III

(Prípravné akty)

EURÓPSKA CENTRÁLNA BANKA

STANOVISKO EURÓPSKEJ CENTRALNEJ BANKY

zo 4. júna 2021

k návrhu nariadenia Európskeho parlamentu a Rady o digitálnej prevádzkovej odolnosti finančného sektora

(CON/2021/20)

(2021/C 343/01)

Úvod a právny základ

Európska centrálna banka (ECB) prijala 22., 23. a 29. decembra 2020 žiadosti Rady Európskej únie a Európskeho parlamentu o stanovisko k návrhu nariadenia Európskeho parlamentu a Rady o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014 a (EÚ) č. 909/2014 ([1]) (ďalej len „navrhované nariadenie“) a k návrhu smernice, ktorou sa menia smernice 2006/43/ES, 2009/65/ES, 2009/138/ES, 2011/61/EÚ, 2013/36/EÚ, 2014/65/EÚ, (EÚ) 2015/2366 a (EÚ) 2016/2341 ([2]) (ďalej len „navrhovaná pozmeňujúca smernica“, ďalej spoločne s navrhovaným nariadením len „navrhované akty“).

Právomoc ECB vydať stanovisko je založená na článku 127 ods. 4 a článku 282 ods. 5 Zmluvy o fungovaní Európskej únie, keďže navrhované akty obsahujú ustanovenia, ktoré patria do oblasti pôsobnosti ECB; konkrétne ide o definovanie a uskutočňovanie menovej politiky, podpora plynulého fungovania platobných systémov, prispievanie k hladkému uskutočňovaniu politík prijatých príslušnými orgánmi, ktoré sa týkajú stability systému finančných trhov, a úlohy ECB týkajúce sa prudenciálneho dohľadu nad úverovými inštitúciami podľa článku 127 ods. 2 prvej a štvrtej zarážky, článku 127 ods. 5 a článku 127 ods. 6 zmluvy. V súlade s článkom 17.5 prvou vetou rokovacieho poriadku Európskej centrálnej banky Rada guvernérov prijala toto stanovisko.

1. Všeobecné pripomienky

1.1 ECB víta navrhované nariadenie, ktorého cieľom je zlepšiť kybernetickú bezpečnosť a prevádzkovú odolnosť finančného sektora. ECB víta najmä cieľ navrhovaného nariadenia spočívajúci v odstránení prekážok a zlepšení tvorby a fungovania vnútorného trhu s finančnými službami harmonizovaním pravidiel uplatňujúcich sa na oblasť riadenia, vykazovania, testovania rizika v oblasti informačných a komunikačných technológií (IKT) a IKT rizika tretej strany. ECB okrem toho víta cieľ navrhovaného nariadenia, ktorým je zjednotiť a zosúladiť všetky prekrývajúce sa regulačné požiadavky alebo očakávania dohľadu, ktoré sa podľa práva Únie v súčasnosti vzťahujú na finančné subjekty.

1.2 ECB vychádza z toho, že navrhované nariadenie predstavuje v súvislosti s finančnými subjektmi identifikovanými ako prevádzkovatelia základných služieb ([3]) právny predpis špecifický pre určité odvetvie (*lex specialis*) v súlade s významom uvedeným v článku 1 ods. 7 smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 ([4]) (ďalej len „smernica NIS“). To znamená, že požiadavky podľa navrhovaného nariadenia by v zásade mali prednosť pred smernicou NIS. V praxi by finančné subjekty identifikované ako prevádzkovatelia základných služieb ([5]) okrem iného oznamovali incidenty v súlade s navrhovaným nariadením, a nie so

([1]) COM(2020) 595 final.
([2]) COM(2020) 596 final.
([3]) Pozri článok 1 ods. 2 navrhovaného nariadenia.
([4]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).
([5]) Pozri článok 5 smernice NIS.

smernicou NIS. Hoci ECB víta zníženie potenciálnych prekrývajúcich sa požiadaviek na finančné subjekty v oblasti oznamovania incidentov, otázka interakcie medzi navrhovaným nariadením a smernicou NIS by sa mala ďalej zvážiť. Podľa navrhovaného nariadenia by sa napríklad na externého poskytovateľa IKT služieb ([6]) mohli vzťahovať odporúčania vydané hlavným orgánom dozoru ([7]). Ten istý externý poskytovateľ IKT služieb zároveň môže byť klasifikovaný ako prevádzkovateľ základných služieb podľa smernice NIS a môžu sa naňho vzťahovať záväzné pokyny vydané príslušným orgánom ([8]). V takom prípade by sa na externého poskytovateľa IKT služieb mohli vzťahovať protichodné odporúčania vydané podľa navrhovaného nariadenia a záväzné pokyny vydané podľa smernice NIS. ECB navrhuje, aby legislatívne orgány Únie ďalej uvažovali o potenciálnom nesúlade medzi navrhovaným nariadením a smernicou NIS, ktorý môže brániť harmonizovaniu a znižovaniu prekrývajúcich sa a protichodných požiadaviek na finančné subjekty.

1.3 ECB tiež vychádza z toho, že podľa návrhu smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148 ([9]) (ďalej len „navrhovaná smernica NIS2“) budú „udalosti odvrátené v poslednej chvíli“ ([10]) podliehať oznamovacím povinnostiam ([11]). Zatiaľ čo v odôvodnení 39 navrhovanej smernice NIS2 sa uvádza význam pojmu „udalosti odvrátené v poslednej chvíli“, nie je zrejmé, či je zámerom vyžadovať oznamovanie udalostí odvrátených v poslednej chvíli od finančných subjektov uvedených v článku 2 navrhovaného nariadenia. V tejto súvislosti, ako aj vzhľadom na to, že udalosti odvrátené v poslednej chvíli možno identifikovať až po tom, ako sa vyskytnú, by ECB privítala včasné oznamovanie významných udalostí odvrátených v poslednej chvíli, ako je tomu v súčasnosti v prípade kybernetických incidentov. ECB odporúča zvýšiť súlad medzi navrhovaným nariadením a navrhovanou smernicou NIS2 s cieľom objasniť presný rozsah oznamovania, ktorému podľa týchto dvoch odlišných no prepojených právnych predpisov Únie môže podliehať ktorýkoľvek finančný subjekt. Zároveň by bolo potrebné vymedziť „udalosti odvrátené v poslednej chvíli“ a vypracovať ustanovenia objasňujúce ich význam.

1.4 ECB víta podnecovanie finančných subjektov k tomu, aby si navzájom dobrovoľne vymieňali spravodajské informácie o kybernetických hrozbách s cieľom posilniť a podporiť ich pozície, pokiaľ ide o kybernetickú odolnosť. Samotná ECB pomáhala s Iniciatívou na výmenu spravodajských informácií o kybernetických hrozbách, ktorá vzišla z potrieb trhu, a jej návrhy sprístupnila s cieľom vybudovať a podporovať túto iniciatívu ([12]).

1.5 ECB podporuje spoluprácu medzi príslušnými orgánmi na účely navrhovaného nariadenia, európskymi orgánmi dohľadu a jednotkami pre riešenie počítačových bezpečnostných incidentov ([13]). Výmena informácií je nevyhnutná na zaistenie prevádzkovej odolnosti Únie, pretože výmena informácií a spolupráca medzi orgánmi môžu prispieť k predchádzaniu kybernetickým útokom a pomôcť znížiť šírenie IKT hrozieb. Malo by sa podporovať spoločné chápanie rizík súvisiacich s IKT a v celej Únii by sa malo zabezpečiť jednotné posudzovanie takýchto rizík. Mimoriadne dôležité je to, aby príslušné orgány poskytovali informácie jednotnému kontaktnému miestu ([14]) a vnútroštátnym jednotkám pre riešenie počítačových bezpečnostných incidentov ([15]) len v prípade, že sú jasne zavedené mechanizmy klasifikácie a výmeny informácií spolu s primeranými zárukami na zabezpečenie dôvernosti.

1.6 ECB by tiež uvítala, keby sa v navrhovanom nariadení zaviedli pravidlá týkajúce sa osobných údajov a uchovávania údajov. Dĺžka obdobia uchovávania by mala zohľadňovať vyšetrovania, kontroly, žiadosti o informácie, komunikáciu, uverejňovanie, hodnotenia, overovanie, posudzovanie a vypracúvanie návrhov plánov dozoru alebo dohľadu, ktoré môžu mať príslušné orgány povinnosť uskutočňovať v rámci svojich príslušných povinností a úloh podľa navrhovaného nariadenia. V tejto súvislosti by bolo primerané obdobie

([6]) Pozri článok 3 ods. 15 navrhovaného nariadenia.
([7]) Pozri článok 31 ods. 1 písm. d) navrhovaného nariadenia.
([8]) Pozri článok 15 ods. 3 smernice NIS.
([9]) COM(2020) 823 final.
([10]) Udalosti, ktoré by mohli spôsobiť škodu, ale úspešne sa zabránilo ich prejaveniu v plnej miere – pozri odôvodnenie 39 smernice NIS2.
([11]) Pozri článok 11 smernice NIS2.
([12]) Iniciatíva na výmenu spravodajských informácií o kybernetických hrozbách (Cyber threat Intelligence Information Sharing Initiative – CIISI-EU) dostupná na webovom sídle ECB www.ecb.europa.eu.
([13]) Pozri článok 42 navrhovaného nariadenia.
([14]) Pozri článok 8 ods. 3 smernice NIS.
([15]) Pozri tiež články 11, 26 a 27 smernice NIS2.

uchovávania v dĺžke 15 rokov. Toto obdobie uchovávania údajov by bolo možné v jednotlivých konkrétnych prípadoch skrátiť alebo predĺžiť. V tejto súvislosti ECB navrhuje, aby legislatívne orgány Únie pri formulovaní príslušného ustanovenia o osobných údajoch a uchovávaní údajov zohľadnili aj zásadu minimalizácie údajov, ako aj ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého či historického výskumu alebo štatistické účely ([16]).

2. Osobitné pripomienky k dohľadu a zúčtovávaniu a vyrovnávaniu cenných papierov

2.1 *Právomoci ESCB a Eurosystému v oblasti dohľadu*

2.1.1 Zmluva a Štatút Európskeho systému centrálnych bánk a Európskej centrálnej banky (ďalej len „štatút ESCB“) stanovujú, že Eurosystém vykonáva dohľad nad zúčtovacími a platobnými systémami, čo úzko súvisí jeho základnými úlohami v oblasti menovej politiky. Podľa článku 127 ods. 2 štvrtej zarážky zmluvy a článku 3.1 štatútu ESCB je jednou zo základných úloh, ktorá sa má uskutočňovať prostredníctvom Európskeho systému centrálnych bánk (ESCB), podporovať plynulé fungovanie platobných systémov. Pri plnení tejto základnej úlohy ECB a národné centrálne banky môžu poskytnúť zariadenia a ECB môže vydávať nariadenia na zabezpečenie účinnosti a spoľahlivosti zúčtovacích a platobných systémov v rámci Únie a voči iným krajinám ([17]). ECB v súlade so svojou úlohou v oblasti dohľadu prijala nariadenie Európskej centrálnej banky (EÚ) č. 795/2014 (ECB/2014/28) (ďalej len „nariadenie o SDPS“) ([18]). Nariadením o SDPS sa normatívne vykonávajú zásady pre infraštruktúry finančného trhu z apríla 2012, ktoré vydali Výbor pre platobné a zúčtovacie systémy a Medzinárodná organizácia komisií pre cenné papiere ([19]), ktoré sú právne záväzné a vzťahujú sa na platobné systémy pre veľké hodnoty, ako aj na retailové platobné systémy systémového významu, ktoré prevádzkuje buď centrálna banka Eurosystému, alebo súkromný subjekt. Rámec politiky Eurosystému v oblasti dohľadu ([20]) identifikuje platobné nástroje ako „integrálnu súčasť platobných systémov“, a preto ich zaraďuje do rozsahu svojej pôsobnosti v oblasti dohľadu. Rámec dohľadu nad platobnými nástrojmi sa v súčasnosti preskúmava ([21]). V tomto rámci sa platobný nástroj (napr. karta, úhrada, inkaso, prevod elektronických peňazí a digitálny platobný token ([22])) vymedzuje ako personalizované zariadenie (alebo súbor zariadení) a/alebo súbor postupov dohodnutých medzi používateľom platobných služieb a poskytovateľom platobných služieb, ktoré sa používajú na iniciovanie prevodu hodnoty ([23]).

2.1.2 Vzhľadom na uvedené ECB víta, že boli z rozsahu pôsobnosti navrhovaného nariadenia vylúčení systémoví prevádzkovatelia vymedzení v článku 2 písm. p) smernice Európskeho parlamentu a Rady 98/26/ES ([24]), platobné systémy (vrátane tých, ktoré sú prevádzkované centrálnymi bankami), platobné schémy a platobné

([16]) Pozri článok 4 písm. b) a článok 13 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

([17]) Pozri článok 22 štatútu ESCB.

([18]) Nariadenie Európskej centrálnej banky (EÚ) č. 795/2014 z 3. júla 2014 o požiadavkách v oblasti dohľadu nad systémovo dôležitými platobnými systémami (ECB/2014/28) (Ú. v. EÚ L 217, 23.7.2014, s. 16).

([19]) Dostupné na webovom sídle Banky pre medzinárodné zúčtovanie www.bis.org.

([20]) Dokument *Eurosystem oversight policy framework*, revidované znenie (júl 2016), dostupný na webovom sídle ECB www.ecb.europa.eu.

([21]) Pozri revidovaný a konsolidovaný dokument *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements* z októbra 2020 (rámec PISA), ktorý je dostupný na webovom sídle ECB www.ecb.europa.eu.

([22]) Digitálny platobný token je digitálnym zobrazením hodnoty krytej pohľadávkami alebo aktívami zaznamenanými na inom mieste, ktorý umožňuje prevod hodnoty medzi koncovými používateľmi. V závislosti od príslušnej koncepcie môžu digitálne platobné tokeny predpokladať prevod hodnoty bez toho, aby bola nevyhnutne zahrnutá centrálna tretia strana a/alebo sa používali platobné účty.

([23]) „Prevod hodnoty“ je „úkon prevodu prostriedkov alebo digitálnych platobných tokenov alebo vkladania hotovosti na užívateľský účet alebo výber hotovosti z užívateľského účtu a to na podnet platiteľa alebo v mene platiteľa alebo na podnet príjemcu platby, a to bez ohľadu na súvisiace povinnosti medzi platiteľom a príjemcom platby. Prevod môže zahŕňať jedného alebo viacerých poskytovateľov platobných služieb.“ Toto vymedzenie pojmu „prevod hodnoty“ podľa rámca PISA sa líši od vymedzenia pojmu prevod „finančných prostriedkov“ podľa smernice Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES (Ú. v. EÚ L 337, 23.12.2015, s. 35). „Prevod hodnoty“ v súvislosti s „platobným nástrojom“ vymedzeným v tejto smernici sa môže vzťahovať len na prevod „finančných prostriedkov“. Podľa tejto smernice „finančné prostriedky“ nezahŕňajú digitálne platobné tokeny, pokiaľ tokeny nemožno klasifikovať ako elektronické peniaze (alebo hypotetickejšie ako bezhotovostné peniaze).

([24]) Smernica Európskeho parlamentu a Rady 98/26/ES z 19. mája 1998 o konečnom zúčtovaní v platobných systémoch a zúčtovacích systémoch cenných papierov (Ú. v. ES L 166, 11.6.1998, s. 45).

dohody vzhľadom na uplatňovanie uvedených rámcov dohľadu. Z týchto dôvodov by sa právomoci ESCB podľa zmluvy a právomoci Eurosystému podľa nariadenia o SDPS mali jasne vymedziť v odôvodneniach navrhovaného nariadenia.

2.1.3 Z rovnakého dôvodu ECB víta vylúčenie externých poskytovateľov IKT služieb, ktorí podliehajú rámcom dozoru zriadeným na účely podpory úloh uvedených v článku 127 ods. 2 zmluvy, z uplatňovania rámca dozoru stanoveného v navrhovanom nariadení ([25]). V tejto súvislosti by ECB chcela zdôrazniť, že centrálne banky ESCB konajúce v rámci svojich menových funkcií ([26]) a Eurosystém pri poskytovaní služieb prostredníctvom systémov TARGET2, TARGET2-Securites (T2S) ([27]) a služieb vyrovnania okamžitých platieb TARGET (TIPS) ([28]) nespadajú do rozsahu pôsobnosti navrhovaného nariadenia ani sa nemôžu považovať za externých poskytovateľov IKT služieb a potenciálne sa tak klasifikovať ako externí poskytovatelia kritických IKT služieb na účely navrhovaného nariadenia. Eurosystém vykonáva dohľad nad T2S v súvislosti so svojím mandátom na zabezpečenie účinnosti a spoľahlivosti zúčtovacích a platobných systémov. Orgán ESMA ďalej objasnil, že T2S nie je poskytovateľ kritických služieb ([29]) v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) č. 909/2014 ([30]) (ďalej len „nariadenie o centrálnych depozitároch“). V dôsledku toho sa organizačná a prevádzková bezpečnosť, efektívnosť a odolnosť T2S zabezpečuje prostredníctvom platného právneho, regulačného a prevádzkového rámca a dohodnutých mechanizmov riadenia T2S, a nie prostredníctvom nariadenia o centrálnych depozitároch.

2.1.4 Rámec politiky Eurosystému v oblasti dohľadu ([31]) sa okrem toho vzťahuje na poskytovateľov kritických služieb, ako je Spoločnosť pre celosvetovú medzibankovú finančnú telekomunikáciu (Society for Worldwide Interbank Financial Telecommunication – SWIFT). SWIFT je spoločnosť s ručením obmedzeným so sídlom v Belgicku, ktorá poskytuje bezpečné služby výmeny správ na medzinárodnej úrovni. Nationale Bank van België/Banque Nationale de Belgique koná ako hlavný orgán dozoru nad spoločnosťou SWIFT a na základe dohody o spolupráci v oblasti dohľadu vykonáva dohľad nad spoločnosťou SWIFT v spolupráci s ostatnými centrálnymi bankami krajín G10 vrátane ECB. Orgány dozoru krajín G10 uznávajú, že hlavným zameraním dohľadu je prevádzkové riziko spoločnosti SWIFT, keďže toto riziko sa považuje za hlavnú kategóriu rizika, prostredníctvom ktorej by spoločnosť SWIFT mohla predstavovať systémové riziko pre finančný systém v Únii. V tejto súvislosti skupina spoločného dohľadu nad spoločnosťou SWIFT vypracovala osobitný súbor zásad a očakávaní na vysokej úrovni, ktoré sa na spoločnosť SWIFT vzťahujú, ako je identifikácia a riadenie rizík, informačná bezpečnosť, spoľahlivosť a odolnosť, technologické plánovanie a komunikácia s používateľmi. Orgány dozoru krajín G10 očakávajú, že spoločnosť SWIFT bude dodržiavať usmernenia Výboru pre platobnú a trhovú infraštruktúru (Committee on Payment and Market Infrastructures – CPMI) a Medzinárodnej organizácie komisií pre cenné papiere (International Organisation of Securities Commissions – IOSCO) o kybernetickej odolnosti ([32]), ako aj ďalšie medzinárodné normy v oblasti bezpečnosti IKT, ktoré spoločne idú nad rámec požiadaviek stanovených v navrhovanom nariadení.

2.1.5 Nie je isté, či by sa na spoločnosť SWIFT a prípadne ďalších poskytovateľov služieb, na ktorých sa uplatňuje rámec politiky Eurosystému v oblasti dohľadu, mohlo začať vzťahovať navrhované nariadenie ako na externých poskytovateľov IKT služieb, ak by mali poskytovať služby, na ktoré sa nevzťahuje článok 127 ods. 2 zmluvy. ECB preto rozhodne víta skutočnosť, že poskytovatelia služieb, na ktorých sa už vzťahuje rámec politiky Eurosystému v oblasti dohľadu, okrem iného vrátane spoločnosti SWIFT, budú vylúčení z rozsahu pôsobnosti rámca dozoru stanoveného v navrhovanom nariadení.

([25]) Pozri článok 28 ods. 5 navrhovaného nariadenia.

([26]) Pozri odsek 1.3 stanoviska Európskej centrálnej banky z 19. februára 2021 k návrhu nariadenia o trhoch s kryptoaktívami a o zmene smernice (EÚ) 2019/1937 (CON/2021/4). Všetky stanoviská ECB sa uverejňujú na webových stránkach EUR-Lex.

([27]) Pozri prílohu IIa k usmerneniu Európskej centrálnej banky ECB/2012/27 z 5. decembra 2012 o Transeurópskom automatizovanom expresnom systéme hrubého vyrovnania platieb v reálnom čase (TARGET2) (Ú. v. EÚ L 30, 30.1.2013, s. 1). Usmernenie Európskej centrálnej banky ECB/2012/13 z 18. júla 2012 o TARGET2-Securities (Ú. v. EÚ L 215, 11.8.2012, s. 19); rozhodnutie Európskej centrálnej banky ECB/2011/20 zo 16. novembra 2011, ktorým sa ustanovujú podrobné pravidlá a postupy na implementáciu kritérií pre prístup centrálnych depozitárov cenných papierov k službám TARGET2-Securities (Ú. v. EÚ L 319, 2.12.2011, s. 117). Pozri tiež rámcovú dohodu o T2S a kolektívnu zmluvu.

([28]) Pozri prílohu IIb k rozhodnutiu ECB/2012/27.

([29]) Pozri článok 30 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 909/2014 z 23. júla 2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii, centrálnych depozitároch cenných papierov a o zmene smerníc 98/26/ES a 2014/65/EÚ a nariadenia (EÚ) č. 236/2012 (Ú. v. EÚ L 257 28.8.2014, s. 1) a článok 68 delegovaného nariadenia Komisie (EÚ) 2017/392 z 11. novembra 2016, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014, pokiaľ ide o regulačné technické predpisy o požiadavkách na povoľovanie centrálnych depozitárov cenných papierov, dohľad nad nimi a prevádzkové požiadavky pre ne (Ú. v. EÚ L 65, 10.3.2017, s. 48).

([30]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014 z 23. júla 2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii, centrálnych depozitároch cenných papierov a o zmene smerníc 98/26/ES a 2014/65/EÚ a nariadenia (EÚ) č. 236/2012 (Ú. v. EÚ L 257 28.8.2014, s. 1).

([31]) Dokument *Eurosystem oversight policy framework*, revidované znenie (júl 2016), dostupný na webovom sídle ECB www.ecb.europa.eu.

([32]) Dokument *Guidance on cyber resilience*, dostupný na webovom sídle Banky pre medzinárodné zúčtovanie www.bis.org.

2.2 *Právomoci ESCB v oblasti vyrovnania transakcií s cennými papiermi*

2.2.1 Centrálne depozitáre cenných papierov (ďalej len „centrálne depozitáre“) sú infraštruktúry finančného trhu, ktoré podliehajú prísnej regulácii a dohľadu rôznych orgánov podľa nariadenia o centrálnych depozitároch, v ktorom sa stanovujú požiadavky v súvislosti s vyrovnaním transakcií s finančnými nástrojmi, ako aj pravidlá týkajúce sa organizácie a konania centrálnych depozitárov. Centrálne depozitáre by navyše mali brať do úvahy usmernenia CPMI-IOSCO o kybernetickej odolnosti, ktoré bolo uvedené do praxe na základe dokumentu Cyber resilience oversight expectations for financial market infrastructures (December 2018) ([33]) . Okrem právomocí v oblasti dohľadu, ktoré boli príslušným vnútroštátnym orgánom zverené podľa nariadenia o centrálnych depozitároch, členovia ESCB konajú aj ako „relevantné orgány“ v postavení orgánov dozoru nad systémami vyrovnania transakcií s cennými papiermi, ktoré prevádzkujú centrálne depozitáre, centrálnych bánk emitujúcich najrelevantnejšie meny, v ktorých sa vykonáva vyrovnanie a centrálnych bánk, na ktorých účtoch sa vyrovnáva peňažná časť transakcií ([34]). V tejto súvislosti sa v odôvodnení 8 nariadenia o centrálnych depozitároch uvádza, že nariadenie by sa malo uplatňovať bez toho, aby boli dotknuté povinnosti ECB a národných centrálnych bánk zabezpečiť efektívne a spoľahlivé zúčtovacie a platobné systémy v rámci Únie a v ďalších krajinách. V odôvodnení 8 sa tiež uvádza, že nariadenie o centrálnych depozitároch by nemalo členom ESCB brániť v prístupe k informáciám, ktoré sú relevantné pre plnenie ich povinností ([35]), a to vrátane dohľadu nad centrálnymi depozitármi a ďalšími infraštruktúrami finančného trhu ([36]).

2.2.2 Členovia ESCB okrem toho často konajú ako agenti vyrovnania pre peňažnú časť transakcií s cennými papiermi a Eurosystém ponúka centrálnym depozitárom služby vyrovnania prostredníctvom T2S. Dohľad Eurosystému nad T2S súvisí s jeho mandátom na zabezpečenie účinnosti a spoľahlivosti zúčtovacích a platobných systémov, zatiaľ čo cieľom príslušných a relevantných orgánov centrálnych depozitárov je zabezpečiť ich riadne fungovanie, bezpečnosť a účinnosť vyrovnania a riadne fungovanie finančných trhov v príslušných jurisdikciách.

2.2.3 Podľa navrhovaného nariadenia ([37]) sa centrálne banky ESCB nezapájajú do vypracúvania technických noriem, pokiaľ ide o vymedzovanie IKT rizík. Podobne sa podľa navrhovaného nariadenia ([38]) relevantné orgány neinformujú o incidentoch súvisiacich s IKT. Centrálne banky ESCB by sa mali zapájať do rovnakej miery, akú v súčasnosti stanovuje nariadenie o centrálnych depozitároch, a relevantné orgány by mali byť informované o incidentoch súvisiacich s IKT. Eurosystém je relevantným orgánom pre všetky centrálne depozitáre eurozóny a pre niekoľko ďalších centrálnych depozitárov v EÚ. Centrálne banky ESCB by bolo potrebné informovať o incidentoch súvisiacich s IKT, ktoré sú relevantné pre plnenie ich povinností vrátane dohľadu nad centrálnymi depozitármi a ďalšími infraštruktúrami finančného trhu. Riziká, ktorým sú centrálne depozitáre vystavené, vrátane IKT rizík, môžu ohroziť riadne fungovanie centrálnych depozitárov. Pre relevantné orgány sú preto IKT riziká dôležité a mal by sa im poskytnúť úplný a podrobný prehľad týchto rizík, aby ich posúdili a ovplyvnili prístup centrálnych depozitárov k riadeniu rizík. V navrhovanom nariadení by sa nemali stanovovať menej reštriktívne požiadavky týkajúce sa IKT rizík v porovnaní s požiadavkami, ktoré stanovuje nariadenie o centrálnych depozitároch a aktuálne súvisiace regulačné technické predpisy.

2.2.4 Legislatívne orgány Únie by okrem toho mali objasniť vzájomné pôsobenie medzi navrhovaným nariadením ([39]) a regulačnými technickými predpismi, ktorými sa dopĺňa nariadenie o centrálnych depozitároch. Predovšetkým nie je jasné, či má byť centrálny depozitár oslobodený od povinnosti mať svoje vlastné druhé miesto spracovania v prípade, že takéto miesto udržiava jeho externý poskytovateľ IKT služieb ([40]). Ak by bol centrálny depozitár oslobodený od tejto povinnosti udržiavať druhé miesto spracovania,

([33]) Dokument *Cyber resilience oversight expectations for financial market infrastructures*, dostupný na webovom sídle ECB www.ecb.europa.eu.

([34]) Pozri článok 12 nariadenia (EÚ) č. 909/2014.

([35]) Pozri aj článok 13, článok 17 ods. 4 a článok 22 ods. 6 nariadenia (EÚ) č. 909/2014.

([36]) Pozri odsek 7.3 stanoviska Európskej centrálnej banky zo 6. apríla 2017 k identifikácii kritických infraštruktúr na účely bezpečnosti informačných technológií (CON/2017/10); odsek 7.2 stanoviska Európskej centrálnej banky z 8. novembra 2018 k určeniu základných služieb a prevádzkovateľov základných služieb na účely bezpečnosti sietí a informačných systémov (CON/2018/47); odsek 3.5.2 stanoviska Európskej centrálnej banky z 2. mája 2019 k bezpečnosti sietí a informačných systémov (CON/2019/17) a odsek 3.5.2 stanoviska Európskej centrálnej banky z 11. novembra 2019 k bezpečnosti sietí a informačných systémov (CON/2019/38).

([37]) Pozri článok 54 ods. 5 navrhovaného nariadenia a článok 45 ods. 7 nariadenia (EÚ) č. 909/2014.

([38]) Pozri článok 54 ods. 4 navrhovaného nariadenia a článok 45 ods. 6 nariadenia (EÚ) č. 909/2014.

([39]) Pozri článok 11 ods. 5 navrhovaného nariadenia.

([40]) Pozri článok 78 ods. 3 delegovaného nariadenia Komisie (EÚ) 2017/392 z 11. novembra 2016, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014, pokiaľ ide o regulačné technické predpisy o požiadavkách na povoľovanie centrálnych depozitárov cenných papierov, dohľad nad nimi a prevádzkové požiadavky pre ne (Ú. v. EÚ L 65, 10.3.2017, s. 48).

nie je jasné, akú právnu silu by táto požiadavka mala. Obdobne sa v navrhovanom nariadení ([41]) odkazuje na cieľ času obnovy a bodové ciele obnovy pre každú funkciu ([42]), zatiaľ čo v príslušnom regulačnom technickom predpise sa rozlišuje medzi kritickými funkciami ([43]) a kritickými operáciami ([44]) v súvislosti s časom obnovy stanoveným pre kritické operácie centrálnych depozitárov. Legislatívne orgány Únie by opodstatnene mali bližšie objasniť a ďalej uvažovať o vzájomnom pôsobení medzi navrhovaným nariadením a regulačnými technickými predpismi, ktorými sa dopĺňa nariadenie o centrálnych depozitároch, s cieľom zabrániť riziku vzniku protichodných požiadaviek. Napokon by sa malo objasniť, že výnimky udelené centrálnym depozitárom, ktoré prevádzkujú určité verejné subjekty, podľa nariadenia o centrálnych depozitároch ([45]) sa uplatňujú aj podľa navrhovaného nariadenia.

2.3 *Právomoci ESCB v oblasti zúčtovania cenných papierov*

2.3.1 Centrálnym bankám ESCB sa zverujú právomoci v oblasti dohľadu v súvislosti s centrálnymi protistranami. V tejto súvislosti národné centrálne banky Eurosystému často spolupracujú s relevantnými príslušnými vnútroštátnymi orgánmi pri výkone funkcií dozoru a dohľadu nad centrálnymi protistranami a zúčastňujú sa v kolégiu príslušnej centrálnej protistrany zriadenom podľa nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012 ([46]) (ďalej len „nariadenie EMIR“). Príslušní členovia Eurosystému ([47]) sa zúčastňujú v kolégiách podľa nariadenia EMIR v rozsahu svojich právomocí v oblasti dohľadu a zastupujú Eurosystém ako emisnú centrálnu banku pre centrálne protistrany v prípadoch, keď je euro jednou z najdôležitejších mien zúčtovávaných finančných nástrojov (a pre centrálne protistrany mimo územia eurozóny, ktoré zúčtovávajú významný podiel finančných nástrojov v eurách). ECB je emisnou centrálnou bankou pre centrálne protistrany mimo eurozóny.

2.3.2 Podľa navrhovaného nariadenia ([48]) sa centrálne banky ESCB nezapájajú do vypracúvania technických noriem, pokiaľ ide o vymedzovanie IKT rizík. Navrhované nariadenie ([49]) navyše neobsahuje žiadny odkaz na požiadavky týkajúce sa cieľa času obnovy a bodového cieľa obnovy stanovené v nariadení EMIR ([50]). Navrhovaný regulačný rámec by v súvislosti s IKT rizikami nemal stanovovať menej reštriktívne požiadavky než tie, ktoré v súčasnosti existujú. Preto je nevyhnutné stanoviť jasné ciele času obnovy a bodové ciele obnovy, aby sa vytvoril spoľahlivý rámec riadenia kontinuity činností. Udržiavanie konkrétnych cieľov času obnovy a bodových cieľov obnovy je tiež súčasťou zásad CPSS-IOSCO pre infraštruktúry finančného trhu ([51]). V súčasnosti platné ustanovenie v nariadení EMIR by sa malo zachovať a navrhované nariadenie by sa malo zodpovedajúcim spôsobom upraviť. Centrálne banky ESCB by sa mali podieľať na príprave všetkých sekundárnych právnych predpisov, ako aj na ďalšom objasňovaní a úvahách legislatívnych orgánov Únie o vzájomnom pôsobení medzi navrhovaným nariadením a doplňujúcimi regulačnými technickými predpismi s cieľom zabrániť riziku vzniku protichodných alebo prekrývajúcich sa požiadaviek.

3. **Osobitné pripomienky k aspektom prudenciálneho dohľadu**

3.1 Nariadením Rady (EÚ) č. 1024/2013 ([52]) (ďalej len „nariadenie o JMD“) sa ECB zverujú osobitné úlohy, pokiaľ ide o prudenciálny dohľad nad úverovými inštitúciami v eurozóne, a ECB sa zveruje zodpovednosť za účinné a konzistentné fungovanie jednotného mechanizmu dohľadu (JMD), v rámci ktorého sa medzi ECB a zúčastnené príslušné vnútroštátne orgány rozdeľujú konkrétne povinnosti dohľadu. ECB má najmä úlohu udeľovať povolenie a odoberať povolenie všetkým úverovým inštitúciám. ECB má tiež okrem iného úlohu zabezpečiť dodržiavanie príslušných právnych predpisov Únie, ktorými sa voči úverovým inštitúciám stanovujú prudenciálne požiadavky vrátane požiadavky mať zavedené spoľahlivé mechanizmy riadenia, ako napríklad vhodné procesy riadenia rizík a mechanizmy vnútornej kontroly ([53]). ECB boli na tento účel udelené všetky právomoci v oblasti dohľadu, ktoré sú potrebné na vykonávanie jej funkcií tak, aby mohla zasahovať do činnosti úverových inštitúcií. ECB a relevantné

([41]) Pozri článok 11 ods. 6 navrhovaného nariadenia.
([42]) Pozri článok 3 ods. 17 navrhovaného nariadenia.
([43]) Pozri článok 76 ods. 2 písm. d) a e) delegovaného nariadenia Komisie (EÚ) 2017/392.
([44]) Pozri článok 78 ods. 2 a 3 delegovaného nariadenia Komisie (EÚ) 2017/392.
([45]) Pozri článok 1 ods. 4 nariadenia (EÚ) č. 909/2014.
([46]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27.7.2012, s. 1).
([47]) Pozri článok 18 ods. 2 písm. g) a h) nariadenia EMIR.
([48]) Pozri článok 53 ods. 2 písm. b) a ods. 3 navrhovaného nariadenia a článok 34 ods. 3 nariadenia EMIR.
([49]) Pozri článok 53 ods. 2 písm. a) navrhovaného nariadenia.
([50]) Pozri článok 34 nariadenia EMIR.
([51]) Pozri dokument *CPMI-IOSCO Principles for Financial Market Infrastructures* dostupný na webovom sídle Banky pre medzinárodné zúčtovanie: www.bis.org.
([52]) Nariadenie Rady (EÚ) č. 1024/2013 z 15. októbra 2013, ktorým sa Európska centrálna banka poveruje osobitnými úlohami, pokiaľ ide o politiky týkajúce sa prudenciálneho dohľadu nad úverovými inštitúciami (Ú. v. EÚ L 287, 29.10.2013, s. 63).
([53]) Pozri článok 4 ods. 1 písm. e) a článok 6 ods. 4 nariadenia (EÚ) č. 1024/2013.

príslušné vnútroštátne orgány sú teda príslušnými orgánmi vykonávajúcimi stanovené právomoci v oblasti prudenciálneho dohľadu podľa nariadenia Európskeho parlamentu a Rady 2013/575/EÚ ([54]) (ďalej len „nariadenie o kapitálových požiadavkách“) a smernice Európskeho parlamentu a Rady 2013/36/EÚ ([55]) (ďalej len „smernica o kapitálových požiadavkách“).

3.2 V navrhovanom nariadení sa uvádza, že jednotný súbor pravidiel a systém dohľadu by sa mali ďalej vypracovať tak, aby zahŕňali digitálnu prevádzkovú odolnosť a bezpečnosť IKT, a to rozšírením mandátov orgánov finančného dohľadu poverených monitorovaním a ochranou finančnej stability a integrity trhu ([56]). Cieľom je podporiť komplexný rámec pre IKT riziká alebo operačné riziká prostredníctvom harmonizácie kľúčových požiadaviek na digitálnu prevádzkovú odolnosť všetkých finančných subjektov ([57]). Cieľom navrhovaného nariadenia je najmä konsolidovať a modernizovať požiadavky na IKT riziko, ktoré sa doteraz riešili samostatne v rôznych právnych predpisoch ([58]).

3.3 Požiadavky týkajúce sa IKT rizík v prípade finančného sektora sa v súčasnosti nachádzajú v celom rade aktov práva Únie vrátane smernice o kapitálových požiadavkách a právne nezáväzných nástrojov (ako sú usmernenia EBA) a sú odlišné a niekedy neúplné. V niektorých prípadoch sa IKT riziká riešia len nepriamo ako súčasť prevádzkového rizika, zatiaľ čo v iných prípadoch sa neriešia vôbec. Táto situácia by sa mala napraviť zosúladením navrhovaného nariadenia a týchto aktov. Na tento účel sa v navrhovanej pozmeňujúcej smernici navrhuje súbor zmien, ktoré sa zdajú potrebné na zabezpečenie právnej zrozumiteľnosti a konzistentnosti v súvislosti s uplatňovaním rôznych požiadaviek na digitálnu prevádzkovú odolnosť. Zmeny smernice o kapitálových požiadavkách, ktoré sa v súčasnosti navrhujú v navrhovanej pozmeňujúcej smernici ([59]), sa však týkajú len ustanovení o plánoch pre nepredvídané udalosti a plánoch na zabezpečenie kontinuity obchodných činností ([60]), keďže údajne nepriamo slúžia ako základ pre riešenie problematiky riadenia IKT rizík.

3.4 Okrem toho sa v navrhovanom nariadení ([61]) ustanovuje, že finančné subjekty vrátane úverových inštitúcií musia mať zavedené rámce vnútornej správy, riadenia a kontroly, ktorými sa zabezpečí účinné a obozretné riadenie všetkých IKT rizík. V navrhovanom nariadení ([62]) sa zabezpečuje uplatňovanie požiadaviek, ktoré sú v ňom stanovené, na individuálnej a konsolidovanej úrovni, ale bez dostatočnej koordinácie s uvedenými právnymi predpismi špecifickými pre určité odvetvie. Napokon sa v navrhovanom nariadení ([63]) ustanovuje, že bez toho, aby boli dotknuté ustanovenia týkajúce sa rámca dozoru pre externých poskytovateľov kritických IKT služieb uvedené v navrhovanom nariadení ([64]), súlad s povinnosťami stanovenými v tomto nariadení zabezpečuje v prípade úverových inštitúcií príslušný orgán určený v súlade s článkom 4 smernice o kapitálových požiadavkách bez toho, aby boli dotknuté osobitné úlohy, ktoré boli ECB udelené nariadením o JMD.

3.5 Vzhľadom na uvedené ECB vychádza z toho, že v súvislosti s úverovými inštitúciami a s výnimkou ustanovení navrhovaného nariadenia týkajúcich sa rámca dozoru pre externých poskytovateľov kritických IKT služieb ([65]) je cieľom navrhovaného nariadenia stanoviť prudenciálny rámec vnútornej správy a riadenia na riadenie IKT rizík, ktorý sa začlení do všeobecného rámca interného riadenia podľa smernice o kapitálových požiadavkách. Vzhľadom na prudenciálny charakter navrhovaného rámca budú okrem toho príslušné orgány zodpovedné za dohľad nad dodržiavaním povinností stanovených v navrhovanom rámci vrátane ECB orgánmi zodpovednými za bankový dohľad v súlade s nariadením o JMD.

([54]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012 (Ú. v. EÚ L 176, 27.6.2013, s. 1).

([55]) Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (Ú. v. EÚ L 176, 27.6.2013, s. 338).

([56]) Pozri odôvodnenie 8 navrhovaného nariadenia.

([57]) Pozri odôvodnenie 11 navrhovaného nariadenia.

([58]) Pozri odôvodnenie 12 navrhovaného nariadenia.

([59]) Pozri odôvodnenia 4 a 5 navrhovanej pozmeňujúcej smernice.

([60]) Pozri článok 85 smernice o kapitálových požiadavkách.

([61]) Pozri článok 4 ods. 1 navrhovaného nariadenia.

([62]) Pozri článok 25 ods. 3 a 4 navrhovaného nariadenia.

([63]) Pozri článok 41 navrhovaného nariadenia.

([64]) Pozri kapitolu V oddiel II navrhovaného nariadenia.

([65]) Pozri kapitolu V oddiel II navrhovaného nariadenia.

3.6 Legislatívne orgány Únie preto môžu chcieť zvážiť nasledujúce návrhy na zlepšenie jednoznačnosti a súladu medzi navrhovaným nariadením a smernicou o kapitálových požiadavkách. Po prvé, požiadavky podľa navrhovaného nariadenia možno výslovne určiť ako prudenciálne tak ako okrem iného aj v nariadení o centrálnych depozitároch ([66]). Po druhé, odôvodnenia navrhovanej pozmeňujúcej smernice ([67]) by bolo možné formulovať širšie, keďže požiadavky podľa navrhovaného nariadenia presahujú fázu plánov pre nepredvídané udalosti a plánov na zabezpečenie kontinuity obchodných činností. Opatrenia na riadenie IKT rizík celkovo patria do všeobecnejšieho rozsahu dôkladných mechanizmov v oblasti riadenia podľa článku 74 smernice o kapitálových požiadavkách ([68]). Po tretie, navrhované nariadenie ([69]) by sa malo zmeniť tak, aby sa v odôvodneniach pripomenula právomoc ECB v oblasti prudenciálneho dohľadu nad úverovými inštitúciami podľa zmluvy a nariadenia o JMD. Po štvrté, odkaz na uplatňovanie požiadaviek, ktoré sú v navrhovanom nariadení stanovené ([70]), na individuálnej a konsolidovanej úrovni, by sa mal prepracovať, keďže subkonsolidovaná a konsolidovaná úroveň nie je v navrhovanom nariadení vymedzená a určité typy sprostredkovateľov nepodliehajú konsolidovanému dohľadu podľa príslušných právnych predpisov (napr. platobné inštitúcie). Úroveň uplatňovania požiadaviek podľa navrhovaného nariadenia by okrem toho mala vychádzať výlučne z právnych predpisov, ktoré sa vzťahujú na jednotlivé typy finančných subjektov. V prípade úverových inštitúcií je zaistené jasné prepojenie medzi smernicou o kapitálových požiadavkách a navrhovaným nariadením, a preto by sa požiadavky podľa navrhovaného nariadenia podľa okolností automaticky uplatňovali na individuálnej, subkonsolidovanej alebo konsolidovanej úrovni ([71]). Legislatívne orgány Únie by napokon mohli zvážiť poskytnutie prechodného režimu pre obdobie medzi nadobudnutím účinnosti navrhovaného nariadenia a nadobudnutím účinnosti regulačných technických predpisov predpokladaných v navrhovanom nariadení, keďže niektorí sprostredkovatelia vrátane úverových inštitúcií už podliehajú pravidlám týkajúcim sa IKT rizík, ktoré sa vzťahujú na konkrétne odvetvia a sú podrobnejšie ako všeobecné ustanovenia navrhovaného nariadenia.

3.7 ECB bola na základe nariadenia o JMD poverená úlohou zabezpečiť, aby úverové inštitúcie dodržiavali požiadavky práva Únie, ktoré od nich vyžadujú, aby mali zavedené spoľahlivé procesy riadenia rizík a mechanizmy vnútornej kontroly ([72]). To znamená, že ECB musí zabezpečiť, aby úverové inštitúcie zaviedli politiky a postupy na hodnotenie a riadenie svojej expozície voči operačnému riziku vrátane rizika modelu a na pokrytie zriedkavo sa vyskytujúcich udalostí, ktoré majú veľmi vážne následky. Úverové inštitúcie sú povinné na účely týchto politík a postupov stanoviť, v čom spočíva operačné riziko ([73]).

3.8 Rada guvernérov Európskej centrálnej banky (ECB) prijala v júli 2017 rámec JMD pre oznamovanie kybernetických incidentov (ďalej len „rámec“) na základe návrhu Rady pre dohľad v súlade s článkom 26 ods. 8 a článkom 6 ods. 2 nariadenia o JMD a článkom 21 ods. 1 nariadenia Európskej centrálnej banky (EÚ) č. 468/2014 (ECB/2014/17) ([74]). Rámec pozostáva zo záväznej žiadosti (individuálne rozhodnutia sa adresujú úverovým inštitúciám) o informácie a/alebo oznamovania na základe článku 10 nariadenia o JMD ([75]). Niektoré krajiny už zaviedli postup oznamovania incidentov, v rámci ktorého sa od úverových inštitúcií vyžaduje, aby oznamovali všetky významné kybernetické incidenty svojim príslušným vnútroštátnym orgánom. V týchto krajinách budú významné úverové inštitúcie

([66]) Pozri kapitolu II oddiel 4 nariadenia o centrálnych depozitároch s názvom Prudenciálne požiadavky.

([67]) Pozri odôvodnenie 4 navrhovanej pozmeňujúcej smernice.

([68]) Článok 85 smernice 2013/36/EÚ je len spresnením. V tejto súvislosti pozri aj strany 4, 11 a 37 usmernení Európskeho orgánu pre bankovníctvo k riadeniu rizík v oblasti IKT a bezpečnosti z 29. novembra 2019 (ďalej len „usmernenia EBA“), ktorých všeobecný právny základ výslovne vychádza z článku 74 smernice 2013/36/EÚ.

([69]) Pozri článok 41 ods. 1 navrhovaného nariadenia.

([70]) Pozri článok 25 ods. 3 a 4 navrhovaného nariadenia.

([71]) Pozri tiež článok 109 smernice o kapitálových požiadavkách.

([72]) Pozri článok 4 ods. 1 písm. e) nariadenia o JMD.

([73]) Pozri článok 85 smernice o kapitálových požiadavkách.

([74]) Nariadenie Európskej centrálnej banky (EÚ) č. 468/2014 zo 16. apríla 2014 o rámci pre spoluprácu v rámci jednotného mechanizmu dohľadu medzi Európskou centrálnou bankou, príslušnými vnútroštátnymi orgánmi a určenými vnútroštátnymi orgánmi (nariadenie o rámci JMD) (ECB/2014/17) (Ú. v. EÚ L 141, 14.5.2014, s. 1).

([75]) Konkrétne je kybernetický incident (identifikované možné narušenie informačnej bezpečnosti, či už zlomyseľné, alebo neúmyselné) potrebné oznámiť ECB, ak je splnená aspoň jedna z týchto podmienok: 1. hrozí potenciálny finančný vplyv vo výške 5 miliónov € alebo 0,1 % kapitálu CET1; 2. incident sa zverejní alebo spôsobí poškodenie dobrého mena; 3. incident bol postúpený vedúcemu pracovníkovi v oblasti IT mimo pravidelného oznamovania; 4. banka incident oznámila tímu CERT/CSIRT, bezpečnostnej agentúre alebo polícii; 5. spustili sa postupy na obnovu po havárii a kontinuitu činnosti alebo bol uplatnený nárok na vyplatenie kybernetického poistenia; 6. došlo k porušeniu právnych alebo regulačných požiadaviek; 7. banka použije interné kritériá a odborné posúdenie (vrátane možného systémového vplyvu) a rozhodne sa ECB informovať.

naďalej oznamovať incidenty príslušným vnútroštátnym orgánom, ktoré ich potom bez zbytočného odkladu postúpia ECB v mene dohliadaných subjektov. Spomínané rozhodnutia sú preto adresované aj príslušným vnútroštátnym orgánom, aby tieto informácie na základe rámca postúpili ECB. ECB podporuje úsilie legislatívnych orgánov Únie o presadzovanie harmonizácie a zjednodušenia okrem iného v súvislosti so súborom pravidiel a povinností týkajúcich sa hlásenia incidentov, ktoré sa vzťahujú na úverové inštitúcie. Vzhľadom na uvedené je ECB pripravená zmeniť (a prípadne zrušiť) rámec, ak to bude potrebné v súvislosti s prípadným prijatím navrhovaného nariadenia.

4. **Osobitné pripomienky k riadeniu IKT rizika, hláseniu incidentov, testovaniu prevádzkovej odolnosti a IKT riziku tretej strany**

4.1 *Riadenie IKT rizika*

4.1.1 ECB víta, že v navrhovanom nariadení sa zavádza spoľahlivý a komplexný rámec riadenia IKT rizika, ktorý zahŕňa usmernenia CPMI-IOSCO o kybernetickej odolnosti a ktorý je úzko zosúladený s osvedčenými postupmi vrátane dokumente Eurosystému s názvom Cyber Resilience Oversight Expectations for financial market infrastructures (očakávania týkajúce sa dohľadu v oblasti kybernetickej odolnosti pre infraštruktúry finančného trhu).

4.1.2 ECB podporuje myšlienku, že finančné subjekty by pri každej „rozsiahlej zmene“ infraštruktúry siete a informačných systémov museli vykonávať posúdenia rizík ([76]). Navrhované nariadenie však neobsahuje vymedzenie pojmu „rozsiahla zmena“, čo vytvára nevítaný priestor pre rozdielne výklady zo strany finančných subjektov, čo by v konečnom dôsledku mohlo brániť harmonizačným cieľom navrhovaného nariadenia. Legislatívne orgány Únie by v záujme zabezpečenia právnej istoty mohli chcieť zvážiť zahrnutie vymedzenia pojmu „rozsiahla zmena“ do navrhovaného nariadenia.

4.1.3 ECB vo všeobecnosti podporuje myšlienku, aby finančné subjekty iné než mikropodniky nahlasovali príslušným orgánom relevantné náklady a straty spôsobené narušeniami IKT a incidentmi súvisiacimi s IKT ([77]). S cieľom zabezpečiť celkovú efektívnosť systému a zabrániť možnosti preťaženia príslušných orgánov a finančných subjektov nadmerným počtom hlásení by však mohlo byť užitočné, ak by sa legislatívne orgány Únie zaoberali otázkou zavedenia príslušných prahových hodnôt, ktoré by mohli mať kvantitatívny charakter.

4.1.4 ECB uznáva možnosť, aby finančné subjekty po schválení príslušnými orgánmi delegovali úlohy overovania súladu s požiadavkami na riadenie IKT rizika na podniky vo vnútri skupiny alebo na externé podniky ([78]). Zároveň je dôležité, aby legislatívne orgány Únie objasnili spôsob schvaľovania príslušnými orgánmi v prípadoch, keď finančný subjekt podlieha viacerým príslušným orgánom. K tomu môže dôjsť, ak je finančný subjekt úverovou inštitúciou, poskytovateľom služieb kryptoaktív a/alebo poskytovateľom platobných služieb. ECB by napokon v súvislosti s identifikáciou a klasifikáciou, ktoré majú podľa navrhovaného nariadenia vykonávať finančné subjekty ([79]), na účely klasifikácie aktív považovala za obozretné, aby navrhované nariadenie tiež vyžadovalo, aby finančné subjekty zohľadňovali kritickosť takýchto aktív (t. j. či podporujú kritické funkcie).

4.2 *Nahlasovanie incidentov*

4.2.1 ECB víta úsilie opísané v navrhovanom nariadení, ktorého cieľom je harmonizovať nahlasovanie incidentov v oblasti IKT v rámci Únie a centralizovať nahlasovanie závažných incidentov súvisiacich s IKT ([80]). Zavedením harmonizovaného rámca na nahlasovanie závažných incidentov súvisiacich s IKT ([81]) relevantným príslušným orgánom by sa v zásade zjednotila a zosúladila záťaž finančných subjektov vrátane úverových inštitúcií spojená s hlásením. Pre príslušné orgány by bol prospešný širší rozsah zahrnutých incidentov presahujúci rámec incidentov súvisiacich s kybernetickou bezpečnosťou, na ktoré sa v súčasnosti vzťahujú existujúce rámce ([82]). Budúce prijatie navrhovaného nariadenia by si vyžadovalo posúdenie a prípadne zrušenie existujúcich rámcov vrátane rámca JMD pre oznamovanie kybernetických incidentov. V záujme dosiahnutia skutočného zjednotenia a úplného zosúladenia

([76]) Pozri článok 7 ods. 3 navrhovaného nariadenia.
([77]) Pozri článok 10 ods. 9 navrhovaného nariadenia.
([78]) Pozri článok 5 ods. 10 navrhovaného nariadenia.
([79]) Pozri článok 7 navrhovaného nariadenia.
([80]) Pozri článok 19 navrhovaného nariadenia.
([81]) Pozri článok 3 ods. 7 a články 17 a 18 navrhovaného nariadenia.
([82]) Pozri napríklad rámec.

vo všetkých rámcoch je však nevyhnutné zabezpečiť, aby rozsah pôsobnosti ustanovení o nahlasovaní incidentov podľa navrhovaného nariadenia vrátane vymedzení všetkých príslušných pojmov, prahových hodnôt a parametrov nahlasovania bol plne zosúladený s príslušnými rámcami. Predovšetkým je mimoriadne dôležité zabezpečiť súlad medzi navrhovaným nariadením na jednej strane a smernicou Európskeho parlamentu a Rady (EÚ) 2015/2366 ([83]) (ďalej len „druhá smernica o platobných službách“) a usmerneniami EBA k oznamovaniu závažných incidentov (ďalej len „usmernenia EBA“) na strane druhej. Navrhovaná pozmeňujúca smernica ([84]) obsahuje zmeny druhej smernice o platobných službách v súvislosti s rozdelením oznamovania (nahlasovania) incidentov medzi navrhovaným nariadením a druhou smernicou o platobných službách, pričom tieto zmeny by mali vplyv najmä na poskytovateľov platobných služieb, ktorým by sa mohlo udeliť povolenie aj ako úverovým inštitúciám, ako aj na príslušné orgány. Postup oznamovania incidentov nie je dostatočne jasný a niektoré povinnosti nahlasovania incidentov, ktoré je potrebné nahlásiť podľa navrhovaného nariadenia aj podľa usmernení EBA, sa môžu prekrývať.

4.2.2 Postupy oznamovania závažných incidentov podľa navrhovaného nariadenia ([85]), druhej smernice o platobných službách a zodpovedajúcich usmernení EBA by od poskytovateľov platobných služieb vyžadovali, aby svojmu príslušnému orgánu predložili správu o incidente po jeho klasifikácii. V pôvodných správach v skutočnosti nie je zachytená podstata a príčina incidentu ani funkčná oblasť, na ktorú mal incident vplyv, a poskytovatelia platobných služieb môžu byť schopní takéto rozlíšenie vykonať až v neskoršej fáze, keď sú k dispozícii podrobnejšie informácie o incidente. V dôsledku toho by sa pôvodné správy o incidentoch mohli predkladať tak podľa navrhovaného nariadenia, ako aj podľa usmernení EBA, alebo si poskytovatelia platobných služieb môžu vybrať jeden rámec pre oznamovanie a predložené správy opraviť neskôr. Rovnaká neistota (napríklad pokiaľ ide o hlavnú príčinu incidentu) sa môže odraziť aj v priebežných a záverečných správach. Tým by sa opäť zvýšila možnosť súbežného predkladania správ príslušným orgánom podľa navrhovaného nariadenia a druhej smernice o platobných službách.

4.2.3 Niektoré incidenty, ktoré možno kategorizovať ako incidenty súvisiace s IKT, môžu mať vplyv aj na iné oblasti, a preto by sa museli oznamovať podľa usmernení EBA. Môže k tomu dôjsť v prípade, keď má incident vplyv z hľadiska IKT, ale zároveň priamo ovplyvnil aj poskytovanie platobných služieb a/alebo iné funkčné oblasti alebo kanály, ktoré sa netýkajú IKT. Okrem toho by sa mohli vyskytnúť prípady, v ktorých nie je možné rozlíšiť prevádzkové incidenty a incidenty súvisiace s IKT. V prípade, že finančný subjekt je zároveň významnou úverovou inštitúciou a poskytovateľom platobných služieb, by okrem toho podľa navrhovaného nariadenia musel incident súvisiaci s IKT nahlásiť dvakrát, pretože by podliehal dvom príslušným orgánom. Vzhľadom na uvedené by sa v navrhovanom nariadení malo jasnejšie vymedziť, ako má interakcia medzi druhou smernicou o platobných službách a usmerneniami EBA fungovať v praxi. Podstatnejšie je, že v záujme zosúladenia a zjednotenia ohlasovacích povinností by bolo dôležité, aby legislatívne orgány Únie zvážili zostávajúce otázky vyplývajúce z dvojitého nahlasovania a aby objasnili, či by navrhované nariadenie na jednej strane a druhá smernica o platobných službách a usmernenia EBA na strane druhej existovali súčasne, alebo by mal existovať jednotný súbor požiadaviek na nahlasovanie incidentov.

4.2.4. Navrhované nariadenie pre príslušné orgány zavádza požiadavku ([86]), aby po prijatí správy potvrdili prijatie oznámenia a čo najskôr poskytli všetku potrebnú spätnú väzbu alebo usmernenia finančnému subjektu, najmä s cieľom prediskutovať nápravné opatrenia na úrovni subjektu alebo spôsoby minimalizovania nepriaznivého vplyvu v jednotlivých sektoroch. To by znamenalo, že príslušné orgány by mali aktívne prispievať k riadeniu a náprave incidentov a zároveň posudzovať reakciu dohliadaného subjektu na kritické incidenty. ECB zdôrazňuje, že zodpovednosť za nápravu, ako aj zodpovednosť za dôsledky incidentu by mali zostať výlučne a jednoznačne na príslušnom finančnom subjekte. ECB preto navrhuje obmedziť spätnú väzbu a usmernenia len na prudenciálnu spätnú väzbu a usmernenia na vysokej úrovni. Ak by bola spätná väzba širšia, vyžadovala by si špecializovaných odborníkov s veľmi veľkými technickými znalosťami, akými odborníci orgánov prudenciálneho dohľadu zvyčajne nedisponujú.

4.3 *Testovanie digitálnej prevádzkovej odolnosti*

4.3.1 ECB víta požiadavky stanovené v navrhovanom nariadení ([87]) týkajúce sa testovania digitálnej prevádzkovej odolnosti vo všetkých finančných subjektoch a toho, že každá inštitúcia musí mať vlastný program na testovanie. V navrhovanom nariadení ([88]) sa uvádzajú rôzne typy testov pre finančné subjekty. Tieto typy testov nie sú veľmi jasné a niektoré testy, ako sú testy kompatibility, dotazníky alebo testy založené na konkrétnych scenároch, si môžu

([83]) Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES (Ú. v. EÚ L 337, 23.12.2015, s. 35).

([84]) Pozri článok 7 ods. 9 navrhovanej pozmeňujúcej smernice.

([85]) Pozri článok 17 ods. 3 navrhovaného nariadenia.

([86]) Pozri článok 20 navrhovaného nariadenia.

([87]) Pozri články 21 a 22 navrhovaného nariadenia.

([88]) Pozri článok 22 ods. 1 navrhovaného nariadenia.

európske orgány dohľadu, príslušné orgány alebo finančné subjekty rôzne vyložiť. Okrem toho navrhované nariadenie neobsahuje ani usmernenie týkajúce sa frekvencie uskutočňovania jednotlivých testov. Možným prístupom by mohlo byť, že v navrhovanom nariadení by sa stanovili všeobecné požiadavky na testovanie, pričom presnejší opis typov testov by sa uviedol v regulačných a vykonávacích technických predpisoch.

4.3.2 Penetračné testovanie na základe konkrétnej hrozby (threat-led penetration testing – TLPT) je účinným nástrojom na testovanie bezpečnostných obranných mechanizmov a pripravenosti. ECB preto podporuje finančné subjekty v používaní nástroja TLPT. Pomocou tohto nástroja sa testujú nielen technické opatrenia, ale aj zamestnanci a postupy. Výsledky týchto testov môžu výrazne zvýšiť informovanosť vrcholového manažmentu testovaných subjektov o bezpečnosti. Európsky rámec TIBER-EU (European framework for Threat Intelligence Based Ethical Red-teaming) ([89]) a ďalšie nástroje TLPT, ktoré sú už k dispozícii mimo Únie, sú pre samotné subjekty hlavnými nástrojmi na posudzovanie, testovanie, uplatňovanie a zlepšovanie si pozície a obranných mechanizmov, pokiaľ ide o kybernetickú odolnosť.

4.3.3 Vo väčšine členských štátov, v ktorých je zavedený rámec TIBER-EU, orgány dozoru a dohľadu nezohrávajú aktívnu úlohu pri vykonávaní miestneho programu TIBER-XX a TIBER Cyber Team je takmer vo všetkých prípadoch umiestnený nezávisle od týchto funkcií. Z tohto dôvodu by sa pokročilé testovanie podľa navrhovaného nariadenia ([90]) prostredníctvom nástroja TLPT malo vykonávať ako nástroj na posilnenie finančného ekosystému a zvýšenie finančnej stability, a nie ako nástroj slúžiaci výlučne na účely dohľadu. Okrem toho nie je potrebné vypracovať nový rámec na pokročilé testovanie kybernetickej odolnosti, keďže členské štáty už vo veľkej miere prijali rámec TIBER-EU – jediný takýto rámec, ktorý v EÚ v súčasnosti existuje.

4.3.4 Požiadavky na testovacie subjekty by nemali byť obsiahnuté v hlavnej časti navrhovaného nariadenia, keďže sektor súvisiaci s nástrojom TLPT sa stále vyvíja a zavedenie osobitných požiadaviek môže brzdiť inovácie. ECB však zastáva názor, že s cieľom zabezpečiť vysoký stupeň nezávislosti pri vykonávaní testov by finančné subjekty nemali zamestnávať ani najímať testovacie subjekty, ktoré zamestnávajú alebo najímajú finančné subjekty v ich skupine alebo ktoré inak vlastnia alebo riadia finančné subjekty, ktoré sa majú testovať.

4.3.5 V navrhovanom nariadení by sa s cieľom znížiť riziko fragmentácie a zabezpečiť harmonizáciu mal stanoviť jeden rámec TLPT, ktorý sa bude vzťahovať na finančný sektor v celej Únii. Fragmentácia môže viesť k zvýšeniu nákladov a požiadaviek na technické, prevádzkové a finančné zdroje tak pre príslušné orgány, ako aj pre finančné inštitúcie. Tieto zvýšené náklady a požiadavky môžu mať v konečnom dôsledku negatívny vplyv na vzájomné uznávanie testov. Táto nedostatočná harmonizácia a výsledné problémy so vzájomným uznávaním sú mimoriadne dôležité pre finančné subjekty, ktoré môžu mať viaceré licencie a/alebo pôsobiť vo viacerých jurisdikciách Únie. Regulačné a vykonávacie technické predpisy, ktorých návrh sa podľa navrhovaného nariadenia má vypracovať pre nástroj TLPT, by mali byť v súlade s rámcom TIBER-EU. ECB okrem toho víta príležitosť zapojiť sa do prípravy týchto regulačných a vykonávacích technických predpisov v spolupráci s európskymi orgánmi dohľadu.

4.3.6 Aktívne zapojenie príslušných orgánov do testovania by mohlo viesť k potenciálnemu konfliktu záujmov s inou funkciou, ktorú vykonávajú, t. j. s posudzovaním testovacieho rámca finančného subjektu. V tejto súvislosti ECB navrhuje, aby sa z navrhovaného nariadenia odstránila akákoľvek povinnosť príslušných orgánov, pokiaľ ide o overovanie dokumentov a vydávanie osvedčenia o teste TLPT.

4.4 IKT riziko tretej strany

4.4.1 ECB víta zavedenie komplexného súboru kľúčových zásad a spoľahlivého rámca dozoru na identifikáciu a riadenie IKT rizík pochádzajúcich od externých poskytovateľov IKT služieb bez ohľadu na to, či patria do rovnakej skupiny finančných subjektov. S cieľom dosiahnuť účinnú identifikáciu a riadenie IKT rizík je však dôležité správne identifikovať a klasifikovať okrem iného externých poskytovateľov kritických IKT služieb. V tejto súvislosti je vítané zavádzanie delegovaných aktov ([91]), ktoré doplnia kritériá, ktoré sa majú použiť na účely klasifikácie ([92]), pred prijatím takýchto delegovaných aktov by sa však mali uskutočniť konzultácie s ECB.

([89]) Dostupné na webovom sídle ECB www.ecb.europa.eu.
([90]) Články 23 a 24 navrhovaného nariadenia.
([91]) Pozri článok 28 ods. 3 navrhovaného nariadenia.
([92]) Pozri článok 28 ods. 2 navrhovaného nariadenia.

4.4.2 Pokiaľ ide o štruktúru rámca dozoru ([93]), je potrebné bližšie objasnenie v súvislosti s úlohou, ktorú má vykonávať spoločný výbor. ECB zároveň víta svoje zaradenie do fóra pre dozor v pozícii pozorovateľa, keďže táto úloha poskytne ECB rovnaký prístup k dokumentácii a informáciám, ako majú členovia s hlasovacím právom ([94]). ECB by chcela upriamiť pozornosť legislatívnych orgánov Únie na to, že vo svojej úlohe pozorovateľa by k práci fóra pre dozor prispievala tak v rámci svojej pozície emisnej centrálnej banky so zodpovednosťou za dohľad nad trhovými infraštruktúrami, ako aj ako orgán prudenciálneho dohľadu nad úverovými inštitúciami. ECB okrem toho poznamenáva, že okrem úlohy pozorovateľa v rámci fóra pre dozor by ECB ako príslušný orgán bola tiež súčasťou spoločného prieskumného tímu. V tejto súvislosti by sa legislatívne orgány Únie mohli ďalej zaoberať zložením spoločných prieskumných tímov ([95]), aby sa zabezpečila primeraná miera zapojenia relevantných príslušných orgánov. Z rovnakého dôvodu sa ECB domnieva, že maximálny počet účastníkov spoločných prieskumných tímov by sa mal zvýšiť vzhľadom na kritickosť, zložitosť a rozsah externých IKT služieb.

4.4.3 ECB poznamenáva, že podľa navrhovaného nariadenia môže hlavný orgán dozoru zabrániť externým poskytovateľom kritických IKT služieb uzatvárať ďalšie subdodávateľské dohody, ak i) plánovaný subdodávateľ je externým poskytovateľom IKT služieb alebo subdodávateľom IKT usadeným v tretej krajine a ii) zadávanie zákaziek subdodávateľom sa týka kritickej alebo dôležitej funkcie finančného subjektu. ECB by chcela zdôrazniť, že tieto právomoci môže hlavný orgán dozoru uplatniť len v kontexte subdodávateľských dohôd v prípade, že externý poskytovateľ kritických IKT služieb zadá kritickú alebo dôležitú funkciu subdodávateľovi, ktorý je samostatnou právnickou osobou usadenou v tretej krajine. ECB vychádza z toho, že hlavný orgán dozoru by nemohol uplatniť porovnateľné právomoci, aby zabránil externému poskytovateľovi kritických IKT služieb externe zabezpečovať kritické alebo dôležité funkcie finančného subjektu v zariadeniach tohto poskytovateľa služieb, ktoré sa nachádzajú v tretej krajine. Mohlo by sa napríklad stať, že z prevádzkového hľadiska môžu kritické údaje a/alebo informácie uchovávať alebo spracúvať zariadenia nachádzajúce sa mimo Európskeho hospodárskeho priestoru (EHP). V takom prípade právomoci hlavného orgánu dozoru nemusia príslušné orgány primerane oprávňovať na prístup ku všetkým informáciám, priestorom, infraštruktúram a zamestnancom relevantným pre vykonávanie všetkých kritických alebo dôležitých funkcií finančného subjektu. S cieľom zabezpečiť, aby príslušné orgány mohli bez prekážok plniť svoje úlohy, ECB navrhuje zveriť hlavnému orgánu dozoru právomoc obmedziť aj používanie zariadení umiestnených mimo EHP externými poskytovateľmi kritických IKT služieb. Táto právomoc by sa mohla uplatňovať v tých osobitných prípadoch, keď nie sú zavedené administratívne dojednania s relevantnými orgánmi tretích krajín, ako sa stanovuje v navrhovanom nariadení ([96]), alebo keď zástupcovia externých poskytovateľov kritických IKT služieb neposkytnú dostatočné záruky podľa rámca príslušnej tretej krajiny, pokiaľ ide o prístup k informáciám, priestorom, infraštruktúram a zamestnancom, ktorý je potrebný na plnenie úloh dozoru alebo dohľadu.

4.4.4 Napokon, existuje riziko, že požiadavka, aby príslušné orgány prijali následné opatrenia podľa odporúčaní hlavného orgánu dozoru ([97]), by sa mohla ukázať ako neúčinná, keďže príslušné orgány nemusia mať celistvý prehľad o rizikách, ktoré vytvárajú jednotliví externí poskytovatelia kritických IKT služieb. Okrem toho sa od príslušných orgánov môže vyžadovať, aby prijali opatrenia proti finančným subjektom, nad ktorými vykonávajú dohľad, ak externí poskytovatelia kritických IKT služieb nedodržia odporúčania. Podľa navrhovaného nariadenia ([98]) môžu príslušné orgány od finančných subjektov, nad ktorými vykonávajú dohľad, požadovať, aby dočasne pozastavili používanie služby externého poskytovateľa kritických služieb alebo aby ukončili zostávajúce zmluvy s externými poskytovateľmi kritických služieb. Predpokladané následné opatrenia je ťažké premietnuť do konkrétnych krokov. Konkrétne nie je jasné, či bude dohliadaný finančný subjekt schopný pozastaviť alebo ukončiť zmluvu s externým poskytovateľom kritických služieb. Je tomu tak preto, že externý poskytovateľ kritických IKT služieb by pre daný finančný subjekt mohol byť významným poskytovateľom alebo by s tým mohli byť spojené náklady a náhrady škôd – či už vyplývajúce zo zmluvy, alebo iné –, ktoré môžu finančnému subjektu vzniknúť v dôsledku takéhoto pozastavenia alebo ukončenia. Tento prístup navyše nepodporuje konvergenciu dozoru, keďže príslušné orgány môžu to isté odporúčanie vykladať rozdielnym spôsobom. To by v konečnom dôsledku mohlo prekážať v plánovanej harmonizácii a konzistentnom prístupe k monitorovaniu kritického IKT rizika tretej strany na úrovni Únie. Vzhľadom na uvedené skutočnosti by legislatívne orgány Únie mohli zvážiť, či zákonným orgánom dohľadu udelia osobitné právomocí v oblasti presadzovania práva vo vzťahu k externým poskytovateľom kritických IKT služieb s prihliadnutím na obmedzenia stanovené v Meroniho doktríne, ktoré čiastočne zmiernil Súdny dvor vo svojom rozsudku vo veci ESMA ([99]).

([93]) Pozri článok 29 navrhovaného nariadenia.
([94]) Pozri článok 29 ods. 3 navrhovaného nariadenia.
([95]) Pozri článok 35 navrhovaného nariadenia.
([96]) Pozri článok 39 ods. 1 navrhovaného nariadenia.
([97]) Pozri článok 29 ods. 4 a článok 37 navrhovaného nariadenia.
([98]) Pozri článok 37 ods. 3 navrhovaného nariadenia.
([99]) Pozri rozsudok Súdneho dvora (veľká komora) z 22. januára 2014, Spojené kráľovstvo Veľkej Británie a Severného Írska/Európsky parlament a Rada Európskej únie, nariadenie (EÚ) č. 236/2012 — vec C-270/12.

V prípadoch, kde ECB odporúča zmenu navrhovaného nariadenia, navrhované znenie príslušných zmien je uvedené spolu s odôvodnením v osobitnom technickom pracovnom dokumente. Technický pracovný dokument je dostupný v anglickom jazyku na webových stránkach EUR-Lex.

Vo Frankfurte nad Mohanom 4. júna 2021.

Prezidentka ECB
Christine LAGARDE