Europski parlament
2019-2024

Dokument s plenarne sjednice

A9-0341/2021

7.12.2021

***I
IZVJEŠĆE

o Prijedlogu uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

Odbor za ekonomsku i monetarnu politiku

Izvjestitelj: Billy Kelleher

Oznake postupaka

*	Postupak savjetovanja
***	Postupak suglasnosti
***I	Redovni zakonodavni postupak (prvo čitanje)
***II	Redovni zakonodavni postupak (drugo čitanje)
***III	Redovni zakonodavni postupak (treće čitanje)

(Navedeni se postupak temelji na pravnoj osnovi predloženoj u nacrtu akta.)

Izmjene nacrta akta

Amandmani Parlamenta u obliku dvaju stupaca

Brisanja su označena ***podebljanim kurzivom*** u lijevom stupcu. Izmjene su označene ***podebljanim kurzivom*** u obama stupcima. Novi tekst označen je ***podebljanim kurzivom*** u desnom stupcu.

U prvom i drugom retku zaglavlja svakog amandmana naznačen je predmetni odlomak iz nacrta akta koji se razmatra. Ako se amandman odnosi na postojeći akt koji se želi izmijeniti nacrtom akta, zaglavlje sadrži i treći redak u kojem se navodi postojeći akt te četvrti redak u kojem se navodi odredba akta na koju se izmjena odnosi.

Amandmani Parlamenta u obliku pročišćenog teksta

Novi dijelovi teksta označuju se ***podebljanim kurzivom***. Brisani dijelovi teksta označuju se oznakom ▌ ili su precrtani. Izmjene se naznačuju tako da se novi tekst označi ***podebljanim kurzivom***, a da se zamijenjeni tekst izbriše ili precrta.
Iznimno, izmjene strogo tehničke prirode koje unesu nadležne službe prilikom izrade konačnog teksta ne označuju se.

SADRŽAJ

Stranica

NACRT ZAKONODAVNE REZOLUCIJE EUROPSKOG PARLAMENTA

o Prijedlogu uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

(Redovni zakonodavni postupak: prvo čitanje)

Europski parlament,

– uzimajući u obzir Prijedlog Komisije upućen Europskom parlamentu i Vijeću (COM(2020)0595),

– uzimajući u obzir članak 294. stavak 2. i članak 114. Ugovora o funkcioniranju Europske unije, u skladu s kojima je Komisija podnijela Prijedlog Parlamentu (C9-0304/2020),

– uzimajući u obzir članak 294. stavak 3. Ugovora o funkcioniranju Europske unije,

– uzimajući u obzir mišljenje Europskog gospodarskog i socijalnog odbora od 24. veljače 2021.[1],

– uzimajući u obzir članak 59. Poslovnika,

– uzimajući u obzir izvješće Odbora za ekonomsku i monetarnu politiku (A9-0341/2021),

1. usvaja sljedeće stajalište u prvom čitanju;

2. poziva Komisiju da predmet ponovno uputi Parlamentu ako zamijeni, bitno izmijeni ili namjerava bitno izmijeniti svoj Prijedlog;

3. nalaže svojem predsjedniku da stajalište Parlamenta proslijedi Vijeću, Komisiji i nacionalnim parlamentima.

Amandman 1

AMANDMANI EUROPSKOG PARLAMENTA[*]

na Prijedlog Komisije

[1] SL C 155, 30.4.2021., str. 38.

[*] Amandmani: novi ili izmijenjeni tekst označava se podebljanim kurzivom, a brisani tekst oznakom ▌.

2020/0266(COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014

(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europske središnje banke[2],

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora[3],

u skladu s redovnim zakonodavnim postupkom,

budući da:

(1) U digitalnom dobu informacijska i komunikacijska tehnologija (IKT) podržava složene sustave koji se upotrebljavaju za svakodnevne društvene aktivnosti. Zaslužna je za funkcioniranje naših gospodarstava u ključnim sektorima, uključujući financije, i bolje funkcioniranje jedinstvenog tržišta. Sve veća digitalizacija i međusobna povezanost povećavaju i IKT rizike, zbog čega je društvo u cjelini, a posebno financijski sustav, osjetljivije na kiberprijetnje ili poremećaje u radu IKT-a. Iako su sveprisutna primjena sustava IKT-a i visok stupanj digitalizacije i povezanosti u današnje vrijeme ključne značajke svih aktivnosti financijskih subjekata u Uniji, digitalna otpornost ***tek treba biti*** u dovoljnoj mjeri ugrađena u njihove operativne okvire.

(2) U proteklim desetljećima primjena IKT-a dobila je središnju funkciju u financijama i u današnje je vrijeme od ključne važnosti za svakodnevno poslovanje svih financijskih subjekata. Digitalizacija obuhvaća primjerice plaćanja, čiji se gotovinski ili papirnati oblik sve više zamjenjuje digitalnim rješenjima, te poravnanje i namiru vrijednosnih papira, elektroničko i algoritamsko trgovanje, poslove kreditiranja i financiranja, uzajamno kreditiranje, kreditni rejting, ▌ upravljanje potraživanjima i poslove pozadinskih ureda. ***Primjena IKT-a promijenila je i sektor osiguranja, od pojave digitalnih posrednika u osiguranju koji rade s tehnologijama osiguranja do digitalnog preuzimanja rizika u osiguranju i distribucije ugovora.*** Ne samo da su financije postale uglavnom digitalne u cijelom sektoru, nego je digitalizacija produbila

[2] [*dodati upućivanje*] SL C , , str. .
[3] SL C 155, 30.4.2021., str. 38.

i međusobnu povezanost i ovisnost unutar financijskog sektora te s infrastrukturom treće strane i trećim stranama pružateljima usluga.

(3) U izvješću o sistemskom kiberriziku iz 2020.[4] Europski odbor za sistemske rizike (ESRB) potvrdio je da bi postojeći visoki stupanj međusobne povezanosti financijskih subjekata, financijskih tržišta i infrastruktura financijskog tržišta, a osobito međusobna ovisnost njihovih sustava IKT-a, mogao biti sistemska ranjivost jer bi se kiberincidenti mogli brzo proširiti iz bilo kojeg od oko 22 000 financijskih subjekata u Uniji[5] na cijeli financijski sustav, neovisno o zemljopisnim granicama. Ozbiljni IKT napadi u području financija ne utječu samo na izolirane financijske subjekte, već olakšavaju i širenje lokaliziranih ranjivosti po svim kanalima financijskog prijenosa i mogli bi negativno utjecati na stabilnost financijskog sustava Unije, uzrokovati pad likvidnosti i opći gubitak povjerenja i pouzdanja u financijska tržišta.

(4) U proteklih nekoliko godina IKT rizici privukli su pozornost nacionalnih, europskih i međunarodnih oblikovatelja politika, regulatornih tijela i tijela za normizaciju koji su pokušali poboljšati otpornost, utvrditi standarde i koordinirati regulatorne ili nadzorne postupke. Na međunarodnoj razini cilj je Bazelskog odbora za nadzor banaka, Odbora za platne i tržišne infrastrukture, Odbora za financijsku stabilnost, Instituta za financijsku stabilnost te zemalja članica skupina G7 i G20 pružiti nadležnim tijelima i tržišnim operaterima u različitim jurisdikcijama alate za poboljšanje otpornosti njihovih financijskih sustava. ***Stoga IKT rizik treba razmotriti u kontekstu međusobno izrazito povezanog globalnog financijskog sustava u kojem prednost treba dati dosljednosti međunarodnih propisa i suradnji među nadležnim tijelima na globalnoj razini.***

(5) Usprkos nacionalnim i europskim ciljanim politikama i zakonodavnim inicijativama IKT rizici i dalje su problem za operativnu otpornost, učinkovitost i stabilnost financijskog sustava Unije. Reformom koja je uslijedila nakon financijske krize 2008. prvenstveno je povećana financijska otpornost financijskog sektora Unije i bila je usmjerena na zaštitu konkurentnosti i stabilnosti Unije u kontekstu gospodarstva, boniteta i ponašanja na tržištu. Iako su sigurnost IKT-a i digitalna otpornost dio operativnog rizika, u regulatornim planovima nakon krize nije im posvećena prevelika pozornost pa su se razvile samo u nekim područjima Unijina političkog i regulatornog okruženja za financijske usluge ili samo u nekoliko država članica.

(6) U Komisijinu Akcijskom planu za financijske tehnologije iz 2018.[6] istaknuto je da je jačanje otpornosti financijskog sektora Unije od ključne važnosti i u operativnom

---

4 Izvješće ESRB-a Systemic Cyber Risk (Sistemski kiberrizik) iz veljače 2020.; https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

5 Prema procjeni učinka priloženoj preispitivanju koje su provela europska nadzorna tijela (SWD(2017) 308) postoji oko 5 665 kreditnih institucija, 5 934 investicijska društva, 2 666 društava za osiguranje, 1 573 institucije za strukovno mirovinsko osiguranje, 2 500 društava za upravljanje ulaganjima, 350 tržišnih infrastruktura (kao što su središnje druge ugovorne strane, burze, sistematski internalizatori, trgovinski repozitoriji i multilateralne trgovinske platforme), 45 agencija za kreditni rejting i 2 500 institucija za platni promet i institucija za elektronički novac s odobrenjem za rad. To je ukupno oko 21 233 subjekta bez subjekata za skupno financiranje, ovlaštenih revizora i revizorskih društava, pružatelja usluga povezanih s kriptoimovinom i administratora referentnih vrijednosti.

6 Komunikacija Komisije Europskom parlamentu, Vijeću, Europskoj središnjoj banci, Europskom gospodarskom i socijalnom odboru i Odboru regija, Akcijski plan za financijske tehnologije: za konkurentniji i inovativniji europski financijski sektor, COM/2018/0109 final; https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

smislu kako bi se osigurali njegova tehnološka sigurnost i dobro funkcioniranje, brz oporavak od IKT napada i incidenata, a time u konačnici omogućilo učinkovito i neometano pružanje financijskih usluga u cijeloj Uniji, među ostalim u stresnim okolnostima, uz istodobno očuvanje povjerenja i pouzdanja potrošača i tržišta.

(7) U travnju 2019. Europsko nadzorno tijelo za bankarstvo (EBA), Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala (ESMA) i Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje (EIOPA) (zajedno „europska nadzorna tijela”) zajedno su izdala dva tehnička savjeta u kojima su pozvali na dosljedan pristup IKT rizicima u financijskom sektoru te preporučila proporcionalno jačanje digitalne operativne otpornosti sektora financijskih usluga u okviru Unijine sektorske inicijative.

(8) Financijski sektor Unije uređen je usklađenim jedinstvenim pravilima i Europskim sustavom financijskog nadzora. Unatoč tome, odredbe o digitalnoj operativnoj otpornosti i sigurnosti IKT-a još nisu potpuno i dosljedno usklađene iako je digitalna otpornost ključna za financijsku stabilnost i integritet tržišta u digitalnom dobu i nije manje važna od, primjerice, zajedničkih bonitetnih standarda ili standarda ponašanja na tržištu. Jedinstvenim pravilima i sustavom nadzora stoga bi trebalo obuhvati i tu komponentu, i to ***jačanjem*** ovlasti financijskih nadzornih tijela ***za upravljanje IKT rizicima u financijskom sektoru, zaštitu*** integriteta i ***učinkovitosti jedinstvenog*** tržišta ***te olakšavanje njegova urednog funkcioniranja***.

(9) Zakonodavne neusklađenosti i neujednačeni nacionalni regulatorni ili nadzorni pristupi IKT rizicima prepreka su jedinstvenom tržištu za financijske usluge i onemogućavaju neometano ostvarivanje slobode poslovnog nastana i pružanja usluga za financijske subjekte koji posluju prekogranično. Moglo bi se narušiti i tržišno natjecanja među financijskim subjektima iste vrste koji posluju u različitim državama članicama. Osobito u područjima u kojima je usklađenost na razini Unije vrlo ograničena, kao što je testiranje digitalne operativne otpornosti, ili ne postoji, na primjer u području praćenja IKT rizika treće strane, neusklađenosti koje proizlaze iz predviđenih razvojnih promjena na nacionalnoj razini mogle bi stvoriti dodatne prepreke funkcioniranju jedinstvenog tržišta na štetu sudionika na tržištu i financijske stabilnosti.

(10) Dosadašnje djelomično razmatranje odredbi o IKT rizicima na razini Unije uzrokovalo je praznine ili preklapanja u važnim područjima kao što je izvješćivanje o IKT incidentima i testiranje digitalne operativne otpornosti i nedosljednosti zbog novih različitih nacionalnih pravila ili troškovno neisplative primjene preklapajućih pravila. To osobito šteti korisnicima koji intenzivno upotrebljavaju IKT, primjerice financijskom sektoru, jer tehnološki rizici ne poznaju granice, a financijski sektor pruža prekogranične usluge unutar i izvan Unije.

Pojedini financijski subjekti koji posluju prekogranično ili imaju nekoliko odobrenja za rad (npr. jedan financijski subjekt može imati odobrenje za rad kao banka, investicijsko društvo i institucija za platni promet, pri čemu svako od tih odobrenja izdaje drugo nadležno tijelo u jednoj ili više država članica) izloženi su operativnim rizicima pri samostalnom i dosljednom troškovno isplativom uklanjanju IKT rizika i ublažavanju negativnih učinaka IKT incidenata.

(10a) Uspostavljanje i održavanje odgovarajućih infrastruktura mrežnih i informacijskih sustava isto je tako temeljni preduvjet za učinkovito objedinjavanje podataka o

riziku i prakse izvješćivanja o riziku koji su ključan uvjet za postupke stabilnog i održivog upravljanja rizikom i donošenja odluka o riziku koje provode kreditne institucije. Bazelski odbor za nadzor banaka (BCBS) objavio je 2013. skup načela učinkovitog objedinjavanja podataka o riziku i izvješćivanja o riziku („BCBS 239”) koja se temelje na dvama sveobuhvatnim načelima upravljanja i IT infrastrukture te koji su se trebali provesti početkom 2016. Prema Izvješću Europske središnje banke (ESB) o tematskom pregledu iz svibnja 2018. o učinkovitom objedinjavanju podataka o riziku i izvješćivanju o riziku i Izvješću Bazelskog odbora za nadzor banaka o napretku iz travnja 2020. globalne sistemski važne banke nisu postigle zadovoljavajući napredak u pogledu uvođenja tih načela. što je predstavljalo razlog za zabrinutost. Kako bi se omogućila sukladnost i usklađenost s međunarodnim standardima, Komisija bi, u bliskoj suradnji s ESB-om i nakon savjetovanja s EBA-om i ESRB-om, trebala izraditi izvješće u svrhu procjene međudjelovanja načela BCBS 239 s odredbama ove Uredbe i, prema potrebi, procjene načina na koji bi ta načela trebalo uključiti u pravo Unije.

(11) Budući da jedinstvena pravila nisu popraćena sveobuhvatnim okvirom za IKT ili operativne rizike, nužno je dodatno uskladiti najvažnije zahtjeve digitalne operativne otpornosti za sve financijske subjekte. Kapaciteti i sveukupna otpornost koju bi financijski subjekti na temelju tih najvažnijih zahtjeva razvili radi otpornosti na prekide u radu pridonijeli bi očuvanju stabilnosti i integriteta financijskih tržišta Unije, a time i visokom stupnju zaštite ulagatelja i potrošača u Uniji. Budući da joj je cilj poboljšanje neometanog funkcioniranja jedinstvenog tržišta, ova bi se Uredba trebala temeljiti na odredbama članka 114. UFEU-a kako se tumači u skladu s dosljednom sudskom praksom Suda Europske unije.

(12) Prvi je cilj ove Uredbe konsolidacija i nadogradnja zahtjeva za IKT rizike koji su dosad obrađeni zasebno u raznim uredbama i direktivama. Iako su tim pravnim aktima Unije obuhvaćene glavne kategorije financijskih rizika (npr. kreditni rizik, tržišni rizik, rizik druge ugovorne strane i rizik likvidnosti, rizik ponašanja na tržištu), u vrijeme njihova donošenja nisu sveobuhvatno obrađene sve komponente operativne otpornosti. Zahtjevi za operativne rizike, dodatno razrađeni u tim pravnim aktima Unije, često su se temeljili na tradicionalnom kvantitativnom pristupu ublažavanju rizika (primjerice određivanjem kapitalnog zahtjeva za pokrivanje IKT rizika), ali bez ciljanih kvalitativnih zahtjeva u cilju poboljšanja kapaciteta za zaštitu, otkrivanje, ograničenje, oporavak i popravak u slučaju IKT incidenata ili izgradnju kapaciteta za izvješćivanje i digitalno testiranje. Tim direktivama i uredbama prvenstveno su se trebala obuhvatiti temeljna pravila o bonitetnom nadzoru, integritetu tržišta i ponašanju na tržištu.

Ovim aktom, kojim se konsolidiraju i ažuriraju pravila o IKT rizicima, prvi put će se dosljedno, u jednom zakonodavnom aktu objediniti sve odredbe o digitalnim rizicima u financijama. Ova bi inicijativa stoga trebala popuniti praznine i ukloniti nedosljednosti u nekim od tih pravnih akata, među ostalim u terminološkom smislu, i izravno obraditi IKT rizike ciljanim pravilima o kapacitetima za upravljanje IKT rizicima, izvješćivanje i testiranje te praćenje rizika trećih strana. ***Ovom se inicijativom također nastoji podići svijest o IKT rizicima te se ističe da bi IKT incidenti i nedostatak operativne otpornosti mogli ugroziti financijsku stabilnost financijskih subjekata.***

(13) Pri ublažavanju IKT rizika ***ovisno o njihovoj veličini, prirodi, složenosti i profilu***

rizičnosti financijski subjekti trebali bi slijediti isti pristup i ista pravila koja se temelje na načelima. Dosljednost pridonosi povećanju povjerenja u financijski sustav te očuvanju njegove stabilnosti, osobito u slučaju ***izrazitog oslanjanja na sustave, platforme i infrastrukture*** IKT-a, ***što*** podrazumijeva sve veći digitalni rizik.

Osnovnom kiberhigijenom trebalo bi izbjeći i velike troškove za gospodarstvo smanjenjem učinka i troškova poremećaja u radu IKT-a.

(14) Uredbom se pridonosi smanjenju regulatorne složenosti, promiče se konvergencija nadzora, povećava pravna sigurnost i istodobno pridonosi ograničavanju troškova usklađivanja, osobito financijskih subjekata koji posluju prekogranično, te smanjenju narušavanja tržišnog natjecanja. Uredbom o uspostavljanju zajedničkog okvira za digitalnu operativnu otpornost financijskih subjekata najbolje bi se zajamčila ujednačena i dosljedna primjena svih komponenti upravljanja IKT rizicima u financijskim sektorima Unije.

(14a) Međutim, provedba ove Uredbe ne bi smjela ometati inovacije u načinu na koji financijski subjekti rješavaju pitanja digitalne operativne otpornosti uz poštovanje njezinih odredbi niti u pogledu usluga koje nude oni ili treće strane pružatelji IKT usluga.

(15) Uz zakonodavne akte o financijskim uslugama, u Direktivi (EU) 2016/1148 Europskog parlamenta i Vijeća[7] propisan je aktualni opći okvir za kibersigurnost na razini Unije. Među sedam ključnih sektora ta se direktiva primjenjuje i na tri vrste financijskih subjekata, tj. kreditne institucije, mjesta trgovanja i središnje druge ugovorne strane. Međutim, s obzirom na to da se Direktivom (EU) 2016/1148 utvrđuje mehanizam identifikacije operatora ključnih usluga na nacionalnoj razini, u praksi su samo neke kreditne institucije, mjesta trgovanja i središnje druge ugovorne strane koje su identificirale države članice obuhvaćeni njezinim područjem primjene i stoga su dužni ispunjavati zahtjeve za sigurnost IKT-a i obavješćivanje o incidentima koji su njome utvrđeni.

(16) Budući da se ovom Uredbom, uvođenjem zahtjeva za upravljanje IKT rizicima i izvješćivanje o IKT incidentima koji su stroži od onih iz postojećih zakonodavnih akata Unije o financijskim uslugama, poboljšava usklađenost komponenti digitalne otpornosti, poboljšava se i usklađenost u odnosu na zahtjeve iz Direktive (EU) 2016/1148. Stoga je ova Uredba ***za financijske subjekte*** lex specialis za Direktivu (EU) 2016/1148.

Iznimno je važno očuvati čvrstu vezu između financijskog sektora i horizontalnog okvira Unije za kibersigurnost ***kako*** bi se ▌ osigurala dosljednost sa strategijama kibersigurnosti koje su države članice već donijele i omogućilo bi se informiranje financijskih nadzornih tijela o kiberincidentima koji utječu na druge sektore obuhvaćene Direktivom (EU) 2016/1148.

(17) Kako bi se omogućilo međusektorsko učenje i djelotvorna primjena iskustava drugih sektora u borbi protiv kiberprijetnji, financijski subjekti iz Direktive (EU) 2016/1148 trebali bi ostati dio „ekosustava” te direktive (npr. skupina za suradnju i timovi za odgovor na računalne sigurnosne incidente iz Direktive NIS).

Europska nadzorna tijela trebala bi moći sudjelovati u raspravama o strateškim

[7] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

politikama, a nacionalna nadležna tijela u tehničkom radu skupine za suradnju iz Direktive NIS, i ta bi tijela trebala razmjenjivati informacije i dodatno surađivati s jedinstvenim kontaktnim točkama imenovanima na temelju Direktive (EU) 2016/1148. ***Zajedničko nadzorno tijelo, glavna nadzorna tijela i*** nadležna tijela iz ove Uredbe trebala bi se savjetovati i surađivati s nacionalnim timovima za odgovor na računalne sigurnosne incidente imenovanima u skladu s člankom 9. Direktive (EU) 2016/1148.

Osim toga, ovom bi se Uredbom trebalo osigurati da mreža timova za odgovor na računalne sigurnosne incidente uspostavljena Direktivom (EU) 2016/1148 prima detaljne informacije o značajnim IKT incidentima.

(18) Važno je također osigurati usklađenost ***i*** s Direktivom o europskoj kritičnoj infrastrukturi (Direktiva ECI), koja se upravo preispituje kako bi se poboljšala zaštita kritičnih infrastruktura od prijetnji iz područja koja nisu povezana s kibersigurnosti te njihova otpornost na te prijetnje, ***i s Direktivom o otpornosti ključnih subjekata***[8] s mogućim posljedicama za financijski sektor.

(19) Pružatelji usluga računalstva u oblaku jedna su od kategorija pružatelja digitalnih usluga obuhvaćenih Direktivom (EU) 2016/1148. Kao takvi su obuhvaćeni ex post nadzorom koji provode nacionalna nadležna tijela imenovana na temelju te direktive i koji je ograničen na zahtjeve za sigurnost IKT-a i obavješćivanje o incidentima koji su njome utvrđeni. Budući da se nadzorni okvir uspostavljen ovom Uredbom primjenjuje na sve treće strane pružatelje ključnih IKT usluga, uključujući pružatelje usluga računalstva u oblaku, kada pružaju IKT usluge financijskim subjektima, trebalo bi ga smatrati dopunom nadzoru koji se provodi na temelju Direktive (EU) 2016/1148***, a i materijalni i postupovni zahtjevi primjenjivi na treće strane pružatelje ključnih IKT usluga na temelju ove Uredbe trebali bi biti usklađeni i funkcionirati neometano s onima koji se primjenjuju na temelju te direktive***. Nadzornim okvirom uspostavljenim ovom Uredbom trebalo bi obuhvatiti i pružatelje usluga računalstva u oblaku jer ne postoji horizontalni nespecijalizirani okvir Unije o osnivanju tijela za digitalni nadzor.

(20) Da bi zadržali punu kontrolu nad IKT rizicima, financijski subjekti trebaju imati sveobuhvatne kapacitete za snažno i djelotvorno upravljanje IKT rizicima, ali i konkretne mehanizme i politike izvješćivanja o IKT incidentima, testiranja sustava, kontrola i procesa IKT-a te upravljanja IKT rizikom treće strane ***i IKT rizikom unutar grupe***. Razinu digitalne operativne otpornosti financijskog sustava trebalo bi povećati te istodobno omogućiti proporcionalnu primjenu zahtjeva ***vodeći računa o njihovoj prirodi, opsegu, složenosti i općem profilu rizičnosti***.

(21) Pragovi i taksonomije za izvješćivanje o IKT incidentima znatno se razlikuju na nacionalnoj razini. Iako bi se zajednička osnova mogla postići relevantnim radom Agencije Europske unije za kibersigurnost (ENISA)[9] i Skupine za suradnju u području sigurnosti mrežnih i informacijskih sustava za financijske subjekte iz Direktive (EU) 2016/1148, i dalje su prisutni različiti pristupi pragovima i taksonomijama ili se mogu pojaviti za preostale financijske subjekte. To znači da financijski subjekti moraju ispuniti višestruke zahtjeve, osobito kada posluju u nekoliko jurisdikcija u

---

[8] Direktiva Vijeća 2008/114/EZ od 8. prosinca 2008. o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite (SL L 345, 23.12.2008., str. 75.).

[9] ENISA, Reference Incident Classification Taxonomy (Referentna taksonomija za klasifikaciju incidenata); https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Uniji i kada su dio financijske grupe. Te razlike usto mogu spriječiti izradu dodatnih ujednačenih ili centraliziranih mehanizama Unije kojima bi se ubrzalo izvješćivanje te podržala brza i neometana razmjena informacija među nadležnim tijelima, što je ključno za ublažavanje IKT rizika u slučaju velikih napada s mogućim posljedicama za cijeli sustav.

(21a) Kako bi se smanjilo administrativno opterećenje te izbjegla složenost i dvostruki zahtjevi za izvješćivanje za pružatelje platnih usluga koji su obuhvaćeni područjem primjene ove Uredbe, trebali bi se prestati primjenjivati zahtjevi za izvješćivanje o incidentima iz Direktive (EU) 2015/2366. Stoga bi kreditne institucije, institucije za elektronički novac i institucije za platni promet u skladu s ovom Uredbom trebale izvješćivati o svim operativnim ili sigurnosnim incidentima povezanima s plaćanjem i onima koji nisu povezani s plaćanjem, a koji su se prethodno prijavljivali u skladu s Direktivom (EU) 2015/2366, neovisno o tome jesu li ti incidenti povezani s IKT-om ili nisu.

(22) Da bi se nadležnim tijelima omogućilo da ispune svoje nadzorne zadaće potpunim uvidom u prirodu, učestalost, značaj i učinak IKT incidenata i da bi se unaprijedila razmjena informacija među relevantnim javnim tijelima, uključujući tijela kaznenog progona i sanacijska tijela, treba utvrditi pravila kako bi se ***postigao pouzdan*** režim izvješćivanja o IKT incidentima ***sa*** zahtjevima ***kojima se rješavaju nedostaci*** u ***sektorskim*** zakonodavnim aktima o ***financijskim uslugama*** i uklonila postojeća preklapanja i udvostručenja radi smanjenja troškova. Stoga je neophodno uskladiti režim izvješćivanja o IKT incidentima tako da se sve financijske subjekte obveže na izvješćivanje ▌njihovim nadležnim tijelima ***s pomoću jedinstvenog pojednostavljenog okvira utvrđenog ovom Uredbom***. Europska nadzorna tijela usto bi trebalo ovlastiti za daljnju razradu elemenata izvješćivanja o IKT incidentima, kao što su taksonomija, rokovi, skupovi podataka, obrasci i primjenjivi pragovi.

(23) Zahtjevi testiranja digitalne operativne otpornosti razvijeni su u određenim financijskim podsektorima u nekoliko ***ponekad*** nekoordiniranih nacionalnih okvira u kojima se istim pitanjima pristupa na drugačiji način. To udvostručuje troškove financijskih subjekata koji posluju prekogranično i ***moglo bi otežati*** uzajamno priznavanje rezultata. Nekoordinirano testiranje može stoga uzrokovati segmentaciju jedinstvenog tržišta.

(24) Osim toga, ako testiranje nije obvezno, ranjivosti se ne otkrivaju zbog čega se financijski subjekt, a u konačnici i stabilnost i integritet financijskog sektora, izlaže većem riziku. Bez intervencije Unije testiranje digitalne operativne otpornosti i dalje bi bilo neujednačeno i rezultati testiranja ne bi se uzajamno priznavali u različitim jurisdikcijama. K tome, malo je vjerojatno da će drugi financijski podsektori u znatnoj mjeri prihvatiti takve sustave i zato neće iskoristiti moguće prednosti, kao što su otkrivanje ranjivosti i rizika, testiranje obrambenih kapaciteta i kontinuiteta poslovanja te veće povjerenje korisnika, dobavljača i poslovnih partnera. Kako bi se uklonila ta preklapanja, razlike i praznine, treba utvrditi pravila za koordinaciju testiranja koja provode financijski subjekti i nadležna tijela, čime bi se značajnim financijskim subjektima olakšalo uzajamno priznavanje rezultata naprednog testiranja.

(25) Oslanjanje financijskih subjekata na IKT usluge djelomično je potaknuto njihovom potrebom da se prilagode novom konkurentnom globalnom gospodarstvu, da povećaju učinkovitost svojeg poslovanja i odgovore na potražnju potrošača. Priroda i opseg tog oslanjanja neprestano su se mijenjali proteklih godina, potičući smanjenje troškova

financijskog posredovanja, omogućujući širenje i skalabilnost poslovanja uvođenjem financijskih aktivnosti i istodobno nudeći razne alate IKT-a za upravljanje složenim unutarnjim procesima.

(26) Široka primjena IKT usluga očituje se u složenim ugovorima, pri čemu financijski subjekti često nailaze na poteškoće ili u pregovorima o ugovornim uvjetima koji su prilagođeni bonitetnim standardima ili drugim regulatornim zahtjevima koji se na njih odnose ili u ostvarivanju određenih prava, kao što su prava pristupa ili revizije, kada su ta prava ugrađena u ugovore. Štoviše, mnogi takvi ugovori ne predviđaju dostatne mjere zaštite kojima bi se omogućilo cjelovito praćenje podugovaranja, čime se financijskom subjektu uskraćuje mogućnost procjene tih povezanih rizika. Osim toga, s obzirom na to da treće strane pružatelji IKT usluga često pružaju standardizirane usluge ranim vrstama klijenata, ti ugovori možda nisu uvijek prilagođeni pojedinačnim ili konkretnim potrebama subjekata u financijskom sektoru.

(27) Iako u nekim zakonodavnim aktima Unije o financijskim uslugama postoje neka opća pravila o eksternalizaciji poslova, praćenje ugovorne dimenzije ne temelji se u potpunosti na zakonodavstvu Unije. Budući da ne postoje jasni i specijalizirani standardi Unije koji bi se primjenjivali na ugovore sklopljene s trećim stranama pružateljima IKT usluga, vanjski izvor IKT rizika nije u detaljno obrađen. Stoga treba utvrditi određena ključna načela za usmjeravanje financijskih subjekata u upravljanju IKT rizikom trećih strana te popratna temeljna ugovorna prava povezana s nekoliko elemenata izvršavanja i raskida ugovora kako bi se ugradile određene minimalne mjere zaštite kapaciteta financijskih subjekata za djelotvorno praćenje svih rizika koji nastaju na razini trećih strana pružatelja IKT usluga.

(28) Nedostaje homogenosti i konvergencije između IKT rizika treće strane i ovisnost o IKT uslugama trećih strana. Unatoč pokušajima da se nešto poduzme u području eksternalizacije, kao što su preporuke iz 2017. za eksternalizaciju usluga računalstva u oblaku[10], pitanje sistemskog rizika koji bi se mogao pojaviti zbog izloženosti financijskog sektora ograničenom broju trećih strana pružatelja ključnih IKT usluga gotovo da i nije obrađeno u zakonodavnim aktima Unije. Takav propust na razini Unije dodatno je naglašen nepostojanjem konkretnih ovlasti i alata koji bi nacionalnim nadzornim tijelima omogućili bolje razumijevanje ovisnosti o IKT uslugama trećih strana i primjereno praćenje rizika koji proizlaze iz koncentracije te ovisnosti o IKT uslugama trećih strana.

(29) Uzimajući u obzir moguće sistemske rizike koji prate sve češću praksu eksternalizacije poslova i koncentraciju IKT usluga trećih strana te vodeći računa o nedostatnosti nacionalnih mehanizama koji financijskim nadzornim tijelima omogućuju da kvantificiraju, kvalificiraju i uklone posljedice IKT rizika koji nastaju kod trećih strana pružatelja ključnih IKT usluga, treba uspostaviti odgovarajući nadzorni okvir Unije koji omogućuje neprekidno praćenje aktivnosti trećih strana pružatelja IKT usluga koji ***pružaju ključne usluge*** financijskim subjektima. ***Budući da pružanje IKT usluga unutar grupe ne nosi iste rizike, pružatelje IKT usluga koji su dio iste grupe ili institucionalnog sustava zaštite ne bi trebalo definirati kao treće strane pružatelje ključnih IKT usluga.***

(30) S obzirom na to da IKT prijetnje postaju sve složenije i sofisticiranije, dobre mjere

[10] Preporuke za eksternalizaciju pružateljima usluga računalstva u oblaku (EBA/REC/2017/03), stavljene izvan snage Smjernicama EBA-e za eksternalizaciju (EBA/GL/2019/02).

otkrivanja i sprečavanja uvelike ovise o redovitoj razmjeni obavještajnih informacija o prijetnjama i ranjivostima među financijskim subjektima. Razmjena informacija pridonosi boljoj informiranosti o kiberprijetnjama, što poboljšava kapacitet financijskih subjekata da spriječe da se prijetnje pretvore u stvarne incidente te omogućuje financijskim subjektima da bolje ograniče učinke IKT incidenata i djelotvornije se od njih oporave. U nedostatku smjernica na razini Unije nekoliko čimbenika sprečava takvu razmjenu informacija, osobito nesigurnost u pogledu usklađenosti s pravilima o zaštiti osobnih podataka, zaštiti od monopola i odgovornosti. ***Stoga je važno ojačati mehanizme suradnje i izvješćivanje među financijskim subjektima i nadležnim tijelima te razmjenu informacija s javnošću u cilju razvoja otvorenog okvira za razmjenu informacija i pristupa „integrirane sigurnosti”, koji su ključni za povećanje operativne otpornosti i pripravnosti financijskog sektora u pogledu IKT rizika. U mehanizmima za razmjenu informacija uvijek bi trebalo uzeti u obzir moguće rizike povezane s kibersigurnošću, zaštitom podataka ili poslovnom tajnom.***

(31) Osim toga, korisne se informacije uskraćuju jer nije jasno koje se vrste informacija smiju podijeliti s drugim sudionicima na tržištu ili s nenadzornim tijelima (kao što je ENISA u analitičke svrhe ili Europol u svrhu kaznenog progona). Opseg i kvaliteta razmjene informacija i dalje su ograničeni i rascjepkani, a relevantne razmjene odvijaju se uglavnom na lokalnoj razini (u okviru nacionalnih inicijativa) i ne postoje dosljedni mehanizmi razmjene informacija na razini Unije koji su prilagođeni potrebama integriranog financijskog sektora. ***Stoga je važno ojačati te komunikacijske kanale i savjetovati se s nenadzornim tijelima, kada je to potrebno i relevantno, tijekom cijelog nadzornog ciklusa.***

(32) Financijske subjekte ***također*** bi trebalo potaknuti da zajednički iskoriste znanje i praktično iskustvo svakog od njih na strateškoj, taktičkoj i operativnoj razini kako bi poboljšali svoje kapacitete za procjenu, praćenje, obranu i odgovor na kiberprijetnje. Zato bi trebalo omogućiti mehanizme dobrovoljne razmjene informacija na razini Unije koji bi u pouzdanim okruženjima pomogli financijskoj zajednici da spriječi i zajednički odgovori na prijetnje brzim ograničenjem širenja IKT rizika i onemogućivanjem širenja zaraze u sve financijske kanale. Ti mehanizmi trebali bi biti potpuno u skladu s primjenjivim pravom Unije o tržišnom natjecanju[11] uz jamstvo potpunog poštovanja pravila Unije o zaštiti podataka, prvenstveno Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća[12], posebno u kontekstu obrade osobnih podataka koja je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, kako je navedeno u članku 6. stavku 1. točki (f) te uredbe.

(33) Iako je obuhvat predviđen ovom Uredbom doista širok, pri primjeni pravila o digitalnoj operativnoj otpornosti***, uključujući zahtjeve u pogledu okvira upravljanja rizicima,*** trebalo bi uzeti u obzir znatne razlike među financijskim subjektima u pogledu veličine, ***prirode, složenosti*** i ***profila rizičnosti***. Opće bi načelo bilo da financijski subjekti pri usmjeravanju resursa i kapaciteta na provedbu okvira upravljanja IKT rizicima trebaju propisno uskladiti svoje potrebe u području IKT-a sa

---

[11] Komunikacija Komisije – Smjernice o primjenjivosti članka 101. Ugovora o funkcioniranju Europske unije na sporazume o horizontalnoj suradnji, 2011/C 11/01.

[12] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

svojom veličinom, ***prirodom, složenošću,*** poslovnim profilom ***i profilom relativne rizičnosti***, a nadležna bi tijela to i dalje trebala procjenjivati i preispitivati.

(34) Budući da veći financijski subjekti imaju na raspolaganju više resursa i mogu brzo preusmjeriti sredstva na razvoj upravljačkih struktura i izradu različitih korporativnih strategija, samo bi financijske subjekte koji nisu mikropoduzeća u smislu ove Uredbe trebalo obvezati na uvođenje složenijih sustava upravljanja. Ti su subjekti bolje opremljeni osobito za uspostavu posebnih upravljačkih funkcija koje će nadzirati sporazume s trećim stranama pružateljima IKT usluga ili upravljati krizama, za organizaciju svojeg upravljanja IKT rizicima u skladu s modelom „tri crte obrane” ili donošenje dokumenta u području ljudskih resursa s detaljnim objašnjenjem politike prava pristupa.

Po istoj bi logici samo te financijske subjekte trebalo pozvati da provedu detaljnu procjenu nakon velikih promjena u infrastrukturi i procesima mrežnog i informacijskog sustava, da redovito analiziraju rizik u naslijeđenim sustavima IKT-a ili da prošire testiranje kontinuiteta poslovanja i planove odgovora i oporavka tako da uključuju i scenarije prebacivanja s primarne infrastrukture IKT-a na redundantnu infrastrukturu i obrnuto.

(35) Nadalje, s obzirom na to da bi samo financijski subjekti koji se smatraju značajnima za potrebe naprednog testiranja digitalne otpornosti trebali obavljati penetracijska testiranja vođenja prijetnjama, administrativni procesi i financijski troškovi koji prate te testove trebali bi se prenijeti samo na mali postotak financijskih subjekata. Konačno, kako bi se smanjilo regulatorno opterećenje, samo bi od financijskih subjekata koji nisu mikropoduzeća trebalo tražiti da redovito izvješćuju nadležna tijela o svim ***procijenjenim*** troškovima i gubicima uzrokovanima ***značajnim*** prekidima u radu IKT-a***, značajnim IKT incidentima*** te o rezultatima preispitivanja nakon incidenta koja se provedu nakon ***takvih*** poremećaja u radu IKT-a.

(36) Kako bi se osigurala potpuna usklađenost i opća dosljednost poslovnih strategija financijskih subjekata s jedne strane te upravljanja IKT rizicima s druge strane, upravljačko tijelo trebalo bi obvezno imati ključnu i aktivnu ulogu u usmjeravanju i prilagodbi okvira upravljanja IKT rizicima i opće strategije digitalne otpornosti. Pristup koji će primijeniti upravljačko tijelo ne bi trebao ovisiti samo o sredstvima za osiguranje otpornosti sustava IKT-a, nego bi trebalo obuhvatiti i osoblje i procese politikama kojima se na svim razinama poduzeća i među svim članovima osoblja podupire odlična informiranost o kiberrizicima i obveza održavanja stroge kiberhigijene na svim razinama.

Krajnja odgovornost upravljačkog tijela za upravljanje IKT rizicima financijskog subjekta trebala bi biti glavno načelo tog sveobuhvatnog pristupa koje će se pretočiti u neprekidno sudjelovanje upravljačkog tijela u kontroli praćenja upravljanja IKT rizicima.

(37) Nadalje, potpuna odgovornost upravljačkog tijela neodvojiva je od ulaganja u IKT i općeg proračuna koji će financijskom subjektu omogućiti da postigne osnovnu digitalnu operativnu otpornost.

(38) Ovom Uredbom, nadahnutom mjerodavnim međunarodnim, nacionalnim i industrijskim standardima, smjernicama, preporukama i pristupima za upravljanje

kiberrizicima[13], promiču se funkcije koje olakšavaju cjelokupno strukturiranje upravljanja IKT rizicima. Sve dok su glavni kapaciteti financijskih subjekata u skladu s potrebama planiranih ciljeva za funkcije (utvrđivanje, zaštita i sprečavanje, otkrivanje, odgovor i oporavak, učenje i razvoj te komunikacija) iz ove Uredbe, financijski subjekti i dalje mogu koristiti modele upravljanja IKT rizicima drugačijeg okvira ili kategorizacije.

(39) Da bi održali korak s kiberprijetnjama, financijski subjekti trebali bi imati ažurne sustave IKT-a koji su pouzdani i imaju dovoljno kapaciteta za obradu podataka koja je ne samo nužna za pružanje njihovih usluga, nego i za tehnološku otpornost koja financijskim subjektima omogućuje da na odgovarajući način odgovore na dodatne potrebe za obradom koje mogu nastati zbog stresnih okolnosti na tržištu ili drugih nepovoljnih situacija. Iako se ovom Uredbom ne normiraju konkretni sustavi, alati i tehnologije IKT-a, računa se da će financijski subjekti primjereno koristiti europske i međunarodno priznate tehničke norme (npr. ISO) ili najbolje primjere sektorske prakse na način koji je u potpunosti u skladu s konkretnim uputama nadzornog tijela o primjeni i provedbi međunarodnih normi.

(40) Učinkoviti planovi kontinuiteta poslovanja i planovi oporavka propisani su kako bi se financijskim subjektima omogućilo da odmah i brzo riješe IKT incidente, osobito kibernapade, ograničenjem štete i davanjem prednosti nastavku poslovanja i mjerama oporavka***, pri čemu se vodi računa o tome jesu li to ključne ili važne funkcije***. Međutim, iako bi rezervni sustavi trebali početi s obradom bez nepotrebne odgode, početak njihova rada ne bi trebao ni na koji način ugroziti cjelovitost i sigurnost mrežnih i informacijskih sustava i povjerljivost podataka.

(41) Iako se ovom Uredbom financijskim subjektima dopušta da fleksibilno utvrde ciljeve vremena oporavka, a time i utvrde te ciljeve vodeći računa o prirodi i nužnosti relevantne funkcije i svih konkretnih poslovnih potreba, a pri utvrđivanju tih ciljeva trebalo bi procijeniti i mogući sveukupni učinak na djelotvornost tržišta.

(42) Ozbiljne posljedice kibernapada još su veće kada se dogode u financijskom sektoru, području koje je izloženo puno većem riziku da bude meta zlonamjernih širitelja koji žele ostvariti financijsku korist izravno na izvoru. Kako bi se smanjili ti rizici i spriječio gubitak cjelovitosti ili dostupnosti sustava IKT-a i povreda povjerljivih podataka ili oštećenje fizičke infrastrukture IKT-a, trebalo bi znatno poboljšati izvješćivanje financijskih subjekata o značajnim IKT incidentima.

Izvješćivanje o IKT incidentima trebalo bi uskladiti tako da se sve financijske subjekte obveže na izvješćivanje samo njihovim nadležnim tijelima. Iako bi bilo obvezno za sve financijske subjekte, to izvješćivanje ne bi na sve utjecalo na isti način jer bi relevantne pragove značajnosti i rokove trebalo kalibrirati tako da se njima obuhvate

---

[13] Odbor za platne i tržišne infrastrukture (CPMI) i Međunarodna organizacija komisija za vrijednosne papire (IOSCO), Guidance on cyber resilience for financial market infrastructures (Smjernice za kiberotpornost za infrastrukture financijskog tržišta), https://www.bis.org/cpmi/publ/d146.pdf, G7, Fundamental Elements of Cybersecurity for the Financial Sector (Temeljni elementi kibersigurnosti za financijski sektor), https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; Okvir kibersigurnosti Nacionalnog instituta za norme i tehnologiju (NIST), https://www.nist.gov/cyberframework; Odbor za financijsku stabilnost (FSB) CIRR toolkit (Komplet alata za odgovor na kiberincidente i oporavak od njih) https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document

samo značajni IKT incidenti. Izravno izvješćivanje omogućilo bi financijskim nadzornim tijelima pristup informacijama o IKT incidentima. No, financijska nadzorna tijela trebala bi te informacije prosljeđivati nefinancijskim javnim tijelima (nadležna tijela iz Direktive NIS, nacionalna tijela za zaštitu podataka i tijela kaznenog progona u slučaju incidenata kaznene prirode). Informacije o IKT incidentima trebale bi se međusobno razmjenjivati: financijska nadzorna tijela trebala bi financijskim subjektima dostaviti sve potrebne povratne informacije ili smjernice, dok bi europska nadzorna tijela trebala dijeliti anonimizirane podatke o prijetnjama i ranjivostima povezanima s određenim događajem kako bi pomogla u široj zajedničkoj obrani.

(43) Trebalo bi dodatno razmotriti mogućnost centralizacije izvješćivanja o IKT incidentima u obliku jedinstvenog ▌EU-ova čvorišta ***za izvješćivanje o značajnim IKT incidentima*** u kojem će se izravno primati relevantna izvješća i automatski obavješćivati nacionalna nadležna tijela ili u kojem će se samo centralizirati čuvanje izvješća koja su proslijedila nacionalna nadležna tijela i koje će imati koordinacijsku ulogu. Od europskih nadzornih tijela trebalo bi zahtijevati da, uz savjetovanje s ESB-om i ENISA-om, do određenog datuma pripreme zajedničko izvješće u kojem će istražiti izvedivost uspostavljanja takvog središnjeg EU-ova čvorišta.

(44) Da bi postigli snažnu digitalnu operativnu otpornost i u skladu s međunarodnim standardima (npr. dokument skupine G7 *Fundamental Elements for Threat-Led Penetration Testing* (Temeljni elementi za penetracijska testiranja vođena prijetnjama)) financijski subjekti***, osim mikropoduzeća,*** trebali bi redovito testirati djelotvornost svojih sustava IKT-a i IKT osoblja u pogledu njihovih kapaciteta za sprečavanje, otkrivanje, odgovor i oporavak kako bi otkrili i uklonili moguće ranjivosti IKT-a. Kako bi se odgovorilo na razlike prisutne u financijskim sektorima u pogledu pripravnosti financijskih subjekata u području kibersigurnosti, testiranje bi trebalo uključivati razne alate i mjere, od procjene osnovnih zahtjeva (npr. procjene i skeniranja ranjivosti, analize otvorenih izvora, procjene mrežne sigurnosti, analize nedostataka, preispitivanja fizičke sigurnosti, upitnici i softverska rješenja za skeniranje, preispitivanja izvornog koda gdje je to izvedivo, testiranja na temelju scenarija, testiranje kompatibilnosti, testiranje radnih karakteristika ili integralno (engl. end-to-end) testiranje) do naprednijeg testiranja (npr. TLPT u slučaju financijskih subjekata koji su dovoljno zreli u kontekstu IKT-a da bi mogli provesti takva testiranja). Stoga bi testiranje digitalne operativne otpornosti trebalo biti zahtjevnije za značajne financijske subjekte (kao što su velike kreditne institucije, burze, središnji depozitoriji vrijednosnih papira, središnje druge ugovorne strane itd.). Istodobno bi testiranje digitalne operativne otpornosti trebalo biti relevantnije za određene podsektore koji imaju glavnu sistemsku funkciju u sustavu (npr. plaćanja, bankarstvo, kliring i namira) i manje relevantno za druge podsektore (npr. upravitelji imovine, agencije za kreditni rejting itd.). Financijski subjekti koji posluju prekogranično i ostvaruju slobodu poslovnog nastana ili pružanja usluga u Uniji trebali bi ispunjavati jedinstvene zahtjeve naprednog testiranja (npr. TLPT) u svojoj matičnoj državi članici i to bi testiranje trebalo uključivati infrastrukture IKT-a u svim jurisdikcijama u kojima prekogranična grupa posluje u Uniji, čime bi te prekogranične grupe imale troškove testiranja samo u jednoj jurisdikciji. ***Nadalje, kako bi se ojačala suradnja s pouzdanim trećim zemljama u području otpornosti financijskih subjekata, Komisija i nadležna tijela trebali bi težiti uspostavi okvira za uzajamno priznavanje rezultata TLPT-a.***

Države članice trebale bi imenovati jedinstveno javno tijelo odgovorno za TLPT u financijskom sektoru na nacionalnoj razini. Jedinstveno javno tijelo moglo bi, među ostalim, biti nacionalno nadležno tijelo ili javno tijelo imenovano u skladu s člankom 8. Direktive (EU) 2016/1148 (NIS). Jedinstveno javno tijelo trebalo bi biti odgovorno za izdavanje potvrda da je TLPT proveden u skladu sa zahtjevima. Takve bi potvrde trebale olakšati uzajamno priznavanje testiranja među nadležnim tijelima.

Neki financijski subjekti imaju kapacitet za provedbu unutarnjeg naprednog testiranja, dok će drugi angažirati vanjske provoditelje testiranja iz Unije ili iz treće zemlje. Stoga je važno da svi provoditelj testiranja podliježu istim jasnim zahtjevima. Kako bi se osigurala neovisnost unutarnjih prevoditelja testiranja, njihov bi angažman trebalo odobriti nadležno tijelo.

Metodologija za TLPT ne bi trebala biti propisana, ali bi se trebalo smatrati da je postojeći okvir TIBER-EU usklađen sa zahtjevima TLPT-a iz ove Uredbe.

Do stupanja na snagu ove Uredbe i dok europska nadzorna tijela ne razviju i ne donesu propisane regulatorne tehničke standarde u pogledu TLPT-a, financijski subjekti trebali bi slijediti relevantne smjernice i okvire Unije koji se primjenjuju na penetracijska testiranja vođena saznanjima, s obzirom na to da će se s njihovom primjenom nastaviti nakon stupanja na snagu ove Uredbe.

(44a) Odgovornost za provođenje TLPT-a, kao i za upravljanje kibersigurnošću općenito i sprečavanje kibernapada, trebala bi i dalje u potpunosti počivati na financijskom subjektu, a potvrde koje dostavljaju tijela trebale bi isključivo služiti u svrhu uzajamnog priznavanja te ne bi trebale sprečavati praćenje poduzetih mjera na razini IKT rizika kojem je financijski subjekt izložen niti bi se trebale smatrati kao odobrenje u smislu njegovih sposobnosti upravljanja IKT rizicima i njihova ublažavanja.

(45) Kako bi se osiguralo pouzdano praćenje IKT rizika treće strane, treba uvesti pravila koja se temelje na načelima kako bi se financijske subjekte usmjerilo u praćenju rizika koji nastaju u kontekstu funkcija eksternaliziranih trećim stranama pružateljima IKT usluga***, osobito u vezi s pružanjem ključnih ili važnih funkcija koje osiguravaju treće strane pružatelji IKT usluga,*** i općenito u kontekstu ovisnosti o IKT uslugama trećih strana.

(46) Financijski subjekt trebao bi u svakom trenutku biti potpuno odgovoran za ispunjenje obveza iz ove Uredbe. Proporcionalno praćenje rizika koji se pojavi na razini treće strane pružatelja IKT usluga trebalo bi organizirati vodeći računa o ***prirodi,*** opsegu, složenosti i nužnosti ovisnosti u području IKT-a, kritičnosti ili važnosti usluga, procesa ili funkcija koje su obuhvaćene ugovorima i, u konačnici, na temelju pažljive procjene mogućih učinaka na kontinuitet i kvalitetu financijskih usluga na razini subjekta i na razini grupe, ovisno o slučaju***, kao i na temelju toga pruža li IKT usluge pružatelj usluga unutar grupe ili treća strana pružatelj IKT usluga.***

(47) Praćenje trebalo bi se odvijati u skladu sa strateškim pristupom IKT riziku treće strane koji je upravljačko tijelo financijskog subjekta formaliziralo donošenjem posebne strategije koja se temelji na neprekidnoj dubinskoj analizi svih takvih ovisnosti o IKT uslugama trećih strana. Kako bi se poboljšala informiranost o nadzoru ovisnosti o IKT uslugama trećih strana i dodatno podržao nadzorni okvir uspostavljen ovom Uredbom, financijska nadzorna tijela trebala bi redovito primati najvažnije informacije iz registara i trebala bi moći zatražiti njihove izvatke na *ad hoc* osnovi.

(48) Temeljita predugovorna analiza trebala bi biti temelj i preduvjet za službeno sklapanje ugovora, a ***korektivne mjere, koje mogu obuhvaćati djelomični ili potpuni*** raskid ugovora***, trebale bi biti poduzete kada postoje*** barem razne okolnosti koje ukazuju na ***ozbiljne*** nedostatke kod treće strane pružatelja IKT usluga.

(49) Kako bi se riješio problem sistemskog učinka koncentracijskog rizika IKT usluga trećih strana, trebalo bi promicati uravnoteženo rješenje u okviru fleksibilnog i postupnog pristupa jer bi stroge gornje granice ili ograničenja mogla biti prepreka poslovanju i ugovornoj slobodi. Financijski subjekti trebali bi temeljito procijeniti ugovore kako bi utvrdili koliko je vjerojatno da će se takav rizik pojaviti, među ostalim u okviru detaljnih analiza podugovora za eksternalizaciju poslova ▌. U toj fazi i u cilju postizanja pravedne ravnoteže između nužnog očuvanja ugovorne slobode i jamstva financijske stabilnosti smatra se da nije primjereno utvrđivati stroge gornje granice i ograničenja za izloženost IKT uslugama trećih strana. ***Zajedničko nadzorno tijelo koje provodi*** nadzor svake treće strane pružatelja ključnih IKT usluga ***i europsko nadzorno tijelo koje je imenovano da provodi svakodnevni nadzor*** („glavno nadzorno tijelo”) ***trebali*** bi pri izvršavanju nadzornih zadaća posebnu pozornost posvetiti potpunom razumijevanju razmjera ovisnosti te otkriti konkretne slučajeve u kojima je vjerojatno da će visok stupanj koncentracije trećih strana pružatelja ključnih IKT usluga opteretiti stabilnost i integritet financijskog sustava Unije te bi trebalo omogućiti dijalog s trećim stranama pružateljima ključnih IKT usluga kada se rizik utvrdi[14].

(50) Kako bi se omogućili redovita evaluacija i praćenje kapaciteta treće strane pružatelja IKT usluga za sigurno pružanje usluga financijskom subjektu bez negativnih učinaka na otpornost tog subjekta, trebalo bi uskladiti ključne ugovorne elemente u svim fazama izvršavanja ugovora s trećim stranama pružateljima IKT usluga. Ti elementi obuhvaćaju samo minimalne ugovorne aspekte koji se smatraju ključnima da bi se financijskim subjektima omogućilo cjelovito praćenje kako bi se postigla njihova digitalna otpornost koja ovisi o stabilnosti i sigurnosti IKT usluge.

(51) Ugovori bi stoga trebali sadržavati cjelovit opis funkcija i usluga, točne lokacije izvršavanja funkcija i obrade podataka te cjelovite opise razina usluga popraćene kvantitativnim i kvalitativnim ciljevima uspješnosti u okviru dogovorenih razina usluga kako bi se financijskom subjektu omogućilo djelotvorno praćenje. Isto tako odredbe o pristupačnosti, dostupnosti, cjelovitosti, sigurnosti i zaštiti osobnih podataka te o jamstvima pristupa, oporavka i vraćanja u slučaju nesolventnosti, sanacije, prestanka poslovanja treće strane pružatelja IKT usluga ***ili raskidu ugovora*** trebale bi se smatrati ključnim elementima kapaciteta financijskog subjekta za osiguranje praćenja rizika treće strane.

(52) Da bi se financijskim subjektima osigurala potpuna kontrola nad svim promjenama koje bi mogle narušiti sigurnost IKT-a, rokovi za prethodnu obavijest i izvještajne obveze treće strane pružatelja IKT usluga trebali bi se utvrditi za slučaj događaja koji bi mogli bitno utjecati na kapacitet treće strane pružatelja IKT usluga za djelotvorno izvršavanje ključne ili važne funkcije, među ostalim pružanjem pomoći u slučaju IKT incidenta ***povezanog s uslugama koje financijskom subjektu na dogovorenim razinama usluga pruža treća strana pružatelj IKT usluga*** bez dodatnih troškova ili uz unaprijed utvrđene

---

[14] Osim toga, pojavi li se rizik da će dominantna treća strana pružatelj IKT usluga to zloupotrijebiti, financijski subjekti trebali bi imati i mogućnost podnošenja službenog ili neslužbenog prigovora Europskoj komisiji ili nacionalnom tijelu za tržišno natjecanje.

troškove. ***Pomoćne IKT usluge o kojima financijski subjekti nisu operativno ovisni nisu obuhvaćene ovom Uredbom.***

Nadalje, definicija „ključne ili važne funkcije" iz ove Uredbe trebala bi obuhvaćati definiciju „ključnih funkcija" iz članka 2. stavka 1. točke 35. Direktive 2014/59/EU Europskog parlamenta i Vijeća od 15. svibnja 2014.[15] ***U skladu s tim, funkcije koje su ključne funkcije u skladu s Direktivom (EU) 2014/59/EU trebale bi biti ključne ili važne funkcije u smislu ove Uredbe.***

(53) ***U slučaju ugovora o ključnim ili važim funkcijama*** uz potpunu suradnju treće strane pružatelja IKT usluga tijekom nadzora, prava financijskih subjekata ili imenovane treće strane na pristup, nadzor i reviziju ključni su instrumenti financijskih subjekata u kontinuiranom praćenju uspješnosti trećih strana pružatelja IKT usluga u izvršavanju usluga. Jednako tako bi ***Zajedničko nadzorno tijelo i glavno nadzorno tijelo*** zaduženo za financijski subjekt trebali, na temelju prethodnih obavijesti, imati ta prava nadzora i revizije treće strane pružatelja IKT usluga, uz poštovanje povjerljivosti, ***pritom vodeći računa da se ne ometaju usluge koje ta treća strana pružatelj IKT usluga pruža drugim kupcima***. ***Financijski subjekt i treća strana pružatelj IKT usluga trebali bi se moći složiti da se prava na pristup, nadzor i reviziju mogu delegirati neovisnoj trećoj strani.***

(54) Ugovori bi trebali sadržavati jasne odredbe o pravima raskida i povezanim minimalnim rokovima za prethodnu obavijest i s time povezanim izlaznim strategijama koje predviđaju prije svega obvezna prijelazna razdoblja tijekom kojih bi treća strana pružatelj IKT usluga trebala nastaviti pružati relevantne funkcije kako bi se smanjio rizik od poremećaja u radu financijskog subjekta ili financijskom subjektu omogućilo da se, u skladu sa složenosti pružane usluge, djelotvorno prebaci na usluge druge treće strane pružatelja IKT usluga ili u protivnom pribjegne ***internim*** rješenjima. ***Nadalje, kreditne institucije trebale bi osigurati da su relevantni ugovori IKT-a pouzdani i u potpunosti provedivi u slučaju sanacije kreditne institucije. U skladu s očekivanjima sanacijskih tijela, kreditne institucije trebale bi osigurati da su relevantni ugovori o uslugama IKT-a otporni na sanaciju. Sve dok se ključne ili važne funkcije IKT-a i dalje provode, ti bi financijski subjekti trebali osigurati da ugovori, među ostalim zahtjevima, sadržavaju klauzule o zabrani raskidanja, suspenzije te izmjena zbog restrukturiranja ili sanacije.***

(55) Nadalje, dobrovoljna primjena standardnih ugovornih klauzula koje Komisija sastavi za usluge računalstva u oblaku mogla bi dodatno olakšati odnos između financijskih subjekata i trećih strana pružatelja IKT usluga jer bi se povećao stupanj pravne sigurnosti u pogledu primjene usluga računalstva u oblaku u financijskom sektoru, što je u potpunosti u skladu sa zahtjevima i očekivanjima utvrđenima regulacijom financijskih usluga. Ta nastojanja nastavak su mjera koje su već predviđene Akcijskim planom za financijske tehnologije iz 2018. u kojem je najavljeno da Komisija namjerava poticati i olakšati sastavljanje standardnih ugovornih klauzula za financijske subjekte

---

[15] ***Direktiva 2014/59/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o uspostavi okvira za oporavak i sanaciju kreditnih institucija i investicijskih društava te o izmjeni Direktive Vijeća 82/891/EEZ i direktiva 2001/24/EZ, 2002/47/EZ, 2004/25/EZ, 2005/56/EZ, 2007/36/EZ, 2011/35/EU, 2012/30/EU i 2013/36/EU te uredbi (EU) br. 1093/2010 i (EU) br. 648/2012 Europskog parlamenta i Vijeća (SL L 173, 12.6.2014., str. 190.).***

koji eksternaliziraju poslove pružateljima usluge računalstva u oblaku, oslanjajući se pritom na napore koje su dionici tog sektora uz pomoć Komisije, koja je osigurala sudjelovanje financijskog sektora u tom postupku, već uložili na međusektorskoj razini.

(55a) Europska nadzorna tijela trebala bi biti ovlaštena za izradu nacrta provedbenih tehničkih i regulatornih standarda kojima se utvrđuju očekivanja od politika u pogledu upravljanja IKT rizicima trećih strana i u pogledu ugovornih obveza. Do stupanja na snagu tih standarda financijski subjekti trebali bi slijediti relevantne smjernice i druge mjere koje su izdala europska nadzorna tijela i nadležna tijela.

(56) Radi promicanja konvergencije i učinkovitosti pristupa nadzoru IKT rizika treće strane u financijskom sektoru, radi jačanja digitalne operativne otpornosti financijskih subjekata koji se pri izvršavanju operativnih funkcija oslanjanju na treće strane pružatelje ključnih IKT usluga i kako bi se tako pridonijelo očuvanju stabilnosti financijskog sustava Unije i integriteta jedinstvenog tržišta za financijske usluge, treće strane pružatelji ključnih IKT usluga trebali bi biti obuhvaćeni nadzornim okvirom Unije.

(57) Budući da je poseban tretman potreban samo za treće strane pružatelje ključnih usluga, trebalo bi uspostaviti mehanizam određivanja subjekata na koje se primjenjuje nadzorni okvir Unije kako bi se uzeli u obzir opseg i priroda oslanjanja financijskog sektora na te treće strane pružatelje IKT usluga, što bi se pretočilo u kvantitativne i kvalitativne kriterije za utvrđivanje parametara nužnosti na temelju kojih bi se subjekt obuhvatio ***nadzornim okvirom***. Treće strane pružatelji ključnih IKT usluga čije usluge nisu automatski određene kao takve primjenom prethodno navedenih kriterija trebale bi imati mogućnost dobrovoljnog uključenja u nadzorni okvir, dok bi iz njega trebalo izuzeti treće strane pružatelje IKT usluga koje su već obuhvaćene nadzornim okvirima koji ***podupiru ispunjavanje zadaća*** na razini eurosustava iz članka 127. stavka 2. Ugovora o funkcioniranju Europske unije. ***Slično tome, poduzeća koja su sastavni dio financijske grupe i pružaju IKT usluge isključivo financijskim subjektima unutar iste financijske grupe ne bi trebali podlijegati mehanizmu za određivanje ključnih tijela.***

(58) Zahtjev da treće strane pružatelji IKT usluga čije su usluge određene kao ključne moraju biti osnovane u Uniji ne predstavlja lokalizaciju podataka jer ovom Uredbom nije predviđen nikakav dodatni zahtjev o pohrani ili obradi podataka u Uniji. ***Svrha zahtjeva da poduzeće, kao što je društvo kći, bude osnovano u Uniji u skladu s pravom države članice jest osigurati kontaktnu točku između treće strane pružatelja IKT usluga, s jedne strane, i glavnog nadzornog i Zajedničkog nadzornog tijela te, s druge strane, zajamčiti da su glavno nadzorno tijelo i Zajedničko nadzorno tijelo sposobni obavljati svoje dužnosti i izvršavati svoje ovlasti nadzora i provedbe kako je predviđeno ovom Uredbom. Ugovorene usluge treće strane pružatelja IKT usluga ne mora pružati njegov subjekt u Uniji.***

(58a) Zbog bitnih implikacija koje bi određivanje ključnim tijelom moglo imati za treće strane pružatelje IKT usluga, europska nadzorna tijela i Zajedničko nadzorno tijelo trebali bi biti dužni predvidjeti prava na prethodno saslušanje kako bi se uzele u obzir sve dodatne informacije koje treće strane pružatelji IKT usluga dostave tijekom postupka određivanja.

(59) ***Nadzorni*** okvir ne bi trebao dovesti u pitanje nadležnost država članica za provedbu vlastitog nadzora trećih strana pružatelja IKT usluga čije usluge u skladu s ovom Uredbom nisu ključne, ali bi se mogle smatrati važnima na nacionalnoj razini.

(60) Kako bi iskoristio postojeću višerazinsku institucijsku arhitekturu u području financijskih usluga, Zajednički odbor europskih nadzornih tijela trebao bi i dalje osiguravati opću međusektorsku koordinaciju svih pitanja povezanih s IKT rizicima u skladu sa svojim zadaćama u području kibersigurnosti, ***u okviru novouspostavljenog Zajedničkog nadzornog tijela koje je zaduženo za izdavanje*** i pojedinačnih odluka, naslovljenih na pružatelje ključnih IKT usluga, i zajedničkih preporuka, prvenstveno o komparativnoj analizi programa nadzora trećih strana pružatelja ključnih IKT usluga, i za utvrđivanje najboljih postupaka za rješavanje problema koncentracijskog rizika IKT-a.

(61) Kako bi se na razini Unije osigurao primjeren nadzor trećih strana pružatelja IKT usluga koje imaju ključnu ulogu u funkcioniranju financijskog sektora, ***trebalo bi uspostaviti Zajedničko nadzorno tijelo za provođenje izravnog nadzora nad trećim stranama pružateljima ključnih IKT usluga***. Nadalje, jedno od europskih nadzornih tijela trebalo bi imenovati glavnim nadzornim tijelom za svaku treću stranu pružatelja ključnih IKT usluga ***kako bi provodilo i koordiniralo svakodnevni nadzor i istražne aktivnosti, djelovalo kao jedinstvena kontaktna točka i osiguravalo kontinuitet***. ***Zajedničko nadzorno tijelo i glavno nadzorno tijelo trebali bi neometano raditi na osiguravanju učinkovitog svakodnevnog nadzora kao i cjelovitog pristupa donošenju odluka i preporukama.***

(62) Glavna nadzorna tijela trebala bi imati potrebne ovlasti za provedbu istraga, izravni nadzor trećih strana pružatelja ključnih IKT usluga, pristup svim relevantnim prostorima i lokacijama te pribavljanje potpunih i ažurnih informacija koje će im omogućiti stvarni uvid u vrstu, opseg i učinak IKT rizika treće strane s kojim se suočavaju financijski subjekti te, u konačnici, i financijski sustav Unije.

(62a) Povjeravanje ***izravnog*** nadzora ***Zajedničkom nadzornom tijelu*** preduvjet je za razumijevanje i rješavanje problema sistemske dimenzije IKT rizika u financijama. Zbog otiska trećih strana pružatelja ključnih IKT usluga u Uniji i s njime povezanih mogućih pitanja koncentracijskog rizika IKT-a potreban je zajednički pristup na razini Unije. Višestruke revizije i prava pristupa, koje bi brojna nadležna tijela obavljala samostalno uz malo ili nimalo koordinacije, ne bi omogućili cjelovit pregled IKT rizika trećih strana i istodobno bi uzrokovali nepotrebnu količinu posla, opterećenje i složenost na razini trećih strana pružatelja ključnih IKT usluga koji bi morali obraditi te brojne zahtjeve.

(63) ***Zajedničko nadzorno tijelo*** usto bi trebalo moći izdati preporuke o pitanjima IKT rizika i odgovarajućim korektivnim mjerama, uključujući protivljenje određenim ugovorima koji u konačnici utječu na stabilnost financijskog subjekta ili financijskog sustava. Nacionalna nadležna tijela trebala bi usklađenje s tim materijalnim preporukama ***Zajedničkog nadzornog tijela*** shvatiti kao dio svoje funkcije koja se odnosi na bonitetni nadzor financijskih subjekata. ***Prije konačnog oblikovanja takvih preporuka trećim stranama pružateljima ključnih IKT usluga trebalo bi omogućiti da dostave informacije za koje opravdano smatraju da bi ih trebalo uzeti u obzir prije konačnog oblikovanja i izdavanja preporuka.***

(63a) Kako bi se izbjeglo udvostručavanje i proturječja s tehničkim i organizacijskim mjerama koje se primjenjuju na treće strane pružatelje ključnih IKT usluga, glavna nadzorna tijela i Zajedničko nadzorno tijelo trebali bi pri izvršavanju svojih ovlasti u skladu s nadzornim okvirom iz ove Uredbe uzeti u obzir okvir uspostavljen Direktivom (EU) 2016/1148. Prije izvršavanja tih ovlasti Zajedničko nadzorno tijelo i glavno

nadzorno tijelo trebali bi se savjetovati s relevantnim nadležnim tijelima koja su nadležna na temelju Direktive (EU) 2016/1148.

(64) Nadzorni okvir ne zamjenjuje i ni na koji način i ni u kojem dijelu ne nadomješta upravljanje financijskih subjekata rizikom od primjene usluga trećih strana pružatelja IKT usluga, uključujući obvezu kontinuiranog praćenja ugovora sklopljenih s trećim stranama pružateljima ključnih IKT usluga, te ne utječe na potpunu odgovornost financijskih subjekata za ispunjavanje i izvršavanje svih zahtjeva iz ove Uredbe i mjerodavnih zakonodavnih akata o financijskim uslugama. Kako bi se izbjegla udvostručenja i preklapanja, nadležna tijela trebala bi se suzdržati od samostalnog poduzimanja mjera čiji je cilj praćenje rizika trećih strana pružatelja ključnih IKT usluga. Sve takve mjere trebale bi se prethodno koordinirati i usuglasiti u kontekstu nadzornog okvira.

(65) Radi promicanja međunarodne konvergencije najboljih primjera iz prakse koji će se primjenjivati pri preispitivanju upravljanja trećih strana pružatelja IKT usluga digitalnim rizikom, europska nadzorna tijela trebalo bi potaknuti na sklapanje sporazuma o suradnji s odgovarajućim nadležnim nadzornim i regulatornim tijelima trećih zemalja radi lakšeg razvoja najboljih postupaka za ublažavanje IKT rizika treće strane.

(66) Kako bi se iskoristilo tehničko stručno znanje stručnjaka nadležnih tijela o upravljanju operativnim i IKT rizicima, glavna nadzorna tijela ***u provedbi općih istraga ili izravnog nadzora*** trebala bi se osloniti na nacionalno iskustvo u nadzoru i formirati posebne timove za provjeru za svaku pojedinu treću stranu pružatelja ključnih IKT usluga te tako stvoriti multidisciplinarne timove koji bi sudjelovali u pripremi i stvarnom izvršavanju nadzornih aktivnosti, uključujući izravan nadzor trećih strana pružatelja ključnih IKT usluga, te potrebno praćenje mjera poduzetih nakon nadzora.

(67) Nadležna tijela trebala bi imati sve ovlasti nadzora, istrage i sankcioniranja potrebne za osiguranje primjene ove Uredbe. Administrativne kazne trebalo bi u načelu javno objavljivati. Budući da financijski subjekti i treće strane pružatelji IKT usluga mogu imati sjedište u različitim državama članicama i mogu ih nadzirati različita nadležna sektorska tijela, trebalo bi osigurati blisku suradnju odgovarajućih nadležnih tijela, uključujući ESB u odnosu na posebne zadaće koje su mu dodijeljene Uredbom Vijeća (EU) br. 1024/2013[16], te savjetovanje s europskim nadzornim tijelima, uzajamnom razmjenom informacija i pružanja pomoći u kontekstu nadzornih aktivnosti. ***Jedinstveni sanacijski odbor, iako nije nadležno tijelo za potrebe ove Uredbe, ipak bi trebao biti uključen u mehanizme za uzajamnu razmjenu informacija za subjekte obuhvaćene područjem primjene Uredbe (EU) br. 806/2014 Europskog parlamenta i Vijeća[17]***.

(68) Kako bi se dodatno kvantificirali i kvalificirali kriteriji za određivanje trećih strana pružatelja ključnih IKT usluga te uskladile naknade za nadzor, ovlast za donošenje akata

---

16 Uredba Vijeća (EU) br. 1024/2013 od 15. listopada 2013. o dodjeli određenih zadaća Europskoj središnjoj banci u vezi s politikama bonitetnog nadzora kreditnih institucija (SL L 287, 29.10.2013., str. 63.).

17 ***Uredba (EU) br. 806/2014 Europskog parlamenta i Vijeća od 15. srpnja 2014. o utvrđivanju jedinstvenih pravila i jedinstvenog postupka za sanaciju kreditnih institucija i određenih investicijskih društava u okviru jedinstvenog sanacijskog mehanizma i jedinstvenog fonda za sanaciju te o izmjeni Uredbe (EU) br. 1093/2010 (SL L 225, 30.7.2014., str. 1.).***

u skladu s člankom 290. Ugovora o funkcioniranju Europske unije trebalo bi delegirati Komisiji u pogledu: detaljnijeg opisa sistemskog učinka koji bi propast treće strane pružatelja IKT usluga mogla imati na financijske subjekte kojima ona pruža usluge, navođenja broja globalnih sistemski važnih institucija (GSV institucije) ili ostalih sistemskih važnih institucija (OSV institucije) koje se oslanjanju na relevantnu treću stranu pružatelja IKT usluga, navođenja broja trećih strana pružatelja IKT usluga koje su aktivne na određenom tržištu, navođenja troškova migracije na usluge druge treće strane pružatelja IKT usluga, navođenja broja država članica u kojima relevantna treća strana pružatelj IKT usluga pruža usluge i u kojima posluju financijski subjekti koji koriste usluge relevantne treće strane pružatelja IKT usluga te određivanja iznosa i načina plaćanja naknada za nadzor.

Posebno je važno da Komisija tijekom svojeg pripremnog rada provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka, te da se ta savjetovanja provedu u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.[18] Osobito, s ciljem osiguravanja ravnopravnog sudjelovanja u pripremi delegiranih akata, Europski parlament i Vijeće primaju sve dokumente istodobno kada i stručnjaci iz država članica te njihovi stručnjaci sustavno imaju pristup sastancima stručnih skupina Komisije koji se odnose na pripremu delegiranih akata.

(69) Budući da se ovom Uredbom, u kombinaciji s Direktivom (EU) 20xx/xx Europskog parlamenta i Vijeća[19], odredbe o upravljanju IKT rizicima koje se protežu kroz nekoliko uredbi i direktiva iz pravne stečevine Unije o financijskim uslugama, uključujući uredbe (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014, konsolidiraju kako bi se osigurala potpuna dosljednost, te bi uredbe trebalo izmijeniti kako bi se pojasnilo da su mjerodavne odredbe o IKT rizicima utvrđene u ovoj Uredbi.

U okviru postupka konsolidacije trebalo bi preispitati i revidirati relevantne smjernice o primjeni navedenih uredbi i direktiva koje su europska nadzorna tijela izdala ili ih upravo pripremaju kako bi pravna osnova za zahtjeve za IKT rizike u pravu Unije proizlazila isključivo iz ove Uredbe, njezinih provedbenih akata te odluka i preporuka koje su donesene u skladu s njom i koje se odnose na subjekte obuhvaćene njezinim područjem primjene.

(69a) Tehnički standardi trebali bi osigurati dosljedno usklađivanje zahtjeva utvrđenih u ovoj Uredbi. Europska nadzorna tijela, kao visokospecijalizirana stručna tijela, trebala bi biti ovlaštena za izradu nacrta regulatornih tehničkih standarda koji nisu povezani s političkim odlukama, a koji bi se potom dostavili Komisiji. Regulatorne tehničke standarde trebalo bi izraditi u područjima upravljanja IKT rizicima, izvješćivanja, testiranja i ključnih zahtjeva za pouzdano praćenje IKT rizika treće strane. ***Pri izradi nacrta regulatornih tehničkih standarda europska nadzorna tijela trebala bi uzeti u obzir svoj mandat u vezi s aspektima proporcionalnosti i zatražiti savjet od svojih savjetodavnih odbora za proporcionalnost, naročito u vezi s primjenom ove Uredbe na MSP-ove i poduzeća srednje tržišne kapitalizacije.***

(70) Posebno je važno da Komisija tijekom svojih priprema provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka. Komisija i europska nadzorna tijela trebali bi osigurati da te standarde i zahtjeve mogu primijeniti svi financijski subjekti na

[18] SL L 123, 12.5.2016., str. 1.

[19] [Unijeti cjelovito upućivanje]

način koji je proporcionalan prirodi, opsegu i složenosti tih subjekata i njihovih djelatnosti.

(71) Kako bi se olakšala usporedivost izvješća o značajnim IKT incidentima i osigurala transparentnost ugovora o korištenju IKT usluga trećih strana pružatelja IKT usluga, europska nadzorna tijela trebala bi biti ovlaštena za izradu nacrta provedbenih tehničkih standarda kojima se utvrđuju standardni obrasci i postupci za izvješćivanje financijskih subjekata o značajnim IKT incidentima te standardizirani predlošci za registar informacija. Pri izradi tih standarda europska nadzorna tijela trebala bi uzeti u obzir ***prirodu,*** veličinu***,*** složenost ***i poslovni profil*** financijskih subjekata te prirodu i rizičnost njihovih djelatnosti. Komisija bi trebala biti ovlaštena za donošenje tih provedbenih tehničkih standarda u obliku provedbenih akata u skladu s člankom 291. UFEU-a i u skladu s člankom 15. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 odnosno Uredbe (EU) br. 1095/2010. Budući da su dodatni zahtjevi već utvrđeni delegiranim i provedbenim aktima na temelju regulatornih i provedbenih tehničkih standarda, u uredbama (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014, primjereno je ovlastiti europska nadzorna tijela da zasebno ili zajednički u okviru Zajedničkog odbora podnose Komisiji regulatorne i provedbene tehničke standarde radi donošenja delegiranih i provedbenih akata kojima se prenose i ažuriraju postojeća pravila za upravljanje IKT rizicima.

(72) Donošenje ovog akta podrazumijeva posljedične izmjene postojećih delegiranih i provedbenih akata u različitim područjima propisa o financijskim uslugama. Područje primjene članaka o operativnim rizicima na temelju kojih su se u skladu s ovlastima iz tih akata donosili delegirani i provedbeni akti trebalo bi se izmijeniti kako bi se u ovu Uredbu prenijele sve odredbe o digitalnoj operativnoj otpornosti koje su sada dio tih uredbi.

(73) S obzirom na to da ciljeve ove Uredbe, to jest postizanje visoke razine digitalne operativne otpornosti svih financijskih subjekata, ne mogu dostatno ostvariti države članice jer je za to potrebno uskladiti velik broj različitih pravila, koja su sada dio određenih akata Unije ili pravnih sustava različitih država članica, te da se mogu bolje ostvariti na razini Unije zbog opsega i učinaka Uredbe, Unija može donijeti mjere u skladu s načelom supsidijarnosti kako je utvrđeno u članku 5. Ugovora o Europskoj uniji. U skladu s načelom proporcionalnosti, utvrđenim u tom članku, ova Uredba ne prelazi ono što je potrebno za ostvarivanje tih ciljeva.

DONIJELI SU OVU UREDBU:

POGLAVLJE I.

OPĆE ODREDBE

Članak 1.

Predmet

1. Ovom se Uredbom utvrđuju sljedeći jedinstveni zahtjevi za sigurnost mrežnih i informacijskih sustava koji podržavaju poslovne procese financijskih subjekata koji su potrebni za postizanje visoke zajedničke razine digitalne operativne otpornosti:

(a) zahtjevi primjenjivi na financijske subjekte koji se odnose na:

– upravljanje rizikom informacijske i komunikacije tehnologije (IKT),

– izvješćivanje nadležnih tijela o značajnim IKT incidentima,

– ***izvješćivanje nadležnih tijela o velikim operativnim incidentima ili sigurnosnim incidentima povezanima s plaćanjima koje osiguravaju financijska tijela iz članka 2. stavka 1. točaka od (a) do (c),***

– testiranje digitalne operativne otpornosti,

– razmjenu informacija i saznanja o kiberprijetnjama i ranjivostima,

– mjere financijskih subjekata za dobro upravljanje ***u području IKT rizika trećih strana***;

(b) zahtjevi koji se odnose na ugovore koje sklapaju treće strane pružatelji IKT usluga i financijski subjekti;

(c) nadzorni okvir za treće strane pružatelje ključnih IKT usluga kada pružaju usluge financijskim subjektima;

(d) pravila za suradnju nadležnih tijela i pravila za nadzor i izvršenje koje provode nadležna tijela u vezi sa svim pitanjima obuhvaćenima ovom Uredbom.

2. Kad je riječ o financijskim subjektima koji su identificirani kao operatori ključnih usluga u skladu s nacionalnim propisima kojima se prenosi članak 5. Direktive (EU) 2016/1148, ova Uredba smatra se pravnim aktom Unije za pojedini sektor za potrebe članka 1. stavka 7. te direktive.

2a. Ovom Uredbom ne dovode se u pitanje nadležnosti država članica u pogledu održavanja javne sigurnosti, obrane i nacionalne sigurnosti.

Članak 2.

Osobno područje primjene

1. Ova se Uredba primjenjuje na sljedeće subjekte:

(a) kreditne institucije;

(b) institucije za platni promet;

(c) institucije za elektronički novac;

(d) investicijska društva;

(e) pružatelje usluga povezanih s kriptoimovinom, izdavatelje ***i ponuditelje*** kriptoimovine, izdavatelje ***i ponuditelje*** tokena vezanih uz kriptoimovinu i izdavatelje značajnih tokena vezanih uz kriptoimovinu;

(f) središnje depozitorije ***i upravitelje sustava za namiru vrijednosnih papira***;

(g) središnje druge ugovorne strane;

(h) mjesta trgovanja;

(i) trgovinske repozitorije;

(j) upravitelje alternativnih investicijskih fondova;

(k) društva za upravljanje;

(l) pružatelje usluga dostave podataka;

(m) društva za osiguranje i društva za reosiguranje;

(n) posrednike u osiguranju, posrednike u reosiguranju i sporedne posrednike u osiguranju ***koji nisu mikro, mala ili srednja poduzeća, osim ako se ta mikro, mala ili srednja poduzeća ne oslanjaju isključivo na organizirane automatizirane sustave prodaje***;

(o) institucije za strukovno mirovinsko osiguranje ***koje ne upravljaju mirovinskim programima koji ukupno broje manje od 15 članova;***

(p) agencije za kreditni rejting;

(q) ovlaštene revizore i revizorska društva ***koji nisu mikro, mala ili srednja poduzeća, osim ako takva mikro, mala ili srednja poduzeća ne pružaju usluge revizije subjektima navedenima u ovom članku, uz iznimku mikro, malih ili srednjih poduzeća koja su neprofitni subjekti za reviziju u skladu s člankom 2. stavkom 3. Uredbe (EU) br. 537/2014, osim ako nadležno tijelo odluči da je ta iznimka nevažeća***;

(r) administratore ključnih referentnih vrijednosti;

(s) pružatelje usluga skupnog financiranja;

(t) sekuritizacijske repozitorije;

(u) treće strane pružatelje IKT usluga.

1a. Ova se Uredba, osim odjeljka II. poglavlja V., primjenjuje i na pružatelje IKT usluga unutar grupe.

2. Za potrebe ove Uredbe subjekti iz stavaka od (a) do (t) zajednički se nazivaju „financijski subjekti”.

2a. Za potrebe ove Uredbe, uz iznimku odjeljka II. Poglavlja V., treće strane pružatelji IKT usluga i pružatelji IKT usluga unutar grupe zajednički se nazivaju „treće strane pružatelji IKT usluga”.

Članak 3.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

(1) „digitalna operativna otpornost” znači sposobnost financijskog subjekta da izgradi, osigura i preispita svoj operativni integritet ▌osiguravajući, izravno ili neizravno, korištenjem usluga trećih strana pružatelja IKT usluga, ▌kontinuirano pružanje financijskih usluga i njihovu kvalitetu ***u slučaju operativnih poremećaja koji utječu na sposobnosti financijskog subjekta u području IKT-a***;

(2) „mrežni i informacijski sustav” znači mrežni i informacijski sustav kako je definiran u članku 4. točki 1. Direktive (EU) br. 2016/1148;

(3) „sigurnost mrežnih i informacijskih sustava” znači sigurnost mrežnih i informacijskih sustava kako je definirana u članku 4. točki 2. Direktive (EU) br. 2016/1148;

(4) „IKT rizik” znači svaka razumno prepoznatljiva okolnost koja se odnosi na korištenje mrežnih i informacijskih sustava, ▌ ***koja***, ako do ***nje*** dođe, može ugroziti sigurnost mrežnih i informacijskih sustava, svih alata ili procesa koji ovise o ***IKT-u***, funkcioniranje operacije i procesa ili pružanja usluga ▌;

(5) „informacijska imovina” znači skup materijalnih ili nematerijalnih informacija koje vrijedi zaštititi;

(6) „IKT incident” znači identificirani ***incident ili niz povezanih incidenata***, koji ***ugrožavaju*** sigurnost mrežnih i informacijskih sustava ▌ili ***imaju*** negativne učinke na dostupnost, povjerljivost, kontinuitet, ***cjelovitost*** ili autentičnost financijskih usluga koje financijski subjekt pruža;

(6a) „operativni incident ili sigurnosni incident povezan s plaćanjima” znači događaj ili niz povezanih događaja koje financijski subjekti iz članka 2. stavka 1. točaka od (a) do (c) nisu predvidjeti ili koji imaju ili vjerojatno mogu imati negativan učinak na cjelovitost, dostupnost, povjerljivost, autentičnost ili kontinuitet usluga povezanih s plaćanjima;

(7) „značajan IKT incident” znači IKT incident koji ***ima ili vjerojatno može imati velik negativan učinak*** na mrežne i informacijske sustave koji podržavaju ključne funkcije financijskog subjekta;

(7a) „velik operativni incident ili sigurnosni incident povezan s plaćanjima” znači operativni incident ili sigurnosni incident povezan s plaćanjima koji ispunjava kriterije utvrđene u članku 16.;

(8) „kiberprijetnja” znači „kiberprijetnja” kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća[20];

(8a) „ozbiljna kiberprijetnja” znači kiberprijetnja čije značajke jasno upućuju na to da će vjerojatno dovesti do značajnog IKT incidenta;

(9) „kibernapad” znači zlonamjeran IKT incident uzrokovan pokušajem uništavanja, objave, izmjene, onemogućavanja, krađe ili neovlaštenog pristupa ili neovlaštenog korištenja imovine koji je počinio neki akter prijetnji;

(10) „saznanja o prijetnjama” znači informacije koje su agregirane, preoblikovane, analizirane, protumačene ili obogaćene kako bi se dobio kontekst potreban za donošenje

[20] Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

odluka i koje omogućavaju relevantno i dostatno razumijevanje za ublažavanje učinka IKT incidenta ili kiberprijetnje, uključujući tehničke pojedinosti kibernapada, osobe odgovorne za napad te njihov način rada i motive;

(11) „dubinska obrana” znači strategija IKT-a koja povezuje ljude, procese i tehnologije radi uspostave raznih prepreka na više različitih razina i dimenzija subjekta;

(12) „ranjivost” znači slabost, osjetljivost ili nedostatak nekog resursa, sustava, procesa ili kontrole koje kiberprijetnja može iskoristiti;

(13) „penetracijska testiranja vođena prijetnjama” znači okvir koji oponaša taktike, tehnike i procedure stvarnih aktera prijetnji koje se smatraju stvarnom kiberprijetnjom, koji omogućuje kontrolirano, prilagođeno testiranje subjektovih ključnih sustava trenutačno u produkciji, na temelju saznanja o prijetnjama („crveni tim”);

(14) „IKT rizik treće strane” znači IKT rizik koji može nastati financijskom subjektu u vezi s njegovim korištenjem IKT usluga trećih strana pružatelja IKT usluga ili podugovaratelja trećih strana;

(15) „treća strana pružatelj IKT usluga” znači poduzetnik koji pruža ***IKT*** usluge, ***uključujući financijski subjekt koji pruža IKT usluge i koji je dio poduzetnika koji pruža širi raspon proizvoda ili usluga***, ali ne uključujući pružatelje hardverskih komponenti i poduzetnike ovlaštene u skladu s pravom Unije koji pružaju elektroničke komunikacijske usluge kako su definirane u članku 2. točki 4. Direktive (EU) 2018/1972 Europskog parlamenta i Vijeća[21];

(15a) „pružatelj IKT usluga unutar grupe” znači poduzetnik koji je dio financijske grupe i koji IKT usluge pruža isključivo financijskim subjektima unutar iste grupe ili financijskim subjektima koji pripadaju istom institucionalnom sustavu zaštite, uključujući njihova matična društva, društva kćeri, podružnice ili druge subjekte koji su u zajedničkom vlasništvu ili pod zajedničkom kontrolom;

(16) „IKT usluge” znači digitalne i podatkovne usluge koje se u okviru sustava IKT-a ***kontinuirano*** pružaju jednom ili više unutarnjih ili vanjskih korisnika***, uz iznimku telekomunikacijskih ugovora***;

(17) „ključna ili važna funkcija” znači ***aktivnost ili usluga koja je od temeljne važnosti za rad financijskog subjekta i čiji bi prekid bitno narušio pouzdanost ili kontinuitet usluga i aktivnosti financijskog subjekta ili*** čiji bi prestanak, neispravnost ili neizvršenje bitno narušilo kontinuirano ispunjavanje uvjeta i obveza financijskog subjekta u skladu s njegovim odobrenjem za rad ili s drugim obvezama u skladu s primjenjivim zakonodavstvom o financijskim uslugama, ***uključujući „ključne funkcije” kako su definirane u članku 2. stavku 1. točki 35. Direktive 2014/59/EU;***

(18) „treća strana pružatelj ključnih IKT usluga” znači treća strana pružatelj IKT usluga imenovana u skladu s člankom ***28***. na koju se primjenjuje nadzorni okvir iz članaka od ***30***. do 37.;

(19) „treća strana pružatelj IKT usluga sa sjedištem u trećoj zemlji” znači treća strana pružatelj IKT usluga koja je pravna osoba sa sjedištem u trećoj zemlji, ▌koja je s financijskim subjektom sklopila ugovor o pružanju IKT usluga;

---

[21] Direktiva (EU) 2018/1972 Europskog parlamenta i Vijeća od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija (preinaka) (SL L 321, 17.12.2018., str. 36.).

(20) „podugovaratelj IKT usluga sa sjedištem u trećoj zemlji” znači podugovaratelj IKT-a koji je pravna osoba sa sjedištem u trećoj zemlji, ▌koji je sklopio ugovor s trećom stranom pružateljem IKT usluga ili s trećom stranom pružateljem IKT usluga sa sjedištem u trećoj zemlji;

(21) „koncentracijski rizik IKT-a” znači izloženost prema jednoj ili više povezanih trećih strana pružatelja ključnih IKT usluga, čime se stvara stupanj ovisnosti o takvim pružateljima tako da nedostupnost, kvar ili druga vrsta nedostatka tih pružatelja može potencijalno ugroziti ***financijsku stabilnost Unije u cjelini ili*** sposobnost financijskog subjekta ▌za obavljanje ključnih funkcija ili može dovesti do drugih vrsta negativnih učinaka, među ostalim velikih gubitaka;

(22) „upravljačko tijelo” znači upravljačko tijelo kako je definirano u članku 4. stavku 1. točki 36. Direktive 2014/65/EU, članku 3. stavku 1. točki 7. Direktive 2013/36/EU, članku 2. stavku 1. točki (s) Direktive 2009/65/EZ, članku 2. stavku 1. točki 45. Uredbe (EU) br. 909/2014, članku 3. stavku 1. točki 20. Uredbe (EU) 2016/1011 Europskog parlamenta i Vijeća[22], članku 3. stavku 1. točki ***18.*** Uredbe (EU) 20xx/xx Europskog parlamenta i Vijeća[23] [MICA] ili ekvivalentne osobe koje djelotvorno upravljaju subjektom ili imaju ključne funkcije u skladu s relevantnim zakonodavstvom Unije ili nacionalnim zakonodavstvom;

(23) „kreditna institucija” znači kreditna institucija kako je definirana u članku 4. stavku 1. točki 1. Uredbe (EU) 575/2013 Europskog parlamenta i Vijeća[24];

(23a) „kreditna institucija izuzeta Direktivom 2013/36/EU” znači institucija koja ostvaruje korist od izuzeća u skladu s člankom 2. stavkom 5. točkama od (4.) do (23.) Direktive 2013/36/EU;

(24) „investicijsko društvo” znači investicijsko društvo kako je definirano u članku 4. stavku 1. točki 1. Direktive 2014/65/EU;

(24a) „malo i međusobno nepovezano investicijsko društvo” znači investicijsko društvo koje ispunjava uvjete utvrđene u članku 12. stavku 1. Uredbe (EU) 2019/2033;

(25) „institucija za platni promet” znači institucija za platni promet kako je definirana u članku 1. stavku 1. točki (d) Direktive (EU) 2015/2366;

(25a) „institucija za platni promet izuzeta Direktivom 2015/2366” znači institucija za platni promet koja ostvaruje korist od izuzeća u skladu s člankom 32. stavkom 1. Direktive (EU) 2015/2366;

(26) „institucija za elektronički novac” znači institucija za elektronički novac kako je definirana u članku 2. točki 1. Direktive 2009/110/EZ Europskog parlamenta i Vijeća[25];

---

22 Uredba (EU) 2016/1011 Europskog parlamenta i Vijeća od 8. lipnja 2016. o indeksima koji se upotrebljavaju kao referentne vrijednosti u financijskim instrumentima i financijskim ugovorima ili za mjerenje uspješnosti investicijskih fondova i o izmjeni direktiva 2008/48/EZ i 2014/17/EU te Uredbe (EU) br. 596/2014 (SL L 171, 29.6.2016., str. 1.).

23 [*Molimo umetnuti puni naslov i podatke o SL-u*]

24 Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1.).

25 Direktiva 2009/110/EZ Europskog parlamenta i Vijeća od 16. rujna 2009. o osnivanju, obavljanju djelatnosti i bonitetnom nadzoru poslovanja institucija za elektronički novac te o izmjeni direktiva 2005/60/EZ i 2006/48/EZ i stavljanju izvan snage Direktive 2000/46/EZ (SL L 267, 10.10.2009., str. 7.).

(26a) „institucija za elektronički novac izuzeta Direktivom 2009/110/EZ" znači institucija za elektronički novac koja ostvaruje korist od izuzeća na temelju članka 9. Direktive 2009/110/EZ;

(27) „središnja druga ugovorna strana" znači središnja druga ugovorna strana kako je definirana u članku 2. točki 1. Uredbe (EU) br. 648/2012;

(28) „trgovinski repozitorij" znači trgovinski repozitorij kako je definiran u članku 2. točki 2. Uredbe (EU) br. 648/2012;

(29) „središnji depozitorij vrijednosnih papira" znači središnji depozitorij vrijednosnih papira kako je definiran u članku 2. stavku 1. točki 1. Uredbe 909/2014;

(30) „mjesto trgovanja" znači mjesto trgovanja kako je definirano u članku 4. stavku 1. točki 24. Direktive 2014/65/EU;

(31) „upravitelj alternativnih investicijskih fondova" znači upravitelj alternativnih investicijskih fondova kako je definiran u članku 4. stavku 1. točki (b) Direktive 2011/61/EU;

(32) „društvo za upravljanje" znači društvo za upravljanje kako je definirano u članku 2. stavku 1. točki (b) Direktive 2009/65/EZ;

(33) „pružatelj usluga dostave podataka" znači pružatelj usluga dostave podataka kako je definiran u članku 4. stavku 1. točki 63. Direktive 2014/65/EU;

(34) „društvo za osiguranje" znači društvo za osiguranje kako je definirano u članku 13. točki 1. Direktive 2009/138/EZ;

(35) „društvo za reosiguranje" znači društvo za reosiguranje kako je definirano u članku 13. točki 4. Direktive 2009/138/EZ;

(36) „posrednik u osiguranju" znači posrednik u osiguranju kako je definiran u članku 2. ***stavku 1.*** točki 3. Direktive (EU) 2016/97;

(37) „sporedni posrednik u osiguranju" znači sporedni posrednik u osiguranju kako je definiran u članku 2. ***stavku 1.*** točki 4. Direktive (EU) 2016/97;

(38) „posrednik u reosiguranju" znači posrednik u reosiguranju kako je definiran u članku 2. ***stavku 1.*** točki 5. Direktive (EU) 2016/97;

(39) „institucija za strukovno mirovinsko osiguranje" znači institucija za strukovno mirovinsko osiguranje kako je definirana u članku 6. točki 1. Direktive 2016/2341;

(40) „agencija za kreditni rejting" znači agencija za kreditni rejting kako je definirana u članku 3. stavku 1. točki (b) Uredbe (EZ) br. 1060/2009;

(41) „ovlašteni revizor" znači ovlašteni revizor kako je definiran u članku 2. točki 2. Direktive 2006/43/EZ;

(42) „revizorsko društvo" znači revizorsko društvo kako je definirano u članku 2. točki 3. Direktive 2006/43/EZ;

(43) „pružatelj usluga povezanih s kriptoimovinom" znači pružatelj usluga povezanih s kriptoimovinom kako je definiran u članku 3. stavku 1. točki (***8***.) Uredbe (EU) 202x/xx [Ured za publikacije: unijeti upućivanje na Uredbu MICA];

(44) „izdavatelj kriptoimovine" znači izdavatelj kriptoimovine kako je definiran u članku 3. stavku 1. točki (***6.***) [Ured za publikacije: unijeti upućivanje na Uredbu MICA];

(44a) „ponuditelj" znači ponuditelj kako je definiran u članku 3. stavku 1. točki [(XX)] [Ured za publikacije: unijeti upućivanje na Uredbu MICA];

(44b) „ponuditelj kriptoimovine" znači ponuditelj kriptoimovine kako je definiran u članku 3. stavku 1. točki [(XX)] [Ured za publikacije: unijeti upućivanje na Uredbu MICA];

(45) „izdavatelj tokena vezanih uz kriptoimovinu" znači izdavatelj tokena vezanih uz kriptoimovinu kako je definiran u članku 3. stavku 1. točki (i) [Ured za publikacije: unijeti upućivanje na Uredbu MICA];

(45a) „ponuditelj tokena vezanih uz kriptoimovinu" znači ponuditelj tokena vezanih uz kriptoimovinu kako je definiran u članku 3. stavku 1. točki [(XX)] [Ured za publikacije: unijeti upućivanje na Uredbu MICA];

(46) „izdavatelj značajnih tokena vezanih uz kriptoimovinu" znači izdavatelj značajnih tokena vezanih uz kriptoimovinu kako je definiran u članku 3. stavku 1. točki (***XX***) [Ured za publikacije: unijeti upućivanje na Uredbu MICA];

(47) „administrator ključnih referentnih vrijednosti" znači administrator ključnih referentnih vrijednosti kako je definiran u članku ***3***. točki ***(25.)*** Uredbe ***2016/1011*** [Ured za publikacije: unijeti upućivanje na Uredbu o referentnim vrijednostima];

(48) „pružatelj usluga skupnog financiranja" znači pružatelj usluga skupnog financiranja kako je definiran u članku ***2***. ***stavku 1.*** točki (***e***) Uredbe (EU) ***2020/1503*** [Ured za publikacije: unijeti upućivanje na Uredbu o skupnom financiranju];

(49) „sekuritizacijski repozitorij" znači sekuritizacijski repozitorij kako je definiran u članku 2. točki 23. Uredbe (EU) 2017/2402;

(50) „mikropoduzeće***, malo i srednje poduzeće***" znači financijski subjekt kako je definiran u članku 2. Priloga Preporuci 2003/361/EZ.

(50a) „sanacijsko tijelo" znači tijelo koje je država članica imenovala u skladu s člankom 3. Direktive 2014/59/EU ili Jedinstveni sanacijski odbor uspostavljen u skladu s člankom 42. Uredbe 806/2014.

Članak 3.a

Načelo proporcionalnosti

1. Financijski subjekti provode pravila uvedena poglavljima II., III. i IV. u skladu s načelom proporcionalnosti, uzimajući u obzir njihovu veličinu, prirodu, opseg i složenost njihovih usluga, aktivnosti i poslovanja te njihov ukupni profil rizičnosti.

2. U skladu s načelom proporcionalnosti, članci od 4. do 14. ove Uredbe ne primjenjuju se na:

(a) mala i međusobno nepovezana investicijska društva ili institucije za platni promet izuzete Direktivom (EU) 2015/2366;

(b) kreditne institucije izuzete Direktivom 2013/36/EU;

(c) institucije za elektronički novac izuzete na temelju Direktive 2009/110/EZ; ili

(d) male institucije za strukovno mirovinsko osiguranje.

3. Na temelju godišnjeg izvješća o preispitivanju okvira upravljanja IKT rizicima iz članka 5. stavka 6. i članka 14.a stavka 2. relevantna nadležna tijela preispituju i ocjenjuju kako financijski subjekt primjenjuje proporcionalnost te utvrđuju osigurava li okvir upravljanja IKT rizicima financijskog subjekta dobro upravljanje i digitalnu operativnu otpornost i pokrivenost IKT rizika. Pritom nadležna tijela uzimaju u obzir veličinu financijskog subjekta, prirodu, opseg i složenost njegovih usluga, aktivnosti i poslovanja te njegov ukupni profil rizičnosti.

4. Ako relevantno nadležno tijelo smatra da je okvir upravljanja IKT rizicima financijskog subjekta nedovoljan i nerazmjeran, ono započinje dijalog s financijskim subjektom kako bi se ispravili nedostaci i osigurala potpuna usklađenost s poglavljem II.

5. Europska nadzorna tijela sastavljaju nacrt regulatornih tehničkih standarda u odnosu na sljedeće:

(a) određivanje u kojoj se mjeri obveze upravljanja IKT rizicima primjenjuju na svaki financijski subjekt naveden u stavku 1.;

(b) dodatno utvrđivanje sadržaja i formata godišnjeg izvješća o preispitivanju okvira upravljanja IKT rizicima iz stavka 3.;

(c) dodatno određivanje pravila i postupaka kojih se nadležna tijela i financijski subjekti moraju pridržavati u dijalogu iz stavka 4.

6. Europska nadzorna tijela nacrt regulatornih tehničkih standarda iz stavka 5. podnose Komisiji do [Ured za publikacije: unijeti datum: jednu godinu od datuma stupanja na snagu].

Komisiji se delegira ovlast za donošenje regulatornih tehničkih standarda iz stavka 5. ovog članka u skladu s člancima od 10. do 14. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 te (EU) br. 1095/2010.

POGLAVLJE II.

UPRAVLJANJE IKT RIZICIMA

ODJELJAK I.

Članak 4.

Upravljanje i organizacija

1. Financijski subjekti dužni su imati ***uspostavljen okvir*** unutarnjeg upravljanja i kontrole kojim se osigurava djelotvorno i razborito upravljanje svim IKT rizicima***, u cilju ostvarivanja visoke razine digitalne operativne otpornosti***.

2. Upravljačko tijelo financijskog subjekta određuje, odobrava, nadzire i odgovorno je za provedbu svih mehanizama povezanih s okvirom upravljanja IKT rizicima iz članka 5. stavka 1.

   Za potrebe prvog podstavka upravljačko tijelo:

   (a) snosi krajnju odgovornost za upravljanje IKT rizicima financijskog subjekta;

   (aa) uspostavlja postupke i politike čiji je cilj osigurati održavanje visokih standarda sigurnosti, povjerljivosti i cjelovitosti podataka;

   (b) određuje jasne uloge i odgovornosti svih funkcija u području IKT-a;

   (c) utvrđuje odgovarajuću razinu tolerancije financijskog subjekta na IKT rizike, kako je navedeno u članku 5. stavku 9. točki (b);

   (d) odobrava, nadzire i periodično preispituje način na koji financijski subjekt provodi politiku kontinuiteta poslovanja u području IKT-a iz članka 10. stavka 1. i plan oporavka u slučaju katastrofe u području IKT-a iz članka 10. stavka 3.***, koji se mogu donijeti kao posebna politika i kao sastavni dio šire politike kontinuiteta poslovanja financijskog subjekta na razini cijelog poslovanja i plana oporavka od kriznih situacija***;

   (e) odobrava i periodično preispituje planove revizije IKT-a, revizije IKT-a i njihove bitne izmjene;

   (f) izrađuje i periodično preispituje odgovarajući proračun za ispunjavanje potreba financijskog subjekta u pogledu digitalne operativne otpornosti, i to za sve vrste resursa, uključujući ***odgovarajuće*** osposobljavanje o IKT rizicima i stjecanje vještina za sve članove osoblja ▌;

   (g) odobrava i periodično preispituje politiku financijskog subjekta za ugovore o korištenju IKT usluga trećih strana pružatelja IKT usluga;

   (h) mora biti pravodobno obaviješteno o ugovorima o korištenju IKT usluga sklopljenima s trećim stranama pružateljima IKT usluga, o svim relevantnim planiranim bitnim promjenama povezanima s trećim stranama pružateljima

IKT usluga te o mogućem učinku tih promjena na ključne ili važne funkcije obuhvaćene tim ugovorima, što uključuje i dobivanje sažetka analize rizika radi procjene učinka tih promjena;

(i) ***redovno*** je obaviješteno ***barem*** o ***većim*** IKT incidentima i njihovu učinku te o odgovoru, oporavku i korektivnim mjerama.

3. Financijski subjekti, osim mikropoduzeća, dužni su uvesti funkciju za praćenje ugovora o korištenju IKT usluga ***unutar financijskog subjekta, posebno onih*** sklopljenih s trećim stranama pružateljima IKT usluga ili odrediti člana višeg rukovodstva koji će biti odgovoran za nadzor povezane izloženosti rizicima i relevantne dokumentacije.

4. Članovi upravljačkog tijela ***financijskog subjekta*** dužni su ***aktivno*** osvježavati znanje i vještine koje će im pomoći u razumijevanju i procjeni IKT rizika i njihova učinka na poslovanje financijskog subjekta***, među ostalim redovitim posebnim osposobljavanjem razmjerno rizicima IKT-a kojima se upravlja***.

ODJELJAK II.

Članak 5.

Okvir upravljanja IKT rizicima

1. Financijski subjekti dužni su imati pouzdan, sveobuhvatan i dobro dokumentiran okvir upravljanja IKT rizicima koji im omogućuje brzo, učinkovito i sveobuhvatno uklanjanje IKT rizika te osigurava visoku razinu digitalne operativne otpornosti ▌.

2. Okvir upravljanja IKT rizicima iz stavka 1. sadržava strategije, politike, postupke te protokole i alate IKT-a koji su potrebni za pravodobnu i djelotvornu zaštitu svih bitnih fizičkih komponenti i infrastruktura, uključujući računalni hardver, poslužitelja te svih bitnih prostora, podatkovnih centara i područja određenih kao osjetljivih kako bi se osiguralo da su svi ti fizički elementi primjereno zaštićeni od rizikâ, među ostalim oštećenja i neovlaštenog pristupa ili uporabe.

3. Financijski subjekti dužni su smanjivati učinak IKT rizika uvođenjem odgovarajućih strategija, politika, postupaka, protokola i alata u skladu s okvirom upravljanja IKT rizicima. Dužni su dostavljati potpune i ažurirane informacije o IKT rizicima ***i o njihovu okviru upravljanja IKT rizicima*** u skladu sa zahtjevima nadležnih tijela.

4. Kao dio okvira upravljanja IKT rizicima iz stavka 1. financijski subjekti, osim mikropoduzeća, dužni su uvesti i redovito preispitivati sustav upravljanja sigurnošću informacija koji se temelji na priznatim međunarodnim standardima i u skladu je sa smjernicama o nadzoru***, ako su već dostupne i primjerene, uključujući smjernice utvrđene u relevantnim smjernicama koje su utvrdila europska nadzorna tijela***.

5. Financijski subjekti, osim mikropoduzeća, ***dodjeljuju odgovornost za upravljanje IKT rizicima i nadzor nad njima kontrolnoj funkciji i osiguravaju neovisnost te kontrolne funkcije kako bi se izbjegli sukobi interesa. Financijski subjekti*** dužni su na odgovarajući način osigurati ***neovisnost*** funkcije upravljanja IKT-om, funkcije kontrole i funkcije unutarnje revizije u skladu s modelom „tri crte obrane” ili modelom unutarnje kontrole i upravljanja rizicima.

6. Okvir upravljanja IKT rizicima iz stavka 1. dokumentira se i preispituje najmanje jednom godišnje i po nastanku svakog značajnog IKT incidenta te u skladu s uputama ili zaključcima nadzornog tijela koji proizlaze iz relevantnog testiranja digitalne operativne otpornosti ili revizijskih procesa. Kontinuirano ga se poboljšava na temelju pouka iz provedbe i praćenja.

Izvješće o preispitivanju okvira upravljanja IKT rizicima podnosi se nadležnom tijelu jednom godišnje.

7. ***Kad je riječ o financijskim subjektima, osim mikropoduzeća,*** okvir upravljanja IKT rizicima iz stavka 1. redovito revidiraju revizori za IKT koji imaju dostatno znanje, vještine i iskustvo s IKT rizicima. Učestalost i predmet revizija IKT-a razmjerni su IKT rizicima financijskog subjekta.

8. Službeni proces praćenja poduzetih mjera, uključujući pravila za pravodobnu provjeru i ispravljanje ključnih nalaza revizije IKT-a, uspostavlja se uzimajući u obzir zaključke revizijskog preispitivanja [redacted].

9. Okvir upravljanja IKT rizicima iz stavka 1. sadržava strategiju digitalne ***operativne*** otpornosti u kojoj je utvrđen način provedbe okvira. U tu svrhu u strategiji se opisuju metode za ublažavanje IKT rizika i ostvarenje posebnih ciljeva u području IKT-a na sljedeći način:

   (a) objasniti kako okvir upravljanja IKT rizicima podržava poslovnu strategiju i ciljeve financijskog subjekta;

   (b) utvrditi razinu tolerancije na IKT rizike u skladu sa sklonošću preuzimanju rizika financijskog subjekta te analizirati učinak tolerancije ***za*** poremećaje u radu IKT-a;

   (c) utvrditi jasne ciljeve informacijske sigurnosti;

   (d) objasniti [redacted]arhitekturu IKT-a i sve promjene koje su potrebne za ostvarenje posebnih poslovnih ciljeva;

   (e) u glavnim crtama izložiti različite mehanizme uspostavljene za otkrivanje IKT incidenata, zaštitu od njih i sprečavanje njihovih učinaka;

   (f) jasno prikazati broj prijavljenih značajnih IKT incidenata i djelotvornost preventivnih mjera;

   (g) ***utvrditi*** ključne ovisnosti o trećim stranama pružateljima IKT usluga ***i detaljno utvrditi izlazne strategije u vezi s tim ključnim ovisnostima***;

   (h) uvesti testiranje digitalne operativne otpornosti***, u skladu s poglavljem IV. ove Uredbe***;

   (i) u glavnim crtama izložiti komunikacijsku strategiju u slučaju IKT incidenata ***koju je potrebno objaviti u skladu s člankom 13***.

10. Po odobrenju nadležnih tijela financijski subjekti mogu ***eksternalizirati*** zadaće provjere usklađenosti sa zahtjevima za upravljanje IKT rizicima [redacted]vanjskom poduzeću.

Nakon što obavijeste nadležna tijela financijski subjekti mogu delegirati zadaće provjere usklađenosti sa zahtjevima za upravljanje IKT rizicima poduzeću unutar grupe.

Ako se uvede delegiranje iz drugog podstavka, financijski subjekt ostaje u potpunosti odgovoran za provjeru usklađenosti sa zahtjevima za upravljanje IKT rizicima.

Članak 6.

Sustavi, protokoli i alati IKT-a

1. ***U cilju uklanjanja IKT rizika i upravljanja njima,*** financijski subjekti dužni su koristiti i održavati sustave, protokole i alate IKT-a koji ispunjavaju sljedeće uvjete:

   (a) sustavi i alati primjereni su ▌razmjeru aktivnosti koje podržavaju poslovanje tih subjekata;

   (b) pouzdani su;

   (c) imaju dostatan kapacitet za preciznu obradu podataka potrebnih da bi se aktivnosti izvršile i usluge pružile pravodobno te za najjače opterećenje nalozima, porukama ili transakcijama prema potrebi, među ostalim u slučaju uvođenja nove tehnologije;

   (d) tehnološki su tako otporni da mogu prema potrebi primjereno ispuniti dodatne potrebe za obradom informacija u stresnim okolnostima na tržištu ili drugim nepovoljnim situacijama.

2. Kada primjenjuju međunarodno priznate tehničke standarde i vodeće sektorske postupke u području informacijske sigurnosti i unutarnjih kontrola IKT-a, financijski subjekti dužni su te standarde i postupke primjenjivati u skladu s mjerodavnim preporukama o nadzoru njihove primjene.

Članak 7.

Utvrđivanje

1. Kao dio okvira upravljanja IKT rizicima iz članka 5. stavka 1. financijski subjekti dužni su utvrditi, klasificirati i na odgovarajući način dokumentirati sve ***ključne ili važne*** poslovne funkcije u području IKT-a, informacijsku imovinu koja podržava te funkcije te konfiguracije sustava IKT-a i međusobnu povezanost unutarnjih i vanjskih sustava IKT-a. Financijski subjekti dužni su preispitati prema potrebi, a najmanje jednom godišnje, ***ključnost ili važnost poslovnih funkcija u području IKT-a, kao i*** primjerenost klasifikacije informacijske imovine i sve relevantne dokumentacije.

2. Financijski subjekti kontinuirano utvrđuju sve izvore IKT rizika, osobito izloženost riziku drugih financijskih subjekata, te procjenjuju kiberprijetnje i ranjivosti IKT-a koje su bitne za njihove ***ključne ili važne*** poslovne funkcije u području IKT-a i informacijsku imovinu. Financijski subjekti dužni su redovito, a najmanje jednom godišnje, preispitivati scenarije rizika koji utječu na njih.

3. Financijski subjekti, osim mikropoduzeća, dužni su ***po potrebi*** provesti procjenu rizika nakon svake velike promjene u infrastrukturi mrežnog i informacijskog sustava, u procesima ili postupcima koji utječu na njihove funkcije, popratne procese ili informacijsku imovinu.

4. Financijski subjekti dužni su utvrditi sve račune u sustavima IKT-a, među ostalima one na udaljenim lokacijama, mrežne resurse i hardversku opremu te popisati fizičku opremu koju smatraju ključnom. Dužni su mapirati konfiguraciju ***ključne ili važne*** IKT imovine ***uzimajući u obzir njihovu svrhu*** te veze i međusobnu ovisnost među ***tom*** različitom IKT imovinom.

5. Financijski subjekti dužni su utvrditi i dokumentirati sve ***ključne ili važne*** procese koji ovise o trećim stranama pružateljima IKT usluga te utvrditi međusobnu povezanost s trećim stranama pružateljima IKT usluga ***kojima se podupiru ključne ili važne funkcije***.

6. Za potrebe stavaka 1., 4. i 5. financijski subjekti dužni su voditi i redovito ažurirati relevantne evidencije.

7. Financijski subjekti, osim mikropoduzeća, dužni su redovito, a najmanje jednom godišnje, provesti posebnu procjenu IKT rizika za sve naslijeđene sustave IKT-a, ***uključujući sustave koji su još u upotrebi i obavljaju svoju funkciju, ali za koje vrijedi sljedeće:***

   (a) stari su ili na kraju njihova vijeka trajanja, u slučaju hardvera;

   (b) njihov dobavljač više ne može osigurati podršku ili održavanje; ili

   (c) ažuriranje nije moguće ili je neisplativo. Godišnje procjene rizika IKT-a provode se za sve naslijeđene sustave IKT-a, posebno prije i nakon povezivanja ▌tehnologija, aplikacija ili sustava.

Članak 8.

Zaštita i sprečavanje

1. Za potrebe primjerene zaštite sustavâ IKT-a i u cilju organizacije mjera odgovora financijski subjekti dužni su kontinuirano pratiti i kontrolirati funkcioniranje sustava i alata IKT-a te smanjivati učinak tih rizika uvođenjem odgovarajućih alata, politika i postupaka za sigurnost IKT-a.

2. Financijski subjekti dužni su osmisliti, izraditi i provoditi strategije, politike, postupke, protokole i alate za sigurnost IKT-a čiji je cilj ponajprije osigurati otpornost, kontinuitet i dostupnost sustava IKT-a ***koji podržavaju ključne ili važne funkcije*** te održavati visoke standarde sigurnosti, povjerljivosti i cjelovitosti podataka, neovisno o tome jesu li u mirovanju, uporabi ili prijenosu.

3. Kako bi ostvarili ciljeve iz stavka 2., financijski subjekti dužni su koristiti ▌tehnologiju i procese u području IKT-a koji:

   (a) ***u najvećoj mogućoj mjeri povećavaju*** sigurnost sredstava prijenosa informacija;

   (b) smanjuju rizik od oštećenja ili gubitka podataka, neovlaštenog pristupa i tehničkih nedostataka koji mogu onemogućiti poslovanje;

   (c) sprečavaju odavanje informacija;

(d) osiguravaju zaštitu podataka od ***internih IKT rizika, uključujući*** lošu administraciju, rizika povezanih s obradom ***i ljudskom greškom***.

4. Kao dio okvira upravljanja IKT rizicima iz članka 5. stavka 1., ***u skladu sa svojim profilom rizičnosti*** financijski subjekti dužni su:

(a) izraditi i dokumentirati politiku informacijske sigurnosti u kojoj se utvrđuju pravila zaštite povjerljivosti, cjelovitosti i dostupnosti ***resursa IKT-a, podataka i informacijske imovine subjekata, uz osiguravanje potpune zaštite*** resursa IKT-a, podataka i informacijske imovine njihovih korisnika ***ako obuhvaćaju dio IKT sustava financijskih subjekata***;

(b) primjenom pristupa koji se temelji na procjeni rizika izgraditi pouzdano upravljanje mrežom i infrastrukturom u kojem se primjenjuju odgovarajuće tehnike, metode i protokoli ***koji mogu uključivati*** mehanizme izoliranja zahvaćene informacijske imovine u slučaju kibernapada;

(c) provoditi politike***, postupke i kontrole*** kojima se fizički i virtualni pristup resursima i podacima u sustavu IKT-a ograničava samo na ono što je nužno za legitimne i odobrene funkcije i aktivnosti ;

(d) provoditi politike i protokole za snažne mehanizme autentifikacije ***i zaštitu kriptografskih ključeva*** na temelju mjerodavnih standarda i namjenskih sustava kontrola ;

(e) provoditi politike, postupke i kontrole za upravljanje promjenama IKT-a, uključujući promjene softvera, hardvera, komponenti ugrađenog softvera, sustava ili sigurnosnih značajki, koje se temelje na procjeni rizika i sastavni su dio općeg procesa upravljanja promjenama financijskog subjekta, kako bi se osiguralo kontrolirano evidentiranje, testiranje, procjena, odobravanje, provedba i provjera promjena u sustavima IKT-a;

(f) primjenjivati odgovarajuće i sveobuhvatne politike za zakrpe i ažuriranja.

Za potrebe točke (b) financijski subjekti dužni su projektirati infrastrukturu za mrežnu vezu tako da ju je moguće prekinuti ***što prije*** i osigurati njezinu segmentaciju i razdvajanje kako bi se smanjila i spriječila zaraza, posebno u slučaju međusobno povezanih financijskih procesa.

Za potrebe točke (e) proces upravljanja promjenama IKT-a dužni su odobriti odgovarajuće razine upravljanja i imati posebne protokole za hitne promjene.

Članak 9.

Otkrivanje

1. Financijski subjekti dužni su uspostaviti mehanizme brzog otkrivanja neobičnih aktivnosti u skladu s člankom 15., uključujući probleme s performansama mreže IKT-a i IKT incidente, te ***ako je to moguće u tehnološkom smislu*** utvrditi ***i nadzirati*** sve moguće bitne jedinstvene točke prekida.

Svi mehanizmi otkrivanja iz prvog podstavka redovito se testiraju u skladu s člankom 22.

2. Mehanizmima otkrivanja iz stavka 1. ▌otkrivaju se IKT incidenti i primjena procesa odgovora na IKT incidente***, među ostalim*** automatski mehanizmi upozoravanja za relevantno osoblje nadležno za odgovor na IKT incidente.

3. Financijski subjekti dužni su izdvojiti dovoljno resursa i kapaciteta ▌za praćenje aktivnosti korisnika, neobičnih pojava u IKT-u i IKT incidenata, posebno kibernapada.

3a Financijski subjekti evidentiraju sve IKT incidente koji utječu na stabilnost, kontinuitet ili kvalitetu financijskih usluga, uključujući slučajeve u kojima incident ima ili bio mogao imati učinak na te usluge;

4. Financijski subjekti iz članka 2. stavka 1. točke (l) usto su dužni uspostaviti sustave koji mogu djelotvorno provjeriti jesu li izvješća o trgovanju potpuna, utvrditi propuste ili očite pogreške te zahtijevati ponovni prijenos takvih pogrešnih izvješća.

Članak 10.

Odgovor i oporavak

1. Kao dio okvira upravljanja IKT rizicima iz članka 5. stavka 1. i na temelju zahtjeva utvrđivanja iz članka 7. financijski subjekti dužni su uvesti ▌ sveobuhvatnu politiku kontinuiteta poslovanja u području IKT-a ***koja se može donijeti kao namjenska posebna politika i*** kao sastavni dio svoje ***šire*** politike za kontinuitet operativnog poslovanja ***na razini cijelog poslovanja***.

Politikom kontinuiteta poslovanja u području IKT-a nastoji se upravljati rizicima i smanjiti rizike koji bi mogli imati štetan učinak na sustave IKT-a i IKT usluge financijskih subjekata te olakšati njihov brz oporavak ako je to potrebno. Pri izradi politike kontinuiteta poslovanja u području IKT-a financijski subjekti posebno uzimaju u obzir rizike koji bi mogli imati štetan učinak na IKT usluge i sustave IKT-a.

2. Financijski subjekti provode politiku kontinuiteta poslovanja u području IKT-a iz stavka 1. s pomoću namjenskih, primjerenih i dokumentiranih sustava, planova, postupaka i mehanizama koji služe za:

(b) osiguravanje kontinuiteta ključnih funkcija financijskog subjekta;

(c) brz, primjeren i djelotvoran odgovor na sve IKT incidente, osobito no ne ograničavajući se na kibernapade, i njihovo rješavanje na način kojim se ograničava šteta i daje prednost nastavku poslovanja i mjerama oporavka;

(d) brzu aktivaciju bez namjenskih planova kojima su osigurane mjere, procesi i tehnologije blokiranja koji su prilagođeni svakoj vrsti IKT incidenta i sprečavaju daljnju štetu, te prilagođenih postupaka odgovora i oporavka uspostavljenih u skladu s člankom 11.;

(e) procjenu preliminarnih učinaka, štete i gubitaka;

(f) utvrđivanje mjera za upravljanje komunikacijom i krizama kojima se osigurava prijenos ažurnih informacija svim relevantnim članovima svojeg osoblja i vanjskim dionicima u skladu s člankom 13. te obavješćivanje nadležnih tijela o njima u skladu s člankom 17.

3. Kao dio okvira upravljanja IKT rizicima iz članka 5. stavka 1. financijski subjekti dužni su uvesti povezani plan oporavka u slučaju katastrofe u području IKT-a koji je podložan neovisnom revizijskom preispitivanju u slučaju financijskih subjekata, osim mikropoduzeća.

4. Financijski subjekti dužni su uvesti, provoditi i periodično testirati odgovarajuće planove kontinuiteta poslovanja u području IKT-a, konkretno za ključne ili važne funkcije koje su eksternalizirane ili ugovorene na temelju ugovora s trećim stranama pružateljima IKT usluga.

5. Kao dio svojeg sveobuhvatnog upravljanja IKT rizicima financijski subjekti dužni su:

   (a) testirati politiku kontinuiteta poslovanja u području IKT-a i plan oporavka u slučaju katastrofe u području IKT-a najmanje jednom godišnje i nakon značajnih promjena u ***ključnim ili važnim*** sustavima IKT-a;

   (b) testirati planove komunikacije u krizi uvedene u skladu s člankom 13.

   Za potrebe točke (a) financijski subjekti, osim mikropoduzeća, dužni su u planove testiranja uključiti scenarije kibernapada i prebacivanja s primarne infrastrukture IKT-a na redundantnu infrastrukturu i obrnuto, sigurnosne kopije i redundantnu infrastrukturu koje su potrebne za ispunjenje obveza iz članka 11.

   Financijski subjekti dužni su redovito preispitivati svoju politiku kontinuiteta poslovanja u području IKT-a i plan oporavka u slučaju katastrofe u području IKT-a uzimajući u obzir rezultate testova provedenih u skladu s prvim podstavkom i preporukama iz revizijskih ili nadzornih provjera.

6. Financijski subjekti, osim mikropoduzeća, dužni su imati funkciju za upravljanje krizama, ***kao posebnu funkciju ili dio funkcija odgovornih za rješavanje incidenata i upravljanje njima. Tom se funkcijom za upravljanje krizama,*** u slučaju aktivacije politike kontinuiteta poslovanja u području IKT-a ili plana oporavka u slučaju katastrofe u području IKT-a, utvrđuje jasne postupke za upravljanje unutarnjom i vanjskom komunikacijom u krizi u skladu s člankom 13.

7. Financijski subjekti dužni su voditi evidenciju ***relevantnih*** aktivnosti prije i nakon poremećaja u radu kada se aktivira politika kontinuiteta poslovanja u području IKT-a ili plan oporavka u slučaju katastrofe u području IKT-a. Te su evidencije lako dostupne.

8. Financijski subjekti iz članka 2. stavka 1. točke (f) dostavljaju nadležnim tijelima primjerke rezultata testiranja kontinuiteta poslovanja u području IKT-a ili sličnih testova provedenih u promatranom razdoblju.

9. Financijski subjekti, osim mikropoduzeća, obavješćuju nadležna tijela o svim ***procijenjenim financijskim*** troškovima i gubicima uzrokovanima ***značajnim*** poremećajima u radu IKT-a i ***značajnim*** IKT incidentima.

9a. Europska nadzorna tijela u okviru Zajedničkog odbora izrađuju zajedničke smjernice o metodologiji za izračun troškova i kvantificiranje gubitaka iz stavka 9.

Članak 11.

Politike izrade sigurnosnih kopija i metode oporavka

1. Kako bi se osigurala ponovna uspostava sustava IKT-a uz minimalno razdoblje prekida rada i ograničene poremećaje u radu, kao dio svojeg okvira upravljanja IKT rizicima financijski subjekti dužni su:

   (a) imati politiku izrade sigurnosnih kopija u kojoj se određuju vrste podataka za koje se izrađuju sigurnosne kopije te minimalna učestalost izrade sigurnosnih kopija, na temelju nužnosti informacija ili osjetljivosti podataka;

   (b) razviti metodu oporavka.

2. ***U skladu s politikom izrade sigurnosnih kopija iz stavka 1. točke (a),*** sustavi izrade sigurnosnih kopija počinju s obradom bez nepotrebne odgode, osim ako bi početak njihova rada ugrozio sigurnost mrežnih i informacijskih sustava ili cjelovitost i povjerljivost podataka.

3. Pri vraćanju podataka sa sigurnosne kopije s pomoću vlastitih sustava financijski subjekti dužni su koristiti sustave IKT-a ***koji su razdvojeni, u fizičkom ili logističkom smislu,*** od ***njihova*** glavnog s***ustava IKT-a*** i zaštićeni od neovlaštenog pristupa ili oštećenja IKT-a.

   Financijskim subjektima iz članka 2. stavka 1. točke (g) planovi oporavka omogućuju oporavak svih transakcija koje su bile u tijeku u trenutku pojave poremećaja u radu kako bi se omogućio siguran nastavak poslovanja središnje druge ugovorne strane te dovršila namira na zakazani datum.

4. Financijski subjekti dužni su ***procijeniti je li potrebno*** osigurati da su njihovi redundantni kapaciteti IKT-a opremljeni resursima, kapacitetima i funkcijama koji su dostatni i primjereni poslovnim potrebama ***te kojima se ispunjavaju zahtjevi za digitalnu operativnu otpornost iz ove Uredbe***.

5. Financijski subjekti iz članka 2. stavka 1. točke (f) dužni su održavati ili osigurati da treće strane pružatelji IKT usluga održavaju najmanje jedno sekundarno mjesto obrade na kojem se nalaze resursi, kapaciteti, funkcije i osoblje koji su dostatni i primjereni poslovnim potrebama.

   Sekundarno mjesto obrade:

   (a) mora biti geografski udaljeno od primarnog mjesta obrade kako bi se osigurao drugačiji profil rizičnosti i kako bi se spriječilo da ga zahvati događaj koji je zahvatio primarno mjesto;

   (b) mora moći osigurati kontinuitet ključnih usluga na isti način kao i primarno mjesto ili pružiti razinu usluga koja je nužna kako bi se osiguralo da financijski subjekt svoje ključne operacije obavi unutar ciljnih vrijednosti za oporavak;

   (c) mora biti dostupno osoblju financijskog subjekta kako bi se osigurao kontinuitet ključnih usluga u slučaju nedostupnosti primarnog mjesta obrade.

6. Pri utvrđivanju ciljnog vremena i točke oporavka za svaku funkciju financijski subjekti dužni su uzeti u obzir ***radi li se o ključnoj ili važnoj funkciji te*** mogući opći učinak na učinkovitost tržišta. Tim ciljnim vremenima mora se osigurati da se u ekstremnim scenarijima postignu dogovorene razine usluga.

7. Pri oporavku od IKT incidenta financijski subjekti dužni su ***osigurati da je razina cjelovitosti podataka na najvišoj razini, primjerice*** obavljanjem višestruke provjere,

uključujući usklađivanje. ***Takve*** se provjere obavljaju i pri rekonstrukciji podataka vanjskih dionika kako bi se osigurala dosljednost podataka među sustavima.

Članak 12.

Učenje i razvoj

1. Financijski subjekti dužni su imati kapacitete i osoblje, a koji služe za prikupljanje informacija o ranjivostima i kiberprijetnjama, IKT incidentima, osobito kibernapadima, te za analizu njihovih vjerojatnih učinaka na digitalnu operativnu otpornost subjekta.

2. Financijski subjekti dužni su uvesti preispitivanja nakon ***značajnih*** IKT incidenata koje će provoditi nakon značajnih poremećaja u radu IKT-a koji su utjecali na njihove osnovne djelatnosti, pri čemu će analizirati uzroke poremećaja u radu i utvrditi što moraju učini da bi poboljšali rad IKT-a ili politiku kontinuiteta poslovanja u području IKT-a iz članka 10.

   Pri uvođenju promjena ***povezanih s IKT rizicima za koje je utvrđeno da su rezultat opsežnih preispitivanja IKT incidenata*** financijski subjekti, osim mikropoduzeća, obavješćuju nadležna tijela o ***svim značajnim*** promjenama***, u kojima detaljno navode potrebna poboljšanja i načine na koje se njima nastoje spriječiti ili ublažiti budući poremećaji. Obavješćivanje nadležnih tijela o promjenama može biti prije ili nakon provedbe tih promjena.***

   U preispitivanjima nakon IKT incidenata iz prvog podstavaka utvrđuje se je li se pridržavalo uspostavljenih postupaka te jesu li poduzete mjere bile djelotvorne, među ostalim u pogledu:

   (a) brzog odgovora na sigurnosna upozorenja i brzog utvrđivanja učinka IKT incidenata i njihove ozbiljnosti;

   (b) kvalitete i brzine provedbe forenzičke analize;

   (c) djelotvornosti eskalacije incidenta unutar financijskog subjekta;

   (d) djelotvornosti unutarnje i vanjske komunikacije.

3. Pouke iz testiranja digitalne operativne otpornosti provedenog u skladu s člancima 23. i 24. te iz stvarnih IKT incidenata, osobito kibernapada, zajedno s problemima na koje se naiđe po aktivaciji plana kontinuiteta poslovanja ili plana oporavka te s informacijama razmijenjenima s drugim ugovornim stranama i ocijenjenima tijekom nadzornih preispitivanja, propisno se i kontinuirano uključuju u proces procjene IKT rizikâ. Ti nalazi moraju se popratiti odgovarajućim preispitivanjima relevantnih komponenti okvira upravljanja IKT rizicima iz članka 5. stavka 1.

4. Financijski subjekti dužni su pratiti djelotvornost provedbe strategije digitalne otpornosti utvrđene u članku 5. stavku 9. Financijski subjekti dužni su mapirati vremensku evoluciju IKT rizika, ***uključujući blizinu tih rizika ključnim ili važnim funkcijama,*** analizirati učestalost, vrste, razmjer i evoluciju IKT incidenata, osobito kibernapada i njihovih obrazaca, kako bi utvrdili razinu izloženosti IKT rizicima i poboljšali svoju kiberzrelost i pripravnost.

5. Više IKT osoblje dužno je najmanje jednom godišnje izvijestiti upravljačko tijelo o nalazima iz stavka 3. te iznijeti preporuke.

6. Financijski subjekti dužni su osmisliti programe informiranja o sigurnosti IKT-a i osposobljavanja o digitalnoj operativnoj otpornosti kao obvezne module u svojim sustavima osposobljavanja osoblja. ***Programi za podizanje svijesti o sigurnosti IKT-a primjenjuju se na cjelokupno osoblje. Osposobljavanja u području digitalne operativne otpornosti primjenjuju se barem*** na sve zaposlenike ***s pravom izravnog pristupa sustavima IKT-a*** i više rukovodstvo. ***Složenost modula osposobljavanja razmjerna je razini izravnog pristupa IKT sustavima člana osoblja i posebno uzima u obzir njihov pristup ključnim ili važnim funkcijama.***

Financijski subjekti***, osim mikropoduzeća,*** dužni su kontinuirano pratiti važna tehnološka dostignuća, među ostalim kako bi saznali više o mogućim učincima uvođenja tih novih tehnologija na zahtjeve sigurnosti IKT-a i digitalnu operativnu otpornost. Dužni su držati korak s najnovijim procesima upravljanja IKT rizicima i tako se djelotvorno boriti protiv postojećih ili novih oblika kibernapada.

Članak 13.

Komunikacija

1. Kao dio okvira upravljanja IKT rizicima iz članka 5. stavka 1. financijski subjekti dužni su uvesti komunikacijske planove kojima se osigurava odgovorna objava informacija ***barem o većim*** IKT incidentima ili velikim ranjivostima za klijente i druge ugovorne strane te javnost, ovisno o slučaju.

   Komunikacijskim planovima iz prvog podstavka osigurava se i godišnja objava sažetka svih IKT incidenata klijentima i drugim ugovornim stranama. Takvom se objavom u potpunosti poštuje poslovna tajna financijskog subjekta, njegovih klijenata i drugih ugovornih strana te se njome ne ugrožava okvir upravljanja IKT rizicima iz članka 5. stavka 1.
2. Kao dio okvira upravljanja IKT rizicima iz članka 5. stavka 1. financijski subjekti dužni su uvesti komunikacijske politike za osoblje i vanjske dionike. U komunikacijskim politikama za osoblje vodi se računa o razlikovanju osoblja uključenog u upravljanje IKT rizicima, posebno u odgovor i oporavak, i osoblja koje treba samo informirati.
3. Najmanje jedna osoba u subjektu zadužena je za provedbu komunikacijske strategije ***barem*** za ***značajne*** IKT incidente i u tu svrhu ima ulogu glasnogovornika u javnosti i medijima.

Članak 14.

Daljnje usklađivanje alata, metoda, procesa i politika za upravljanje IKT rizicima

Europsko nadzorno tijelo za bankarstvo (EBA), Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala (ESMA) i Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje (EIOPA), uz savjetovanje s Agencijom Europske unije za kibersigurnost (ENISA), izrađuju nacrt regulatornih tehničkih standarda u sljedeće svrhe:

(a) pobliže opisati elemente koji trebaju biti uključeni u politike, postupke, protokole i alate za sigurnost IKT-a iz članka 8. stavka 2. kako bi se osigurala sigurnost mreža, odgovarajuće mjere zaštite od neovlaštenih upada i zlouporabe podataka, očuvale autentičnost i cjelovitost podataka, uključujući

kriptografske tehnike, i zajamčio točan i brz prijenos podataka bez velikih poremećaja ***i nepotrebnih odlaganja***;

(d) dodatno razraditi komponente kontrola prava upravljanja pristupom iz članka 8. stavka 4. točke (c) i povezanu politiku ljudskih resursa u kojoj se pobliže opisuju prava pristupa, postupci dodjele i opoziva prava, praćenje neobičnog ponašanja u pogledu IKT rizika s pomoću odgovarajućih pokazatelja, među ostalim za obrasce korištenja mreže, sate, IT aktivnost i nepoznate uređaje;

(e) dodatno razraditi elemente iz članka 9. stavka 1. koji omogućuju brzo otkrivanje neobičnih aktivnosti te kriterije iz članka 9. stavka 2. za otkrivanje IKT incidenata i primjenu procesa odgovora;

(f) pobliže opisati komponente politike kontinuiteta poslovanja u području IKT-a iz članka 10. stavka 1.;

(g) pobliže opisati testiranje planova kontinuiteta poslovanja u području IKT-a iz članka 10. stavka 5. da bi se osiguralo da se u njima propisno uzmu u obzir scenariji u kojima se kvaliteta pružanja ključne ili važne funkcije snizi na neprihvatljivu razinu ili njezino pružanje nije moguće te da se propisno razmotri mogući učinak nesolventnosti ili drugih načina propasti relevantne treće strane pružatelja IKT usluga i, ako je relevantno, politički rizici u jurisdikcijama u kojima posluju ti pružatelji;

(h) pobliže opisati komponente plana oporavka u slučaju katastrofe u području IKT-a iz članka 10. stavka 3.

EBA, ESMA i EIOPA taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do [Ured za publikacije: unijeti datum: jednu godinu od datuma stupanja na snagu].

Komisiji se dodjeljuje ovlast za donošenje regulatornih tehničkih standarda iz prvog podstavka u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 odnosno Uredbe (EU) br. 1095/2010.

Članak 14.a

Okvir upravljanja IKT rizicima za male, međusobno nepovezane i izuzete subjekte

1. U skladu s člankom 3.a mala i međusobno nepovezana investicijska društva, institucije za platni promet izuzete Direktivom (EU) 2015/2366, kreditne institucije izuzete Direktivom 2013/36/EU, institucije za elektronički novac izuzete Direktivom 2009/110/EZ i male institucije za strukovno mirovinsko osiguranje uspostavljaju i održavaju stabilan i dokumentiran okvir za upravljanje IKT rizicima kojim se:

(a) detaljno navode mehanizmi i mjere usmjerene na brzo, učinkovito i sveobuhvatno upravljanje svim IKT rizicima, uključujući zaštitu relevantnih fizičkih komponenti i infrastruktura;

(b) kontinuirano prati sigurnost i funkcioniranje svih sustava IKT-a;

(c) učinci IKT rizika svode na najmanju moguću mjeru upotrebom pouzdanih, otpornih i ažuriranih sustava, protokola i alata IKT-a koji su prikladni za potporu obavljanju njihovih aktivnosti i pružanju usluga;

(d) primjereno štiti povjerljivost, cjelovitost i dostupnost podatkovnih mreža i informacijskih sustava;

(e) omogućuje brzo utvrđivanje i otkrivanje izvora rizika i nepravilnosti u mrežnim i informacijskim sustavima te brzo rješavanje IKT incidenata.

2. Okvir upravljanja IKT rizicima iz stavka 1. dokumentira se i preispituje najmanje jednom godišnje i po nastanku svakog značajnog IKT incidenta te u skladu s uputama ili zaključcima nadzornog tijela koji proizlaze iz relevantnog testiranja digitalne operativne otpornosti ili revizijskih procesa. Kontinuirano ga se poboljšava na temelju pouka iz provedbe i praćenja.

Izvješće o preispitivanju okvira upravljanja IKT rizicima podnosi se nadležnom tijelu jednom godišnje.

POGLAVLJE III.

IKT INCIDENTI

UPRAVLJANJE, KLASIFIKACIJA I IZVJEŠĆIVANJE

Članak 15.

Proces upravljanja IKT incidentima

1. Financijski subjekti dužni su uspostaviti i provoditi procese upravljanja IKT rizicima radi otkrivanja IKT incidenata, upravljanja njima i obavješćivanja o njima te uvesti pokazatelje ranog upozoravanja u obliku upozorenja.

2. Financijski subjekti dužni su uspostaviti odgovarajuće ***postupke i*** procese za osiguravanje dosljednog i integriranog praćenja, rješavanja IKT incidenata i praćenja mjera poduzetih nakon njih kako bi se osiguralo utvrđivanje i ***rješavanje*** glavnih uzroka u cilju sprečavanja pojave takvih incidenata.

3. U procesu upravljanja IKT incidentima iz stavka 1.:

   (a) uspostavljaju se postupci za utvrđivanje, praćenje, evidentiranje, kategorizaciju i klasifikaciju IKT incidenata u skladu s njihovim prioritetom te ozbiljnosti i nužnosti zahvaćenih usluga, u skladu s kriterijima iz članka 16. stavka 1.;

   (b) dodjeljuju se uloge i odgovornosti koje se aktiviraju za različite vrste IKT incidenata i scenarija;

   (c) utvrđuju se planovi komunikacije s osobljem, vanjskim dionicima i medijima u skladu s člankom 13. te planovi obavješćivanja klijenata, unutarnji postupci eskalacije, uključujući prigovore korisnika povezane s IKT-om, te prema potrebi planovi informiranja financijskih subjekata koji su druge ugovorne strane;

   (d) osigurava se ***barem*** izvješćivanje relevantnog višeg rukovodstva o značajnim IKT incidentima te informiranje upravljačkog tijela o značajnim IKT incidentima uz objašnjenje učinka, odgovora i dodatnih kontrola koje se moraju uvesti zbog ***značajnih*** IKT incidenata;

   (e) uspostavljaju se postupci odgovora na IKT incidente kako bi se smanjili učinci i osiguralo pravodobno pružanje usluga i njihova sigurnost.

Članak 16.

Klasifikacija IKT incidenata

1. Financijski subjekti klasificiraju IKT incidente i utvrđuju njihov učinak na temelju sljedećih kriterija:

   (a) broj korisnika ili financijskih drugih ugovornih strana koji su zahvaćeni poremećajem u radu koji je uzrokovao IKT incident ;

   (b) trajanje IKT incidenta, uključujući razdoblje prekida rada usluge;

(c) zemljopisna raširenost u smislu područja koje je incident zahvatio, osobito ako je zahvatio više od dvije države članice;

(d) gubitak podataka koji proizlazi iz IKT incidenata, kao što je gubitak cjelovitosti, povjerljivosti ili dostupnosti;

(e) ozbiljnost učinka IKT incidenta na sustave IKT-a financijskog subjekta;

(f) nužnost zahvaćenih usluga, uključujući transakcije i operacije financijskog subjekta;

(g) ekonomski učinak IKT incidenta u apsolutnom i relativnom smislu.

2. Europska nadzorna tijela, u okviru Zajedničkog odbora europskih nadzornih tijela („Zajednički odbor”) i ***u koordinaciji*** s Europskom središnjom bankom (ESB) i ENISA-om, izrađuju zajednički nacrt regulatornih tehničkih standarda u kojem pobliže opisuju sljedeće:

(a) kriterije utvrđene u stavku 1., uključujući pragove značajnosti za utvrđivanje značajnih IKT incidenata koji su obuhvaćeni obvezom izvješćivanja iz članka 17. stavka 1.;

(b) kriterije koje nadležna tijela primjenjuju u svrhu procjene važnosti značajnih IKT incidenata za jurisdikcije drugih država članica, te pojedinosti u izvješćima o ***značajnim*** IKT incidentima koje se moraju podijeliti s ostalim nadležnim tijelima u skladu s člankom 17. stavcima 5. i 6.

3. Pri izradi zajedničkog nacrta regulatornih tehničkih standarda iz stavka 2. europska nadzorna tijela uzimaju u obzir međunarodne standarde te specifikacije koje izradi i objavi ENISA, uključujući prema potrebi specifikacije za druge gospodarske sektore. ***Europska nadzorna tijela nadalje uzimaju u obzir da pravodobno i učinkovito upravljanje incidentom od strane malih poduzeća i mikropoduzeća nije ograničeno potrebom za poštovanjem zahtjeva za klasifikaciju iz ovog članka. Europska nadzorna tijela uzimaju u obzir i veličinu financijskih subjekata, prirodu, opseg i složenost njihovih usluga, aktivnosti i poslovanja te njihov ukupni profil rizičnosti.***

Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do [Ured za publikacije: unijeti datum: ***dvije godine*** od datuma stupanja na snagu].

Komisiji se dodjeljuje ovlast za dopunu ove Uredbe donošenjem regulatornih tehničkih standarda iz stavka 2. u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 odnosno Uredbe (EU) br. 1095/2010.

Članak 17.

Izvješćivanje o značajnim IKT incidentima

1. Financijski subjekti izvješćuju relevantna nadležna tijela iz članka 41. o značajnim IKT incidentima u rokovima utvrđenima u stavku 3.

Za potrebe prvog podstavka, a nakon što prikupe i analiziraju sve relevantne informacije, financijski subjekti sastavljaju izvješće o incidentu koristeći obrazac iz članka 18. i dostavljaju ga nadležnom tijelu.

Izvješće sadržava sve informacije koje su nadležnom tijelu potrebne da bi utvrdilo važnost značajnog IKT incidenta i procijenilo moguće prekogranične učinke.

1a. Financijski subjekti mogu, na dobrovoljnoj osnovi, obavijestiti relevantno nadležno tijelo o ozbiljnim kiberprijetnjama ako smatraju da je prijetnja važna za financijski sustav, korisnike usluga ili klijente. Relevantno nadležno tijelo može dostaviti takve informacije drugim relevantnim tijelima u skladu sa stavkom 5.

2. Kada ***se dogodi značajan*** IKT incident ***i kad on značajno*** utječe ▌ na financijske interese korisnika usluge i klijenata, financijski subjekti dužni su bez odgode***, nakon što postanu svjesni tog incidenta,*** obavijestiti svoje korisnike usluga i klijente o značajnom IKT incidentu i obavijestiti ***ih*** o ***relevantnim*** mjerama koje su poduzete da bi se smanjili negativni učinci takvog incidenta. ***Ako se zbog protumjera koje je poduzeo financijski subjekt ne nanese šteta korisnicima usluga i klijentima, ne primjenjuje se zahtjev za obavješćivanje korisnika usluga i klijenata.***

3. Financijski subjekti dostavljaju nadležnom tijelu iz članka 41.:

(a) početnu obavijest ▌ ***o značajnom IKT incidentu koja će sadržavati informacije dostupne subjektu koji šalje obavijest na temelju načela najvećih napora kako slijedi:***

(i) u pogledu incidenata koji značajno remete dostupnost usluga koje pruža financijski subjekt, nadležno tijelo obavještava se bez odgode, a u svakom slučaju u roku od 24 sata od primitka informacije o incidentu;

(ii) u pogledu incidenata koji imaju značajan učinak na financijski subjekt osim na dostupnost usluga koje pruža financijski subjekt, nadležno tijelo obavještava se bez odgode, a u svakom slučaju u roku od 72 sata od primitka informacije o incidentu;

(iii) u pogledu incidenata koji utječu na cjelovitost, povjerljivost ili sigurnost osobnih podataka koje održava taj financijski subjekt, nadležno tijelo obavještava se bez odgode, a u svakom slučaju u roku od 24 sata od primitka informacije o incidentu;

(b) privremeno izvješće***, čim se znatno promijeni status izvornog incidenta ili se otkriju nove informacije koje bi mogle imati velik utjecaj na način na koji nadležno tijelo rješava IKT incident, nakon*** početne obavijesti iz točke (a), a nakon toga prema potrebi ažurirane obavijesti svaki put kada relevantno ažuriranje statusa postane dostupno te na izričit zahtjev nadležnog tijela;

(c) završno izvješće kada se dovrši analiza temeljnog uzroka, neovisno o tome jesu li mjere za ublažavanje učinka već provedene, i kada se procijenjene vrijednosti mogu zamijeniti stvarnim podacima o učinku, ali najkasnije mjesec dana od ***datuma*** slanja početnog izvješća.

(ca) u slučaju incidenta koji traje u trenutku podnošenja završnog izvješća iz točke (c), završno izvješće dostavlja se jedan mjesec nakon što je incident riješen;

Relevantno nadležno tijelo iz članka 41. osigurava da je financijskom subjektu u propisno opravdanim slučajevima dopušteno odstupanje od rokova utvrđenih u točkama (a), (b), (c) i (ca) ovog stavka, uzimajući u obzir sposobnost financijskih subjekata da dostave točne i smislene informacije u vezi sa značajnim IKT incidentima.

4. Financijski subjekti mogu delegirati izvještajne obveze iz ovog članka trećoj strani pružatelju usluga samo nakon što to delegiranje odobri odgovarajuće nadležno tijelo iz članka 41. ***U slučaju takvog delegiranja financijski subjekt ostaje u potpunosti odgovoran za ispunjavanje zahtjeva o izvješćivanju o incidentima.***

5. Po primitku izvješća iz stavka 1. nadležno tijelo bez nepotrebne odgode dostavlja pojedinosti o ***značajnom IKT*** incidentu:

   (a) EBA-i, ESMA-i ili EIOPA-i, ovisno o slučaju;

   (b) ESB-u prema potrebi u slučaju financijskih subjekata iz članka 2. stavka 1. točaka (a), (b) i (c); i

   (c) jedinstvenoj kontaktnoj točki određenoj na temelju članka 8. Direktive (EU) 2016/1148 ***ili timovima za odgovor na računalne sigurnosne incidente imenovanima u skladu s člankom 9. Direktive (EU) 2016/1149;***

   (ca) sanacijskom tijelu odgovornom za relevantni financijski subjekt. Jedinstveni sanacijski odbor (SRB) u pogledu subjekata iz članka 7. stavka 2. Uredbe (EU) br. 806/2014 te subjekata i grupa iz članka 7. stavka 4. točke (b) i članka 7. stavka 5. Uredbe (EU) br. 806/2014 ako su ispunjeni uvjeti za primjenu tih stavaka;

   (cb) nadležnim sanacijskim tijelima u vezi sa subjektima i grupama iz članka 7. stavka 3. Uredbe (EU) br. 806/2014. Nacionalna sanacijska tijela svaka tri mjeseca dostavljaju Jedinstvenom sanacijskom odboru sažetak izvješća koja su zaprimila u skladu s ovom točkom u vezi sa subjektima i grupama iz članka 7. stavka 3. Uredbe (EU) br. 806/2014;

   (cc) drugim relevantnim javnim tijelima, uključujući ona u drugim državama članicama.

6. EBA, ESMA ili EIOPA i ESB***, u suradnji s ENISA-om,*** procjenjuju važnost značajnog IKT incidenta za druga relevantna javna tijela i obavješćuje ih o tome što prije. ESB je dužan obavijestiti članove Europskog sustava središnjih banaka o pitanjima od važnosti za platni sustav. Na temelju te obavijesti nadležna tijela prema potrebi poduzimaju sve potrebne mjere u svrhu zaštite neposredne stabilnosti financijskog sustava.

Članak 18.

Usklađivanje sadržaja izvješća i obrazaca

1. Europska nadzorna tijela, u okviru Zajedničkog odbora i nakon savjetovanja s ENISA-om i ESB-om, izrađuju:

   (a) zajednički nacrt regulatornih tehničkih standarda kako bi:

      (1) utvrdila sadržaj izvješća o značajnim IKT incidentima;

      (2) pobliže opisala uvjete pod kojima financijski subjekti mogu delegirati izvještajne obveze utvrđene u ovom poglavlju trećoj strani pružatelju usluga nakon prethodnog odobrenja nadležnog tijela;

(3) dodatno utvrdila kriterije za utvrđivanje učinka značajnog IKT incidenta na financijski subjekt za potrebe članka 17. stavka 3. točke (a).

(b) zajednički nacrt provedbenih tehničkih standarda kako bi utvrdila standardne obrasce, predloške i postupke za izvješćivanje o značajnim IKT incidentima za financijske subjekte.

Europska nadzorna tijela zajednički nacrt regulatornih tehničkih standarda iz ▌ točke (a) ***prvog podstavka*** i zajednički nacrt provedbenih tehničkih standarda iz ▌ točke (b) ***prvog podstavka*** do xx 202x. dostavljaju Komisiji do [Ured za publikacije: unijeti datum: ***dvije godine*** od datuma stupanja na snagu].

Komisiji se dodjeljuje ovlast za dopunu ove Uredbe donošenjem zajedničkih regulatornih tehničkih standarda iz ▌ točke (a) ***prvog podstavka*** u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1095/2010 odnosno Uredbe (EU) br. 1094/2010.

Komisiji se dodjeljuje ovlast za donošenje zajedničkih provedbenih tehničkih standarda iz ▌ točke (b) ***prvog podstavka*** u skladu s člankom 15. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1095/2010 odnosno Uredbe (EU) br. 1094/2010.

2. U očekivanju ishoda izvješća o izvedivosti iz članka 19. o daljnjoj centralizaciji izvješćivanja o incidentima, europska nadzorna tijela, putem Zajedničkog odbora i u suradnji s nadležnim tijelima, ESB-om, SRB-om i ENISA-om, izrađuju smjernice za razmjenu informacija o izvješćima o značajnim IKT incidentima u skladu s člankom 17. stavkom 5.

Smjernicama iz prvog podstavka razmatra se barem sljedeće:

(a) najučinkovitije komunikacijske linije;

(b) održavanje sigurnosti, povjerljivosti i cjelovitosti podataka koji se razmjenjuju;

(c) moguće sudjelovanje financijskih subjekata kako bi se dopunila razmjena informacija iz članka 40.

Članak 19.

Centralizacija izvješćivanja o značajnim IKT incidentima

1. Europska nadzorna tijela, u okviru Zajedničkog odbora i uz savjetovanje s ESB-om i ENISA-om, izrađuju zajedničko izvješće u kojem se procjenjuje izvedivost daljnje centralizacije izvješćivanja o incidentima uvođenjem jedinstvenog EU-ova čvorišta za izvješćivanje o značajnim IKT incidentima za financijske subjekte. U izvješću se istražuje kako se može olakšati tijek izvješćivanja o IKT incidentima, smanjiti povezani troškovi i podržati tematske analize radi poboljšanja konvergencije nadzora.

2. Izvješće iz stavka 1. sadržava barem sljedeće elemente:

(a) preduvjete za uvođenje ***jedinstvenog*** EU-ova čvorišta;

(b) prednosti, ograničenja i moguće rizike;

(ba) sposobnost uspostave interoperabilnosti i procjene njezine dodane vrijednosti

u pogledu drugih relevantnih sustava izvješćivanja, uključujući Direktivu (EU) 2016/1148.

(c) elemente operativnog upravljanja;

(d) uvjete članstva;

(e) modalitete pristupa ***jedinstvenom*** EU-ovu čvorištu za financijske subjekte i za nacionalna nadležna tijela;

(f) preliminarnu procjenu financijskih troškova koje iziskuje uspostavljanje operativne platforme koja podržava ***jedinstveno*** EU-ovo čvorište, uključujući potrebno stručno znanje.

3. Europska nadzorna tijela izvješće iz stavka 1. dostavljaju Komisiji, Europskom parlamentu i Vijeću do xx 202x. [Ured za publikacije: unijeti datum: tri godine od datuma stupanja na snagu].

Članak 20.

Povratne informacije o nadzoru

1. Po primitku izvješća iz članka 17. stavka 1. nadležno tijelo potvrđuje primitak obavijesti i što prije dostavlja financijskom subjektu sve potrebne povratne informacije ili smjernice, posebno kako bi se razmotrile korektivne mjere na razini subjekta ili načini na koje se može smanjiti negativni učinak u svim sektorima ***te dostavlja i primjereno anonimizirane povratne informacije, uvide i saznanja svim relevantnim financijskim subjektima, ako bi one mogle biti korisne, na temelju izvješća o značajnim IKT incidentima koja prima***.

2. Europska nadzorna tijela, u okviru Zajedničkog odbora, svake godine sastavljaju anonimizirano i agregirano izvješće o obavijestima o ***značajnim*** IKT incidentima koje su primila od nadležnih tijela i pri tome navode barem broj značajnih IKT incidenata, njihovu prirodu, učinak na poslovanje financijskih subjekata ili korisnika, ***procijenjene*** troškove i poduzete korektivne mjere.

Europska nadzorna tijela izdaju upozorenja i izrađuju statistike na visokoj razini kao podršku procjenama prijetnji i ranjivosti u području IKT-a.

Članak 20.a

Operativni ili sigurnosni incidenti povezani s plaćanjima koji se odnose na određene financijske subjekte

Zahtjevi utvrđeni u ovom poglavlju primjenjuju se i na operativne ili sigurnosne incidente povezane s plaćanjima te na značajne operativne ili sigurnosne incidente povezane s plaćanjima ako se odnose na financijske subjekte iz članka 2. stavka 1. točaka (a), (b) i (c).

POGLAVLJE IV.

TESTIRANJE DIGITALNE OPERATIVNE OTPORNOSTI

Članak 21.

Opći zahtjevi za provedbu testiranja digitalne operativne otpornosti

1. Za potrebe procjene pripravnosti za IKT incidente, utvrđivanja slabosti, nedostataka ili praznina u digitalnoj operativnoj otpornosti te brze provedbe korektivnih mjera financijski subjekti***, osim mikropoduzeća,*** dužni su izraditi, provoditi i preispitivati ▌pouzdan i sveobuhvatan program testiranja digitalne operativne otpornosti kao sastavni dio okvira upravljanja IKT rizicima iz članka 5.

2. Program testiranja digitalne operativne otpornosti uključuje razne procjene, testove, metodologije, postupke i alata koje treba primjenjivati u skladu s odredbama članaka 22. i 23.

3. Financijski subjekti primjenjuju pristup koji se temelji na procjeni rizika kada provode program testiranja digitalne operativne otpornosti iz stavka 1. uzimajući u obzir razvoj IKT rizika, konkretne rizike kojima je financijski subjekt izložen ili bi mogao biti izložen, nužnost informacijske imovine i pružanih usluga te druge čimbenike koje financijski subjekt smatra primjerenima.

4. Financijski subjekti osiguravaju da testove provode neovisne strane, unutarnje ili vanjske. ***Ako testove provodi unutarnji provoditelj testiranja, financijski subjekti izdvajaju dostatna sredstva i osiguravaju izbjegavanje sukoba interesa tijekom faza osmišljanja i provedbe testa.***

5. Financijski subjekti uvode postupke i politike za utvrđivanje prioriteta problema uočenih tijekom testova, njihovu klasifikaciju i ***rješavanje*** te metodologije unutarnje provjere kako bi osigurali cjelovito otklanjanje svih utvrđenih slabosti, nedostataka ili praznina.

6. Financijski subjekti dužni su ***osigurati da se provedu primjereni testovi svih ključnih sustava i aplikacija*** IKT-a najmanje jednom godišnje.

Članak 22.

Testiranje alata i sustava IKT-a

1. Programom testiranja digitalne operativne otpornosti iz članka 21. predviđa se provedba cijelog dijapazona odgovarajućih testova.

Ti testovi mogu obuhvaćati procjene i skeniranja ranjivosti, analize otvorenih izvora, procjene mrežne sigurnosti, analize praznina, preispitivanja fizičke sigurnosti, upitnike i softverska rješenja za skeniranje, preispitivanja izvornog koda ako je to izvedivo, testiranja na temelju scenarija, testiranje kompatibilnosti, testiranje radnih karakteristika, integralno (engl. end-to-end) testiranje ili penetracijsko testiranje.

2. Financijski subjekti iz članka 2. stavka 1. točaka (f) i (g) provode procjene ranjivosti prije svakog uvođenja ili ponovnog uvođenja novih ili postojećih usluga koje podržavaju ključne funkcije, aplikacije ili infrastrukturne komponente financijskog subjekta.

Članak 23.

Napredno testiranje alata, sustava i procesa IKT-a na temelju penetracijskog testiranja vođenog prijetnjama

1. Financijski subjekti utvrđeni u skladu s ***drugim podstavkom trećeg stavka*** provode napredno testiranje u obliku penetracijskog testiranja vođenog prijetnjama barem svake tri godine.

2. Penetracijsko testiranje vođeno prijetnjama obuhvaća barem ključne ***ili važne*** funkcije i usluge financijskog subjekta i provodi se ***po mogućnosti*** na sustavima trenutačno u produkciji koji podržavaju te funkcije ***ili u pretprodukcijskim sustavima s istom sigurnosnom konfiguracijom***. Točan opseg penetracijskog testiranja vođenog prijetnjama utvrđuju financijski subjekti na temelju procjene ključnih ***ili važnih*** funkcija i usluga, a potvrđuju ga nadležna tijela. ***Nije potrebno da jedno*** penetracijsko testiranje vođeno prijetnjama ***obuhvati sve ključne ili važne funkcije.***

   Za potrebe prvog podstavka, financijski subjekti utvrđuju sve relevantne osnovne procese, sustave i tehnologije IKT-a koji podržavaju ključne ***ili važne*** funkcije i usluge, među ostalim ***ključne ili važne*** funkcije i usluge koje su eksternalizirane ili ugovorene s trećim stranama pružateljima IKT usluga.

   Ako su treće strane pružatelji ***ključnih*** IKT usluga ***i, prema potrebi, treće strane pružatelji neključnih IKT usluga,*** obuhvaćene opsegom penetracijskog testiranja vođenog prijetnjama, financijski subjekt poduzima potrebne mjere kako bi osigurao sudjelovanje tih pružatelja. ***Od tih trećih strana pružatelja IKT usluga ne zahtijeva se dostavljanje informacija ili pružanje bilo kakvih pojedinosti o stavkama koje nisu relevantne za kontrole upravljanja rizicima relevantnih ključnih ili važnih funkcija relevantnih financijskih subjekata. Takvo testiranje ne smije negativno utjecati na druge klijente trećih strana pružatelja IKT usluga.***

   U slučajevima kada bi sudjelovanje treće strane pružatelja IKT usluga u penetracijskom testiranju vođenom prijetnjama potencijalno moglo utjecati na kvalitetu, povjerljivost ili sigurnost IKT usluga koje treće strane pružaju drugim korisnicima koji nisu obuhvaćeni područjem primjene ove Uredbe, ili na opću cjelovitost operacija trećih strana pružatelja IKT usluga, financijski subjekt i treća strana pružatelj IKT usluga mogu se ugovorno dogovoriti da je trećim stranama pružateljima IKT usluga dopušteno izravno sklapati ugovore s vanjskim provoditeljem testiranja. Treće strane pružatelji IKT usluga mogu sklapati takve sporazume u ime svih svojih korisnika usluga financijskih subjekata kako bi proveli udruženo testiranje.

   Financijski subjekti provode djelotvorne kontrole upravljanja rizicima kako bi ***ublažili*** rizik od mogućeg učinka na podatke, rizik oštećenja imovine i poremećaja u radu ključnih ***ili važnih funkcija*** ili operacija samog financijskog subjekta, drugih ugovornih strana ili poremećaja u financijskom sektoru.

   Na kraju testiranja, nakon što usuglase izvješća i planove sanacije, financijski subjekt i vanjski provoditelj testiranja dostavljaju ***jedinstvenom javnom nadzornom tijelu, imenovanom u skladu sa stavkom 3.a, ili, u slučaju trećih strana pružatelja IKT usluga koji izravno sklapaju sporazume s vanjskim provoditeljima testiranja, ENISA-i, povjerljiv sažetak rezultata testiranja i*** dokumentaciju koja potvrđuje da je penetracijsko testiranje vođeno prijetnjama provedeno u skladu sa zahtjevima.

Jedinstveno javno nadzorno tijelo ili ENISA, ovisno o slučaju, izdaju potvrdu ***kojom se potvrđuje da je testiranje provedeno u skladu sa zahtjevima utvrđenima u dokumentaciji kako bi se omogućilo uzajamno priznavanje penetracijskih testova vođenih prijetnjama među nadležnim tijelima. Potvrda se dostavlja nadležnom tijelu financijskog subjekta i, prema potrebi, glavnom nadzornom tijelu treće strane pružatelja ključnih IKT usluga.***

3. Za potrebe provedbe penetracijskog testiranja vođenog prijetnjama financijski subjekti***, ili treće strane pružatelji IKT usluga kojima je dopušteno izravno sklapanje ugovora s vanjskim provoditeljem testiranja u skladu sa stavkom 2. ovog članka,*** angažiraju provoditelje testiranja u skladu s člankom 24.

Ne dovodeći u pitanje njihovu sposobnost delegiranja zadaća i nadležnosti na temelju ovog članka drugim nadležnim tijelima zaduženima za penetracijsko testiranje vođeno prijetnjama, nadležna tijela utvrđuju financijske subjekte koji su dužni provesti penetracijsko testiranje vođeno prijetnjama proporcionalno ▌, i to nakon procjene sljedećih čimbenika:

(a) čimbenika povezanih s učinkom, posebno nužnost usluga i aktivnosti koje pruža i poduzima financijski subjekt;

(b) mogućih problema financijske stabilnosti, uključujući sistemsku prirodu financijskog subjekta na nacionalnoj razini ili razini Unije, ovisno o slučaju;

(c) konkretnog profila IKT rizičnosti, zrelosti financijskog subjekta u području IKT-a ili uključenih tehnoloških značajki.

3a Države članice imenuju jedinstveno javno tijelo koje će biti odgovorno za penetracijsko testiranje vođeno prijetnjama u financijskom sektoru na nacionalnoj razini, osim za utvrđivanje financijskih subjekata u skladu sa stavkom 3., uključujući penetracijsko testiranje vođeno prijetnjama koje provode financijski subjekti i treće strane pružatelji IKT usluga koji izravno sklapaju ugovore s vanjskim provoditeljima testiranja. Imenovanom jedinstvenom javnom tijelu povjeravaju se sve nadležnosti i zadaće u tu svrhu.

4. ***Europska nadzorna tijela***, ***u suradnji s ENISA-om***, nakon savjetovanja s ESB-om i uzimajući u obzir relevantne Unijine okvire koji se primjenjuju na penetracijska testiranja vođena saznanjima ***i prijetnjama***, ***uključujući okvir TIBER-EU,*** izrađuju ***jedan skup nacrta*** regulatornih tehničkih standarda kojima se preciznije utvrđuju:

(a) kriteriji koji se primjenjuju za potrebe primjene ***drugog podstavka trećeg stavka*** ovog članka;

(b) zahtjevi povezani s:

(i) opsegom penetracijskog testiranja vođenog prijetnjama iz stavka 2. ovog članka;

(ii) metodologija i pristup testiranju u svakoj pojedinačnoj fazi testiranja;

(iii) rezultati i faze završetka testiranja i utvrđivanja korektivnih mjera;

(c) vrsta nadzorne suradnje koja je potrebna za provedbu ***i omogućivanje punog uzajamnog priznavanja*** penetracijskog testiranja vođenog prijetnjama u kontekstu financijskih subjekata koji posluju u više država članica ***i testiranje***

koje provode vanjski provoditelji testiranja koji su izravno sklopili ugovore s trećim stranama pružateljima IKT usluga u skladu sa stavkom 2. ovoga članka kako bi se osigurala odgovarajuća razina sudjelovanja nadzornog tijela i prilagodljiva provedba prikladna za posebnosti financijskih podsektora ili lokalnih financijskih tržišta.

Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do [Ured za publikacije: unijeti datum: ***šest mjeseci*** prije datuma stupanja na snagu].

Komisiji se dodjeljuje ovlast za dopunu ove Uredbe donošenjem regulatornih tehničkih standarda iz drugog podstavka u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1095/2010 odnosno Uredbe (EU) br. 1094/2010.

Članak 24.

Zahtjevi za provoditelje testiranja

1. Financijski subjekti ***i treće strane pružatelji IKT usluga kojima je dopušteno izravno sklapati ugovore s vanjskim provoditeljima testiranja u skladu s člankom 23. stavkom 2.*** za provedbu penetracijskog testiranja vođenog prijetnjama mogu angažirati samo provoditelje testiranja:

   (a) koji su među najprikladnijim i najuglednijim provoditeljima testiranja;

   (b) koji posjeduju tehničke i organizacijske kapacitete i posebno stručno znanje u području saznanja o prijetnjama, penetracijskog testiranja ili testiranja crvenog tima;

   (c) koje je akreditiralo akreditacijsko tijelo u državi članici ili koji se pridržavaju službenog kodeksa ponašanja ili etičkih okvira***, bez obzira na to jesu li provoditelji testiranja iz Unije ili iz treće zemlje***;

   (d) koji izdaju neovisno uvjerenje ili revizorsko izvješće o dobrom upravljanju rizicima povezanima s provedbom penetracijskog testiranja vođenog prijetnjama, uključujući odgovarajuću zaštitu povjerljivih informacija financijskog subjekta i ublažavanje poslovnih rizika financijskog subjekta;

   (e) koji su propisno i u cijelosti pokriveni odgovarajućim osiguranjem od profesionalne odgovornosti, uključujući rizike od namjernog i nemarnog postupanja.

   (ea) u slučaju internih provoditelja testiranja, njihovu je upotrebu odobrilo relevantno nadležno tijelo i jedinstveno javno tijelo imenovano u skladu s člankom 23. stavkom 3.a, a ta su tijela provjerila da financijski subjekt ima dovoljno sredstava i da se pobrinuo da se tijekom faze osmišljanja i provedbe testa izbjegavaju sukobi interesa.

2. Financijski subjekti ***i treće strane pružatelji IKT usluga kojima je dopušteno izravno sklapati ugovore s vanjskim provoditeljima testiranja u skladu s člankom 23. stavkom 2.*** dužni su osigurati da se u ugovorima sklopljenima s vanjskim provoditeljima testiranja zahtijeva dobro upravljanje rezultatima penetracijskog testiranja vođenog prijetnjama i da njihova obrada, uključujući proizvodnju, izradu preliminarnih rezultata, pohranu, agregiranje, izvješćivanje, obavješćivanje ili uništenje, ne stvara rizike za financijski subjekt.

POGLAVLJE V.

UPRAVLJANJE IKT RIZIKOM TREĆE STRANE

ODJELJAK I.

KLJUČNA NAČELA DOBROG UPRAVLJANJA IKT RIZIKOM TREĆE STRANE

Članak 25.

Opća načela

Financijski subjekti upravljaju IKT rizikom treće strane kao sastavnim dijelom IKT rizika u njihovu okviru upravljanja IKT rizicima i u skladu sa sljedećim načelima:

1. Financijski subjekti koji imaju sklopljene ugovore o korištenju IKT usluga za potrebe poslovanja snose u svakom trenutku potpunu odgovornost za ispunjavanje i izvršavanje svih obveza iz ove Uredbe i primjenjivih propisa o financijskim uslugama.

2. Financijski subjekti upravljaju IKT rizikom treće strane poštujući načela proporcionalnosti i uzimajući u obzir:

   (a) ***prirodu,*** opseg, složenost i važnost ovisnosti u području IKT-a;

   (b) rizike koji proizlaze iz ugovora o korištenju IKT usluga sklopljenih s trećim stranama pružateljima IKT usluga, vodeći računa o nužnosti ili važnosti relevantne usluge, procesa ili funkcije te o mogućem učinku na kontinuitet i kvalitetu financijskih usluga i aktivnosti na razini subjekta i na razini grupe;

   (ba) je li pružatelj IKT usluga pružatelj IKT usluga unutar grupe.

3. Kao dio okvira upravljanja IKT rizicima financijski subjekti ***koji nisu mikropoduzeća*** donose i redovito preispituju strategiju za IKT rizik treće strane . Ta strategija sadržava politiku korištenja IKT usluga trećih strana pružatelja IKT usluga i primjenjuje se na pojedinačnoj i prema potrebi na potkonsolidiranoj i konsolidiranoj osnovi. Upravljačko tijelo redovito preispituje utvrđene rizike eksternalizacije ključnih ili važnih funkcija.

4. Kao dio okvira upravljanja IKT rizicima financijski subjekti vode i ažuriraju na razini subjekta te na potkonsolidiranoj i konsolidiranoj razini registar informacija o svim ugovorima o korištenju IKT usluga ***kojima se pruža potpora ključnim ili važnim funkcijama*** trećih strana pružatelja IKT usluga.

   Ugovori iz prvog podstavka na odgovarajući se način dokumentiraju .

   Ako su dostupne, financijski subjekti dužni su slijediti smjernice i druge mjere koje su izdala europska nadzorna tijela i nadležna tijela do stupanja na snagu provedbenih tehničkih standarda iz stavka 10.

   Financijski subjekti dostavljaju nadležnim tijelima najmanje jednom godišnje informacije o broju novih ugovora o korištenju IKT usluga ***kojima se pruža potpora za ključne ili važne funkcije***, kategorijama trećih strana pružatelja IKT usluga, vrsti ugovora te uslugama i funkcijama koje se pružaju.

   Financijski subjekti stavljaju na raspolaganje nadležnom tijelu, na njegov zahtjev, cjelovit registar informacija ili, ovisno o zahtjevu, njegove određene dijelove te sve

informacije koje se smatraju nužnima za djelotvoran nadzor financijskog subjekta.

Financijski subjekti pravodobno obavješćuju nadležno tijelo o planiranom ugovaranju ključnih ili važnih funkcija te o trenutku kada funkcija postane ključna ili važna.

5. Prije sklapanja ugovora o korištenju IKT usluga financijski subjekti:

(a) ocjenjuju obuhvaća li ugovor ključnu ili važnu funkciju;

(b) ocjenjuju jesu li ispunjeni uvjeti za nadzor ugovaranja;

(c) utvrđuju i ocjenjuju sve relevantne rizike ugovora, među ostalim mogu li ti ugovori pridonijeti jačanju koncentracijskog IKT rizika;

(d) provode dubinske analize potencijalnih trećih strana pružatelja IKT usluga i osiguravaju prikladnost treće strane pružatelja IKT usluga tijekom cijelog procesa odabira i ocjene;

(e) utvrđuju i ocjenjuju sukobe interesa koje bi ugovor mogao izazvati.

6. Financijski subjekti mogu sklapati ugovore samo s trećim stranama pružateljima IKT usluga koje ispunjavaju visoke, odgovarajuće i ***ažurirane sigurnosne*** standarde ▌. ***Najnoviji standardi također se uzimaju u obzir pri utvrđivanju jesu li postojeći sigurnosni standardi primjereni.***

7. Pri ostvarivanju prava pristupa, nadzora i revizije treće strane pružatelja IKT usluga ***u vezi s ključnim ili važnim funkcijama*** financijski subjekti na temelju procjene rizika unaprijed utvrđuju učestalost revizija i nadzora te područja revizije poštujući općeprihvaćene revizijske standarde u skladu s uputama nadzornog tijela o primjeni i uvrštenju tih revizijskih standarda.

U slučaju ***detaljno*** tehnološki ▌složenih ugovora financijski subjekti provjeravaju imaju li revizori, neovisno o tome jesu li unutarnji revizori, skupina revizora ili vanjski revizori, odgovarajuće vještine i znanje za djelotvornu provedbu relevantnih revizija i ocjena.

8. Financijski subjekti osiguravaju ***da se ugovorima*** o korištenju IKT usluga ***financijskim subjektima omogućuje poduzimanje odgovarajućih korektivnih mjera, koje bi mogle obuhvaćati potpuni raskid ugovora, ako ispravak nije moguć, ili djelomični raskid ugovora, ako je ispravak moguć, u skladu s primjenjivim pravom*** barem u sljedećim okolnostima:

(a) treća strana pružatelj IKT usluga ***značajno*** krši primjenjive zakone, propise ili ugovorne uvjete;

(aa) Zajedničko nadzorno tijelo izdalo je preporuku u skladu s člankom 37. trećoj strani pružatelju ključne IKT usluge;

(b) praćenjem IKT rizika trećih strana utvrđene su okolnosti za koje se smatra da bi mogle dovesti do promjena u izvršavanju funkcija koje se pružaju na temelju ugovora, uključujući bitne promjene koje utječu na ugovor ili stanje treće strane pružatelja IKT usluga;

(c) postoje dokazi o slabostima ***koje se odnose na ukupno upravljanje*** IKT rizicima na razini treće strane pružatelja IKT usluga ***u okviru njegova ugovora s financijskim subjektom*** te osobito načina na koji osigurava sigurnost i cjelovitost povjerljivih, osobnih ili drugih osjetljivih ili neosobnih podataka;

(d) nadležno tijelo zbog predmetnog ugovora ***dokazano*** više ne može djelotvorno nadzirati financijski subjekt.

8a. U cilju smanjenja rizika od poremećaja na razini financijskog subjekta, u propisno opravdanim okolnostima i u dogovoru s nadležnim tijelima, financijski subjekt može odlučiti da neće raskinuti ugovore s trećom stranom pružateljem IKT usluga sve dok je ne bude u mogućnosti zamijeniti drugom trećom stranom pružateljem IKT usluga ili promijeniti interna rješenja koja su u skladu sa složenošću pružene usluge, u skladu s izlaznom strategijom iz stavka 9.

8b. U slučaju raskida ugovora s trećim stranama pružateljima IKT usluga u bilo kojoj od okolnosti navedenih u stavku 8. točkama od (a) do (d), financijski subjekti ne snose troškove prijenosa podataka od treće strane pružatelja IKT usluga ako je taj prijenos veći od troška prijenosa podataka predviđenog početnim ugovorom.

9. ***Za IKT usluge povezane s ključnim ili važnim funkcijama*** financijski subjekti uvode izlazne strategije***, koje treba redovito preispitivati***. ***Izlaznim strategijama uzimaju se*** u obzir ***rizici*** koji bi se mogli pojaviti na razini ***trećih strana*** pružatelja IKT usluga, osobito ***moguća*** propast treće strane, pogoršanje kvalitete pružanih funkcija, poremećaj u poslovanju zbog neprikladnog ili neuspješnog pružanja usluga ili mogući značajan rizik koji nastaje u vezi s prikladnošću i kontinuitetom uvođenja funkcije***, ili u slučaju raskida ugovora s trećom stranom pružateljem IKT usluga u bilo kojoj od okolnosti navedenih u stavku 8. točkama od (a) do (d)***.

Financijski subjekti osiguravaju mogućnost raskida ugovora bez:

(a) poremećaja u njihovim poslovnim aktivnostima;

(b) ograničenja usklađenosti s regulatornim zahtjevima;

(c) štete za kontinuitet i kvalitetu njihova pružanja usluga klijentima.

Izlazni su planovi sveobuhvatni, dokumentirani i prema potrebi dostatno testirani.

Financijski subjekti utvrđuju alternativna rješenja i izrađuju tranzicijski plan koji će im omogućiti da se ugovorene funkcije i relevantni podaci od treće strane pružatelja IKT usluga sigurno i u cijelosti prenesu na alternativne pružatelje ili ponovno uključe u interni sustav.

Financijski subjekti poduzimaju odgovarajuće mjere za izvanredne situacije kako bi održali kontinuitet poslovanja u svim okolnostima iz prvog podstavka.

10. Europska nadzorna tijela, u okviru Zajedničkog odbora, izrađuju nacrt provedbenih tehničkih standarda kako bi utvrdila standardne obrasce za potrebe registra informacija iz stavka 4.

Europska nadzorna tijela taj nacrt provedbenih tehničkih standarda dostavljaju Komisiji do [Ured za publikacije: unijeti datum: jednu godinu od datuma stupanja na snagu ove Uredbe].

Komisiji se dodjeljuje ovlast za donošenje provedbenih tehničkih standarda iz prvog podstavka u skladu s člankom 15. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1095/2010 odnosno Uredbe (EU) br. 1094/2010.

11. Europska nadzorna tijela, u okviru Zajedničkog odbora, izrađuju nacrt regulatornih standarda:

(a) kako bi pobliže opisala detaljan sadržaj politike iz stavka 3. u pogledu ugovorâ o korištenju IKT usluga trećih strana pružatelja IKT usluga uz upućivanje na glavne faze životnog ciklusa pojedinačnih ugovora o korištenju IKT usluga;

(b) vrste informacija koje trebaju biti uključene u registar informacija iz stavka 4.

Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do [Ured za publikacije: uneseni datum treba biti ***18 mjeseci*** nakon datuma stupanja na snagu].

Komisiji se dodjeljuje ovlast za dopunu ove Uredbe donošenjem regulatornih tehničkih standarda iz drugog podstavka u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1095/2010 odnosno Uredbe (EU) br. 1094/2010.

Članak 26.

Preliminarna procjena koncentracijskog IKT rizika i dodatnog podugovaranja eksternalizacije

1. Pri utvrđivanju i procjeni koncentracijskog IKT rizika iz članka 25. stavka 5. točke (c) financijski subjekti uzimaju u obzir hoće li sklapanje ugovora o IKT uslugama ***kojima se podržavaju ključne ili važne funkcije*** za posljedicu imati bilo što od sljedećeg:

(a) sklapanja ugovora s trećom stranom pružateljem IKT usluga kojeg nije lako zamijeniti; ili

(b) više sklopljenih ugovora o pružanju IKT usluga s istom trećom stranom pružateljem IKT usluga ***kojima se podržavaju ključne ili važne funkcije*** ili s usko povezanim trećim stranama pružateljima IKT usluga.

Financijski subjekti analiziraju koristi i troškove alternativnih rješenja, kao što je angažman drugih trećih strana pružatelja IKT usluga, uzimajući u obzir podudaraju li se i u kojoj se mjeri predviđena rješenja s poslovnim potrebama i ciljevima iz njihove strategije digitalne otpornosti.

2. Ako je ugovorom o korištenju IKT usluga ***kojima se podržavaju ključne ili važne funkcije*** predviđeno da treća strana pružatelj IKT usluga može ključnu ili važnu funkciju podugovoriti drugoj trećoj strani pružatelju IKT usluga, financijski subjekti analiziraju moguće koristi i rizike tog mogućeg podugovaranja ▌.

Ako se ugovor u korištenju IKT usluga ***kojima se podržavaju ključne ili važne funkcije*** sklopi s trećom stranom pružateljem IKT usluga ▌, financijski subjekti smatraju važnima barem sljedeće čimbenike:

(a) ▌

(b) ▌

(c) odredbe prava o nesolventnosti koje bi se primjenjivale u slučaju stečaja treće strane pružatelja IKT usluga; ***i***

(d) sva moguća ograničenja u slučaju hitnog oporavka podataka financijskog subjekta.

Ako se ugovor u korištenju IKT usluga kojima se podržavaju ključne ili važne funkcije sklopljeni s trećom stranom pružateljem IKT usluga s poslovnim nastanom

u trećoj zemlji, financijski subjekti, uz razmatranja iz prvog i drugog podstavka, uzimaju u obzir i sljedeće:

(i) poštovanje pravila Unije o zaštiti podataka; i

(ii) učinkovitu provedbu pravila utvrđenih u ovoj Uredbi.

Ako takvi ugovorni aranžmani uključuju podugovaranje ključnih ili važnih funkcija, financijski subjekti procjenjuju mogu li i u kojoj mjeri potencijalno dugi ili složeni lanci podugovaranja utjecati na njihov kapacitet ***cjelovite procjene čimbenika navedenih u drugom i trećem podstavku za praćenje*** ugovorenih funkcija i u tom smislu na kapacitet nadležnog tijela za djelotvoran nadzor financijskog subjekta.

Članak 27.

Ključne ugovorne odredbe

1. Prava i obveze financijskog subjekta i treće strane pružatelja IKT usluga jasno se utvrđuju i navode u pisanom obliku. Cijeli ugovor, koji uključuje sporazume o razini usluga, dokumentira se ***kao pisani dokument*** i dostupan je stranama u papirnatom obliku ili nekom pristupačnom formatu koji se može preuzeti.

2. ***Financijski subjekti i treće strane pružatelji IKT usluga osiguravaju da*** ugovori o korištenju IKT usluga sadržavaju barem sljedeće:

(a) jasan i cjelovit opis svih funkcija i usluga koje će pružati treća strana pružatelj IKT usluga, uz naznaku je li dopušteno podugovaranje ključne ili važne funkcije ili njezinih bitnih dijelova te ako jest, uvjete takvog podugovaranja;

(b) lokacije***, to jest regije ili zemlje,*** na kojima će se pružati ugovorene ili podugovorene ***IKT*** funkcije i usluge i lokacije na kojima će se obrađivati podaci, uključujući lokaciju pohrane, te zahtjev da treća strana pružatelj IKT usluga ***unaprijed*** obavijesti financijski subjekt ako planira mijenjati te lokacije;

(c) odredbe o pristupačnosti, dostupnosti, cjelovitosti, sigurnosti, ***povjerljivosti*** i zaštiti ***podataka***, ***uključujući osobne podatke***;

(ca) odredbe o osiguravanju pristupa osobnim i neosobnim podacima koje obrađuje financijski subjekt, njihova oporavka i vraćanja u lako dostupnom formatu u slučaju nesolventnosti, sanacije ili prestanka poslovanja treće strane pružatelja IKT usluga, ***ili u slučaju raskida ugovora***;

(d) cjelovit opis razinâ usluga, uključujući njihova ažuriranja i revizije, te precizne kvantitativne i kvalitativne ciljeve uspješnosti na dogovorenim razinama usluga kako bi se financijskom subjektu omogućilo djelotvorno praćenje i brzo poduzimanje odgovarajućih korektivnih mjera ako se ne postignu dogovorene razine usluga;

(e) ▌

(f) obvezu treće strane pružatelja IKT usluga da u slučaju IKT incidenta povezanog s pruženom uslugom pruži pomoć bez dodatnih troškova ili unaprijed utvrđene troškove;

(g) zahtjeve da treća strana pružatelj IKT usluga uvede i testira planove za nepredvidive situacije u poslovanju i da ima uvedene mjere, alate i politike za sigurnost IKT-a koji na odgovarajući način jamče financijskom subjektu sigurno

pružanje usluga u skladu s regulatornim okvirom koji se na njega odnosi;

(h) ▌

(i) obvezu treće strane pružatelja IKT usluga da u cijelosti surađuje s nadležnim i sanacijskim tijelima zaduženima za financijski subjekt, uključujući osobe koje ta tijela imenuju;

(j) prava raskida ugovora i povezane minimalne rokove za prethodnu obavijest o raskidu ugovora u skladu s očekivanjima nadležnih ***i sanacijskih*** tijela ***te, ako taj ugovorni aranžman utječe na pružatelja IKT usluga unutar iste grupe, analizu u skladu s pristupom koji se temelji na riziku***;

(k) izlazne strategije, osobito odredbu o obveznom primjerenom prijelaznom razdoblju:

(i) tijekom kojega će treća strana pružatelj IKT usluga nastaviti pružati relevantne funkcije ili usluge kako bi se smanjio rizik od poremećaja u radu financijskog subjekta ***ili kako bi se osigurala njegova učinkovita sanacija i restrukturiranje***;

(ii) u kojem, u skladu sa složenosti pružane usluge, financijski subjekt može početi koristiti usluge druge treće strane pružatelja IKT usluga ili primjenjivati lokalna rješenja;

(iia) ako taj ugovorni aranžman utječe na pružatelja IKT usluga unutar iste grupe, analizira se u skladu s pristupom koji se temelji na riziku;

(ka) odredbu o obradi osobnih podataka koju provodi treća strana pružatelj IKT usluga koja mora biti u skladu s Uredbom (EU) 2016/679;

2a. ugovori za pružanje ključnih ili važnih funkcija, uz odredbe iz stavka 2., uključuju barem sljedeće:

(a) rokove za prethodnu obavijest i izvještajne obveze treće strane pružatelja IKT usluga prema financijskom subjektu, uključujući obavijesti o svim događajima koji bi mogli bitno utjecati na kapacitet treće strane pružatelja IKT usluga za djelotvorno izvršavanje ključnih ili važnih funkcija u skladu s dogovorenim razinama usluga;

(b) pravo kontinuiranog praćenja uspješnosti treće strane pružatelja IKT usluga, što uključuje:

(i) prava financijskog subjekta ili imenovane treće strane na pristup, nadzor i reviziju te pravo na preslike relevantne dokumentacije na licu mjesta ako su ključne za poslovanje treće strane pružatelja IKT usluga, čije se djelotvorno izvršenje ne smije spriječiti ni ograničiti drugim ugovorima ili provedbenim politikama;

(ii) pravo ugovaranja alternativnih razina osiguranja ako utječu na prava drugih klijenata;

(iii) obvezu treće strane pružatelja IKT usluga da u potpunosti surađuje tijekom izravnog nadzora i revizija koje provode nadležna tijela, glavni nadzornik, financijski subjekt ili imenovana treća strana te pojedinosti o opsegu, modalitetima i učestalosti takvih inspekcija i revizija.

Odstupajući od točke (b), treća strana pružatelj IKT usluga i financijski subjekt mogu se dogovoriti da se prava pristupa, nadzora i revizije mogu delegirati neovisnoj trećoj strani, koju imenuje treća strana pružatelj IKT usluga, te da financijski subjekt može od treće strane u bilo kojem trenutku zatražiti informacije i uvjerenje o uspješnosti treće strane pružatelja IKT usluga.

2b. Ugovori za IKT usluge koje su određene kao ključne u skladu s člankom 28. stavkom 9. koje pruža treća strana pružatelj IKT usluga sa sjedištem u trećoj zemlji, uz stavak 2. i 2.a ovog članka, moraju:

(a) odrediti da se na ugovor primjenjuje pravo države članice; i

(b) jamčiti da Zajedničko nadzorno tijelo i glavno nadzorno tijelo mogu izvršavati svoje dužnosti navedene u članku 30. na temelju svojih nadležnosti utvrđenih u članku 31.

Ne zahtijeva se da usluge za koje su sklopljeni ugovori pruža poduzeće osnovano u Uniji u skladu s pravom države članice.

3. Tijekom pregovora o ugovorima financijski subjekti i treće strane pružatelji IKT usluga dužni su razmotriti primjenu standardnih ugovornih klauzula za pojedinačne usluge.

3a. Nadležna tijela mogu pristupiti ugovorima iz ovog članka. Stranke tih ugovora mogu se dogovoriti da će izbrisati poslovno osjetljive ili povjerljive informacije prije odobravanja takvog pristupa nadležnim tijelima, pod uvjetom da su ta tijela u potpunosti obaviještena o opsegu i prirodi brisanja.

4. Europska nadzorna tijela u okviru Zajedničkog odbora izrađuju nacrt regulatornih tehničkih standarda kojima se preciznije utvrđuju elementi koje financijski subjekt treba utvrditi i procijeniti pri podugovaranju ključnih ili važnih funkcija radi pravilne provedbe odredbi stavka 2. točke (a). ***Pri izradi tih nacrta regulatornih tehničkih standarda europska nadzorna tijela uzimaju u obzir veličinu financijskih subjekata, prirodu, opseg i složenost njihovih usluga, aktivnosti i poslovanja te njihov ukupni profil rizičnosti.***

Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do [Ured za publikacije: unijeti datum: ***18 mjeseci*** nakon datuma stupanja na snagu].

Komisiji se dodjeljuje ovlast za dopunu ove Uredbe donošenjem regulatornih tehničkih standarda iz prvog podstavka u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1095/2010 odnosno Uredbe (EU) br. 1094/2010.

ODJELJAK II.

NADZORNI OKVIR ZA TREĆE STRANE PRUŽATELJE KLJUČNIH IKT USLUGA

Članak 28.

Imenovanje trećih strana pružatelja ključnih IKT usluga

1. Europska nadzorna tijela u okviru Zajedničkog odbora i na preporuku Nadzornog ***tijela*** osnovanog u skladu s člankom 29. stavkom 1., ***nakon savjetovanja s ENISA-om***:

   (a) imenuju treće strane pružatelje IKT usluga čije su usluge ključne za financijske subjekte, uzimajući u obzir kriterije iz stavka 2.;

   (b) imenuju EBA-u, ESMA-u ili EIOPA-u glavnim nadzornim tijelom za svaku treću stranu pružatelja ključnih IKT usluga, ovisno o tome je li ukupna vrijednost imovine financijskih subjekata koji koriste usluge te treće strane pružatelja IKT usluga i koji su obuhvaćeni Uredbom (EU) br. 1093/2010, Uredbom (EU) br. 1094/2010 ili Uredbom (EU) br. 1095/2010 veća od polovine vrijednosti ukupne imovine svih financijskih subjekata koji koriste usluge te treće strane pružatelja ključnih IKT usluga, što dokazuju konsolidirane bilance tih financijskih subjekata ili njihove pojedinačne bilance ako bilance nisu konsolidirane.

   Glavno nadzorno tijelo imenovano u skladu s prvim podstavkom točkom (b) odgovorno je za svakodnevni nadzor treće strane pružatelja ključnih IKT usluga.

2. Imenovanje iz stavka 1. točke (a) temelji se na svim kriterijima u nastavku:

   (a) sistemski učinak na stabilnost, kontinuitet ili kvalitetu pružanja financijskih usluga u slučaju opsežnog operativnog prekida pružanja usluga relevantne treće strane pružatelja IKT usluga, uzimajući u obzir broj financijskih subjekata kojima relevantna treća strana pružatelj IKT usluga pruža usluge;

   (b) sistemska priroda ili važnost financijskih subjekata koji se oslanjaju na relevantnu treću stranu pružatelja IKT usluga, što se procjenjuje prema sljedećim parametrima:

      i) broj globalnih sistemski važnih institucija (GSV institucije) ili ostalih sistemski važnih institucija (OSV institucije) koje se oslanjaju na na relevantnu treću stranu pružatelja IKT usluga;

      ii) međusobna ovisnost GSV institucija ili OSV institucija iz točke i. i drugih financijskih subjekata, uključujući slučajeve u kojima GSV ili OSV institucije pružaju usluge financijske infrastrukture drugim financijskim subjektima;

   (c) oslanjanje financijskih subjekata na usluge relevantne treće strane pružatelja IKT usluga koje se odnose na ključne ili važne funkcije financijskih subjekata u čije je pružanje u konačnici uključena ista treća strana pružatelj IKT usluga, neovisno o tome oslanjaju li se financijski subjekti na te usluge izravno ili neizravno, na temelju ili putem podugovora;

   (d) stupanj zamjenjivosti treće strane pružatelja IKT usluga, uzimajući u obzir sljedeće parametre:

      i) nepostojanje stvarnih alternativa, čak ni djelomičnih, zbog ograničenog

broja trećih strana pružatelja IKT usluga koji su aktivni na određenom tržištu ili tržišnog udjela treće strane pružatelja IKT usluga ili relevantne tehničke složenosti ili sofisticiranosti, među ostalim u pogledu zaštićene tehnologije, ili posebnosti organizacije ili djelatnosti treće strane pružatelja IKT usluga;

ii) poteškoće s djelomičnom ili potpunom migracijom relevantnih podataka i radnih opterećenja s relevantne na drugu treću stranu pružatelja IKT usluga zbog velikih financijskih troškova, vremena ili druge vrste resursa koji bi bili potrebni za migraciju ili zbog povećanih IKT rizika ili drugih operativnih rizika kojima bi financijski subjekt mogao biti izložen tijekom te migracije;

(e) broj država članica u kojima relevantna treća strana pružatelj IKT usluga pruža usluge;

(f) broj država članica u kojima posluju financijski subjekti koji koriste usluge relevantne treće strane pružatelja IKT usluga.

(fa) značajnost i važnost usluga koje pruža relevantna treća strana pružatelj IKT usluga.

2a. Zajedničko nadzorno tijelo obavješćuje treću stranu pružatelja IKT usluga prije nego što započne svoju procjenu za potrebe imenovanja iz stavka 1. točke (a).

Zajedničko nadzorno tijelo obavješćuje treću stranu pružatelja IKT usluga o ishodu procjene iz prvog podstavka dostavljanjem nacrta preporuke o nužnosti. U roku od šest tjedana od datuma primitka tog nacrta preporuke treća strana pružatelj IKT usluga može Zajedničkom nadzornom tijelu dostaviti obrazloženu izjavu o ocjeni. Ta obrazložena izjava sadržava sve relevantne dodatne informacije koje treća strana pružatelj IKT usluga smatra primjerenima za potpunost i točnost postupka imenovanja ili za osporavanje nacrta preporuke o nužnosti. Zajednički odbor europskih nadzornih tijela uzima u obzir obrazloženu izjavu i može od treće strane pružatelja IKT usluga zatražiti dodatne informacije ili dokaze prije donošenja odluke o određivanju ključnih usluga.

Zajednički odbor europskih nadzornih tijela obavješćuju treću stranu pružatelja IKT usluga o tome da su usluge koje pruža određene kao ključne. Treća strana pružatelj IKT usluga ima rok od najmanje tri mjeseca od datuma primitka obavijesti da izvrši sve potrebne prilagodbe kako bi Zajedničko nadzorno tijelo moglo izvršavati svoje zadaće u skladu s člankom 30. te obavijesti financijske subjekte kojima treća strana pružatelj IKT usluga pruža usluge. Zajedničko nadzorno tijelo može dopustiti produljenje razdoblja prilagodbe za najviše tri mjeseca ako to zatraži imenovana treća strana pružatelj IKT usluga i ako to propisno obrazloži.

3. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 50. radi ***preciznijeg utvrđivanja*** kriterija iz stavka 2.

4. Mehanizam imenovanja iz stavka 1. točke (a) ne primjenjuje se dok Komisija ne donese delegirani akt u skladu sa stavkom 3.

5. Mehanizam imenovanja iz stavka 1. točke (a) ne primjenjuje se na treće strane pružatelje IKT usluga obuhvaćene nadzornim okvirima uspostavljenima za potrebe podrške zadaćama iz članka 127. stavka 2. Ugovora o funkcioniranju Europske unije.

6. ***Zajedničko nadzorno tijelo, uz savjetovanje s ENISA-om,*** izrađuje, objavljuje i ***redovito*** ažurira popis trećih strana pružatelja ključnih IKT usluga na razini Unije.

7. Za potrebe stavka 1. točke (a) nadležna tijela svake godine dostavljaju ***Zajedničkom nadzornom tijelu*** osnovanom u skladu s člankom 29. agregirana izvješća iz članka 25. stavka 4. ***Zajedničko nadzorno tijelo*** procjenjuje ovisnost financijskih subjekata o IKT uslugama trećih strana na temelju informacija koje dobije od nadležnih tijela.

8. Treće strane pružatelji IKT usluga koji nisu obuhvaćeni popisom iz stavka 6. mogu zatražiti uvrštenje na taj popis.

   Za potrebe prvog podstavka treća strana pružatelj IKT usluga dostavlja obrazložen zahtjev EBA-i, ESMA-i ili EIOPA-i, koje u okviru Zajedničkog odbora odlučuju hoće li tu treću stranu pružatelja IKT usluga uvrstiti na taj popis u skladu sa stavkom 1. točkom (a).

   Odluka iz drugog podstavka donosi se i o njoj se obavješćuje treću stranu pružatelja IKT usluga u roku od šest mjeseci od zaprimanja zahtjeva.

8a. Zajednički odbor europskih nadzornih tijela na preporuku Zajedničkog nadzornog tijela imenuje treće strane pružatelje IKT usluga s poslovnim nastanom u trećoj zemlji koji su ključni za financijske subjekte u skladu sa stavkom 1. točkom (a).

Pri imenovanju iz prvog podstavka ovog stavka europska nadzorna tijela i Zajedničko nadzorno tijelo slijede postupovne korake utvrđene u stavku 2.a.

9. Financijski subjekti ne koriste usluge treće strane pružatelja ***ključnih*** IKT usluga sa sjedištem u trećoj zemlji, ***osim ako ta treća strana pružatelj IKT usluga ima društvo osnovano u Uniji u skladu s pravom države članice i ako je sklopila ugovore u skladu s člankom 27. stavkom 2.b***.

Članak 29.

Struktura nadzornog okvira

1. ***Zajedničko nadzorno tijelo osniva se*** za ***nadziranje IKT rizika treće strane*** za sve financijske sektore ***i provedbu izravnog nadzora nad trećim stranama pružateljima IKT usluga koji su određeni kao ključni u skladu s člankom 28.***

   Uloga Zajedničkog nadzornog tijela ograničena je na nadzorne ovlasti u pogledu IKT rizika povezanih s IKT uslugama koje financijskim subjektima pružaju treće strane pružatelji ključnih IKT usluga.

   Zajedničko nadzorno tijelo redovito raspravlja o relevantnim kretanjima u području IKT rizika i osjetljivosti te promiče dosljedan pristup praćenju IKT rizika treće strane na razini Unije.

2. ***Zajedničko nadzorno tijelo*** svake godine provodi kolektivnu procjenu rezultata i nalaza nadzornih aktivnosti provedenih nad svim trećim stranama pružateljima ključnih IKT usluga te promiče koordinacijske mjere radi povećanja digitalne operativne otpornosti financijskih subjekata, poticanja najboljih primjera iz prakse uklanjanja koncentracijskog IKT rizika i potrage za instrumentima za smanjenje prijenosa rizika među sektorima.

   Zajedničko nadzorno tijelo predlaže sveobuhvatne referentne vrijednosti za treće strane pružatelje ključnih IKT usluga koje Zajednički odbor donosi u obliku zajedničkih stajališta europskih nadzornih tijela u skladu s člankom 56. stavkom 1. uredbi (EU)

br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010.

3. ***Zajedničko nadzorno tijelo*** sastoji se od ***izvršnih direktora*** europskih nadzornih tijela, jednog predstavnika na visokoj razini koji je sadašnji član osoblja ***europskog nadzornog tijela i po jednog predstavnika na visokoj razini iz najmanje osam nacionalnih nadležnih tijela***. Jedan predstavnik Europske komisije, ESRB-a, ESB-a i ENISA-e ***te najmanje jedan neovisni stručnjak imenovan u skladu sa stavkom 3.a ovog članka*** sudjeluju ▌ kao promatrači.

Nakon godišnjeg određivanja trećih strana pružatelja ključnih IKT usluga u skladu s člankom 28. stavkom 1. točkom (a) Zajednički odbor europskih nadzornih tijela odlučuje koja će nacionalna nadležna tijela biti članovi Zajedničkog nadzornog izvršnog tijela, uzimajući u obzir sljedeće čimbenike:

(a) broj trećih strana pružatelja ključnih IKT usluga koje imaju sjedište ili pružaju usluge u državi članici;

(b) oslanjanje financijskih subjekata u državi članici na treće strane pružatelje ključnih IKT usluga;

(c) relativno stručno znanje nacionalnog nadležnog tijela;

(d) dostupne resurse i kapacitete nacionalnog nadležnog tijela;

(e) potrebu za jednostavnim, racionalnim i učinkovitim djelovanjem i donošenjem odluka Zajedničkog nadzornog tijela.

Zajedničko nadzorno tijelo dijeli svoju dokumentaciju i odluke sa svim nacionalnim nadležnim tijelima koja nisu članovi Zajedničkog nadzornog tijela.

Zajedničko nadzorno tijelo u radu podupire i pomaže mu namjensko osoblje iz svih europskih nadzornih tijela.

3a. Nakon javnog i transparentnog postupka podnošenja zahtjeva Zajedničko nadzorno tijelo imenuje neovisnog stručnjaka iz stavka 3. ovoga članka kao promatrača.

Neovisni stručnjak imenuje se na temelju stručnog znanja o financijskoj stabilnosti, digitalnoj operativnoj otpornosti i pitanjima sigurnosti IKT-a na mandat od dvije godine.

Imenovani neovisni stručnjak ne smiju obnašati dužnost na nacionalnoj ili međunarodnoj razini ili razini Unije. Neovisni stručnjak djeluje neovisno i objektivno u isključivom interesu Unije kao cjeline, i ne traži niti prima upute od institucija ili tijela Unije, bilo koje vlade države članice ili bilo kojeg drugog javnog ili privatnog tijela.

Zajedničko nadzorno tijelo može odlučiti imenovati više od jednog neovisnog stručnog promatrača.

4. U skladu s člankom 16. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010 europska nadzorna tijela izdaju smjernice ***do [SL: unijeti datum 18 mjeseci nakon datuma stupanja na snagu ove Uredbe]*** o suradnji ***Zajedničkog nadzornog tijela, glavnog nadzornog tijela*** i nadležnih tijela za potrebe ovog odjeljka u pogledu detaljnih postupaka i uvjeta koji se odnose na izvršenje zadaća nadležnih tijela i ***Zajedničkog nadzornog tijela*** te pojedinosti o razmjenama informacija koje su nadležnim tijelima potrebne za poduzimanje mjera na temelju preporuka koje ***Zajedničko nadzorno tijelo uputi*** trećim stranama pružateljima ključnih IKT usluga u

skladu s člankom 31. stavkom 1. točkom (d).

5. Zahtjevima utvrđenima u ovom odjeljku ne dovodi se u pitanje primjena Direktive (EU) 2016/1148 i drugih propisa Unije o nadzoru koji su primjenjivi na pružatelje usluga računalstva u oblaku.

6. ***Zajedničko nadzorno tijelo*** ▌ svake godine dostavlja Europskom parlamentu, Vijeću i Komisiji izvješće o primjeni ovog odjeljka.

Članak 30.

Zadaće glavnog nadzornog tijela

1. Glavno nadzorno tijelo, ***imenovano u skladu s člankom 28. stavkom 1. točkom (b), vodi i koordinira dnevni nadzor trećih strana pružatelja ključnih IKT usluga te je glavna kontaktna točka za te treće strane pružatelje ključnih IKT usluga***.

1a. ***Glavno nadzorno tijelo*** procjenjuje je li svaka treća strana pružatelj ključnih IKT usluga uvela sveobuhvatna, pouzdana i djelotvorna pravila, postupke, mehanizme i sustave za upravljanje IKT rizicima kojima bi mogla izložiti financijske subjekte. ***Ta se procjena prvenstveno usredotočuje na IKT usluge kojima se podržavaju ključne ili važne funkcije koje treće strane pružatelji ključnih IKT usluga pružaju financijskim subjektima, ali može biti i šira ako je to relevantno za procjenu rizika za te funkcije.***

2. Procjena iz stavka ***1.a*** mora obuhvaćati:

   (a) zahtjeve u području IKT-a kojima se osobito osiguravaju sigurnost, dostupnost, kontinuitet, skalabilnost i kvaliteta usluga koje treća strana pružatelj ključnih IKT usluga pruža financijskim subjektima te kapacitet održanja visokih standarda sigurnosti, povjerljivosti i cjelovitosti podataka u svakom trenutku;

   (b) fizičku sigurnost koja pridonosi sigurnosti IKT-a, uključujući sigurnost prostora, objekata, podatkovnih centara;

   (c) procese upravljanja rizicima, uključujući politike upravljanja IKT rizicima, plan kontinuiteta poslovanja u području IKT-a i plan oporavka u slučaju katastrofe u području IKT-a;

   (d) sustave upravljanja, uključujući organizacijsku strukturu s jasnim, transparentnim i dosljednim razinama odgovornosti te pravila odgovornosti koji omogućuju djelotvorno upravljanje IKT rizicima;

   (e) utvrđivanje i praćenje velikih IKT incidenata te brzo izvješćivanje financijskih subjekata o njima, upravljanje tim incidentima, osobito kibernapadima, i njihovo rješavanje;

   (f) mehanizme za prenosivost podataka, prenosivost aplikacija i interoperabilnost, kojima se financijskim subjektima osigurava djelotvorno ostvarivanje prava raskida;

   (g) testiranje sustava, infrastrukture i kontrola IKT-a;

   (h) revizije IKT-a;

   (i) primjenu mjerodavnih nacionalnih i međunarodnih standarda koji su primjenjivi na treću stranu u pružanju IKT usluga financijskim subjektima.

3. Na temelju procjene iz stavka ***1.a koju provodi*** glavno nadzorno tijelo, ***Zajedničko***

nadzorno tijelo, pod koordinacijom i vodstvom glavnog nadzornog tijela, izrađuje i predlaže jasan, detaljan i obrazložen individualni plan nadzora za svaku treću stranu pružatelja ključnih IKT usluga.

Pri pripremi nacrta plana nadzora Zajedničko nadzorno tijelo savjetuje se sa svim relevantnim nadležnim tijelima i jedinstvenim kontaktnim točkama iz članka 8. Direktive (EU) 2016/1148 kako bi se osiguralo da nema nedosljednosti ili udvostručavanja s obvezama treće strane pružatelja ključnih IKT usluga na temelju te direktive.

Upravni odbor glavnog nadzornog tijela svake godine donosi plan nadzora.

Prije usvajanja, o nacrtu plana nadzora obavješćuje ***se*** treću stranu pružatelja ključnih IKT usluga.

Nakon primitka nacrta plana nadzora treća strana pružatelj ključnih IKT usluga ima rok od šest tjedana za preispitivanje i podnošenje obrazložene izjave o nacrtu plana nadzora. Takva obrazložena izjava može se podnijeti samo ako treća strana pružatelj ključnih IKT usluga može pružiti dokaze da bi izvršenje plana nadzora uzrokovalo nerazmjeran učinak ili poremećaj za potrošače koji ne podliježu ovoj Uredbi ili da postoji djelotvornije ili učinkovitije rješenje za upravljanje utvrđenim IKT rizicima. Ako se podnese takva izjava, treća strana pružatelj ključnih IKT usluga predlaže Zajedničkom nadzornom tijelu djelotvornije ili učinkovitije rješenje za postizanje ciljeva iz nacrta plana nadzora.

Prije donošenja plana nadzora glavni odbor glavnog nadzornog tijela uzima u obzir obrazloženu izjavu i može zatražiti dodatne informacije ili dokaze od treće strane pružatelja IKT usluga.

4. Nakon što se ***usvoje*** planovi nadzora iz stavka 3. i o njima se obavijeste treće strane pružatelji ključnih IKT usluga, nadležna tijela mogu u pogledu trećih strana pružatelja ključnih IKT usluga poduzimati mjere samo u dogovoru ***sa Zajedničkim nadzornim tijelom***.

Članak 31.

Nadzorne ovlasti

1. Za potrebe izvršavanja zadaća utvrđenih u ovom odjeljku glavno nadzorno tijelo ovlašteno je ***u pogledu usluga koje treće strane pružatelji ključnih IKT usluga pružaju financijskim subjektima***:

   (a) zahtijevati sve relevantne informacije i dokumentaciju u skladu s člankom 32.;

   (b) provoditi opće istrage i ***izravni*** nadzor u skladu s člancima 33. i 34.;

   (c) zahtijevati izvješća nakon završetka nadzornih aktivnosti u kojima se navode mjere ili korektivne mjere koje su treće strane pružatelji ključnih IKT usluga poduzele ili provele u vezi s preporukama iz stavka ***1.a***;

1a. Za potrebe izvršavanja dužnosti utvrđenih u ovom odjeljku i na temelju informacija koje je dobilo vodeće nadzorno tijelo i rezultata istraga koje je provelo glavno nadzorno tijelo, Zajedničko nadzorno tijelo ima ovlasti uputiti preporuke iz područjâ iz članka 30. stavka 2., posebno o sljedećem:

   (i) primjeni posebnih zahtjeva ili procesa za sigurnost i kvalitetu IKT-a, točnije u pogledu uvođenja zakrpa, ažuriranja, enkripcije i drugih

sigurnosnih mjera koje ***Zajedničko*** nadzorno tijelo smatra važnima za sigurnost IKT-a za usluge koje se pružaju financijskim subjektima;

(ii) primjeni uvjeta, uključujući njihovu tehničku provedbu, pod kojima treće strane pružatelji ključnih IKT usluga pružaju usluge financijskim subjektima, a koje ***Zajedničko*** nadzorno tijelo smatra važnima za sprečavanje nastanka ili širenja jedinstvenih točaka prekida te za smanjenje mogućeg sistemskog učinka u cijelom financijskom sektoru Unije u slučaju koncentracijskog IKT rizika;

(iii) nakon provjere podugovora u skladu s člancima 32. i 33., uključujući podugovore o eksternalizaciji koje treće strane pružatelji ključnih IKT usluga namjeravaju sklopiti s drugim trećim stranama pružateljima IKT usluga ili podugovarateljima IKT usluga sa sjedištem u trećoj zemlji, o svim planiranim podugovorima, uključujući podugovore o eksternalizaciji, ako ***Zajedničko*** nadzorno tijelo smatra da bi podugovaranje moglo prouzročiti rizike financijskom subjektu u pogledu pružanja usluga ili rizike za financijsku stabilnost;

(iv) suzdržavanju od sklapanja podugovora ako su ispunjeni sljedeći kumulativni uvjeti:

– predviđeni je podugovaratelj treća strana pružatelj IKT usluga ili podugovaratelj IKT usluga sa sjedištem u trećoj zemlji ***i nema poduzeće osnovano u Uniji u skladu s pravom države članice***;

– podugovara se ključna ili važna funkcija financijskog subjekta;

– ***podugovaranje će dovesti do ozbiljnih i jasnih rizika za financijski subjekt ili financijsku stabilnost financijskog sustava Unije.***

1b. Ovlasti iz stavaka 1. i 1.a izvršavaju se u pogledu IKT usluga kojima se podupiru funkcije koje nisu ključne ili važne, a koje pruža treća strana pružatelj ključnih IKT usluga kada je to potrebno.

1c. Pri izvršavanju ovlasti iz stavaka 1. i 1.a ovog članka glavno nadzorno tijelo i Zajedničko nadzorno tijelo uzimaju u obzir okvir uspostavljen Direktivom (EU) 2016/1148 i, prema potrebi, savjetuju se s relevantnim nadležnim tijelima uspostavljenima tom direktivom kako bi se izbjeglo nepotrebno udvostručavanje tehničkih i organizacijskih mjera koje bi se mogle primjenjivati na treće strane pružatelje ključnih IKT usluga u skladu s tom Direktivom.

2. ***Prije finaliziranja i izdavanja preporuka u skladu sa stavkom 1.a Zajedničko nadzorno tijelo obavješćuje treću stranu pružatelja ključnih IKT usluga o svojim namjerama i daje mogućnost trećoj strani pružatelju IKT usluga da pruži informacije za koje razumno smatra da bi ih trebalo uzeti u obzir prije finaliziranja preporuke ili kako bi se osporile predviđene preporuke. Razlozi za osporavanje preporuke mogu uključivati nerazmjeran učinak ili poremećaje za korisnike koji ne podliježu ovoj Uredbi ili postojanje djelotvornijeg ili učinkovitijeg rješenja za upravljanje utvrđenim rizikom.***

3. Treće strane pružatelji ključnih IKT usluga surađuju u dobroj vjeri s glavnim nadzornim tijelom ***i Zajedničkim nadzornim tijelom te im*** pomažu u obavljanju ***njihovih*** zadaća.

4. Glavno nadzorno tijelo može ***odlučiti, u slučaju potpune ili djelomične neusklađenosti***

s mjerama koje se moraju poduzeti u skladu sa stavkom 1. točkama (a), (b) ili (c) i nakon isteka razdoblja od najmanje 60 kalendarskih dana od datuma kada je treća strana pružatelj ključnih IKT usluga primila obavijest o mjeri, izreći periodičnu novčanu kaznu kako bi treću stranu pružatelja ključnih IKT usluga primorao na poštovanje ***tih mjera***.

4a. ***Glavno nadzorno tijelo izriče periodičnu novčanu kaznu iz stavka 4. samo kao krajnju mjeru i u slučajevima kada treća strana pružatelj ključnih IKT usluga nije poštovala mjere koje se moraju poduzeti u skladu sa stavkom 1. točkama (a), (b) ili (c).***

5. Periodična novčana kazna iz stavka 4. izriče se svakodnevno sve dok se ne osigura usklađenost, a najviše šest mjeseci od obavijesti trećoj strani pružatelju ključnih IKT usluga.

6. Iznos periodične novčane kazne, koji se izračunava od datuma iz odluke kojom se izriče periodična novčana kazna, ***iznosi do*** 1 % prosječnog dnevnog svjetskog prometa usluga treće strane pružatelja ključnih IKT usluga ***koje su se pružale financijskim subjektima obuhvaćenima ovom Uredbom*** u prethodnoj poslovnoj godini.

7. Novčane kazne su administrativne prirode i izvršive su. Izvršenje se uređuje pravilima građanskog postupka koja su na snazi u državi članici na čijem se državnom području provodi nadzor i pristup. Sudovi predmetne države članice imaju nadležnost nad pritužbama o nepravilnom izvršenju. Uplaćeni iznosi novčanih kazni prihod su općeg proračuna Europske unije.

8. Europska nadzorna tijela javno objavljuju svaku izrečenu periodičnu novčanu kaznu, osim ako bi takva objava ozbiljno ugrozila financijska tržišta ili prouzročila nerazmjernu štetu uključenim stranama.

9. Prije izricanja periodične novčane kazne iz stavka 4. glavno nadzorno tijelo daje predstavnicima treće strane pružatelja ključnih IKT usluga koja je predmet postupka mogućnost da se očituju o nalazima i svoje odluke temelji samo na nalazima o kojima se treća strana pružatelj ključnih IKT usluga koja je predmet postupka mogla očitovati. U postupku se u potpunosti poštuje pravo na obranu osoba koje su predmet postupka. One imaju pravo na pristup spisu, pri čemu se mora uvažavati legitimni interes drugih osoba u pogledu zaštite njihovih poslovnih tajni. Pravo pristupa spisu ne odnosi se na povjerljive informacije ili interne pripremne dokumente glavnog nadzornog tijela.

Članak 32.

Zahtjev za informacije

1. Glavno nadzorno tijelo može običnim zahtjevom ili odlukom zatražiti da treće strane pružatelje ključnih IKT usluga dostave sve informacije koje su glavnom nadzornom tijelu potrebne za izvršavanje njegovih zadaća iz ove Uredbe, među ostalim sve relevantne poslovne ili operativne dokumente, ugovore, dokumentaciju o politikama, izvješća o reviziji sigurnosti IKT-a, izvješća o IKT incidentima, te sve informacije o stranama kojima je treća strana pružatelj ključnih IKT usluga eksternalizirala operativne funkcije ili aktivnosti.

Treće strane pružatelji ključnih IKT usluga dužne su pružati informacije iz prvog podstavka samo u pogledu usluga koje se pružaju financijskim subjektima na koje se primjenjuje ova Uredba i koji se koriste uslugama trećih strana pružatelja ključnih IKT usluga za ključne ili važne funkcije. Treće strane pružatelji ključnih IKT usluga

obavješćuju relevantni financijski subjekt o zahtjevima specifičnima za taj financijski subjekt.

2. Pri slanju običnog zahtjeva za informacije iz stavka 1. glavno nadzorno tijelo:

   (a) upućuje na ovaj članak kao pravni temelj za zahtjev;

   (b) navodi svrhu zahtjeva;

   (c) navodi koje se informacije traže;

   (d) utvrđuje rok za dostavu informacija;

   (e) obavješćuje predstavnika treće strane pružatelja ključnih IKT usluga od koje se zahtijevaju informacije da nije dužna dostaviti informacije, ali da u slučaju dobrovoljnog odgovora na zahtjev dostavljene informacije ne smiju biti netočne ili obmanjujuće.

3. Kada ***odlukom*** zahtijeva dostavu informacija iz stavka 1. glavno nadzorno tijelo:

   (a) upućuje na ovaj članak kao pravni temelj za zahtjev;

   (b) navodi svrhu zahtjeva;

   (c) navodi koje se informacije traže;

   (d) utvrđuje ***razuman*** rok za dostavu informacija;

   (e) navodi periodične novčane kazne predviđene člankom 31. stavkom 4. ako su dostavljene tražene informacije nepotpune ***ili ako takve informacije nisu dostavljene u roku iz točke (d)***;

   (f) navodi pravo na podnošenje žalbe protiv odluke Odboru za žalbe europskog nadzornog tijela i pravo na preispitivanje te odluke u postupku pred Sudom Europske unije („Sud”) u skladu s člancima 60. i 61. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 odnosno Uredbe (EU) br. 1095/2010.

4. Predstavnici trećih strana pružatelja ključnih IKT usluga dostavljaju tražene informacije. Propisno ovlašteni odvjetnici mogu dostaviti informacije u ime svojih klijenata. Treća strana pružatelj ključnih IKT usluga ostaje i nadalje u potpunosti odgovorna za nepotpunost, netočnost ili obmanjujuću prirodu dostavljenih informacija.

5. Glavno nadzorno tijelo bez odgode šalje primjerak odluke o dostavi informacija nadležnim tijelima zaduženima za financijske subjekte koji koriste usluge trećih strana pružatelja ključnih IKT usluga.

Članak 33.

Opće istrage

1. Radi izvršavanja svojih zadaća iz ove Uredbe, glavno nadzorno tijelo uz pomoć tima za provjeru iz članka ***35.*** stavka 1. može provoditi potrebne istrage trećih strana pružatelja ključnih IKT usluga ***u skladu s načelom proporcionalnosti***. ***Pri provođenju istraga glavno nadzorno tijelo postupa oprezno i vodi računa o zaštiti prava korisnika trećih strana pružatelja ključnih IKT usluga koje nisu predmet ove Uredbe, među ostalim u pogledu učinka na razinu usluge, dostupnost podataka i povjerljivost.***

2. Glavno nadzorno tijelo ovlašteno je:

(a) pregledavati evidenciju, podatke, postupke i sve ostale materijale važne za obavljanje svojih zadaća, neovisno o tome na kojem su mediju pohranjeni;

(b) ***na siguran način pregledati*** ovjerene preslike ili izvatke iz te evidencije, podataka, postupaka i ostalih materijala;

(c) pozvati predstavnike treće strane pružatelja IKT usluga i tražiti od njih usmena ili pisana objašnjenja o činjenicama ili dokumente koji se odnose na predmet i svrhu istrage te zabilježiti odgovore;

(d) obaviti razgovor sa svakom fizičkom ili pravnom osobom koja pristane na razgovor s ciljem prikupljanja informacija koje se odnose na predmet istrage;

(e) zatražiti evidenciju telefonskih razgovora i prometa podataka.

3. Službenici i druge osobe koje glavno nadzorno tijelo ovlasti za potrebe istraga iz stavka 1. izvršavaju svoje ovlasti uz predočenje pisanog ovlaštenja u kojem se navodi predmet i svrha istrage.

U tom se ovlaštenju navode i periodične novčane kazne predviđene člankom 31. stavkom 4. ako tražena evidencija, podaci, postupci ili svi ostali materijali ili odgovori na pitanja postavljena predstavnicima treće strane pružatelja IKT usluga nisu dostavljeni ili su nepotpuni.

4. Predstavnici trećih strana pružatelja IKT usluga dužni su pristati na istrage koje se pokrenu na temelju odluke glavnog nadzornog tijela. U odluci se navode predmet i svrha istrage, periodične novčane kazne predviđene člankom 31. stavkom 4., pravni lijekovi dostupni u skladu s uredbama (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010 te pravo na pokretanje postupka pred Sudom radi preispitivanja odluke.

5. Pravodobno prije istrage glavna nadzorna tijela o istrazi i identitetu ovlaštenih osoba obavješćuju nadležno tijelo zaduženo za financijske subjekte koji koriste usluge treće strane pružatelja IKT usluga.

Članak 34.

Izravni nadzor

1. Radi izvršavanja svojih zadaća iz ove Uredbe, glavno nadzorno tijelo uz pomoć timova za provjeru iz članka 35. stavka 1. može ulaziti u sve poslovne prostore, nekretnine ili na zemljište treće strane pružatelja IKT usluga, kao što su registrirana sjedišta, operativni centri, sekundarni poslovni prostori, i u njima provoditi potrebni izravni nadzor, kao i neizravni nadzor dokumentacije.

Ovlast za provođenje izravnog nadzora iz prvog podstavka nije ograničena na lokacije u Uniji, pod uvjetom da nadzor lokacije u trećoj zemlji ispunjava sve sljedeće zahtjeve:

- ***glavno nadzorno tijelo mora izvršavati svoje dužnosti na temelju ove Uredbe;***
- ***izravno je povezan s pružanjem IKT usluga financijskim subjektima Unije;***
- ***važan je za istragu koja je u tijeku.***

1a. Pri provođenju izravnog nadzora glavno nadzorno tijelo preko tima za provjere postupa oprezno i vodi računa o zaštiti prava korisnika trećih strana pružatelja ključnih IKT usluga koje nisu predmet ove Uredbe, među ostalim u pogledu učinka na razinu usluge, dostupnost podataka i povjerljivost.

2. Službenici i druge osobe koje glavno nadzorno tijelo ovlasti za potrebe provedbe izravnog nadzora mogu ulaziti u sve poslovne prostore, nekretnine ili na zemljište i ovlašteni su za pečaćenje svih poslovnih prostora i knjiga ili evidencije tijekom nadzora i u mjeri u kojoj je to potrebno za nadzor.

   Oni izvršavaju svoje ovlasti uz predočenje pisanog ovlaštenja u kojem se navodi predmet i svrha nadzora te periodične novčane kazne predviđene člankom 31. stavkom 4. ako predstavnici predmetne treće strane pružatelja IKT usluga ne pristanu na nadzor.

3. Pravodobno prije nadzora glavna nadzorna tijela šalju obavijest o nadzoru nadležnim tijelima zaduženima za financijske subjekte koji koriste usluge treće strane pružatelja IKT usluga.

4. Nadzor obuhvaća cijeli dijapazon relevantnih sustava IKT-a, mreže, uređaje, informacije i podatke***, koje glavno nadzorno tijelo procijeni primjerenima i tehnološki relevantnima,*** koji se koriste za pružanje usluga financijskim subjektima ili mu pridonose.

5. Prije planiranog terenskog ***nadzora*** glavna nadzorna tijela u razumnom roku o tome obavješćuju treću stranu pružatelja ključnih IKT usluga, osim ako u tom roku obavijest nije moguća zbog hitne ili krizne situacije ili ako bi slanje obavijesti utjecalo na djelotvornost nadzora ili revizije.

6. Treća strana pružatelj ključnih IKT usluga dužna je pristati na izravni nadzor naložen odlukom glavnog nadzornog tijela. U odluci se navode predmet i svrha nadzora, određuje datum njegova početka te navode periodične novčane kazne predviđene člankom 31. stavkom 4., pravni lijekovi dostupni u skladu s uredbama (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010 te pravo na pokretanje postupka pred Sudom radi preispitivanja odluke.

7. Ako službenici i ostale osobe koje glavno nadzorno tijelo ovlasti utvrde da se treća strana pružatelj ključnih IKT usluga protivi nadzoru naloženom na temelju ovog članka, glavno nadzorno tijelo obavješćuje ***treću stranu pružatelja*** ključnih IKT usluga o posljedicama tog protivljenja, među ostalim o mogućnosti da nadležna tijela zadužena za relevantne financijske subjekte raskinu ugovore sklopljene s tom trećom stranom pružateljem ključnih IKT usluga.

Članak 35.

Kontinuirani nadzor

1. U provedbi općih istraga ili izravnog nadzora glavnim nadzornim tijelima pomaže zajednički tim za provjere koji se osniva za svaku pojedinu treću stranu pružatelja ključnih IKT usluga.

2. Zajednički tim za provjere iz stavka 1. sastoji se od članova osoblja glavnog nadzornog tijela***, od drugih europskih nadzornih tijela*** i relevantnih nadležnih tijela koja nadziru financijske subjekte kojima usluge pruža treća strana pružatelj ključnih IKT usluga, koja će se pridružiti pripremi i izvršenju nadzornih aktivnosti s najviše 10 članova. Svi članovi zajedničkog tima za provjere moraju imati stručno znanje iz područja IKT-a i operativnih rizika. Rad zajedničkog tima za provjere koordinira član osoblja europskog nadzornog tijela koji se odredi za to („koordinator glavnog nadzornog tijela”).

3. Europska nadzorna tijela, u okviru Zajedničkog odbora, izrađuju zajednički nacrt

regulatornih tehničkih standarda kojima se preciznije utvrđuje imenovanje članova zajedničkog tima za provjere koji dolaze iz nadležnih tijela te zadaće i način rada tima za provjere. Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do [Ured za publikacije: unijeti datum: jednu godinu od datuma stupanja na snagu].

Komisiji se dodjeljuje ovlast za donošenje regulatornih tehničkih standarda iz prvog podstavka u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 odnosno Uredbe (EU) br. 1095/2010.

4. U roku od tri mjeseca od završetka istrage ili izravnog nadzora, ***Zajedničko nadzorno tijelo*** donosi preporuke upućene trećoj strani pružatelju ključnih IKT usluga u skladu sa svojim ovlastima iz članka 31.

5. O preporukama iz stavka 4. odmah se obavješćuje treću stranu pružatelja ključnih IKT usluga i nadležna tijela zadužena za financijske subjekte kojima ona pruža usluge.

Za potrebe izvršavanja nadzornih aktivnosti glavna nadzorna tijela ***i Zajedničko nadzorno tijelo*** mogu uzeti u obzir sve relevantne certifikate treće strane i izvješća unutarnjih ili vanjskih revizora o IKT uslugama treće strane koje im na raspolaganje stavi treća strana pružatelj ključnih IKT usluga.

Članak 36.

Usklađivanje uvjeta koji omogućuju provedbu nadzora

1. Europska nadzorna tijela, u okviru Zajedničkog odbora, izrađuju nacrt regulatornih tehničkih standarda kako bi pobliže opisala:

(a) informacije koje treća strana pružatelj ključnih IKT usluga treba dostaviti u zahtjevu za dobrovoljno uvrštenje iz članka 28. stavka 8.;

(b) sadržaj i format izvješća koji bi se mogli zahtijevati za potrebe članka 31. stavka 1. točke (c);

(c) način prikaza informacija, uključujući strukturu, formate i metode, koje će treća strana pružatelj ključnih IKT usluga biti dužna dostavljati, objavljivati ili iskazivati u skladu s člankom 31. stavkom 1.;

(d) pojedinosti o procjeni nadležnih tijela u pogledu mjera koje je treća strana pružatelj ključnih IKT usluga poduzela na temelju preporuka ***Zajedničkog nadzornog tijela*** u skladu s člankom 37. stavkom 2.

2. Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do 1. siječnja 20xx. [Ured za publikacije: unijeti datum: jednu godinu od datuma stupanja na snagu].

Komisiji se dodjeljuje ovlast za dopunu ove Uredbe donošenjem regulatornih tehničkih standarda iz prvog podstavka u skladu s postupkom utvrđenim u člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 odnosno Uredbe (EU) br. 1095/2010.

Članak 37.

Praćenje poduzetih mjera koje provode nadležna tijela

1. U roku 30 kalendarskih dana od primitka preporuka koje je ***Zajedničko nadzorno tijelo*** izdalo u skladu s člankom 31. stavkom ***1.a*** treće strane pružatelji ključnih IKT usluga dužne su obavijestiti ***Zajedničko nadzorno tijelo*** o tome namjeravaju li slijediti te preporuke. ***Zajedničko nadzorno tijelo*** odmah tu informaciju prosljeđuje nadležnim tijelima ***relevantnih financijskih subjekata***.

2. Nadležna tijela ***obavješćuju financijske subjekte koji su sklopili ugovore s trećim stranama pružateljima ključnih IKT usluga o rizicima utvrđenima u preporukama koje je Zajedničko nadzorno tijelo uputilo tim trećim stranama pružateljima ključnih IKT usluga u skladu s člankom 31. stavkom 1.a te*** prate jesu li financijski subjekti uzeli u obzir utvrđene rizike. ***Zajedničko nadzorno tijelo prati jesu li treće strane pružatelji ključnih IKT usluga otklonile rizike utvrđene u tim preporukama.***

3. ***Ako se regulatorni ciljevi ne mogu postići drugim mjerama, a nacionalna nadležna tijela zahvaćenim financijskim subjektima izdaju upozorenja na temelju informacija koje je dostavio Zajednički nadzorni odbor, odbor glavnog nadzornog tijela može, na preporuku Zajedničkog nadzornog tijela i nakon savjetovanja s*** nadležnim tijelima ***zahvaćenih*** financijskih subjekata, donijeti odluku o privremenoj obustavi, djelomično ili u cijelosti, korištenja ili uvođenja usluge koja se pruža ***financijskim subjektima izloženima*** rizicima utvrđenima u preporukama upućenima trećim stranama pružateljima ključnih IKT ***usluga dok se ti rizici*** ne uklone. Ona prema potrebi***, i kao krajnju mjeru,*** mogu od ***trećih strana pružatelja ključnih IKT usluga*** zatražiti da raskinu, djelomično ili u cijelosti, relevantne ugovore sklopljene s ***financijskim subjektima izloženima utvrđenim rizicima***.

4. Pri donošenju odluka iz stavka 3.***, odbor glavnog nadzornog tijela,*** uzima u obzir vrstu i razmjer rizika koji treća strana pružatelj ključnih IKT usluga nije uklonila te ozbiljnost neusklađenosti, vodeći računa o sljedećim kriterijima:

   (a) težina i trajanje neusklađenosti;

   (b) je li neusklađenost otkrila ozbiljne slabosti u postupcima, sustavima upravljanja, upravljanju rizicima i unutarnjim kontrolama treće strane pružatelja ključnih IKT usluga;

   (c) je li neusklađenost olakšala ili prouzročila financijska kaznena djela ili se na neki drugi način može povezati s takvim djelima;

   (d) je li neusklađenost posljedica namjere ili nemara.

   (da) uvodi li suspenzija ili prekid poslovanja rizik za kontinuitet poslovanja korisnika koji koriste usluge treće strane pružatelja ključnih IKT usluga.

4a. Odluke predviđene stavkom 3. provode se tek nakon što se o tome propisno obavijeste svi zahvaćeni financijski subjekti. Zahvaćenim financijskim subjektima određuje se vremensko razdoblje, koje ne prelazi najmanje moguće vremensko razdoblje, da prilagode svoju eksternalizaciju i ugovore s trećim stranama pružateljima ključnih IKT usluga na način kojim se ne ugrožava digitalna operativna otpornost te da provedu svoje izlazne strategije i planove tranzicije iz članka 25.

Treće strane pružatelji ključnih IKT usluga na koje se primjenjuju odluke iz stavka 3. u potpunosti surađuju sa zahvaćenim financijskim subjektima.

5. Nadležna tijela redovito informiraju ***Zajedničko nadzorno tijelo*** o pristupima i mjerama koje su poduzela u okviru svojih zadaća nadzora financijskih subjekata.

Članak 38.

Naknade za nadzor

1. Europska nadzorna tijela obračunavaju trećim stranama pružateljima ključnih IKT usluga naknade koje u potpunosti pokrivaju rashode europskih nadzornih tijela potrebnih za provedbu nadzornih zadaća iz ove Uredbe, uključujući povrat mogućih troškova rada nadležnih tijela koja su se pridružila nadzornim aktivnostima u skladu s člankom 35.

   Iznos naknade koja se obračunava na promet treće strane pružatelja ključnih IKT usluga pokriva sve troškove ***koji proizlaze iz izvršavanja zadaća predviđenih ovim odjeljkom*** i razmjeran je prometu treće strane.

1a. Ako je administrativni ugovor s regulatornim i nadzornim tijelom treće zemlje donesen u skladu sa stavkom 1. ovog članka, to tijelo može biti dio tima za provjere iz članka 35. stavka 1.

2. Komisija je ovlaštena za donošenje delegiranog akta u skladu s člankom 50. radi dopune ove Uredbe utvrđivanjem iznosa i načina plaćanja naknada.

Članak 39.

Međunarodna suradnja

1. EBA, ESMA i EIOPA mogu, u skladu s člankom 33. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 odnosno Uredbe (EU) br. 1095/2010, sklapati administrativne sporazume s regulatornim i nadzornim tijelima trećih zemalja kako bi se potaknula međunarodna suradnja u području IKT rizika treće strane u različitim financijskim sektorima, prije svega razvojem najboljih postupaka preispitivanja postupaka i kontrola upravljanja IKT rizicima, mjera za ublažavanje i odgovora na incidente.

2. Europska nadzorna tijela, u okviru Zajedničkog odbora, podnose Europskom parlamentu, Vijeću i Komisiji svakih pet godina zajedničko povjerljivo izvješće sa sažetkom nalaza relevantnih rasprava s tijelima trećih zemalja iz stavka 1., s posebnim naglaskom na razvoj IKT rizika treće strane i posljedice za financijsku stabilnost, cjelovitost tržišta, zaštitu ulagatelja ili funkcioniranje jedinstvenog tržišta.

POGLAVLJE VI.

MEHANIZMI RAZMJENE INFORMACIJA

Članak 40.

Mehanizmi razmjene informacija i saznanja o kiberprijetnjama

1. Financijski subjekti ***trebaju se potruditi*** međusobno ***i s trećim stranama pružateljima ključnih IKT usluga*** razmjenjivati informacije i saznanja o kiberprijetnjama, uključujući pokazatelje ugroženosti, taktike, tehnike i postupke, kibersigurnosna upozorenja i konfiguracijske alate, u mjeri u kojoj te razmjene informacija i saznanja:

   (a) imaju za cilj poboljšanje digitalne operativne otpornosti financijskih subjekata ***i trećih strana pružatelja ključnih IKT usluga***, osobito informiranjem o kiberprijetnjama, ograničavanjem ili sprečavanjem širenja kiberprijetnji, podrškom obrambenim kapacitetima, tehnikama otkrivanja prijetnji, strategija ublažavanja učinka ili faza odgovora i oporavka;

   (b) odvijaju se u pouzdanim zajednicama financijskih subjekata ***i trećih strana pružatelja IKT usluga***;

   (c) provode se u okviru mehanizama razmjene informacija kojima se štiti potencijalno osjetljiva priroda informacija koje se razmjenjuju i koji su uređeni pravilima poslovnog ponašanja kojima se u potpunosti poštuju poslovna tajna, zaštita osobnih podataka[26] i smjernice o politici tržišnog natjecanja[27].

2. Za potrebe stavka 1. točke (c) u mehanizmima razmjene informacija utvrđuju se uvjeti sudjelovanja te prema potrebi pojedinosti o sudjelovanju javnih tijela i u kojem se svojstvu ta tijela mogu povezivati s mehanizmima razmjene informacija te o operativnim elementima, uključujući korištenje namjenskih IT platformi.

3. Financijski subjekti obavješćuju nadležna tijela o svojem sudjelovanju u mehanizmima razmjene informacija iz stavka 1. po potvrdi njihova članstva ili po prestanku njihova članstva, ovisno o slučaju, kada prestanak stupi na snagu.

---

[26] U skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

[27] Komunikacija Komisije – Smjernice o primjenjivosti članka 101. Ugovora o funkcioniranju Europske unije na sporazume o horizontalnoj suradnji, 2011/C 11/01.

POGLAVLJE VII.

NADLEŽNA TIJELA

Članak 41.

Nadležna tijela

Ne dovodeći u pitanje odredbe o nadzornom okviru za treće strane pružatelje ključnih IKT usluga iz odjeljka II. poglavlja V. ove Uredbe, usklađenost s obvezama iz ove Uredbe osiguravaju sljedeća nadležna tijela u skladu s ovlastima koje su im dodijeljene odgovarajućim pravnim aktima:

(a) za kreditne institucije, nadležno tijelo određeno u skladu s člankom 4. Direktive 2013/36/EU, ne dovodeći u pitanje posebne zadaće dodijeljene ESB-u Uredbom (EU) br. 1024/2013;

(b) za pružatelje platnih usluga, nadležno tijelo određeno u skladu s člankom 22. Direktive (EU) 2015/2366;

(c) za institucije za elektronički novac, nadležno tijelo određeno u skladu s člankom 37. Direktive 2009/110/EZ;

(d) za investicijska društva, nadležno tijelo određeno u skladu s člankom 4. Direktive (EU) 2019/2034;

(e) za pružatelje usluga povezanih s kriptoimovinom, izdavatelje ***i ponuditelje*** kriptoimovine, izdavatelje ***i ponuditelje*** tokena vezanih uz kriptoimovinu i izdavatelje značajnih tokena vezanih uz kriptoimovinu nadležno tijelo određeno u skladu s člankom 3. stavkom 1. točkom (ee) prvom alinejom [Uredbe (EU) 20xx, Uredba MICA];

(f) za središnje depozitorije vrijednosnih papira ***i upravitelje sustava za namiru vrijednosnih papira***, nadležno tijelo određeno u skladu s člankom 11. Uredbe (EU) br. 909/2014;

(g) za središnje druge ugovorne strane, nadležno tijelo određeno u skladu s člankom 22. Uredbe (EU) br. 648/2012;

(h) za mjesta trgovanja i pružatelje usluga dostave podataka, nadležno tijelo određeno u skladu s člankom 67. Direktive 2014/65/EU;

(i) za trgovinske repozitorije, nadležno tijelo određeno u skladu s člankom 55. Uredbe (EU) br. 648/2012;

(j) za upravitelje alternativnih investicijskih fondova, nadležno tijelo određeno u skladu s člankom 44. Direktive 2011/61/EU;

(k) za društva za upravljanje, nadležno tijelo određeno u skladu s člankom 97. Direktive 2009/65/EZ;

(l) za društva za osiguranje i društva za reosiguranje, nadležno tijelo određeno u skladu s člankom 30. Direktive 2009/138/EZ;

(m) za posrednike u osiguranju, posrednike u reosiguranju i sporedne posrednike u osiguranju, nadležno tijelo određeno u skladu s člankom 12. Direktive (EU) 2016/97;

(n) za ***odredbe*** institucija za strukovno mirovinsko osiguranje, nadležno tijelo određeno u skladu s člankom 47. Direktive (EU) 2016/2341;

(o) za agencije za kreditni rejting, nadležno tijelo određeno u skladu s člankom 21. Uredbe (EZ) br. 1060/2009;

(p) za ovlaštene revizore i revizorska društva, nadležno tijelo određeno u skladu s člankom 3. stavkom 2. i člankom 32. Direktive 2006/43/EZ;

(q) za administratore ključnih referentnih vrijednosti, nadležno tijelo određeno u skladu s člancima 40. i 41. Uredbe ***(EU) 20161011***;

(r) za pružatelje usluga skupnog financiranja, nadležno tijelo određeno u skladu s člankom ***29.*** Direktive ***(EU) 2020/1503***;

(s) za sekuritizacijske repozitorije, nadležno tijelo određeno u skladu s člankom 10. i člankom 14. stavkom 1. Uredbe (EU) 2017/2402.

Članak 42.

Suradnja sa strukturama i tijelima osnovanima Direktivom (EU) 2016/1148

1. Da bi se potaknula suradnja i omogućile razmjene nadzornih informacija između nadležnih tijela određenih na temelju ove Uredbe i skupine za suradnju uspostavljene člankom 11. Direktive (EU) 2016/1148, europska nadzorna tijela i nadležna tijela ***pozivaju se*** da sudjeluju u ***radu*** skupine za suradnju ***u mjeri u kojoj se taj rad odnosi na aktivnosti nadzora i kontrole u odnosu na subjekte navedene u točki 7. Priloga II. Direktivi (EU) 2016/1148 koji su također imenovani kao treće strane pružatelji ključnih IKT usluga u skladu s člankom 28. ove Uredbe.***

2. Nadležna tijela mogu se prema potrebi savjetovati s jedinstvenom kontaktnom točkom iz članka 8. Direktive (EU) 2016/1148 i nacionalnim timovima za odgovor na računalne sigurnosne incidente iz članka 9. te direktive.

2a. Glavno nadzorno tijelo obavješćuje i surađuje s nadležnim tijelima imenovanima na temelju Direktive (EU) 2016/1148 prije provođenja općih istraga i izravnih nadzora u skladu s člancima 33. i 34. ove Uredbe.

Članak 43.

Financijske međusektorske vježbe, komunikacija i suradnja

1. Europska nadzorna tijela, u okviru Zajedničkog odbora i u suradnji s nadležnim tijelima, ESB-om, ***Jedinstvenim sanacijskim odborom za informacije koje se odnose na tijela iz područja primjene Uredbe (EU) br. 806/2014*** i ESRB-om, mogu uspostaviti mehanizme za razmjenu djelotvornih primjera iz prakse među svim financijskim sektorima kako bi se poboljšala informiranost o stanju i utvrdile zajedničke kiberranjivosti i kiberrizici na međusektorskoj razini.

   Mogu izraditi vježbe za upravljanje krizama i nepredvidive situacije, koje će uključivati scenarije kibernapada, kako bi razradila komunikacijske kanale i postupno omogućila djelotvoran koordiniran odgovor na razini EU-a u slučaju ozbiljnog prekograničnog IKT incidenta ili ***znatne kiberprijetnje*** koja ima sistemski učinak na cijeli financijski sektor Unije.

Te vježbe mogle bi biti primjerene i za testiranje ovisnosti financijskog sektora o drugim gospodarskim sektorima.

2. Nadležna tijela, EBA, ESMA ili EIOPA, ESB***, nacionalna sanacijska tijela i Jedinstveni sanacijski odbor u pogledu informacija koje se odnose na subjekte koji potpadaju pod područje primjene Uredbe (EU) br. 806/2014*** međusobno blisko surađuju i razmjenjuju informacije radi izvršavanja svojih zadaća iz članaka od 42. do 48. Blisko koordiniraju svoj nadzor kako bi utvrdili i uklonili povrede ove Uredbe, izradili i promicali najbolje primjere iz prakse, olakšali suradnju, poticali dosljednost tumačenja i u slučaju neslaganja omogućili uzajamnu pravnu procjenu.

Članak 44.

Administrativne kazne i korektivne mjere

1. Nadležna tijela imaju sve ovlasti nadzora, istrage i sankcioniranja potrebne za izvršavanje svojih zadaća iz ove Uredbe.

2. Ovlasti iz stavka 1. uključuju najmanje sljedeće:

   (a) pristup svim dokumentima ili podacima u bilo kojem obliku ***koji*** nadležno tijelo smatra relevantnim za izvršavanje svojih zadaća te dobivanje ili uzimanje njihovih preslika;

   (b) provedba izravnih nadzora ili istraga;

   (c) zahtjev za provedbu korektivnih mjera zbog kršenja zahtjeva iz ove Uredbe.

3. Ne dovodeći u pitanje pravo država članica na izricanje kaznenih sankcija u skladu s člankom 46., države članice donose propise kojima se utvrđuju odgovarajuće administrativne kazne i korektivne mjere za povrede ove Uredbe te osiguravaju njihovu djelotvornu provedbu.

Te kazne i mjere moraju biti djelotvorne, proporcionalne i odvraćajuće.

4. Države članice dodjeljuju nadležnim tijelima ovlast za primjenu sljedećih administrativnih kazni ili korektivnih mjera za povrede ove Uredbe:

   (a) nalog fizičkoj ili pravnoj osobi za prestanak takvog ponašanja i odustajanje od ponavljanja takvog ponašanja;

   (b) zahtjev za privremeni ili trajni prestanak postupanja ili ponašanja koje nadležno tijelo ***smatra*** suprotnim odredbama ove Uredbe te sprečavanje ponavljanja takvog postupanja ili ponašanja;

   (c) donošenje mjera, među ostalim novčane prirode, kojima se osigurava da financijski subjekti nastave ispunjavati pravne zahtjeve;

   (d) zahtjev, u mjeri u kojoj je to dopušteno nacionalnim pravom, za dostavu postojeće evidencije telekomunikacijskog operatera o podatkovnom prometu ako postoji opravdana sumnja u povredu ove Uredbe te ako takva evidencija može biti važna za istragu povreda ove Uredbe; i

   (e) javne objave, uključujući javne izjave u kojima se navodi identitet fizičke ili pravne osobe i priroda povrede.

5. Ako se odredbe iz stavka 2. točke (c) i stavka 4. primjenjuju na pravne osobe, države članice dodjeljuju nadležnim tijelima ovlast za primjenu administrativnih kazni i korektivnih mjera, ovisno o uvjetima utvrđenima nacionalnim pravom, na članove upravljačkog tijela i na druge osobe koje su na temelju nacionalnog prava odgovorne za povredu.

6. Države članice osiguravaju da su sve odluke kojima se izriču administrativne kazne ili korektivne mjere utvrđene u stavku 2. točki (c) propisno obrazložene i podliježu pravu žalbe.

Članak 45.

Izvršavanje ovlasti za izricanje administrativnih kazni i korektivnih mjera

1. Nadležna tijela izvršavaju ovlasti za izricanje administrativnih kazni i korektivnih mjera iz članka 44. u skladu sa svojim nacionalnim pravnim okvirima, prema potrebi:

   (a) izravno;

   (b) u suradnji s drugim tijelima;

   (c) delegiranjem drugim tijelima na vlastitu odgovornost;

   (d) podnošenjem zahtjeva nadležnim pravosudnim tijelima.

2. Pri utvrđivanju vrste i razine administrativnih kazni ili korektivnih mjera koje se izriču u skladu s člankom 44. nadležna tijela uzimaju u obzir do koje je mjere povreda posljedica namjere ili nemara i sve druge relevantne okolnosti, uključujući prema potrebi sljedeće:

   (a) značajnost, težinu i trajanje povrede;

   (b) stupanj odgovornosti fizičke ili pravne osobe koja je odgovorna za povredu;

   (c) financijsku snagu odgovorne fizičke ili pravne osobe;

   (d) važnost ostvarene dobiti ili izbjegnutih gubitaka odgovorne fizičke ili pravne osobe, ako je to moguće utvrditi;

   (e) gubitke koje su zbog povrede ostvarile treće osobe, ako ih je moguće utvrditi;

   (f) razinu suradnje odgovorne fizičke ili pravne osobe s nadležnim tijelom, ne dovodeći u pitanje potrebu da se osigura povrat ostvarene dobiti ili izbjegnutih gubitaka te osobe;

   (g) prethodne povrede odgovorne fizičke ili pravne osobe.

Članak 46.

Kaznene sankcije

1. Države članice mogu odlučiti da neće propisati pravila o administrativnim kaznama ili korektivnim mjerama za povrede ***koje*** u njihovu nacionalnom pravu podliježu kaznenim sankcijama.

2. Ako odluče propisati kaznene sankcije za povrede ove Uredbe, države članice dužne su osigurati primjerene mjere kako bi nadležna tijela imala sve potrebne ovlasti za suradnju

s pravosudnim tijelima, tijelima kaznenog progona ili kaznenopravnim tijelima u okviru njihove nadležnosti u pogledu dobivanja specifičnih informacija povezanih s kaznenim istragama ili postupcima pokrenutima zbog povreda ove Uredbe te za dostavu tih informacija drugim nadležnim tijelima te EBA-i, ESMA-i ili EIOPA-i kako bi ispunile svoje obveze suradnje za potrebe ove Uredbe.

Članak 47.

Dužnosti obavješćivanja

Države članice obavješćuju Komisiju, ESMA-u, EBA-u i EIOPA-u o zakonima i drugim propisima, uključujući odgovarajuće kaznenopravne odredbe, kojima se provode odredbe ovog poglavlja do [Ured za publikacije: uneseni datum treba biti ***12 mjeseci*** nakon datuma stupanja na snagu]. Države članice bez nepotrebne odgode obavješćuju Komisiju, ESMA-u, EBA-u i EIOPA-u o svim naknadnim izmjenama tih zakona i propisa.

Članak 48.

Objava administrativnih kazni

1. Nadležna tijela bez nepotrebne odgode na svojim službenim internetskim stranicama objavljuju svaku odluku o administrativnoj kazni protiv koje se ne može podnijeti žalba, nakon što se osoba kojoj je kazna izrečena obavijesti o toj odluci.

2. U objavu iz stavka 1. uključene su informacije o vrsti i prirodi povrede, ***izrečenim sankcijama te, iznimno,*** identitetu odgovornih osoba te izrečenim kaznama.

3. Ako na temelju ocjene od slučaja do slučaja smatra da bi objava identiteta, u slučaju pravnih osoba, ili identiteta i osobnih podataka, u slučaju fizičkih osoba, bila neproporcionalna ili da se njome ugrožava stabilnost financijskih tržišta ili provedba kaznene istrage u tijeku ili ako bi ona, u mjeri u kojoj je to moguće utvrditi, predmetnoj osobi prouzročila neproporcionalnu štetu, nadležno tijelo na odluku o izricanju administrativne kazne primjenjuje jedno od sljedećih rješenja:

   (a) odgađa objavu odluke do trenutka kada razlozi za neobjavljivanje prestanu postojati;

   (b) objavljuje odluku na anonimnoj osnovi, u skladu s nacionalnim pravom; ili

   (c) ne objavljuje odluku ako smatra da opcije iz točaka (a) i (b) nisu dostatne da se osigura neugrožavanje stabilnosti financijskih tržišta ili da takva objava nije proporcionalna u odnosu na blagu narav izrečene kazne.

4. U slučaju odluke o objavi administrativne kazne na anonimnoj osnovi u skladu sa stavkom 3. točkom (b) objava relevantnih podataka može se odgoditi.

5. Ako nadležno tijelo objavi odluku o izricanju administrativne sankcije protiv koje je podnesena žalba mjerodavnim pravosudnim tijelima, nadležna tijela bez odgode na svojim službenim internetskim stranicama dodaju tu informaciju, a kasnije i sve naknadne povezane informacije o ishodu te žalbe. Objavljuje se i svaka pravosudna odluka kojom se poništava odluka o izricanju administrativne kazne.

6. Nadležna tijela osiguravaju da svaka objava iz stavaka od 1. do 4. ostane na njihovim službenim internetskim stranicama najmanje pet godina nakon objave. Osobni podaci

sadržani u objavi pohranjuju se samo na službenim internetskim stranicama nadležnog tijela u razdoblju koje je potrebno u skladu s važećim propisima o zaštiti podataka.

Članak 49.

Čuvanje poslovne tajne

1. Svi povjerljivi podaci primljeni, razmijenjeni ili preneseni na temelju ove Uredbe podliježu obvezi čuvanja poslovne tajne utvrđene u stavku 2.
2. Obveza čuvanja poslovne tajne primjenjuje se na sve osobe koje rade ili su radile za nadležna tijela iz ove Uredbe ili za bilo koje tijelo ili poduzeće na tržištu ili fizičku ili pravnu osobu kojima su ta nadležna tijela delegirala svoje ovlasti, uključujući njihove ugovorne revizore i stručnjake.
3. Informacije obuhvaćene poslovnom tajnom ne smiju se odavati drugoj osobi ili tijelu, osim na temelju odredaba utvrđenih pravom Unije ili nacionalnim pravom.
4. Sve informacije razmijenjene među nadležnim tijelima iz ove Uredbe koje se odnose na poslovanje ili operativne uvjete i druga ekonomska ili osobna pitanja smatraju se povjerljivima i podliježu zahtjevima čuvanja poslovne tajne, osim ako nadležno tijelo u trenutku dostave izjavi da se predmetne informacije mogu objaviti ili da je njihova objava potrebna zbog sudskog postupka.

POGLAVLJE VIII.

DELEGIRANI AKTI

Članak 50.

Izvršavanje delegiranja ovlasti

1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku.

2. Ovlast za donošenje delegiranih akata iz članka 28. stavka 3. i članka 38. stavka 2. dodjeljuje se Komisiji na pet godina počevši od [Ured za publikacije: unijeti datum: pet godina od datuma stupanja na snagu ove Uredbe]. ***Komisija izrađuje izvješće o delegiranju ovlasti najkasnije devet mjeseci prije kraja razdoblja od pet godina. Delegiranje ovlasti prešutno se produljuje za razdoblja jednakog trajanja, osim ako se Europski parlament ili Vijeće tom produljenju usprotive najkasnije tri mjeseca prije kraja svakog razdoblja.***

3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 28. stavka 3. i članka 38. stavka 2. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u Službenom listu Europske unije ili na kasniji dan naveden u spomenutoj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.

4. Prije donošenja delegiranog akta Komisija se savjetuje sa stručnjacima koje je imenovala svaka država članica u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.

5. Čim donese delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.

6. Delegirani akt donesen na temelju članka 28. stavka 3. i članka 38. stavka 2. stupa na snagu samo ako ni Europski parlament ni Vijeće u roku od ***tri*** mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne podnesu nikakav prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće podnijeti prigovore. Taj se rok produljuje za ***tri*** mjeseca na inicijativu Europskog parlamenta ili Vijeća.

POGLAVLJE IX.

PRIJELAZNE I ZAVRŠNE ODREDBE

ODJELJAK I.

Članak 51.

Klauzula o preispitivanju

Do [Ured za publikacije: unijeti datum: pet godina od datuma stupanja na snagu ove Uredbe], a nakon savjetovanja s EBA-om, ESMA-om, EIOPA-om ili ESRB-om, ovisno o slučaju, Komisija provodi reviziju te Europskom parlamentu i Vijeću dostavlja izvješće, prema potrebi zajedno s prijedlogom zakonodavnog akta. ***U izvješću će se preispitati barem sljedeće:***

(a) ***mogućnost proširenja područja primjene ove Uredbe na upravitelje platnih sustava;***

(b) ***dobrovoljna priroda izvješćivanja o teškim kiberprijetnjama;***

(c) kriterije za određivanje trećih strana pružatelja ključnih IKT usluga iz članka 28. stavka 2.; ***i***

(d) ***učinkovitost donošenja odluka Zajedničkog nadzornog tijela i razmjene informacija između Zajedničkog nadzornog tijela i nacionalnih nadležnih tijela koja nisu članovi.***

ODJELJAK II.

IZMJENE

Članak 52.

Izmjene Uredbe (EZ) br. 1060/2009

U Prilogu I. Uredbi (EZ) br. 1060/2009, odjeljak A točka 4. prvi podstavak zamjenjuje se sljedećim:

„Agencija za kreditni rejting mora imati dobre administrativne i računovodstvene postupke, mehanizme unutarnje kontrole, učinkovite postupke za procjenu rizika i učinkovite mehanizme kontrole i osiguranja za upravljanje sustavima IKT-a u skladu s Uredbom (EU) 2021/xx Europskog parlamenta i Vijeća* [DORA].

* Uredba (EU) 2021/xx Europskog parlamenta i Vijeća […] (SL L XX, DD.MM.GGGG., str. X.).”

Članak 53.

Izmjene Uredbe (EU) br. 648/2012

Uredba (EU) br. 648/2012 mijenja se kako slijedi:

(1) Članak 26. mijenja se kako slijedi:

(a) stavak 3. zamjenjuje se sljedećim:

„ 3. Središnja druga ugovorna strana održava i upravlja organizacijskom strukturom koja osigurava kontinuitet i uredno funkcioniranje u obavljanju njezinih usluga i aktivnosti. Koristi se primjerenim i proporcionalnim sustavima, resursima i postupcima, uključujući sustave IKT-a kojima upravlja u skladu s Uredbom (EU) 2021/xx Europskog parlamenta i Vijeća* [DORA].

* Uredba (EU) 2021/xx Europskog parlamenta i Vijeća […] (SL L XX, DD.MM.GGGG., str. X.).”;

(b) briše se stavak 6.;

(2) Članak 34. mijenja se kako slijedi:

(a) stavak 1. zamjenjuje se sljedećim:

„1. Središnja druga ugovorna strana uspostavlja, provodi i održava primjerenu politiku kontinuiteta poslovanja i plan oporavka u slučaju katastrofe, koji uključuju planove kontinuiteta poslovanja i oporavka u slučaju katastrofe u području IKT-a uspostavljene u skladu s Uredbom (EU) 2021/xx [DORA], koji imaju za cilj osigurati očuvanje njezinih funkcija, pravovremen oporavak operacija i ispunjavanje obveza središnje druge ugovorne strane.”;

(b) u stavku 3. prvi podstavak zamjenjuje se sljedećim:

„Kako bi se osigurala dosljedna primjena ovog članka, ESMA, nakon savjetovanja s članovima ESSB-a, izrađuje nacrt regulatornih tehničkih standarda kojima se određuju minimalni sadržaj i zahtjevi za politiku kontinuiteta poslovanja i plan oporavka u slučaju katastrofe, isključujući plan kontinuiteta poslovanja i plan oporavka u slučaju katastrofe u području IKT-a.”;

(3) u članku 56. prvi podstavak stavka 3. zamjenjuje se sljedećim:

„3. Kako bi se osigurala dosljedna primjena ovog članka, ESMA izrađuje nacrt regulatornih tehničkih standarda kojima se određuju pojedinosti o zahtjevu za registraciju iz članka 1., osim za zahtjeve za upravljanje IKT rizicima.”;

(4) u članku 79. stavci 1. i 2. zamjenjuju se sljedećim:

„1. Trgovinski repozitorij utvrđuje izvore operativnog rizika i minimizira ih razvojem odgovarajućih sustava, kontrola i postupaka, među ostalim sustavâ IKT-a kojima upravlja u skladu s Uredbom (EU) 2021/xx [DORA].

2. Trgovinski repozitorij uspostavlja, provodi i održava primjerenu politiku kontinuiteta poslovanja i plan oporavka u slučaju katastrofe, uključujući planove kontinuiteta poslovanja i oporavka u slučaju katastrofe u području IKT-a uspostavljene u skladu s Uredbom (EU) 2021/xx [DORA], koji imaju za cilj osigurati održanje njegovih funkcija, pravovremeni oporavak operacija i ispunjavanje obveza trgovinskog repozitorija.”;

(5) u članku 80. briše se stavak 1.

Članak 54.

Izmjene Uredbe (EU) br. 909/2014

Članak 45. Uredbe (EU) br. 909/2014 mijenja se kako slijedi:

(1) stavak 1. zamjenjuje se sljedećim:

„1. CSD utvrđuje izvore operativnog rizika, kako unutarnje tako i vanjske, te minimizira njihov utjecaj primjenom odgovarajućih alata, procesa i politika IKT-a koji su uspostavljeni i kojima se upravlja u skladu s Uredbom (EU) 2021/xx Europskog parlamenta i Vijeća* [DORA], te s pomoću svih drugih relevantnih alata, kontrola i postupaka za druge vrste operativnog rizika, među ostalim za sve sustave za namiru vrijednosnih papira kojima upravlja.

* Uredba (EU) 2021/xx Europskog parlamenta i Vijeća […] (SL L XX, DD.MM.GGGG., str. X.).”;

(2) stavak 2. briše se;

(3) stavci 3. i 4. zamjenjuju se sljedećim:

„3. Za usluge koje pruža, kao i za sve sustave za namiru vrijednosnih papira kojima upravlja, CSD uspostavlja, provodi i održava odgovarajuću politiku kontinuiteta poslovanja te plan oporavak u slučaju katastrofe, uključujući planove kontinuiteta poslovanja i oporavka u slučaju katastrofe u području IKT-a uspostavljene u skladu s Uredbom (EU) 2021/xx [DORA], kako bi osigurao očuvanje svojih usluga, pravodoban oporavak operacija i ispunjavanje obveza CSD-a u slučaju događaja koji predstavljaju značajan rizik za prekid operacija.

4. Planom iz stavka 3. predviđa se oporavak svih transakcija i pozicija sudionika u trenutku prekida kako bi se sudionicima CSD-a omogućilo da nastave poslovati sa sigurnošću i dovrše namiru na predviđeni datum, među ostalim osiguravanjem da ključni IT sustavi mogu nastaviti operacije nakon prekida kako je predviđeno člankom 11. stavcima 5. i 7. Uredbe (EU) 2021/xx [DORA].”;

Članak 55.

Izmjene Uredbe (EU) br. 600/2014

Uredba (EU) br. 600/2014 mijenja se kako slijedi:

(1) članak 27.g mijenja se kako slijedi:

(a) stavak 4. briše se;

(b) u stavku 8. točka (c) zamjenjuje se sljedećim:

(c) „(c) konkretni organizacijski zahtjevi utvrđeni u stavcima 3. i 5.”;

(2) članak 27.h mijenja se kako slijedi:

(a) stavak 5. briše se;

(b) u stavku 8. točka (e) zamjenjuje se sljedećim:

„(e) konkretne organizacijske zahtjeve utvrđene u stavku 4.”;

(3) članak 27.i mijenja se kako slijedi:

(a) stavak 3. briše se;

(b) u stavku 5. točka (b) zamjenjuje se sljedećim:

„(b) konkretni organizacijski zahtjevi utvrđeni u stavcima 2. i 4.”

Članak 56.

Stupanje na snagu i primjena

Ova Uredba stupa na snagu dvadesetog dana od dana objave u Službenom listu Europske unije.

Primjenjuje se od [Ured za publikacije: unijeti datum: ***24*** mjeseca od datuma stupanja na snagu].

Međutim, članci 23. i 24. primjenjuju se od [Ured za publikacije: unijeti datum: 36 mjeseci od datuma stupanja na snagu ove Uredbe].

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu,

Za Europski parlament	*Za Vijeće*
Predsjednik	*Predsjednik*

POSTUPAK U NADLEŽNOM ODBORU

Naslov	Digitalna operativna otpornost financijskog sektora i izmjena uredaba (EU) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014
Referentni dokumenti	COM(2020)0595 – C9-0304/2020 – 2020/0266(COD)
Datum podnošenja EP-u	24.9.2020
Nadležni odbor Datum objave na plenarnoj sjednici	ECON 17.12.2020
Odbori koji daju mišljenje Datum objave na plenarnoj sjednici	ITRE IMCO 17.12.2020 17.12.2020
Odbori koji nisu dali mišljenje Datum odluke	ITRE IMCO 15.10.2020 27.10.2020
Izvjestitelji Datum imenovanja	Billy Kelleher 15.10.2020
Razmatranje u odboru	14.4.2021 14.6.2021
Datum usvajanja	1.12.2021
Rezultat konačnog glasovanja	+: 44 –: 5 0: 5
Zastupnici nazočni na konačnom glasovanju	Gerolf Annemans, Gunnar Beck, Marek Belka, Isabel Benjumea Benjumea, Stefan Berger, Gilles Boyer, Engin Eroglu, Markus Ferber, Jonás Fernández, Raffaele Fitto, Frances Fitzgerald, Luis Garicano, Sven Giegold, Valentino Grant, Claude Gruffat, José Gusmão, Enikő Győri, Eero Heinäluoma, Danuta Maria Hübner, Stasys Jakeliūnas, France Jamet, Billy Kelleher, Ondřej Kovařík, Georgios Kyrtsos, Aurore Lalucq, Philippe Lamberts, Aušra Maldeikienė, Pedro Marques, Costas Mavrides, Jörg Meuthen, Csaba Molnár, Siegfried Mureşan, Caroline Nagtegaal, Luděk Niedermayer, Lefteris Nikolaou-Alavanos, Lídia Pereira, Kira Marie Peter-Hansen, Sirpa Pietikäinen, Evelyn Regner, Antonio Maria Rinaldi, Alfred Sant, Martin Schirdewan, Joachim Schuster, Ralf Seekatz, Pedro Silva Pereira, Paul Tang, Irene Tinagli, Ernest Urtasun, Inese Vaidere, Johan Van Overtveldt, Stéphanie Yon-Courtin, Marco Zanni, Roberts Zīle
Zamjenici nazočni na konačnom glasovanju	Lefteris Christoforou
Datum podnošenja	7.12.2021

POIMENIČNO KONAČNO GLASOVANJE U NADLEŽNOM ODBORU

44	+
ECR	Raffaele Fitto, Johan Van Overtveldt, Roberts Zīle
NI	Enikő Győri
PPE	Isabel Benjumea Benjumea, Stefan Berger, Lefteris Christoforou, Markus Ferber, Frances Fitzgerald, Danuta Maria Hübner, Georgios Kyrtsos, Aušra Maldeikienė, Siegfried Mureşan, Luděk Niedermayer, Lídia Pereira, Sirpa Pietikäinen, Ralf Seekatz, Inese Vaidere
Renew	Gilles Boyer, Engin Eroglu, Luis Garicano, Billy Kelleher, Ondřej Kovařík, Caroline Nagtegaal, Stéphanie Yon-Courtin
S&D	Marek Belka, Jonás Fernández, Eero Heinäluoma, Aurore Lalucq, Pedro Marques, Costas Mavrides, Csaba Molnár, Evelyn Regner, Alfred Sant, Joachim Schuster, Pedro Silva Pereira, Paul Tang, Irene Tinagli
Verts/ALE	Sven Giegold, Claude Gruffat, Stasys Jakeliūnas, Philippe Lamberts, Kira Marie Peter-Hansen, Ernest Urtasun

5	-
ID	Gerolf Annemans, Gunnar Beck, France Jamet, Jörg Meuthen
NI	Lefteris Nikolaou-Alavanos

5	0
ID	Valentino Grant, Antonio Maria Rinaldi, Marco Zanni
The Left	José Gusmão, Martin Schirdewan

Korišteni znakovi:
+ : za
- : protiv
0 : suzdržani