej obravnavane ločeno v različnih zakonodajnih aktih ([58]).

3.3 Zahteve za finančni sektor v zvezi s tveganji na področju IKT so trenutno določene v številnih aktih prava Unije, med drugim v direktivi o kapitalskih zahtevah, in instrumentih mehkega prava (na primer smernicah EBA), ter so raznolike in občasno nepopolne. V nekaterih primerih so bila tveganja na področju IKT obravnavana le implicitno kot del operativnega tveganja, v drugih pa sploh niso bila obravnavana. To bi bilo treba odpraviti z uskladitvijo predlagane uredbe in navedenih aktov. V ta namen predlagana direktiva o spremembi vsebuje sklop sprememb, ki se zdijo potrebne za zagotovitev pravne jasnosti in doslednosti v zvezi z uporabo različnih zahtev glede digitalne operativne odpornosti. Vendar se trenutno predlagane spremembe direktive o kapitalskih zahtevah v predlagani direktivi o spremembi ([59]) nanašajo le na določbe o kriznih načrtih in načrtih neprekinjenega poslovanja ([60]), saj naj bi bile implicitno podlaga za obravnavanje obvladovanja tveganj na področju IKT.

3.4 Predlagana uredba ([61]) določa tudi, da finančni subjekti, vključno s kreditnimi institucijami, vzpostavijo okvire notranjega upravljanja in nadzora, ki zagotavljajo učinkovito in skrbno upravljanje vseh tveganj na področju IKT. Predlagana uredba ([62]) določa, da se v njej določene zahteve uporabljajo na posamični in konsolidirani ravni, vendar brez zadostne usklajenosti z navedenimi sektorskimi pravnimi akti. Nazadnje, v predlagani uredbi ([63]) je določeno, da brez poseganja v določbe o okviru nadzora za ključne tretje ponudnike storitev IKT iz predlagane uredbe ([64]) izpolnjevanje obveznosti iz predlagane uredbe za kreditne institucije zagotavlja pristojni organ, imenovan v skladu s členom 4 direktive o kapitalskih zahtevah, brez poseganja v posebne naloge, prenesene na ECB z uredbo o EMN.

3.5 Glede na navedeno ECB razume, da je v zvezi s kreditnimi institucijami – z izjemo določb predlagane uredbe, ki se nanašajo na okvir nadzora nad ključnimi tretjimi ponudniki storitev IKT ([65]), – namen predlagane uredbe, da se določi bonitetni okvir notranjega upravljanja za upravljanje tveganj na področju IKT, ki bo vključen v splošni okvir notranjega upravljanja v skladu z direktivo o kapitalskih zahtevah. Poleg tega bodo zaradi bonitetne narave predlaganega okvira organi, pristojni za nadzor izpolnjevanja obveznosti iz predlaganega okvira, vključno z ECB, tisti organi, ki so odgovorni za bančni nadzor v skladu z uredbo o EMN.

([54]) Uredba (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).

([55]) Direktiva 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).

([56]) Glej uvodno izjavo 8 predlagane uredbe.

([57]) Glej uvodno izjavo 11 predlagane uredbe.

([58]) Glej uvodno izjavo 12 predlagane uredbe.

([59]) Glej uvodni izjavi 4 in 5 predlagane direktive o spremembi.

([60]) Glej člen 85 direktive o kapitalskih zahtevah.

([61]) Glej člen 4(1) predlagane uredbe.

([62]) Glej člen 25(3) in (4) predlagane uredbe.

([63]) Glej člen 41 predlagane uredbe.

([64]) Glej oddelek II poglavja V predlagane uredbe.

([65]) Glej oddelek II poglavja V predlagane uredbe.

3.6 Zakonodajna organa Unije bi zato morda lahko upoštevala naslednje predloge za večjo jasnost in usklajenost med predlagano uredbo in direktivo o kapitalskih zahtevah. Prvič, zahteve iz predlagane uredbe lahko izrecno opredelili kot bonitetne, podobno kot med drugim v uredbi o CDD ([66]). Drugič, besedilo uvodnih izjav predlagane direktive o spremembi ([67]) bi lahko razširili, glede na to, da zahteve iz predlagane uredbe presegajo zgolj fazo kriznih načrtov in načrtov neprekinjenega poslovanja. Ukrepi za obvladovanje tveganj na področju IKT na splošno spadajo v splošnejši okvir stabilne ureditve upravljanja v skladu s členom 74 direktive o kapitalskih zahtevah ([68]). Tretjič, predlagano uredbo ([69]) bi bilo treba spremeniti, da se uvodnih izjavah opozorit na pristojnost ECB za bonitetni nadzor kreditnih institucij v skladu s Pogodbo in uredbo o EMN. Četrtič, sklicevanje na uporabo zahtev iz predlagane uredbe na posamični in konsolidirani ravni ([70]) bi bilo treba revidirati, saj subkonsolidirana in konsolidirana raven v predlagani uredbi nista opredeljeni, za nekatere vrste posrednikov pa v skladu z ustrezno zakonodajo ne velja konsolidirani nadzor (npr. plačilne institucije). Poleg tega bi morala raven uporabe zahtev iz predlagane uredbe izhajati izključno iz zakonodaje, ki se uporablja za posamezno vrsto finančnega subjekta. Pri kreditnih institucijah je določena jasna povezava med direktivo o kapitalskih zahtevah in predlagano uredbo, zato bi se zahteve iz predlagane uredbe samodejno uporabljale na posamični, subkonsolidirani ali konsolidirani ravni ([71]), odvisno od primera. Nazadnje, zakonodajna organa Unije bi lahko razmislila o uvedbi prehodne ureditve za obdobje med začetkom veljavnosti predlagane uredbe in začetkom veljavnosti regulativnih tehničnih standardov, predvidenih v predlagani uredbi, saj za nekatere posrednike, vključno s kreditnimi institucijami, že veljajo pravila o tveganjih na področju IKT, ki se uporabljajo za posamezne sektorje in so podrobnejša od splošnih določb predlagane uredbe.

3.7 V skladu z uredbo o EMN je naloga ECB zagotoviti, da kreditne institucije izpolnjujejo zahteve prava Unije, ki od kreditnih institucij zahtevajo, da imajo vzpostavljene stabilne postopke obvladovanja tveganj in mehanizme notranjih kontrol ([72]). To pomeni, da mora ECB zagotoviti, da kreditne institucije izvajajo politike in procese za ovrednotenje in upravljanje svoje izpostavljenosti operativnemu tveganju, vključno z modelskim tveganjem, in za dogodke vrste „majhna pogostost – velik vpliv“. Kreditne institucije morajo določiti, kaj je operativno tveganje za namene teh politik in postopkov ([73]).

3.8 Svet Evropske centralne banke (ECB) je julija 2017 sprejel okvir za poročanje o kibernetskih incidentih v EMN na podlagi osnutka, ki ga je predlagal Nadzorni odbor v skladu s členoma 26(8) in 6(2) uredbe o EMN ter členom 21(1) Uredbe (EU) št. 468/2014 Evropske centralne banke (ECB/2014/17) ([74]). Navedeni okvir vsebuje zavezujočo zahtevo (posamične odločitve, naslovljene na kreditne institucije) za informacije in/ali poročanje na podlagi člena 10 uredbe o EMN ([75]). Nekatere države že imajo vzpostavljen postopek poročanja o incidentih, po katerem morajo kreditne institucije svojim pristojnim nacionalnim organom poročati o vseh pomembnih kibernetskih incidentih. V teh državah bodo pomembne kreditne institucije še vedno poročale o incidentih pristojnim nacionalnim organom, ti pa bodo nato v imenu nadzorovanih subjektov poročila brez nepotrebnega odlašanja

([66]) Glej naslov oddelka 4 poglavja II uredbe o CDD, „Bonitetne zahteve“.
([67]) Glej uvodno izjavo 4 predlagane direktive o spremembi.
([68]) Člen 85 Direktive 2013/36/EU je zgolj podrobnejša določba. V zvezi s tem glej tudi strani 4, 11 in 37 Smernic Evropskega bančnega organa o upravljanju tveganj, povezanih z IKT in varnostjo, z dne 29. novembra 2019 (v nadaljnjem besedilu: smernice EBA), v katerih je kot splošna pravna podlaga izrecno naveden člen 74 Direktive 2013/36/EU.
([69]) Glej člen 41(1) predlagane uredbe.
([70]) Glej člen 25(3) in (4) predlagane uredbe.
([71]) Glej tudi člen 109 direktive o kapitalskih zahtevah.
([72]) Glej člen 4(1)(e) uredbe o EMN.
([73]) Glej člen 85 direktive o kapitalskih zahtevah.
([74]) Uredba (EU) št. 468/2014 Evropske centralne banke z dne 16. aprila 2014 o vzpostavitvi okvira za sodelovanje znotraj enotnega mehanizma nadzora med Evropsko centralno banko in pristojnimi nacionalnimi organi ter z imenovanimi nacionalnimi organi (okvirna uredba o EMN) (ECB/2014/17) (UL L 141, 14.5.2014, str. 1).
([75]) Kibernetski incident (ugotovljeno možno zlonamerno ali naključno kršitev informacijske varnosti) je treba sporočiti ECB, če je izpolnjen vsaj eden od naslednjih pogojev: (1) možne finančne posledice znašajo 5 milijonov EUR ali 0,1 % navadnega lastniškega temeljnega kapitala; (2) o incidentu je obveščena javnost ali je prizadet ugled institucije; (3) incident je zunaj rednega poročanja prenesen na višjo raven do direktorja informatike; (4) banka je o incidentu obvestila skupino za urgentno odzivanje na računalniške incidente, skupino za odzivanje na kršitve varnosti računalniških sistemov, varnostno službo ali policijo, (5) sproženi so bili postopki za okrevanje po katastrofi ali za neprekinjeno poslovanje ali pa je bil vložen odškodninski zahtevek za kibernetsko zavarovanje; (6) kršene so bile pravne ali regulativne zahteve; (7) banka na podlagi internih meril ali strokovne presoje (vključno z možnostjo sistemskega učinka) sklene, da bo obvestila ECB.

posredovali ECB. Zato se zgoraj navedene odločitve naslovijo tudi na navedene pristojne nacionalne organe, da te informacije na podlagi okvira za poročanje o kibernetskih incidentih v EMN posredujejo ECB. ECB podpira prizadevanja zakonodajnih organov Unije za spodbujanje harmonizacije in poenostavitve, med drugim v zvezi s sklopom pravil in obveznosti, ki veljajo za kreditne institucije v zvezi s poročanjem o incidentih. V zvezi s tem je ECB pripravljena okvir za poročanje o kibernetskih incidentih v EMN po potrebi spremeniti (in morebiti razveljaviti) glede na morebitno sprejetje predlagane uredbe.

4. **Posebne pripombe o upravljanju tveganj na področju IKT, poročanju o incidentih, testiranju operativne odpornosti in tveganju tretjih oseb na področju IKT**

4.1 *Upravljanje tveganj na področju IKT*

4.1.1 ECB pozdravlja dejstvo, da je bil s predlagano uredbo uveden stabilen in celovit okvir za upravljanje tveganj na področju IKT, ki vključuje smernice CPMI-IOSCO o kibernetski odpornosti in je dosledno usklajen z dobrimi praksami, vključno s pregledniškimi pričakovanji Eurosistema glede kibernetske odpornosti infrastruktur finančnega trga.

4.1.2 ECB podpira zamisel, da bi morali finančni subjekti izvajati ocene tveganja ob vsaki „večji spremembi“ infrastrukture omrežja in infrastrukture informacijskega sistema ([76]). Vendar predlagana uredba ne vsebuje opredelitve pojma „večja sprememba“, kar ustvarja neželene možnosti za različne razlage finančnih subjektov, ki bi lahko na koncu ovirale harmonizacijske cilje predlagane uredbe. Zaradi pravne varnosti bi zakonodajna organa Unije morda lahko razmislila o vključitvi opredelitve pojma „večja sprememba“ v predlagano uredbo.

4.1.3 ECB na splošno podpira zamisel, da morajo finančni subjekti, ki niso mikro podjetja, pristojnim organom poročati o stroških in izgubah, ki nastanejo zaradi motenj na področju IKT in incidentov, povezanih z IKT ([77]). Da pa bi zagotovili splošno učinkovitost sistema in preprečili možnost preobremenitve pristojnih organov in finančnih subjektov s prevelikim številom poročil, bi bilo morda koristno, če bi zakonodajna organa Unije proučila možnost uvedbe ustreznih pragov, po možnosti kvantitativnih.

4.1.4 ECB priznava možnost, da finančni subjekti naloge preverjanja skladnosti z zahtevami glede upravljanja tveganj na področju IKT po odobritvi pristojnih organov prenesejo znotraj skupine ali na zunanja podjetja ([78]). Hkrati pa je pomembno, da zakonodajna organa Unije pojasnita, kako bodo pristojni organi to odobrili, kadar je za finančni subjekt pristojnih več pristojnih organov. To se lahko zgodi, kadar je finančni subjekt kreditna institucija, ponudnik storitev v zvezi s kriptoimetji in/ali ponudnik plačilnih storitev. V zvezi z opredelitvijo in razvrstitvijo, ki jo morajo finančni subjekti opraviti v skladu s predlagano uredbo ([79]), ECB meni, da bi bilo preudarno, če bi predlagana uredba za namene razvrščanja sredstev od finančnih subjektov zahtevala tudi upoštevanje kritičnosti takih sredstev (tj. ali podpirajo kritične funkcije).

4.2 *Poročanje o incidentih*

4.2.1 ECB pozdravlja prizadevanja, ki izhajajo iz predlagane uredbe, za harmonizacijo poročanja o incidentih na področju IKT v Uniji in za centralizirano poročanje o večjih incidentih, povezanih z IKT ([80]). Uvedba harmoniziranega okvira za poročanje o večjih incidentih, povezanih z IKT ([81]), ustreznim pristojnim organom bi načeloma poenostavila in harmonizirala breme poročanja finančnih subjektov, vključno s kreditnimi institucijami. To bi bilo za pristojne organe koristno zaradi širšega obsega zajetih incidentov, ki bi obsegali več kot samo kibernetske incidente, ki so trenutno zajeti v obstoječih okvirih ([82]). Zaradi prihodnjega sprejetja predlagane uredbe bi bilo treba pregledati in morebiti razveljaviti obstoječe okvire, vključno z okvirom za poročanje o kibernetskih incidentih v EMN. Da bi dosegli resnično poenostavitev in popolno usklajenost vseh okvirov, pa je ključno zagotoviti, da bo obseg določb o poročanju o incidentih iz predlagane uredbe, vključno z vsemi ustreznimi opredelitvami, pragovi in parametri poročanja, v celoti usklajen z ustreznimi okviri. Izjemno pomembno je zagotoviti zlasti usklajenost med

([76]) Glej člen 7(3) predlagane uredbe.
([77]) Glej člen 10(9) predlagane uredbe.
([78]) Glej člen 5(10) predlagane uredbe.
([79]) Glej člen 7 predlagane uredbe.
([80]) Glej člen 19 predlagane uredbe.
([81]) Glej člene 3(7), 17 in 18 predlagane uredbe.
([82]) Glej na primer okvir za poročanje o kibernetskih incidentih v EMN.

predlagano uredbo na eni strani ter Direktivo (EU) 2015/2366 Evropskega parlamenta in Sveta ([83]) (v nadaljnjem besedilu: direktiva PSD2) in Smernicami EBA o poročanju o večjih incidentih (v nadaljnjem besedilu: smernice EBA) na drugi strani. Predlagana direktiva o spremembi ([84]) vsebuje spremembe direktive PSD2 v zvezi z razmejitvijo poročanja o incidentih med predlagano uredbo in direktivo PSD2, kar bi vplivalo predvsem na ponudnike plačilnih storitev, ki bi lahko pridobili dovoljenje tudi kot kreditne institucije, pa tudi pristojne organe. Postopek obveščanja o incidentih ni dovolj jasen, obstaja pa tudi možnost prekrivanja pri nekaterih incidentih, o katerih je treba poročati tako v skladu s predlagano uredbo kot smernicami EBA.

4.2.2 Postopki za obveščanje o večjih incidentih v skladu s predlagano uredbo ([85]), direktivo PSD2 oziroma ustreznimi smernicami EBA bi od ponudnikov plačilnih storitev zahtevali, da po razvrstitvi incidenta predložijo poročilo o incidentu ustreznemu pristojnemu organu. Začetna poročila dejansko ne vsebujejo bistva, vzroka ali delovnega področja, na katerega vpliva incident, ponudniki plačilnih storitev pa lahko to opredelijo šele pozneje, ko so na voljo podrobnejše informacije o incidentu. Zato bi se lahko začetna poročila o incidentih predložila tako v skladu s predlagano uredbo kot smernicami EBA ali pa bi se ponudniki plačilnih storitev lahko odločili za enoten okvir poročanja in pozneje popravili predloženo. Enaka negotovost (na primer glede temeljnega vzroka za incident) se lahko odraža tudi v vmesnih in končnih poročilih. To bi spet povečalo možnost vzporednega poročanja pristojnim organom v skladu s predlagano uredbo in direktivo PSD2.

4.2.3 Nekateri incidenti, ki jih je mogoče opredeliti kot incidente, povezane z IKT, lahko vplivajo tudi na druga področja in bi bilo zato treba o njih obveščati v skladu s smernicami EBA. To je lahko takrat, kadar ima incident vpliv z vidika IKT, obenem pa neposredno vpliva na opravljanje plačilnih storitev in/ali na druga delovna področja ali kanale, ki niso povezani z IKT. Prav tako bi se lahko zgodilo, da ne bi bilo mogoče razlikovati med operativnimi incidenti in incidenti, povezanimi z IKT. Poleg tega bi moral v primeru, kadar je isti finančni subjekt pomembna kreditna institucija in ponudnik plačilnih storitev, isti subjekt v skladu s predlagano uredbo dvakrat poročati o incidentu, povezanem z IKT, ker sta zanj pristojna dva organa. Glede na navedeno bi bilo treba v predlagani uredbi jasneje opredeliti, kako naj bi medsebojno vplivanje direktive PSD2 in smernic organa EBA delovalo v praksi. Še bolj pa bi bilo zaradi harmonizacije in poenostavitve obveznosti poročanja pomembno, da bi zakonodajna organa Unije razmislila tudi o preostalih vprašanjih v zvezi z dvojnim poročanjem in pojasnili, ali naj bi predlagana uredba na eni strani ter direktiva PSD2 in smernice EBA na drugi strani soobstajale ali pa bi moral obstajati enoten sklop zahtev za poročanje o incidentih.

4.2.4. Predlagana uredba uvaja zahtevo, da pristojni organi ([86]) po prejemu poročila potrdijo prejem uradnega obvestila in finančnemu subjektu čim prej zagotovijo vse potrebne povratne informacije ali smernice, zlasti za razpravo o popravnih ukrepih na ravni subjekta ali načinih za zmanjšanje škodljivih učinkov med sektorji. To bi pomenilo, da bi morali pristojni organi dejavno prispevati k obvladovanju incidentov in popravnim ukrepom v zvezi z njimi ter hkrati oceniti odziv nadzorovanega subjekta na kritične incidente. ECB poudarja, da bi moral biti za popravne ukrepe in posledice incidenta izključno in jasno odgovoren zadevni finančni subjekt. ECB zato predlaga, da se povratne informacije in smernice omejijo le na bonitetne povratne informacije in smernice na visoki ravni. Če bi bile povratne informacije obsežnejše, bi bili za to potrebni specializirani strokovnjaki s obsežnim tehničnim znanjem, s katerim zaposleni v bonitetnih organih običajno ne razpolagajo.

4.3 *Testiranje digitalne operativne odpornosti*

4.3.1 ECB pozdravlja zahteve iz predlagane uredbe ([87]) glede testiranja digitalne operativne odpornosti v vseh finančnih subjektih, in tega, da mora imeti vsaka institucija svoj program za testiranje. Predlagana uredba ([88]) opisuje različne vrste testov kot napotilo za finančne subjekte. Vrste testov niso preveč jasne in nekatere teste, na primer teste združljivosti, vprašalnike ali teste na podlagi scenarijev, bi si evropski nadzorni organi, pristojni organi ali finančni

([83]) 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).

([84]) Glej člen 7(9) predlagane direktive o spremembi.

([85]) Glej člen 17(3) predlagane uredbe.

([86]) Glej člen 20 predlagane uredbe.

([87]) Glej člena 21 in 22 predlagane uredbe.

([88]) Glej člen 22(1) predlagane uredbe.

subjekti lahko različno razlagali. Ne obstajajo niti smernice o pogostosti posameznega testiranja. Predlagana uredba bi lahko na primer določila splošne zahteve za testiranje, natančnejši opis vrst testov pa bi vsebovali regulativni in izvedbeni tehnični standardi.

4.3.2 Penetracijsko testiranje na podlagi analize groženj je učinkovito orodje za testiranje varnostnih obrambnih mehanizmov in pripravljenosti. ECB zato spodbuja penetracijsko testiranje na podlagi analize groženj pri finančnih subjektih. S tem orodjem se ne testirajo samo tehnični ukrepi, ampak tudi osebje in postopki. Rezultati teh testov lahko znatno izboljšajo ozaveščenost višjega vodstva o varnosti v testiranih subjektih. Evropski okvir za etično vdiranje v računalniške sisteme na podlagi obveščevalnih podatkov o grožnjah (TIBER-EU) ([89]) in druga orodja za penetracijsko testiranje na podlagi analize groženj, ki so že na voljo zunaj Unije, so primarni instrumenti, s katerimi lahko subjekti sami ocenijo, testirajo, vadijo in izboljšujejo svoje ravnanje in obrambne mehanizme na področju kibernetske odpornosti.

4.3.3 V večini držav članic, v katerih se izvaja okvir TIBER-EU, pregledniki in nadzorniki nimajo dejavne vloge pri izvajanju lokaliziranega programa TIBER-XX, skupina TIBER za kibernetsko varnost pa je v skoraj vseh primerih neodvisna od teh funkcij. Zato bi bilo treba napredno testiranje v skladu s predlagano uredbo ([90]) s pomočjo penetracijskega testiranja na podlagi analize groženj uporabljati kot orodje za krepitev finančnega ekosistema in povečanje finančne stabilnosti, ne pa izključno kot nadzorno orodje. Poleg tega ni potrebe po razvoju novega naprednega okvira za testiranje kibernetske odpornosti, saj so države članice v glavnem že sprejele okvir TIBER-EU, ki je trenutno edini tak okvir v EU.

4.3.4 Zahteve za preizkuševalce ne bi smele biti v normativnem delu predlagane uredbe, saj se sektor, povezan s penetracijskim testiranjem na podlagi analize groženj, še razvija, zato bi lahko predpisovanje posebnih zahtev oviralo inovacije. Ne glede na to pa ECB meni, da finančni subjekti zaradi zagotavljanja visoke stopnje neodvisnosti pri testiranju ne bi smeli uporabljati preizkuševalcev ali pogodbeno sodelovati s preizkuševalci, ki jih finančni subjekti uporabljajo ali z njimi pogodbeno sodelujejo v svoji skupini, ali ki so sicer v lasti in/ali pod nadzorom finančnih subjektov, ki naj bi jih testirali.

4.3.5 Zaradi zmanjšanja tveganja razdrobljenosti in zagotovitve harmonizacije bi bilo treba s predlagano uredbo predpisati en okvir penetracijskega testiranja na podlagi analize groženj, ki bi se uporabljal za finančni sektor po vsej Uniji. Zaradi razdrobljenosti se lahko povečajo stroški ter zahteve po tehničnih, operativnih in finančnih virih tako za pristojne organe kot finančne institucije. Ti večji stroški in zahteve lahko nazadnje negativno vplivajo na vzajemno priznavanje testov. To pomanjkanje harmonizacije in posledične težave z vzajemnim priznavanjem so zlasti ključnega pomena za finančne subjekte, ki imajo lahko več dovoljenj in/ali poslujejo v več jurisdikcijah po vsej Uniji. Regulativni in izvedbeni tehnični standardi za penetracijsko testiranje na podlagi analize groženj, ki bodo pripravljeni v skladu s predlagano uredbo, bi morali biti v skladu z okvirom TIBER-EU. ECB pozdravlja tudi možnost sodelovanja pri pripravi teh regulativnih in izvedbenih tehničnih standardov v sodelovanju z evropskimi nadzornimi organi.

4.3.6 Dejavno sodelovanje pristojnih organov pri testih bi lahko povzročilo nasprotje interesov z njihovo drugo funkcijo, tj. oceno okvira testiranja finančnega subjekta. Zato ECB predlaga, da se iz predlagane uredbe črtajo vse obveznosti pristojnih organov v zvezi s potrditvijo dokumentov in izdajo potrdila za penetracijski test na podlagi analize groženj.

4.4 Tveganje tretjih oseb na področju IKT

4.4.1 ECB pozdravlja uvedbo celovitega sklopa ključnih načel in stabilnega nadzornega okvira nadzora za opredelitev in upravljanje tveganj na področju IKT, ki izhajajo iz tretjih ponudnikov storitev IKT, ne glede na to, ali ti spadajo v isto skupino finančnih subjektov. Za učinkovito prepoznavanje in obvladovanje tveganj na področju IKT pa je treba med drugim pravilno opredeliti in razvrstiti ključne tretje ponudnike storitev IKT. V zvezi s tem je dobrodošla uvedba delegiranih aktov ([91]), ki bodo dopolnjevali merila za razvrščanje ([92]), vendar bi se bilo treba pred sprejetjem takšnih delegiranih aktov posvetovati z ECB.

([89]) Dostopno na spletni strani ECB na naslovu www.ecb.europa.eu.
([90]) Člena 23 in 24 predlagane uredbe.
([91]) Glej člen 28(3) predlagane uredbe.
([92]) Glej člen 28(2) predlagane uredbe.

4.4.2 V zvezi s strukturo nadzornega okvira ([93]) bi bilo treba dodatno pojasniti vlogo Skupnega odbora. ECB hkrati pozdravlja to, da je kot opazovalka vključena v nadzorniški forum, saj bo ta vloga ECB omogočila enak dostop do dokumentacije in informacij kot članom z glasovalno pravico ([94]). ECB želi zakonodajna organa Unije opozoriti na to, da bi ECB kot opazovalka prispevala k delu nadzorniškega foruma tako kot centralna banka izdajateljica, odgovorna za pregled nad tržnimi infrastrukturami, kot tudi kot bonitetni nadzornik kreditnih institucij. ECB ugotavlja tudi, da bi bila sama – poleg tega, da bi bila opazovalka v nadzorniškem forumu – kot pristojni organ tudi članica skupne pregledniške ekipe. V zvezi s tem bi lahko zakonodajna organa Unije dodatno razmislila o sestavi skupnih pregledniških ekip ([95]), da bi zagotovili ustrezno intenzivno sodelovanje ustreznih pristojnih organov. ECB prav tako meni, da bi bilo treba povečati največje možno število članov skupnih pregledniških ekip, pri tem pa upoštevati kritičnost, zapletenost in obseg storitev tretjih oseb na področju IKT.

4.4.3 ECB ugotavlja, da lahko glavni nadzornik v skladu s predlagano uredbo prepreči, da bi ključni tretji ponudniki storitev IKT sklepali nadaljnje dogovore o podizvajanju, če (i) je predvideni podizvajalec tretji ponudnik storitev IKT ali podizvajalec storitev IKT s sedežem v tretji državi in (ii) se oddaja v podizvajanje nanaša na kritično ali pomembno funkcijo finančnega subjekta. ECB želi poudariti, da lahko glavni nadzornik ta pooblastila izvaja le v okviru podizvajalskih dogovorov, kadar ključni tretji ponudnik storitev IKT kritično ali pomembno funkcijo odda v podizvajanje ločenemu pravnemu subjektu s sedežem v tretji državi. ECB razume, da glavni nadzornik takih pooblastil ne more uporabljati za to, da bi ključnemu tretjemu ponudniku storitev IKT preprečil, da za kritične ali pomembne funkcije finančnega subjekta uporablja zmogljivosti tega ponudnika storitev, ki se nahajajo v tretji državi. Z operativnega vidika bi se lahko na primer kritični podatki in/ali informacije hranili ali obdelovali v zmogljivostih zunaj Evropskega gospodarskega prostora (EGP). V takem primeru glavni nadzornik morda pristojnim organom ne bo mogel ustrezno omogočiti dostopa do vseh informacij, prostorov, infrastruktur in osebja, ki so pomembni za izvajanje vseh kritičnih ali pomembnih funkcij finančnega subjekta. ECB zaradi zagotovitve neoviranega opravljanja nalog pristojnih organov predlaga, da se glavnega nadzornika pooblasti za to, da ključnim tretjim ponudnikom storitev IKT omeji tudi uporabo zmogljivosti zunaj EGP. To pooblastilo bi se lahko uporabilo v tistih posebnih primerih, kadar z ustreznimi organi tretjih držav niso sklenjeni upravni dogovori, kot je določeno v predlagani uredbi ([96]), ali če predstavniki ključnih tretjih ponudnikov storitev IKT v skladu z okvirom zadevne tretje države ne dajo zadostnih zagotovil glede dostopa do informacij, prostorov, infrastrukture in osebja, potrebnega za izvajanje pregledniških ali nadzornih nalog.

4.4.4 Nazadnje, zahteva glede nadaljnjega ukrepanja pristojnih organov na podlagi priporočil glavnega nadzornika ([97]) bi se lahko izkazala za neučinkovito, saj pristojni organi morda nimajo celostnega pregleda nad tveganji, ki jih povzroča posamezni ključni tretji ponudnik storitev IKT. Poleg tega bi pristojni organi morda morali ukrepati proti svojim nadzorovanim finančnim subjektom, kadar ključni tretji ponudniki storitev IKT priporočil ne bi upoštevali. Pristojni organi lahko v skladu s predlagano uredbo ([98]) od svojih nadzorovanih finančnih subjektov zahtevajo, da začasno ustavijo storitev ključnega tretjega ponudnika ali prekinejo odprte pogodbe s ključnimi tretjimi ponudniki storitev. Predvideni postopek nadaljnjega ukrepanja je težko prenesti v konkretne ukrepe. Natančneje, ni jasno, ali bo nadzorovani finančni subjekt lahko začasno ustavil izvajanje pogodbe ali prekinil pogodbo s ključnim tretjim ponudnikom storitev. To je zato, ker bi lahko bil ključni tretji ponudnik storitev IKT pomemben ponudnik za ta finančni subjekt, ali zaradi pogodbenih ali drugih stroškov in odškodnin, ki bi jih finančni subjekt lahko utrpel zaradi take začasne ustavitve ali prekinitve. Poleg tega ta pristop ne podpira konvergence pregleda, saj lahko pristojni organi isto priporočilo razlagajo različno. To bi lahko nazadnje oviralo predvideno harmonizacijo in dosleden pristop pri spremljanju tveganja ključnih tretjih oseb na področju IKT na ravni Unije. Zato bi lahko zakonodajna organa Unije razmislila o tem, da bi zakonitim preglednikom podelila posebna izvršilna pooblastila v zvezi s ključnimi tretjimi ponudniki storitev IKT, ob upoštevanju omejitev na podlagi doktrine *Meroni*, ki jih je Sodišče delno omililo v sodbi v zadevi ESMA ([99]).

([93]) Glej člen 29 predlagane uredbe.
([94]) Glej člen 29(3) predlagane uredbe.
([95]) Glej člen 35 predlagane uredbe.
([96]) Glej člen 39(1) predlagane uredbe.
([97]) Glej člen 29(4) in člen 37 predlagane uredbe.
([98]) Glej člen 37(3) predlagane uredbe.
([99]) Glej sodbo Sodišča (veliki senat) z dne 22. januarja 2014, Združeno kraljestvo Velika Britanija in Severna Irska proti Evropskemu parlamentu in Svetu Evropske unije, Uredba (EU) št. 236/2012 – zadeva C-270/12.

Kadar ECB priporoča, da se predlagana uredba spremeni, so konkretni predlogi sprememb besedila s pripadajočimi pojasnili navedeni v ločenem tehničnem delovnem dokumentu. Tehnični delovni dokument je dostopen v angleščini na spletni strani EUR-Lex.

V Frankfurtu na Majni, 4. junija 2021

Predsednica ECB
Christine LAGARD