H R V A T S K I   S A B O R
Odbor za europske poslove

Klasa: 022-03/21-03/11
Urbroj: 6521-31-20-01
Zagreb, 18. veljače 2021.

D.E.U. br. 20/023

**ODBOR ZA FINANCIJE I
DRŽAVNI PRORAČUN
Predsjednica Grozdana Perić**

Poštovana predsjednice Odbora,

Odbor za europske poslove na temelju članka 154. stavka 1. Poslovnika Hrvatskoga sabora prosljeđuje Odboru za financije i državni proračun stajalište o dokumentu Europske unije iz Radnog programa za razmatranje stajališta Republike Hrvatske za 2020. godinu:

**Stajalište Republike Hrvatske o
Paketu za digitalne financije (DORA) - 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) 595
i Prijedlogu direktive Europskog parlamenta i Vijeća o izmjeni direktiva 2006/43/EZ, 2009/65/EZ, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 i EU/2016/2341
COM (2020) 596**

koje je Koordinacija za unutarnju i vanjsku politiku Vlade Republike Hrvatske usvojila Zaključkom: Klasa: 022-03/20-07/381, Urbroj: 50301-21/32-20-3 na sjednici održanoj 14. prosinca 2020.

Predmetni paket Europska komisija je dostavila Hrvatskom saboru 17. prosinca 2020., te je u tijeku njegovo donošenje u Europskom parlamentu i Vijeću Europske unije.

U skladu s člankom 154. stavkom 2. Poslovnika Hrvatskoga sabora, molim Vas da Odboru za europske poslove dostavite mišljenje o Stajalištu Republike Hrvatske najkasnije do 12. ožujka 2021. godine.

S poštovanjem,

**PREDSJEDNIK ODBORA
Domagoj Hajduković**

U prilogu:
- Stajalište Republike Hrvatske o COM (2020) 595 i COM (2020) 596
- COM (2020) 595 i COM (2020) 596

Na znanje:
- INFODOK služba

PRIJEDLOG OKVIRNOG STAJALIŠTA RH

Naziv dokumenta (na hrvatskom i engleskom):

Prijedlog Uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni Uredbi (EK) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014

Proposal for a Regulation of the European parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, EU No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

Prijedlog Direktive Europskog parlamenta i Vijeća o izmjeni Direktiva 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, 2015/23696/EU i 2016/2341/EU

Proposal for a Directive of the European parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, 2015/23696/EU and 2016/2341/EU

Brojčana oznaka dokumenta: COM(2020) 595 final, COM (2020) 596 final

Nadležno TDU za izradu prijedloga i ustrojstvena jedinica:

Nadležno tijelo državne uprave: Ministarstvo financija
Ustrojstvena jedinica: Sektor za financijski sustav

Druga tijela državne uprave, agencije i javne ustanove uključene u izradu Prijedloga okvirnog stajališta: Hrvatska narodna banka, Hrvatska agencija za nadzor financijskih usluga

Nadležna služba u MVEP:
Sektor za COREPER II, Služba za ekonomske i financijske poslove

Nadležna radna skupina Vijeća EU:
Radna skupina za financijske usluge – Digitalna operativna otpornost (Digital Operational Resilience – DORA)

Osnovne sadržajne odredbe prijedloga EU:

Glavni cilj **Prijedloga Uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni Uredbi (EK) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014 (u daljnjem tekstu: Prijedlog DORA)** jest ojačati digitalnu operativnu otpornost subjekata financijskog sektora u Europskoj uniji i to putem usklađivanja i nadogradnje već postojećih pravila te uvođenjem novih zahtjeva tamo gdje postoje praznine.

Posljedično se time pridonosi: 1. smanjenju rizika od financijskih poremećaja i nestabilnosti, 2. smanjenju administrativnog tereta i povećanju nadzorne učinkovitosti te 3. povećanju zaštite potrošača i investitora.

Prijedlog DORA će zamijeniti i uskladiti postojeće smjernice u vezi s Informacijskom komunikacijskom tehnologijom (*Information and Communications Technology*; u daljnjem tekstu IKT) i upravljanjem sigurnosnim rizicima te će glavne pružatelje IKT usluga podvesti direktno u djelokrug nadzora europskih nadzornih tijela. Ključni elementi Prijedloga DORA su sljedeći:

1) Opseg i predmet primjene
Prijedlog DORA sastoji se od dva dijela: prvi koji se odnosi na financijske subjekte i drugi koji se odnosi na pružatelje tehnologijskih usluga tim financijskim subjektima.

Prijedlog DORA obuhvaća širok spektar financijskih subjekata (neke od njih su: kreditne institucije, institucije za elektronički novac, investicijska društva, pružatelje usluga kripto-imovine, središnje depozitorije vrijednosnih papira, središnje druge ugovorne strane, mjesta trgovanja, društva za upravljanje, pružatelje usluga o izvještavanju podataka, osiguravajuća društva i društva za reosiguranje, posrednici u osiguranju i reosiguranju, agencije za kreditni rejting, statutarne revizijske i revizorske kuće…).
Predloženim zakonodavstvom utvrđuju se zahtjevi koji se primjenjuju na financijske subjekte u pogledu upravljanja IKT rizikom, ugovorni aranžmani između pružatelja usluga IKT-a treće strane i financijskih subjekata, okvir nadzora za ključne pružatelje usluga treće strane i pravila o suradnji između nadležnih tijela.

2) Definicije
Prijedlog uključuje sveobuhvatan set definicija koje se odnose na subjekte i usluga iz djelokruga DORA-e, uključujući definicije digitalne operativne otpornosti, IKT rizika, IKT rizika treće strane, pružatelja IKT usluga treće strane (uključujući usluge računalstva u oblaku (*cloud computing*)) i IKT pružatelja treće strane sa sjedištem u trećoj zemlji.

3) Upravljanje IKT rizikom
Prijedlog DORA od financijskih subjekata zahtijeva stvaranje i održavanje zdravog, sveobuhvatnog i dobro dokumentiranog okvira upravljanja IKT rizikom. To mora uključivati namjensku i sveobuhvatnu politiku kontinuiteta poslovanja (*ICT Business Continuity Policy*), planove oporavka od katastrofe i komunikacijsku politiku koja omogućava „odgovorno otkrivanje incidenata povezanih s IKT-om ili glavnih ranjivosti“.
Uz ovaj okvir, financijski bi subjekti morali koristiti i održavati IKT sustave koji udovoljavaju određenim zahtjevima, kontinuirano identificirati sve izvore IKT rizika, dizajnirati i provoditi mjere sigurnosti i prevencije prijetnji te odmah otkrivati anomalne aktivnosti.

4) Incidenti povezani s IKT-om: upravljanje, klasifikacija i izvještavanje
Prijedlog DORA zahtijeva od financijskih subjekata da uspostave i implementiraju određeni postupak upravljanja incidentima povezanim s IKT-om radi identificiranja, praćenja, evidentiranja, kategorizacije i klasifikacije incidenata povezanih s IKT-om. Takav postupak morat će omogućiti klasifikaciju incidenata povezanih s IKT-om u skladu s nizom kriterija koji će dalje razvijati Zajednički odbor europskih nadzornih tijela. Financijski subjekti bit će dužni prijaviti svojim nadležnim nacionalnim nadzornim tijelima sve veće incidente povezane s IKT-om, u propisanim rokovima i koristeći usklađene predloške izvještaja.

5) Testiranje digitalne operativne otpornosti

Za potrebe svog okvira za upravljanje IKT rizicima, financijski subjekti morat će uspostaviti zdrav i sveobuhvatan program testiranja digitalne operativne otpornosti koji se sastoji od alata, sustava i metodologija za testiranje IKT-a kako je utvrđeno u prijedlogu DORA.

6) Ključni principi za zdravo upravljanje rizikom IKT-a treće strane
Prijedlog DORA utvrđuje ključna načela za upravljanje IKT rizikom treće strane, a pokriva odgovornost financijskog subjekta, proporcionalnost, strategiju o IKT riziku, dokumentaciju i vođenje evidencije, analizu predugovora, informacijsku sigurnost, revizije, raskid prava i izlazne strategije. Prava i obveze financijskog subjekta i pružatelja usluga IKT-a treće strane morat će biti jasno dodijeljeni i utvrđeni ugovornim sporazumom, čiji će detaljni opseg biti utvrđen u zakonodavnom. okviru.
Između ostalih obveza, financijski subjekti morat će izvršiti preliminarnu procjenu rizika koncentracije.

7) Okvir nadzora nad kritičnim pružateljima usluga IKT-a trećih strana
Prijedlog utvrđuje zaseban skup odredbi koji se primjenjuju na kritične pružatelje usluga IKT treće strane (*critical third-party service providers* - CTPPs), a koje će odrediti Zajednički odbor ESA-a, na temelju popisa kriterija utvrđenih u DORA-i. To je dijelom odgovor na strah od koncentracijskog rizika, tj. gdje se mnoge tvrtke za financijske usluge oslanjaju na nekolicinu pružatelja tehnologije.
Prijedlog DORA također zahtijeva uspostavljanje okvira za nadzor CTTPs-a odgovornih za, između ostalog, provjeru da li CTPPs imaju uspostavljena i poštuju „zdrava, sveobuhvatna i učinkovita pravila, postupke i aranžmane“ koji su primjereni za upravljanje rizicima koje CTPP mogu „predstavljati financijskim subjektima i za ukupnu financijsku stabilnost“.

DORA bi ESA-ma omogućila da određene pružatelje usluga - uključujući pružatelje usluga računalstva u oblaku (*cloud computing services*), softvera i analitike podataka - odrede kao „ključne“ za funkcioniranje financijskog sektora. Tada bi jedna od ESA bila imenovana vodećim nadzornim tijelom (*Lead Overseer*) za svakog kritičnog IKT pružatelja usluga treće strane. Ta bi ESA nadzirala ima li pružatelj IKT usluge, sveobuhvatna, zdrava i učinkovita pravila, postupke i mehanizme za upravljanje IKT rizicima koje može predstavljati financijskim subjektima. Vodeće nadzorno tijelo imalo bi neograničeno pravo pristupa svim informacijama koje su potrebne za izvršavanje njegovih dužnosti, uključujući sve relevantne poslovne i operativne dokumente, ugovore i politike. Vodeće nadzorno tijelo također bi dobio ovlasti za provođenje inspekcija na terenu (*on-site*) bilo kojih prostorija kritičnih pružatelja usluga IKT-a treće strane.
Očekuje se da će kritični davatelji usluga IKT-a treće strane surađivati "u dobroj vjeri" s vodećim nadzornim tijelom. Ako se ne pridržavaju, vodeće nadzorno tijelo može izreći dnevne novčane kazne u iznosu do šest mjeseci u iznosu od 1% prosječnog dnevnog prometa kritičnog pružatelja usluga IKT-a treće strane u prethodnoj poslovnoj godini.
ESA bi također naplaćivala naknade za nadzor kritičnim davateljima usluga IKT-a treće strane. Iznos naplaćene naknade pokrivat će sve administrativne troškove nadzora i biti "proporcionalan" prometu kritičnog dobavljača usluga IKT-a treće strane.

8) Aranžmani za razmjenu informacija
Prijedlog DORA omogućit će financijskim subjektima da međusobno razmjenjuju informacije i obavještajne podatke o kiber prijetnjama, uključujući pokazatelje kompromisa (*indicators of compromise*), taktike, tehnike, postupke, upozorenja o kiber sigurnosti i alate za konfiguriranje.

9) Nadležna tijela

Prijedlog DORA uključuje detaljna pravila koja se odnose na nadzorne ovlasti. EK je predložila da nadzor u odnosu na usklađenost s zahtjevima DORA-e postavi odgovarajućim nadležnim tijelima odgovornim za nadzor u okviru financijskih subjekata.

S obzirom da su zahtjevi u odnosu na IKT rizike obuhvaćeni različitima direktivama unutar financijskog sektora, i to: Direktivom 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, 2015/23696/EU i 2016/2341/EU, te su često nepotpuni i različiti, potrebno je uskladiti Prijedlog DORA-e s tim aktima, a što je upravo i cilj **Prijedloga Direktive Europskog parlamenta i Vijeća o izmjeni Direktiva 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, 2015/23696/EU i 2016/2341/EU** (u daljnjem tekstu: Direktiva). Nizom izmjena relevantnih propisa, Direktivom se postiže pravna jasnoća i konzistentnost u odnosu na primjenu financijskih subjekata koji imaju odobrenje i koji su nadzirani sukladno tim različitim pravilima u odnosu na zahtjeve za digitalnu operativnu otpornost. Posljedično se time doprinosi i neometanom funkcioniranju unutarnjeg tržišta.

Razlozi za donošenje i pozadina dokumenta:

Nepostojanje detaljnih i sveobuhvatnih pravila o digitalnoj operativnoj otpornosti na razini Europske unije dovelo je do sve većeg širenja nacionalnih regulatornih inicijativa i nadzornih pristupa. Međutim, djelovanje na nacionalnoj razini država članica ima samo ograničeni učinak s obzirom na prekograničnu prirodu IKT rizika. Štoviše, neusklađene nacionalne inicijative rezultirale su preklapanjima, nedosljednostima, dupliciranim zahtjevima, visokim administrativnim troškovima i troškovima usklađenosti - posebno za prekogranične financijske subjekte - ili rizikom da IKT ostanu neotkriveni i stoga neadresirani. Takva situacija rascjepkava jedinstveno tržište, potkopava stabilnost i integritet financijskog sektora Europske unije te ugrožava zaštitu potrošača i investitora.

Slijedom navedenog potrebno je uspostaviti detaljan i sveobuhvatan okvir za digitalnu operativnu otpornost za financijske subjekte Europske unije. Osobito će poboljšati i usmjeriti ponašanje financijskih subjekata u upravljanju IKT rizicima, uspostaviti temeljito testiranje IKT sustava, povećati svijest nadležnih tijela o kiber rizicima i incidentima povezanim s IKT s kojima se suočavaju financijski subjekti, kao i uvesti ovlasti za nadležnim tijelima u financijskom sustavu da nadziru rizike koji proizlaze iz ovisnosti financijskih subjekata o IKT pružateljima usluga treće strane. Prijedlog će kreirati dosljedan mehanizam izvještavanja o incidentima koji će pomoći smanjenju administrativnog opterećenja za financijske subjekte i ojačati nadzornu učinkovitost.

Prijedlog DORA dio Paketa digitalnih financija kojeg je Europska komisija predstavila 24. rujna 2020. godine. Paket digitalnih financija obuhvaća mjere (strategiju za digitalne financije i strategiju za plaćanja malih vrijednosti te zakonodavne prijedloge o kripto imovini i o digitalnoj otpornosti) kojima je cilj potaknuti europsku konkurentnost i inovacije u financijskom sektoru i omogućiti Europi da određuje standarde na globalnoj razini. Potrošačima će se dati više izbora i mogućnosti u području financijskih usluga i modernih plaćanja, a istodobno će se osigurati zaštita potrošača i financijska stabilnost.

Status dokumenta:
U raspravi u Vijeću.

<u>Stajalište RH – ključni elementi:</u>

HR načelno podržava Prijedlog DORA, a kojim se uspostavlja regulatorni okvir za digitalnu otpornost, odnosno kojim se želi osigurati da svi sudionici financijskog sustava, u skladu s načelom proporcionalnosti, imaju potrebne zaštitne mjere za ublažavanje kiber napada i drugih rizika.

Sporna/otvorena pitanja za RH:

HR ima općeniti komentar u odnosu na samu dinamiku rasprave u predmetu DORA. S obzirom da je riječ o kompleksnom tekstu, smatra da je potrebno osigurati dovoljno vremena za raspravu. Tim više što je potrebna i dodatna rasprava s relevantnim dionicima. Posljedično bi neke posljedice primjene DORA-e mogle ostati neadekvatno adresirane. Nadalje, kvaliteta odredaba kao i njihova primjena bi mogla ostati umanjena zbog predviđenog kratkog razdoblja primjene (12 mjeseci) te brojnih mandata prema ESA-ma (10 regulatorno tehničkih standarda) što će staviti dodatan pritisak na ESA-e kao i nacionalna nadležna/nadzorna tijela. Stoga HR predlaže temeljitiji pristup i rasprave po člancima, kao i produženje razdoblja primjene DORA-e.

Nadalje, HR problem vidi i u provedbi načela proporcionalnosti u DORA-i. Stoga predlaže postavljanje praga kako bi se uključila mikro i mala poduzeća (posebice u odnosu na okvir upravljanja rizikom IKT). Brojni zahtjevi u DORA-i su prezahtjevni za mala i ne kritična poduzeća, što nije u skladu s rizikom kojem su izložena. Princip proporcionalnosti potrebno je razmotriti i kod manjih subjekata ne-bankarskog sektora, a u odnosu na ciljeve koji se žele postići DORA prijedlogom te rizike kojima su takvi manji subjekti izloženi. Potrebno je razmotriti i izuzeća od odredbi/obveza za sistemski manje bitne subjekte (primjerice subjekti koji nisu kreditne institucije, društva za osiguranje ili reosiguranje, središnje druge ugovorne strane, središnji depozitoriji vrijednosnih papira, mjesta trgovanja, agencije za izdavanje kreditnih rejtinga, trgovinski repozitoriji ili administratori ključnih referentnih vrijednosti). U tom smislu se HR zalaže za pristup u kojem bi se za svaki članak i obvezu procijenilo je li takva odredba neproporcionalno opterećujuća za manje i sistemski nevažne subjekte. U sadašnjem zakonodavnom prijedlogu se izuzeća za mikro poduzeća također provode nedosljedno kroz tekst prijedloga. Nadalje potrebno je razmotriti opterećujuće zahtjeve za mala poduzeća u pogledu zahtjeva za redovitom IKT revizijom te korištenje najmodernijih IKT tehnologija što je uz načelo proporcionalnosti također i teško provedivo u praksi. Nadalje potrebno je razmotriti primjenu obveze testiranja digitalne operativne otpornosti od strane vanjskih testera i uvjete koje isti moraju zadovoljiti. Trenutno se ovakva obveza primjenjuje na za sve vrste financijskih subjekata, što predstavlja iznimno opterećujući zahtjev.

Također, HR smatra kako postoje i otvorena pitanja vezana uz interakciju DORA-e sa srodnim direktivama i sektorskim pravilima, što može rezultirati nejednakim uvjetima i dupliciranjem aktivnosti. Specifično, nije jasan odnos DORA-e s:
- detaljnijim zahtjevima koji proizlaze iz nacionalne transpozicije tzv. NIS direktive[1], odnosno odredbi Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga te pripadajuće Uredbe Vlade RH o kibernetičkoj sigurnosti koje se primjenjuju na sektor bankarstva,

[1] 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)

- preklapajućim zahtjevima o izvješćivanju o (ne)IKT incidentima iz PSD2[2] direktive.
- preklapajućim zahtjevima koji proizlaze iz sektorskih pravila za eksternalizaciju (primjerice, EBA Smjernica za eksternalizaciju).

HR nadalje smatra da Prijedlog DORA nije dovoljno jasan u dijelu koji se odnosi na određivanje vodećeg nadzornog tijela *(„lead overseer“)* za svakog individualnog ključnog pružatelja IKT usluga (CTPPs), te da u svakom slučaju kriterij veličine bilance klijenata takvog pružatelja usluge nije dovoljno precizan, odnosno relevantan, da bi se temeljem istoga odredilo tko će biti vodeće nadzorno tijelo (EBA, ESMA ili EIOPA). Dodatna implikacija ovog kriterija može biti i naknadna rotacija ESAs u toj ulozi, ako se struktura klijenata individualnog ključnog pružatelja IKT usluga značajno izmijeni. Dok tekst Prijedloga DORA-e eksplicitno ne predviđa ovakvu rotaciju (nakon inicijalnog određivanja), ovakva mogućnost je implicirana u samom kriteriju/načinu podjele te i u stavcima 6. i 7. članka 28. Prijedloga DORA. Ovisno o tome kakva je namjera, HR smatra da bi u svakom slučaju u tekstu trebalo jasno isključiti mogućnost rotacije/izmjene ESAs u ulozi vodećeg nadzornog tijela, a radi troškovne i operativne neefikasnosti takvog prijedloga. S obzirom da je izvor ovakve nejasnoće i predloženi kriterij veličine bilance klijenata individualnog ključnog pružatelja IKT usluga, HR također smatra da je ovaj kriterij nužno revidirati.

Dodatni aspekt koji bi se trebao razmotriti u daljnjim raspravama je i pitanje paralelne angažiranosti resursa EBA-e, ESMA-e ili EIOPA-e u ovom području. Trenutni tekst podrazumijeva da bi se kompetencije za ovakav tip nadzora, koje su zahtjevne i specijalizirane, potencijalno paralelno gradile u sve tri ESA-e, što će imati značajnu troškovnu komponentu, a koju će financirati DČ kroz obvezne doprinose njihovih nacionalnih nadležnih tijela proračunu ESAs. U ovom trenutku nije moguće procijeniti koliki bi to troškovi bili, ili koliko je izgledno da bi sve tri ESA-e obavljale ulogu vodećeg nadzornog tijela za nekog od ključnog pružatelja IKT usluga.
Što se tiče IKT ključnih pružatelja usluge, HR smatra da je nužno u tekstu Prijedloga DORA predvidjeti i sljedeće:
- u kriterije sistemske/ključne važnosti (prema kojima se određuje lista ključnih pružatelja IKT usluga) predvidjeti i kriterij pruža li se usluga financijskim infrastrukturama ili mjestima trgovanja,
- predvidjeti mogućnost da u *Oversight* forumu sudjeluje više od jednog predstavnika po DČ (a radi podjele nadležnosti u HR).

HR također smatra da je nužno produljenje razdoblja za primjenu na najmanje 24 mjeseca nakon stupanja na snagu uredbe, a radi kompleksnosti implementacije.

Stajališta DČ, EK i Predsjedništva EU: Kada je riječ o stajalištima DČ, ključno stajalište značajne većine DČ (IE, CZ, LT, PL, LU, RO, BG, DK, MT, HU, LV i SE, te u određenoj mjeri i IT i ES) je vezano za proceduru tj. dinamiku pregovora. Iako niti jedna DČ ne dovodi u pitanje važnost/relevantnost Prijedloga DORA, istovremeno su vrlo kritične u pogledu namjera DE PRES za brzim postizanjem dogovora u Vijeću (do kraja 2020.). DE PRES, kao ni EK nisu dali dovoljno argumenata koji bi opravdali implicitnu ubrzanu proceduru. Odnosno, općeniti argument da je pandemija COVID 19 ukazala na potrebu daljnjeg osiguranja digitalne otpornosti financijskog sustava nije dovoljan da se ishitreno postigne dogovor. Posebice ako se uzme u obzir da je riječ o najznačajnijem i najopsežnijem reguliranju ovog područja u kontekstu financijskih usluga.

[2] Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ (Tekst značajan za EGP) SL L 337, 23.12.2015

Sporna/otvorena pitanja za DČ, EK i Predsjedništvo EU:

Područje primjene

Jedno od ključnih pitanja jest uključivanje platnih sustava (prijedlog DK su podržale SI, ES, IE, EE i FR). EK nije uključila platne sustave jer u euro području platne sustave nadzire Europska središnja banka tj. spremna je razmotriti eventualno uključivanje platnih sustava u nečlanicama europodručja. Nadalje, postoji i protivljenje u pogledu uključivanja ovlaštenih revizora u područje primjene Prijedloga DORA-e. CZ, RO, PL, FI, SE i IE se protive prijedlogu EK. EK ističe da ovlašteni revizori imaju pristup ključnim informacijama financijskih subjekata te su zbog toga uključeni u područje primjene. Prijedlog EK u pogledu područja primjene su izričito podržale NL, IT i BE.

Pored područja primjene, većina DČ smatra da je jedno od otvorenih pitanja i interakcija DORA-e i nacionalnih zakona kojima se prenosi NIS Direktiva (neusklađenost područja primjene), posebice u pogledu prijedloga EK da se primjenjuje pristup *lex specialis* (LS) u provođenju DORA-e u odnosu na postojeću legislativu. EK je istaknula da je u procesu izrade DORA-e naišla na problem u pogledu samo djelomične uključenosti financijskog sektora u područje primjene NIS Direktive te dodatnog smanjenja područja primjene kroz proces identifikacije operatora ključnih usluga. EK je također istaknula problem funkcioniranja LS pristupa uslijed izazova naslijeđenih iz NIS Direktive.. Istovremeno je bilo teško predložiti sveobuhvatne/značajne promjene područja primjene NIS Direktive (EK je razmatrala i tu mogućnost) uzevši u obzir predstojeće redovno preispitivanje NIS Direktive. Stoga je i predložila „oprezan“ pristup u DORA-i.

Također, značajan broj DČ je zatražio dodatna pojašnjenja u pogledu interakcije DORA-e i postojećih zahtjeva u pogledu eksternalizacije/izdvajanja. EK smatra da je teško razlikovati sve oblike eksternalizacije te da bi bilo vrlo složeno detaljno razlikovati eksternalizaciju IKT usluga od eksternalizacije usluga koje nisu vezane za IKT. Također, EK smatra da su postojeće sektorske odredbe o eksternalizaciji u većoj mjeri načelne i nisu kontradiktorne DORA-i. Odredbe u postojećoj regulativi bi ostale na snazi.

Kao jedno od otvorenih pitanja, značajan broj DČ ističe i problem preklapajućih zahtjeva u pogledu izvješćivanja o (ne)IKT incidentima iz PSD2 direktive.

Stav RH o spornim/otvorenim pitanjima DČ, EK i Predsjedništva EU:

Područje primjene

HR smatra područje primjene preširokim s obzirom da obuhvaća mnoštvo različitih pružatelja financijskih usluga, što vodi nesrazmjernosti Prijedloga DORA za veliki broj subjekata. S druge strane, u opseg bi mogli biti uključeni i drugi subjekti koji nisu uzeti u obzir u prijedlogu. HR je stava da bi se statutarni revizori i revizorska društva trebali ukloniti iz područja primjene, s obzirom kako nisu tretirani kao financijske institucije (s regulatorne i nadzorne perspektive). Revizorska društva imaju pristup samo podacima ili dijelovima informacijskih sustava financijskih institucija koji su obuhvaćeni ugovorima.

Uzimajući u obzir sistemski kiber rizik i postizanje jednakih uvjeta, HR podržava raspravu o uključivanju platnih sustava/operatera platnih sustava u područje primjene.
Što se tiče pitanja primjene DORA-e na **posrednike i sporedne posrednike u osiguranju, kao i na institucije za strukovno mirovinsko osiguranje i pružatelje usluga skupnog**

financiranja, HR je stava da bi Prijedlog DORA trebao predvidjeti više proporcionalnosti te da nije opravdano/realno očekivati da će takvi (mali) subjekti moći ispuniti iste zahtjeve kao i banke, veliki upravitelji imovinom i osiguranja. U tom smislu, HR preliminarno podržava DČ koje se protive trenutnom opsegu primjene, no to ne znači da se neki opći principi (prilagođeno i proporcionalno) ne bi mogli primjenjivati i na ove kategorije subjekata, ali ne ovako kako je trenutno predviđeno. Djelomična izuzeća za mala poduzeća ne rješavaju ovaj problem.

Postojeće zakonodavstvo RH i potreba njegove izmjene slijedom usvajanja dokumenta:
Bit će potrebno donijeti zakonodavni okvir kojim će se omogućiti pretpostavke za izravnu primjenu Prijedloga DORA te posljedično izmijeniti nacionalno zakonodavstvo.

Utjecaj provedbe dokumenta na proračun RH:
Ne očekuje se da će Prijedlog DORA utjecati na proračun Republike Hrvatske.

EUROPSKA
KOMISIJA

Bruxelles, 24.9.2020.
COM(2020) 595 final

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)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

OBRAZLOŽENJE

1. KONTEKST PRIJEDLOGA

- Razlozi i ciljevi prijedloga

Ovaj je prijedlog dio paketa za digitalne financije, paketa mjera kojima se dodatno, uz istodobno ublažavanje rizika, omogućuje i podupire potencijal digitalnih financija u kontekstu inovacija i tržišnog natjecanja. Usklađen je s prioritetima Komisije koji se odnose na pripremanje Europe za digitalno doba i izgradnju gospodarstva u interesu građana spremnog za budućnost. Paket za digitalne financije sadržava novu Strategiju za digitalne financije u financijskom sektoru[1] EU-a s ciljem da EU prihvati digitalnu revoluciju te da ju pod vodstvom inovativnih europskih poduzeća potakne i tako svim europskim potrošačima i poduzećima omogući prednosti digitalnih financija Osim ovog prijedloga, paket sadržava i prijedlog uredbe o tržištima kriptoimovine[2], prijedlog uredbe o pilot-režimu za tržišne infrastrukture koje se temelje na tehnologiji decentraliziranog vođenja evidencije transakcija (DLT)[3] i prijedlog direktive kojom bi se pojasnila ili izmijenila određena povezana pravila EU-a o financijskim uslugama[4]. Digitalizacija i operativna otpornost u financijskom sektoru dvije su strane iste medalje. Digitalne ili informacijske i komunikacijske tehnologije (IKT) istodobno donose prilike i rizike. Treba ih dobro razumjeti i njima treba dobro upravljati, osobito u razdobljima stresa.

Tvorci politike i nadzorna tijela stoga se sve više bave rizicima koji proizlaze iz oslanjanja na IKT. Osobito pokušavaju poboljšati otpornost poduzećâ uvođenjem standarda i koordinacijom regulatornog ili nadzornog djelovanja, na međunarodnoj i europskoj razini, u raznim sektorima i nekoliko specifičnih sektora, uključujući financijske usluge.

Unatoč tome IKT rizici i dalje su problem za operativnu otpornost, učinkovitost i stabilnost financijskog sustava EU-a. Reformom koja je uslijedila nakon financijske krize 2008. prvenstveno je povećana financijska otpornost[5] financijskog sektora Unije, a IKT rizike nastojalo se neizravno ukloniti u određenim područjima u okviru mjera za općenitije ublažavanje operativnih rizika.

Iako su izmjenama zakonodavnih akata EU-a o financijskim uslugama koje su uslijedile nakon krize uvedena jedinstvena pravila kojima je uređen velik dio financijskih rizika povezanih s financijskim uslugama, pitanje digitalne operativne otpornosti nije u cijelosti obrađeno. Mjere poduzete u vezi s potonjim imale su niz značajki koje su ograničavale njihovu djelotvornost. Na primjer, često su to bile direktive o minimalnom usklađivanju ili uredbe koje su se temeljile na načelima, što je ostavljalo prilično prostora za različite pristupe na jedinstvenom tržištu. Usto su u kontekstu pokrića operativnog rizika IKT rizici tek vrlo

---

1 Komunikacija Komisije Europskom parlamentu, Europskom vijeću, Vijeću, Europskoj središnjoj banci, Europskom gospodarskom i socijalnom odboru i Odboru regija o Strategiji za digitalne financije za EU, 23. rujna 2020., COM(2020) 591.

2 Prijedlog uredbe Europskog parlamenta i Vijeća o tržištima kriptoimovine i izmjeni Direktive (EU) 2019/1937, COM(2020) 593.

3 Prijedlog uredbe Europskog parlamenta i Vijeća o pilot-režimu za tržišne infrastrukture koje se temelje na tehnologiji decentraliziranog vođenja evidencije transakcija, COM(2020) 594.

4 Prijedlog direktive Europskog parlamenta i Vijeća o izmjeni direktiva 2006/43/EZ, 2009/65/EZ, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 i EU/2016/2341, COM(2020) 596.

5 Cilj raznih donesenih mjera bilo je povećanje izvora sredstava i likvidnosti financijskih subjekata te smanjenje tržišnih i kreditnih rizika.

ograničeno i nepotpuno obrađeni. Naposljetku, te se mjere razlikuju ovisno o sektorskim zakonodavnim aktima o financijskim uslugama. Stoga intervencije na razini Unije nisu u potpunosti usklađene s potrebama europskih financijskih subjekata u smislu upravljanja operativnim rizicima tako da budu otporni na IKT incidente, mogu na njih odgovoriti i oporaviti se od njihovih posljedica. Financijska nadzorna tijela nisu dobila najprimjerenije alate za ispunjenje svojih obveza sprečavanja financijske nestabilnosti koja proizlazi iz ostvarenja tih IKT rizika.

Zbog nepostojanja detaljnih i sveobuhvatnih pravila o digitalnoj operativnoj otpornosti na razini EU-a rastao je broj nacionalnih regulatornih inicijativa (npr. testiranje digitalne operativne otpornosti) i nadzornih pristupa (npr. rješavanje problema ovisnosti o IKT uslugama trećih strana). Međutim, djelovanje na razini država članica ima samo ograničeni učinak zbog prekogranične prirode IKT rizika. Osim toga, nekoordinirane nacionalne inicijative uzrokovale su preklapanja, nedosljednosti, dvostruke zahtjeve, visoke administrativne troškove i troškove usklađivanja, osobito za financijske subjekte koji posluju prekogranično, ili neotkrivanje, a time i neuklanjanje, IKT rizika. Zato je jedinstveno tržište rascjepkano, narušava se stabilnost i integritet financijskog sektora EU-a i ugrožava zaštita potrošača i ulagatelja.

Stoga treba uspostaviti detaljan i sveobuhvatan okvir za digitalnu operativnu otpornost za financijske subjekte u EU-u, kojim će se produbiti dimenzija jedinstvenih pravila koja se odnosi na upravljanje digitalnim rizicima. Njime će se osobito poboljšati i pojednostavniti način na koji financijski subjekti upravljaju IKT rizicima, uvesti temeljito testiranje IKT sustava, povećati upućenost nadzornih tijela u kiberrizike i IKT incidente kojima su izloženi financijski subjekti te uvesti ovlasti za financijska nadzorna tijela za nadzor rizika koji proizlaze iz ovisnosti financijskih subjekata o trećim stranama pružateljima IKT usluga. Predlaže se dosljedan mehanizam izvješćivanja o incidentima koji će pridonijeti smanjenju administrativnog opterećenja financijskih subjekata i povećanju djelotvornosti nadzora.

- Dosljednost s postojećim odredbama politike u tom području

Ovaj je prijedlog dio šireg međunarodnog i europskog angažmana na jačanju kibersigurnosti u financijskim uslugama i uklanjanju širih operativnih rizika[6].

Usto je i odgovor na Zajednički tehnički savjet iz 2019.[7] europskih nadzornih tijela koja su pozvala na koherentniji pristup uklanjanju IKT rizika u financijskom sektoru i preporučila Komisiji da digitalnu operativnu otpornost djelatnosti financijskih usluga razmjerno poveća u okviru inicijative EU-a za pojedini sektor. Savjet europskih nadzornih tijela bio je odgovor na Komisijin Akcijski plan za financijske tehnologije iz 2018.[8]

- Dosljednost u odnosu na druge politike Unije

---

[6] Bazelski odbor za nadzor banaka, *Cyber-resilience: Range of practices* (Kiberotpornost: razne prakse), prosinac 2018., i *Principles for sound management of operational risk (PSMOR)* (Načela za dobro upravljanje operativnim rizikom (PSMOR)), listopad 2014.

[7] *Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector* (Zajednički savjet europskih nadzornih tijela Europskoj komisiji o potrebi za zakonodavnim poboljšanjima u pogledu zahtjeva za upravljanje IKT rizicima u financijskom sektoru EU-a), JC 2019 26 (2019.).

[8] Europska komisija, *Akcijski plan za financijske tehnologije*, COM/2018/0109 final.

Kako je navedeno u političkim smjernicama predsjednice von der Leyen[9] i utvrđeno u Komunikaciji „Izgradnja digitalne budućnosti Europe”[10], od ključne je važnosti za Europu iskoristiti sve prednosti digitalnog doba i ojačati industrijski i inovacijski kapacitet unutar sigurnog i etičkog okvira. U Europskoj strategiji za podatke[11] utvrđeno je da ključne preduvjete za društvo osnaženo korištenjem podataka čine četiri stupa – zaštita podataka, temeljna prava, sigurnost i kibersigurnost. U posljednje vrijeme Europski parlament radi na izvješću o digitalnim financijama, u kojem među ostalim poziva na zajednički pristup kiberotpornosti financijskog sektora[12]. Zakonodavni okvir koji jača digitalnu operativnu otpornost financijskih subjekata u EU-u u skladu je s tim ciljevima politike. Prijedlog podržava i politike oporavka od koronavirusa jer bi se njime osigurala povezanost sve većeg oslanjanja na digitalne financije i operativne otpornosti.

Inicijativa omogućuje da se očuvaju pogodnosti povezane s horizontalnim okvirom za kibersigurnost (npr. Direktiva o sigurnosti mrežnih i informacijskih sustava, Direktiva NIS) jer bi financijski sektor ostao u njezinu području primjene. Financijski sektor i dalje bi bio usko povezan s tijelom za suradnju za mrežne i informacijske sustave, a financijska nadzorna tijela mogla bi razmjenjivati važne informacije unutar postojećeg ekosustava Direktive NIS. Inicijativa je u skladu s Direktivom o europskoj kritičnoj infrastrukturi (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. Naposljetku, ovaj je prijedlog u cijelosti u skladu sa strategijom za sigurnosnu uniju[13] u kojoj se poziva na inicijativu za digitalnu operativnu otpornost financijskog sektora s obzirom na veliku ovisnost tog sektora o IKT uslugama i njegovu veliku osjetljivost na kibernapade.

2. PRAVNA OSNOVA, SUPSIDIJARNOST I PROPORCIONALNOST

- Pravna osnova

Prijedlog uredbe temelji se na članku 114. UFEU-a.

Njime se uklanjanju prepreke uspostavljanju i funkcioniranju unutarnjeg tržišta za financijske usluge i poboljšava se njegovo uspostavljanje i funkcioniranje jer se usklađuju pravila primjenjiva u području upravljanja IKT rizicima, izvješćivanja, testiranja i IKT rizika treće strane. Postojeće neusklađenosti u tom području na zakonodavnoj i nadzornoj razini te nacionalnoj razini i razini EU-a prepreke su jedinstvenom tržištu za financijske usluge jer se financijski subjekti koji posluju prekogranično suočavaju s drugačijim, ako se ne preklapaju, regulatornim zahtjevima ili nadzornim očekivanjima koji bi im mogli onemogućiti ostvarivanje slobode poslovnog nastana ili pružanja usluga. Različita pravila usto narušavaju tržišno natjecanje među istom vrstom financijskih subjekata iz različitih država članica. Nadalje, u područjima u kojima pravila nisu usklađena, usklađena su samo djelomično ili u

9 Predsjednica Ursula von der Leyen, Političke smjernice za sljedeću Europsku komisiju, 2019.–2024.; https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_hr.pdf

10 Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, *Izgradnja digitalne budućnosti Europe*, COM(2020) 67 final.

11 Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, *Europska strategija za podatke*, COM(2020) 66 final.

12 „Izvješće s preporukama Komisiji o digitalizaciji financijskih usluga: novi rizici u pogledu kriptoimovine – izazovi povezani s regulativom i nadzorom u području financijskih usluga, institucija i tržišta (2020/2034(INL))”, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en

13 Komunikacija Komisije Europskom parlamentu, Europskom vijeću, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija o strategiji EU-a za sigurnosnu uniju, COM(2020) 605 final.

ograničenoj mjeri, različita nacionalnih pravila ili pristupi, koji su već na snazi ili u postupku donošenja i provedbe na nacionalnoj razini, mogu spriječiti ostvarivanje sloboda jedinstvenog tržišta za financijske usluge. To se osobito odnosi na okvire za testiranje digitalne operativne otpornosti i nadzor trećih strana pružatelja ključnih IKT usluga.

Budući da prijedlog utječe na nekoliko direktiva Europskog parlamenta i Vijeća donesenih na temelju članka 53. stavka 1. UFEU-a, istodobno se donosi i Prijedlog direktive radi potrebnih izmjena tih direktiva.

- Supsidijarnost

Zbog visokog stupnja uzajamne povezanosti financijskih usluga, znatne prekogranične aktivnosti financijskih subjekata i izražene ovisnosti financijskog sektora o trećim stranama pružateljima IKT usluga, snažna digitalna operativna otpornost pitanje je od zajedničkog interesa za održanje stabilnosti financijskih tržišta EU-a. Neusklađenosti koje proizlaze iz neujednačenih ili djelomičnih režima, preklapanja ili primjene višestrukih zahtjeva na iste financijske subjekte s prekograničnim poslovanjem ili nekoliko odobrenja za rad[14] na cijelom jedinstvenom tržištu mogu se učinkovito ukloniti samo na razini Unije.

Ovim se prijedlogom usklađuje digitalna operativna komponenta duboko integriranog i međusobno povezanog sektora koji već ostvaruje pogodnosti od jedinstvenih pravila i nadzora u većini drugih ključnih područja. Za pitanja kao što je izvješćivanje o IKT incidentima samo bi usklađena pravila na razini Unije mogla smanjiti administrativno opterećenje i financijske troškove izvješćivanja različitih Unijinih i nacionalnih tijela o istom IKT incidentu. Djelovanje na razini Unije potrebno je i kako bi se olakšalo uzajamno priznavanje rezultata naprednog testiranja digitalne operativne otpornosti subjekata koji posluju prekogranično, koji u nedostatku pravila na razini Unije jesu ili mogu biti obuhvaćeni različitim okvirima u različitim državama članicama. Samo djelovanjem na razini Unije mogu se ukloniti razlike u pristupima testiranju koje su uvele države članice. Djelovanje na razini Unije potrebno je i kako bi se riješio problem nepostojanja odgovarajućih nadzornih ovlasti za praćenje rizika povezanih s trećim stranama pružateljima IKT usluga, uključujući rizike koncentracije i zaraze za financijski sektor Unije.

- Proporcionalnost

Predložena pravila ne nadilaze ono što je potrebno za ostvarenje ciljeva prijedloga. Obuhvaćaju samo one aspekte koje države članice ne mogu same ostvariti i slučajeve u kojima su administrativno opterećenje i troškovi razmjerni posebnim i općim ciljevima koji se nastoje ostvariti.

Proporcionalnost u području primjene i intenzitetu ostvarena je kvalitativnim i kvantitativnim kriterijima procjene. Njihov je cilj osigurati da su nova pravila, iako obuhvaćaju sve financijske subjekte, istodobno prilagođena rizicima i potrebama koji proizlaze iz njihovih konkretnih značajki u smislu njihove veličine i poslovnih profila. Proporcionalnost je ugrađena i u pravila o upravljanju IKT rizicima, testiranju digitalne otpornosti, izvješćivanju o značajnim IKT incidentima i nadzoru trećih strana pružatelja ključnih IKT usluga.

- Odabir instrumenta

[14] Isti financijski subjekt može posjedovati odobrenja za rad kao banka, investicijsko društvo i institucija za platni promet, pri čemu svako od tih odobrenja izdaje drugo nadzorno tijelo u jednoj ili više država članica.

Mjere potrebne za uređenje upravljanja IKT rizicima, izvješćivanja o IKT incidentima, testiranja i nadzora trećih strana pružatelja ključnih IKT usluga moraju biti utvrđene uredbom kako bi se osigurala djelotvorna i izravna ujednačena primjena detaljnih zahtjeva, a da se pritom ne dovedu u pitanje proporcionalnost i konkretna pravila predviđena ovom Uredbom. Dosljednost u uklanjanju digitalnih operativnih rizika pridonosi jačanju povjerenja u financijski sustav i štiti njegovu stabilnost. Budući da uredba pridonosi smanjenju regulatorne složenosti, promiče konvergenciju nadzora i povećava pravnu sigurnost, ova Uredba pridonosi i ograničavanju troškova usklađivanja financijskih subjekata, osobito onih koji posluju prekogranično, što bi moglo pridonijeti i suzbijanju narušavanja tržišnog natjecanja.

Ovom se Uredbom usto uklanjaju zakonodavne neusklađenosti i neujednačeni nacionalni regulatorni i nadzorni pristupi IKT rizicima, a time i prepreke jedinstvenom tržištu za financijske usluge, osobito neometanom ostvarivanju slobode poslovnog nastana i pružanja usluga za financijske subjekte koji posluju prekogranično.

Konačno, jedinstvena pravila uglavnom su razrađena u uredbama pa bi isti pravni instrument trebalo iskoristiti da ih se ažurira dodavanjem komponente digitalne operativne otpornosti.

3. REZULTATI *EX POST* EVALUACIJA, SAVJETOVANJA S DIONICIMA I PROCJENA UČINKA

- *Ex post* evaluacije/provjere primjerenosti postojećeg zakonodavstva

Nijedan zakonodavni akt Unije o financijskim uslugama do sad se nije odnosio na operativnu otpornost i nijednim nije sveobuhvatno riješen problem rizika koji proizlaze iz digitalizacije, čak ni onima koji sadržavaju pravila u kojima se općenito obrađuje dimenzija operativnog rizika s IKT rizikom kao potkomponentom. Intervencija Unije do sad je pomogla da se odgovori na potrebe i probleme nakon financijske krize 2008.: kreditne institucije nisu bile dovoljno kapitalizirane, financijska tržišna nisu bila dovoljno integrirana, a usklađenost je dotad bila minimalna. IKT rizik tada se nije smatrao prioritetom, što je dovelo do nekoordiniranog razvoja pravnih okvira za različite financijske podsektore. Unatoč tome, djelovanjem na razini Unije ostvareni su postavljeni ciljevi osiguranja financijske stabilnosti i utvrđivanja jedinstvenih usklađenih bonitetnih pravila i pravila ponašanja na tržištu koja su primjenjiva na financijske subjekte u cijeloj Uniji. U prošlosti se zbog čimbenika koji potiču zakonodavne intervencije na razini Unije posebnim ili sveobuhvatnim pravilima nije moglo riješiti pitanje primjene digitalnih tehnologija i posljedičnih rizika u području financija, eksplicitna evaluacija čini se teškom. Implicitna evaluacija i posljedične zakonodavne izmjene sastavni su dio svakog stupa ove Uredbe.

- Savjetovanja s dionicima

Komisija se savjetovala s dionicima tijekom cijelog postupka pripreme ovog prijedloga, posebno:

i. Komisija je provela posebno otvoreno javno savjetovanje (19. prosinca 2019. – 19. ožujka 2020.)[15];

ii. Komisija se savjetovala s javnošću u okviru početne procjene učinka (19. prosinca 2019. – 16. siječnja 2020.)[16];

15 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

iii. službe Komisije dvaput su se savjetovale sa stručnjacima iz država članica u Stručnoj skupini za bankarstvo, plaćanja i osiguranja (EGBPI) (18. svibnja 2020. i 16. srpnja 2020.)[17];

iv. službe Komisije održale su tematski *webinar* o digitalnoj operativnoj otpornosti u okviru niza događanja za informiranje o digitalnim financijama u 2020. (19. svibnja 2020.).

Javno savjetovanje poslužilo je Komisiji za informiranje o izradi mogućih međusektorskih okvira EU-a za digitalnu operativnu otpornost u području financijskih usluga. Odgovori su potvrdili široku potporu uvođenju namjenskog okvira s mjerama za četiri područja koja su bila tema savjetovanja, no istaknuto je da treba zajamčiti proporcionalnost te pažljivo obraditi i objasniti interakciju s horizontalnim pravilima iz Direktive NIS. Komisija je zaprimila dva odgovora o početnoj procjeni učinka u kojima su se ispitanici osvrnuli na posebne aspekte povezane s njihovim područjem poslovanja.

Na sastanku EGBPI-ja održanog 18. svibnja 2020. države članice iskazale su veliku potporu jačanju digitalne operativne otpornosti financijskog sektora u okviru mjera predviđenih za četiri elementa koje je iznijela Komisija. Države članice istaknule su da nova pravila treba jasno povezati s pravilima o operativnom riziku (u okviru Unijinih propisa o financijskim uslugama) i horizontalnim pravilima o kibersigurnosti (Direktiva NIS). Na drugom su sastanku neke države članice istaknule da treba zajamčiti proporcionalnost i razmotriti specifičnu situaciju malih društava ili društava kćeri većih grupa te da nadležna nacionalna tijela uključena u nadzor trebaju imati vrlo jasan mandat.

Prijedlog se temelji i na povratnim informacijama sa sastanaka održanih s dionicima te tijelima i institucijama Unije koje su njegov sastavni dio. Dionici, uključujući treće strane pružatelje IKT usluga, uglavnom su podržali prijedlog. Analiza primljenih povratnih informacija pokazuje da se traži da se pri izradi pravila očuva proporcionalnost i primijeni pristup koji se temelji na načelima i procjeni rizika. Što se tiče institucija, najviše informacija dostavili su Europski odbor za sistemske rizike (ESRB), europska nadzorna tijela, Agencija Europske unije za kibersigurnost (ENISA) i Europska središnja banka (ESB) te nadležna tijela država članica.

- Prikupljanje i primjena stručnog znanja

Komisija je u pripremi prijedloga koristila kvalitativne i kvantitativne podatke iz pouzdanih izvora, uključujući dva zajednička tehnička savjeta europskih nadzornih tijela, koji su dopunjeni povjerljivim podacima i javno dostupnim izvješćima nadzornih tijela, međunarodnih tijela za normizaciju i vodećih istraživačkih instituta, kao i kvantitativnim i kvalitativnim doprinosima poznatih dionika u globalnom financijskom sektoru.

- Procjena učinka

Ovom prijedlogu priložena je procjena učinka[18], koja je 29. travnja 2020. dostavljena Odboru za nadzor regulative i odobrena 29. svibnja 2020. Odbor za nadzor regulative preporučio je

---

16 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

17 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

poboljšanja u određenim područjima: i. više informacija o tome kako će se osigurati proporcionalnost; ii. jasnije istaknuti koliko se opcija kojoj se daje prednost razlikuje od zajedničkog tehničkog savjeta europskih nadzornih tijela i zašto je ta opcija optimalna; te iii. dodatno istaknuti interakciju prijedloga i postojećih Unijinih propisa, uključujući pravila čije je preispitivanje u tijeku. Prilagodbom procjene učinka odgovoreno je na ta pitanja i na detaljnije primjedbe Odbora za nadzor regulative.

Komisija je razmotrila niz opcija politike za izradu okvira za digitalnu operativnu otpornost:

- „Nema djelovanja”: pravila o operativnoj otpornosti i dalje bi se utvrđivala postojećim, različitim odredbama Unije o financijskim uslugama, djelomično u okviru Direktive NIS, te u okviru postojećih ili budućih nacionalnih režima.
- Opcija 1: jačanje zaštitnih slojeva kapitala: uveli bi se dodatni zaštitni slojevi kapitala kako bi se povećao kapacitet financijskih subjekata za pokriće gubitaka koji bi mogli nastati zbog digitalne operativne neotpornosti.
- Opcija 2: uvođenje akta o digitalnoj operativnoj otpornosti financijskih usluga: omogućavanje sveobuhvatnog okvira na razini Unije s dosljednim pravilima kojima se nastoji odgovoriti na potrebe svih reguliranih financijskih subjekata povezane s digitalnom operativnom otpornosti i uspostavljanje nadzornog okvira za treće strane pružatelje ključnih IKT usluga.
- Opcija 3.: akt o digitalnoj operativnoj otpornosti financijskih usluga u kombinaciji s centraliziranim nadzorom trećih strana pružatelja ključnih IKT usluga: uz akt o digitalnoj operativnoj otpornosti (2. opcija) osnovalo bi se novo tijelo za nadzor pružanja usluga trećih strana pružatelja IKT usluga.

Odabrana je 2. opcija jer se većina predviđenih ciljeva njome ostvaruje djelotvorno, učinkovito i dosljedno s ostalim politikama Unije. I većina dionika dala je prednost toj opciji.

Odabrana opcija podrazumijeva jednokratne i periodične troškove[19]. Jednokratni troškovi uglavnom se odnose na ulaganja u IT sustave i kao takve ih je teško kvantificirati jer se složena informatička okruženja, osobito naslijeđeni IT sustavi, razlikuju ovisno o poduzeću. No i u tom slučaju velika poduzeća vjerojatno će imati ograničene troškove s obzirom na dosadašnja znatna ulaganja u IKT. Očekuje se da će i manja poduzeća, zbog primjene proporcionalnih mjera, imati ograničene troškove s obzirom na to da su izložena manjem riziku.

Odabrana opcija pozitivno će utjecati na MSP-ove koji posluju u sektoru financijskih usluga u ekonomskom, socijalnom i ekološkom smislu. MSP-ovima će iz prijedloga biti jasno koja se pravila primjenjuju, čime će se smanjiti troškovi usklađivanja.

Glavne društvene učinke odabrane opcije osjetit će potrošači i ulagatelji. Zahvaljujući većoj digitalnoj operativnoj otpornosti financijskog sustava Unije smanjit će se broj incidenata i njihovi prosječni troškovi. Društvo u cjelini imat će koristi od većeg povjerenja u djelatnost financijskih usluga.

---

[18] Radni dokument službi – Izvješće o procjeni učinka priloženo dokumentu Uredba 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, SWD(2020) 198 od 24.9.2020.

[19] *Ibid., str. 89.–94.*

Konačno, kad je riječ o utjecajima na okoliš, odabranom opcijom politike potaknut će se šira primjena najnovije generacije infrastruktura i usluga IKT-a, za koje se očekuje da će postati okolišno održivije.

- Primjerenost i pojednostavnjenje propisa

Ukidanjem preklapajućih zahtjeva izvješćivanja o IKT incidentima smanjit će se administrativno opterećenje i povezani troškovi. Troškovi će se smanjiti i usklađenim testiranjem digitalne operativne otpornosti uz uzajamno priznavanje rezultata na cijelom jedinstvenom tržištu, osobito za poduzeća koja posluju prekogranično koja bi inače bila izložena višestrukim testovima u različitim državama članicama[20].

- Temeljna prava

Unija je odlučna osigurati visoke standarde zaštite temeljnih prava. Svi mehanizmi dobrovoljne razmjene informacija među financijskim subjektima, koje se promiče u ovoj Uredbi, provodili bi se u pouzdanim okruženjima uz puno poštovanje pravila Unije o zaštiti osobnih podataka odnosno Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća[21], osobito kada je obrada osobnih podataka nužna za potrebe legitimnih interesa voditelja obrade.

4. UTJECAJ NA PRORAČUN

Budući da se ovom Uredbom predviđa veća uloga europskih nadzornih tijela na temelju dodijeljenih im ovlasti za odgovarajući nadzor trećih strana pružatelja ključnih IKT usluga, u proračunskom će se smislu za prijedlog trebati izdvojiti veća sredstva, osobito kako bi se ispunile zadaće nadzora (kao što su izravni i internetski nadzor i revizija) i pokrili troškovi osoblja koji posjeduju konkretno stručno znanje o sigurnosti IKT-a.

Opseg i raspodjela tih troškova ovisit će o opsegu novih ovlasti nadzora i (konkretnim) zadaćama europskih nadzornih tijela. Kad je riječ o novim članovima osoblja, EBA, ESMA i EIOPA trebat će ukupno 18 zaposlenika na puno radno vrijeme – po šest za svako tijelo – kada se počnu primjenjivati razne odredbe prijedloga (procijenjeno na 15,71 milijun EUR za razdoblje 2022.–2027.). Europska nadzorna tijela snosit će i dodatne troškove za informatičke tehnologije, troškove službenih putovanja za provođenje izravnog nadzora i troškove pismenog prevođenja (procijenjeno na 12 milijuna EUR za razdoblje 2022.–2027.) i ostale administrativne rashode (procijenjeno na 2,48 milijuna EUR za razdoblje 2022.–2027.). Stoga se procjenjuje da će ukupni trošak za razdoblje 2022.–2027. iznositi 30,19 milijuna EUR.

Treba napomenuti i da će se rashodi za nove zaposlenike (tj. novi članovi osoblja i ostali rashodi povezani s novim zadaćama), čiji će broj tijekom vremena ovisiti o kretanju broja i veličini trećih strana pružatelja ključnih IKT usluga koje će trebati nadzirati, u potpunosti financirati naknadama od sudionika na tržištu. Stoga se ne predviđa učinak na odobrena sredstva EU-a (osim za dodatno osoblje) jer će se ti troškovi u potpunosti financirati naknadama.

Financijski i proračunski učinci ovog prijedloga detaljno su objašnjeni u zakonodavnom financijskom izvještaju koji je priložen ovom Prijedlogu.

[20] *Ibid*.
[21] 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.).

5. DRUGI ELEMENTI

- Planovi provedbe i mehanizmi praćenja, evaluacije i izvješćivanja

Prijedlog uključuje opći plan nadzora i procjene učinka na posebne ciljeve, a Komisija će ga najmanje svake tri godine nakon stupanja na snagu preispitati te o svojim glavnim nalazima izvijestiti Europski parlament i Vijeće.

Preispitivanje se provodi u skladu sa smjernicama Komisije za bolju regulativu.

- Detaljno obrazloženje posebnih odredaba prijedloga

Prijedlog je strukturiran u nekoliko glavnih područja politike koji su ujedno najvažniji međusobno povezani stupovi koji su sporazumno uključeni u europske i međunarodne smjernice i primjere najbolje prakse čiji je cilj poboljšanje kiberotpornosti i operativne otpornosti financijskog sektora.

Područje primjene Uredbe i primjena proporcionalnosti potrebnih mjera (članak 2.)

Kako bi se osigurala dosljednost zahtjeva za upravljanje IKT rizicima koji su primjenjivi na financijski sektor, Uredba se odnosi na razne financijske subjekte regulirane na razini Unije, a to su kreditne institucije, institucije za platni promet, institucije za elektronički novac, investicijska društva, pružatelji usluga povezanih s kriptoimovinom, središnji depozitoriji vrijednosnih papira, središnje druge ugovorne strane, mjesta trgovanja, trgovinski repozitoriji, upravitelji alternativnih investicijskih fondova i društva za upravljanje, pružatelji usluga dostave podataka, društva za osiguranje i društva za reosiguranje, posrednici u osiguranju, posrednici u reosiguranju i sporedni posrednici u osiguranju, institucije za strukovno mirovinsko osiguranje, agencije za kreditni rejting, ovlašteni revizori i revizorska društva, administratori ključnih referentnih vrijednosti i pružatelji usluga skupnog financiranja.

Takav obuhvat olakšava ujednačenu i dosljednu primjenu svih komponenti upravljanja rizicima u IKT područjima i istodobno osigurava ravnopravne uvjete za sve financijske subjekte u pogledu njihovih regulatornih obveza povezanih s IKT rizicima. U Uredbi se ujedno uvažava i činjenica da se financijski subjekti znatno razlikuju po veličini, poslovnom profilu i izloženosti digitalnim rizicima. Budući da veći financijski subjekti imaju više resursa, svi financijski subjekti osim mikropoduzeća dužni su, primjerice, uspostaviti složene sustave upravljanja i posebne upravljačke funkcije, provesti detaljnu procjenu nakon velikih promjena u infrastrukturi mrežnih i informacijskih sustava, redovito analizirati rizike u naslijeđenim sustavima IKT-a, proširiti testiranje kontinuiteta poslovanja te planove odgovora i oporavka tako da uključuju i scenarije prebacivanja s primarne infrastrukture IKT-a na redundantnu infrastrukturu i obrnuto. Nadalje, samo će financijski subjekti koji se smatraju značajnima za potrebe naprednog testiranja digitalne otpornosti morati obavljati penetracijska testiranja vođena prijetnjama.

Iako je obuhvat širok, nije i sveobuhvatan. Konkretno, ovom Uredbom nisu obuhvaćeni upravitelji sustava, kako su definirani u članku 2. točki (p) Direktive 98/26/EZ[22] o konačnosti namire u platnim sustavima i sustavima za namiru vrijednosnih papira (Direktiva SF), ni sudionici sustava osim ako je sudionik financijski subjekt reguliran na razini EU-a i kao takav bi bio obuhvaćen ovom Uredbom (tj. kreditna institucija, investicijsko društvo, središnja

[22] Direktiva 98/26/EZ Europskog parlamenta i Vijeća od 19. svibnja 1998. o konačnosti namire u platnim sustavima i sustavima za namiru vrijednosnih papira (SL L 166, 11.6.1998., str. 45.).

druga ugovorna strana). Područjem primjene nije obuhvaćen ni Registar Unije za emisijske jedinice kojim, u skladu s Direktivom 2003/87/EZ[23], upravlja Europska komisija.

Ti subjekti iz Direktive SF nisu uključeni zbog pravnih pitanja i pitanja politike koja se odnose na upravitelje sustava i sudionike iz Direktive SF koja treba dodatno preispitati vodeći računa o učinku okvira koji se sada primjenjuju na platne sustave[24] kojima upravljaju središnje banke. Budući da bi ta pitanja mogla uključivati aspekte koji se razlikuju od pitanja obuhvaćenih ovom Uredbom, Komisija će nastaviti s procjenom nužnosti i utjecaja daljnjeg proširenja područja primjene ove Uredbe na subjekte i infrastrukture IKT-a koje zasad nisu njime obuhvaćene.

Zahtjevi za upravljanje (članak 4.)

Cilj je ove Uredbe bolje usklađenje poslovnih strategija financijskih subjekata i njihova upravljanja IKT rizicima. U tu će svrhu upravljačko tijelo imati ključnu, aktivnu ulogu u usmjeravanju razvoja okvira upravljanja IKT rizicima uz održavanje stroge kiberhigijene. Potpuna odgovornost upravljačkog tijela za upravljanje IKT rizicima financijskog subjekta bit će glavno načelo koje će se pretočiti u skup konkretnih zahtjeva, kao što su dodjela jasnih uloga i odgovornosti svim funkcijama u području IKT-a, kontinuirano sudjelovanje u kontroli praćenja upravljanja IKT rizicima te cijeli niz procesa odobrenja i kontrole te primjerena raspodjela ulaganja u IKT i osposobljavanja o IKT-u.

Zahtjevi za upravljanje IKT rizicima (članci od 5. do 14.)

Digitalna operativna otpornost temelji se na ključnim načelima i zahtjevima koji se primjenjuju na okvir upravljanja IKT rizicima u skladu sa zajedničkim tehničkim savjetom europskih nadzornih tijela. Ti zahtjevi, nadahnuti mjerodavnim međunarodnim, nacionalnim i sektorskim standardima, smjernicama i preporukama, odnose se na konkretne funkcije u upravljanju IKT rizicima (utvrđivanje, zaštita i sprečavanje, otkrivanje, odgovor i oporavak, učenje i razvoj te komunikacija). Kako bi održali korak sa sve bržim razvojem kiberprijetnji, financijski subjekti dužni su uspostaviti i održavati otporne sustave i alate IKT-a koji smanjuju učinak IKT rizika, redovito utvrđivati sve izvore IKT rizika, uvesti mjere zaštite i sprečavanja, brzo otkriti neobične aktivnosti, uvesti namjenske i sveobuhvatne politike kontinuiteta poslovanja te izraditi planove oporavka od katastrofe kao sastavne dijelove politike za kontinuitet operativnog poslovanja. Potonje komponente nužne su za brzi oporavak nakon IKT incidenata, osobito kibernapada, jer se ograničava šteta i daje prednost sigurnom nastavku poslovanja. Uredbom se ne uvode konkretni standardi, nego se nadograđuju europski i međunarodno priznati standardi ili najbolji primjeri sektorske prakse u mjeri u kojoj su potpuno u skladu s uputama nadzornog tijela o primjeni i provedbi tih međunarodnih standarda. Kao dio digitalnog otiska poslovanja financijskih subjekata, Uredbom su obuhvaćene i cjelovitost, sigurnost i otpornost fizičke infrastrukture i objekata koji podržavaju korištenje tehnologije, relevantne procese i osoblje u području IKT-a.

Izvješćivanje o IKT incidentima (članci od 15. do 20.)

Izvješćivanje o IKT incidentima uskladit će se i pojednostavniti, ponajprije općim zahtjevom za uspostavu i provedbu upravljačkog procesa za praćenje i evidentiranje IKT incidenata u

[23] Direktiva 2003/87/EZ Europskog parlamenta i Vijeća od 13. listopada 2003. o uspostavi sustava trgovanja emisijskim jedinicama stakleničkih plinova unutar Zajednice i o izmjeni Direktive Vijeća 96/61/EZ (SL L 275, 25.10.2003., str. 32.).

[24] Posebno Uredba Europske središnje banke (EU) br. 795/2014 od 3. srpnja 2014. o nadzornim zahtjevima za sistemski važne platne sustave.

financijskim subjektima te uvođenjem obveze klasifikacije tih incidenata na temelju kriterija koji su detaljno opisani u Uredbi i koje su razradila europska nadzorna tijela kako bi se utvrdili pragovi značajnosti. Drugo, nadležnim tijelima moraju se prijaviti samo značajni IKT incidenti. Za izvješćivanje bi trebalo koristiti jedinstveni obrazac i usklađeni postupak koji izrade europska nadzorna tijela. Financijski subjekti trebali bi dostaviti početno, prijelazno i završno izvješće te svoje korisnike i klijente obavijestiti kada incident utječe ili bi mogao utjecati na njihove financijske interese. Nadležna tijela trebala bi relevantne pojedinosti o incidentima dostaviti drugim institucijama ili tijelima: europskim nadzornim tijelima, ESB-u i jedinstvenim kontaktnim točkama određenima na temelju Direktive (EU) 2016/1148.

Kako bi se pokrenuo dijalog između financijskih subjekata i nadležnih tijela koji bi pridonio smanjenju učinka i utvrđivanju primjerenih korektivnih mjera, izvješćivanje o značajnim IKT incidentima trebalo bi dopuniti povratnim informacijama i smjernicama o nadzoru.

Naposljetku, mogućnost centralizacije izvješćivanja o IKT incidentima na razini Unije trebalo bi dodatno ispitati u zajedničkom izvješću europskih nadzornih tijela, ESB-a i ENISA-e u kojem će se ocijeniti izvedivost uspostave jedinstvenog EU-ova čvorišta za izvješćivanje o značajnim IKT incidentima za financijske subjekte.

Testiranje digitalne operativne otpornosti (članci od 21. do 24.)

Kapacitete i funkcije obuhvaćene okvirom upravljanja IKT rizicima treba redovito testirati u pogledu pripravnosti i utvrđivanja slabosti, nedostataka ili propusta te brze provedbe korektivnih mjera. Ovom Uredbom omogućuje se proporcionalna primjena zahtjevâ za testiranje digitalne operativne otpornosti ovisno o veličini, poslovnom profilu i profilu rizičnosti financijskih subjekata: iako bi svi subjekti trebali testirati alate i sustave IKT-a, samo bi subjektima za koje nadležno tijelo utvrdi (na temelju kriterija iz ove Uredbe i onih koje dodatno razrade europska nadzorna tijela) da su značajni i dokazane kibersigurnosti trebalo propisati obvezu naprednog testiranja provedbom penetracijskih testiranja vođenih prijetnjama (TLPT). U ovoj su Uredbi utvrđeni i zahtjevi za provoditelje testiranja te priznavanje rezultata TLPT-a u cijeloj Uniji u slučaju financijskih subjekata koji posluju u nekoliko država članica.

IKT rizik treće strane (članci od 25. do 39.)

Uredba je formulirana tako da osigurava pouzdano praćenje IKT rizika treće strane. Taj će se cilj postići prvo poštovanjem pravila koja se temelje na načelima, a primjenjuju se na praćenje rizika trećih strana pružatelja IKT usluga koje provode financijski subjekti. Drugo, ovom se Uredbom usklađuju ključni elementi usluge i odnosa s trećim stranama pružateljima IKT usluga. Ti elementi obuhvaćaju minimalne aspekte koji se smatraju ključnima da bi se financijskim subjektima omogućilo potpuno praćenje IKT rizika treće strane u svim fazama njihova odnosa, od sklapanja ugovora, njegova izvršenja i raskida do razdoblja nakon njegova raskida.

Točnije, u ugovorima kojima se uređuje taj odnos morat će se navesti cjelovit opis usluga, točne lokacije obrade podataka, cjeloviti opisi razina usluga popraćeni kvantitativnim i kvalitativnim ciljevima uspješnosti, odgovarajuće odredbe o pristupačnosti, dostupnosti, cjelovitosti, sigurnosti i zaštiti osobnih podataka te jamstva pristupa, oporavka i vraćanja u slučaju propasti treće strane pružatelja IKT usluga, rokovi za prethodnu obavijest i izvještajne obveze treće strane pružatelja IKT usluga, prava financijskih subjekata ili imenovane treće strane na pristup, nadzor i reviziju, jasne odredbe o pravima raskida i s time povezanim izlaznim strategijama. Nadalje, s obzirom na to da se neki od tih ugovornih elemenata mogu standardizirati, Uredbom se promiče dobrovoljna primjena standardnih ugovornih klauzula koje će Komisija izraditi za usluge računalstva u oblaku.

Naposljetku, Uredbom se nastoji promicati konvergencija pristupa za nadzor IKT rizika trećih strana u financijskom sektoru tako da se treće strane pružatelje ključnih IKT usluga uključi u nadzorni okvir Unije. U novom usklađenom zakonodavnom okviru europskom nadzornom tijelu koje je određeno kao glavno nadzorno tijelo za svaku takvu treću stranu pružatelja ključnih IKT usluga dodjeljuju se ovlasti za osiguranje primjerenog paneuropskog praćenja pružatelja tehnoloških usluga koji su važni za funkcioniranje financijskog sektora. Nadzorni okvir predviđen ovom Uredbom nadograđuje postojeću institucijsku arhitekturu u području financijskih usluga, u okviru koje Zajednički odbor europskih nadzornih tijela osigurava međusektorsku koordinaciju svih pitanja povezanih s IKT rizicima u skladu sa svojim zadaćama u području kibersigurnosti, a u tome mu podršku pruža relevantni pododbor (Nadzorni forum) koji je odgovoran za sve pripreme za donošenje pojedinačnih odluka i zajedničkih preporuka za treće strane pružatelje ključnih IKT usluga.

Razmjena informacija (članak 40.)

U svrhu informiranja o IKT rizicima, smanjenja njihova širenja, potpore obrambenim kapacitetima financijskih subjekata i njihovih tehnika otkrivanja prijetnji, Uredbom se financijskim subjektima dopušta da uspostave mehanizme međusobne razmjene informacija i saznanja o kiberprijetnjama.

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[25],

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora[26],

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 i dalje nije 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, preuzimanje rizika u osiguranju, upravljanje potraživanjima i poslove pozadinskih ureda. Ne samo da su financije postale uglavnom digitalne u cijelom sektoru, nego je digitalizacija produbila 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.[27] Europski odbor za sistemske rizike (ESRB) potvrdio je da bi postojeći visoki stupanj međusobne povezanosti financijskih

---

[25] [*dodati upućivanje*] SL C , , str. .

[26] [*dodati upućivanje*] SL C , , str. .

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[28] 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.

(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.[29] istaknuto je da je jačanje otpornosti financijskog sektora Unije od ključne važnosti i u operativnom 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

---

27 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

28 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.

29 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.

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 komponenta, i to proširenjem ovlasti financijskih nadzornih tijela koja su zadužena za praćenje i zaštitu financijske stabilnosti i integriteta tržišta.

(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.

(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.

(13) Pri ublažavanju IKT rizika 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 prekomjerne upotrebe sustava, platformi i infrastruktura IKT-a koja 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.

(15) Uz zakonodavne akte o financijskim uslugama, u Direktivi (EU) 2016/1148 Europskog parlamenta i Vijeća[30] 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 *lex specialis* za Direktivu (EU) 2016/1148.

30 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.).

Iznimno je važno očuvati čvrstu vezu između financijskog sektora i horizontalnog okvira Unije za kibersigurnost jer bi se tako 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 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. 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.

(18) Važno je osigurati i usklađenost 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, s mogućim posljedicama za financijski sektor[31].

(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. 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. Razinu digitalne operativne otpornosti financijskog sustava trebalo bi povećati te istodobno omogućiti proporcionalnu primjenu zahtjeva na financijske subjekte koji su mikropoduzeća kako su definirana u Preporuci Komisije 2003/361/EZ[32].

(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)[33] i Skupine za suradnju u

---

[31] 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.).

[32] Preporuka Komisije od 6. svibnja 2003. o definiciji mikro, malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

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

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 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.

(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 režim izvješćivanja o IKT incidentima upotpunio zahtjevima koji nedostaju u zakonodavnim aktima o tom financijskom podsektoru 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 samo njihovim nadležnim tijelima. 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 nekoordiniranih nacionalnih okvira u kojima se istim pitanjima pristupa na drugačiji način. To udvostručuje troškove financijskih subjekata koji posluju prekogranično i otežava 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[34], 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 su ključni pružatelji usluga financijskim subjektima.

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

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

(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.

(32) Financijske subjekte stoga 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[35] uz jamstvo potpunog poštovanja pravila Unije o zaštiti podataka, prvenstveno Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća[36], 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 trebalo bi uzeti u obzir znatne razlike među financijskim subjektima u pogledu veličine, poslovnog profila i izloženosti digitalnim rizicima. 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 svojom veličinom i poslovnim profilom, 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] Komunikacija Komisije – Smjernice o primjenjivosti članka 101. Ugovora o funkcioniranju Europske unije na sporazume o horizontalnoj suradnji, 2011/C 11/01.

[36] 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.).

(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 troškovima i gubicima uzrokovanima prekidima u radu IKT-a te o rezultatima preispitivanja nakon incidenta koja se provedu nakon značajnih 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[37], 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

[37] 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

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. 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 ostavriti 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 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 središnjeg EU-ova čvorišta 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 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.

(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 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 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.

(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 raskid ugovora trebao bi biti posljedica barem raznih okolnosti koje ukazuju na 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, posebno

kada se sklapaju s trećim stranama pružateljima IKT usluga sa sjedištem u trećoj zemlji. 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. Europsko nadzorno tijelo imenovano za nadzor svake treće strane pružatelja ključnih IKT usluga („glavno nadzorno tijelo”) trebalo 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[38].

(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 ili prestanka poslovanja treće strane pružatelja IKT usluga 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 bez dodatnih troškova ili uz unaprijed utvrđene troškove.

(53) 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 nadležno tijelo zaduženo za financijski subjekt trebalo, na temelju prethodnih obavijesti, imati ta prava nadzora i revizije treće strane pružatelja IKT usluga, uz poštovanje povjerljivosti.

(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

[38] 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.

omogućilo da se, u skladu sa složenosti pružane usluge, djelotvorno prebaci na usluge druge treće strane pružatelja IKT usluga ili u protivnom pribjegne lokalnim rješenjima.

(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 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.

(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 nadzorom. 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 su uspostavljeni na razini eurosustava kako bi podržali zadaće iz članka 127. stavka 2. Ugovora o funkcioniranju Europske unije.

(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.

(59) Taj 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, a u tome bi mu podršku trebao pružati relevantni pododbor (Nadzorni forum) koji bi bio odgovoran za sve pripreme za donošenje pojedinačnih odluka 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, jedno od europskih nadzornih tijela trebalo bi imenovati glavnim nadzornim tijelom za svaku treću stranu pružatelja ključnih IKT usluga.

(62) Glavna nadzorna tijela trebala bi imati potrebne ovlasti za provedbu istraga, izravni i neizravni 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.

Povjeravanje glavnog nadzora europskim nadzornim tijelima 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) Glavna nadzorna tijela usto bi trebala 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 glavnih nadzornih tijela shvatiti kao dio svoje funkcije koja se odnosi na bonitetni nadzor financijskih subjekata.

(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 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[39], te savjetovanje s europskim nadzornim tijelima, uzajamnom razmjenom informacija i pružanja pomoći u kontekstu nadzornih aktivnosti.

(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 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 priprema provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka, te da se ta savjetovanja provedu u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu od 13. travnja 2016. o boljoj izradi zakonodavstva[40]. Osobito, s ciljem 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[41], 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.

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.

---

39 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.).

40 SL L 123, 12.5.2016., str. 1.

41 [*unijeti cjelovito upućivanje*]

(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 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 veličinu i složenost 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,

– testiranje digitalne operativne otpornosti,

– razmjenu informacija i saznanja o kiberprijetnjama i ranjivostima,

– mjere za dobro upravljanje financijskih subjekata IKT rizikom 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.

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 kriptoimovine, izdavatelje tokena vezanih uz kriptoimovinu i izdavatelje značajnih tokena vezanih uz kriptoimovinu;

(f) središnje depozitorije 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;

(o) institucije za strukovno mirovinsko osiguranje;

(p) agencije za kreditni rejting;

(q) ovlaštene revizore i revizorska društva;

(r) administratore ključnih referentnih vrijednosti;

(s) pružatelje usluga skupnog financiranja;

(t) sekuritizacijske repozitorije;

(u) treće strane pružatelje IKT usluga.

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

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 s tehnološkog aspekta osiguravajući, izravno ili neizravno, korištenjem usluga trećih strana pružatelja IKT usluga, cijeli dijapazon kapaciteta koji se odnose na IKT i potrebni su za sigurnost mrežnih i informacijskih sustava koje financijski subjekt koristi te koji podržavaju kontinuirano pružanje financijskih usluga i njihovu kvalitetu;

(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, uključujući neispravnost, prekoračenje kapaciteta, kvar, poremećaje, zlouporabu, gubitak ili drugu vrstu zlonamjernog ili nezlonamjernog događaja koji, ako do njega dođe, može ugroziti sigurnost mrežnih i informacijskih sustava, alata ili procesa koji ovise o tehnologiji, funkcioniranje operacije i procesa, ili pružanja usluga, što bi ugrozilo cjelovitost ili dostupnost podataka, softvera ili koje druge komponente usluga i infrastruktura IKT-a, ili bi uzrokovalo kršenje povjerljivosti, štetu na fizičkoj infrastrukturi IKT-a ili druge negativne učinke;

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

(6) „IKT incident” znači identificirani nepredviđeni događaj u mrežnim i informacijskim sustavima, koji može ili ne mora biti posljedica zlonamjerne aktivnosti, koji ugrožava sigurnost mrežnih i informacijskih sustava, informacija koje takvi sustavi obrađuju, pohranjuju ili prenose, ili ima negativne učinke na dostupnost, povjerljivost, kontinuitet ili autentičnost financijskih usluga koje financijski subjekt pruža;

(7) „značajan IKT incident” znači IKT incident potencijalno velikog negativnog učinka na mrežne i informacijske sustave koji podržavaju ključne funkcije financijskog subjekta;

(8) „kiberprijetnja” znači „kiberprijetnja” kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća[42];

(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 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 neke imovine, sustava, procesa ili kontrole koji prijetnja 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 digitalne i podatkovne usluge, uključujući pružatelje usluga računalstva u oblaku, softvera, usluga analize podataka, podatkovnih centara, 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[43];

(16) „IKT usluge” znači digitalne i podatkovne usluge koje se preko sustava IKT-a pružaju jednom ili više unutarnjih ili vanjskih korisnika, uključujući pružanje

[42] 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.).

[43] 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.).

podataka, unos podataka, pohranu podataka i usluge izvješćivanja, praćenje podataka te usluge podrške za potrebe poslovanja i odlučivanja na temelju podataka;

(17) „ključna ili važna funkcija” znači funkcija 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, ili njegovu financijsku uspješnost ili stabilnost ili kontinuitet njegovih usluga i aktivnosti;

(18) „treća strana pružatelj ključnih IKT usluga” znači treća strana pružatelj IKT usluga imenovana u skladu s člankom 29. 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 nije osnovala poduzeće/nije prisutna u Uniji i koja je s financijskim subjektom sklopila ugovor o pružanju IKT usluga;

(20) „podugovaratelj IKT usluga sa sjedištem u trećoj zemlji” znači podugovaratelj IKT-a koji je pravna osoba sa sjedištem u trećoj zemlji, koji nije osnovao poduzeće/nije prisutan u Uniji i 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 sposobnost financijskog subjekta, a u konačnici financijskog sustava Unije u cjelini, 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[44], članku 3. stavku 1. točki (u) Uredbe (EU) 20xx/xx Europskog parlamenta i Vijeća[45] [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[46];

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

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

44 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.).

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

46 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.).

(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[47];

(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. točki 3. Direktive (EU) 2016/97;

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

(38) „posrednik u reosiguranju” znači posrednik u reosiguranju kako je definiran u članku 2. 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;

[47] 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.).

(43) „pružatelj usluga povezanih s kriptoimovinom” znači pružatelj usluga povezanih s kriptoimovinom kako je definiran u članku 3. stavku 1. točki (n) 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 (h) [*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*];

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

(47) „administrator ključnih referentnih vrijednosti” znači administrator ključnih referentnih vrijednosti kako je definiran u članku x. točki (x) Uredbe xx/202x [*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 x. točki (x) Uredbe (EU) 202x/xx [*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” znači financijski subjekt kako je definiran u članku 2. stavku 3. Priloga Preporuci 2003/361/EZ.

POGLAVLJE II.

UPRAVLJANJE IKT RIZICIMA

ODJELJAK I.

Članak 4.

Upravljanje i organizacija

1. Financijski subjekti dužni su imati uspostavljene okvire unutarnjeg upravljanja i kontrole kojima se osigurava djelotvorno i razborito upravljanje svim IKT rizicima.

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;

(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.;

(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 osposobljavanje o IKT rizicima i stjecanje vještina za sve članove osoblja za koje je to bitno;

(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) propisno je obaviješteno o 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 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 dužni su redovito pohađati posebno osposobljavanje kako bi stekli i osvježili znanje i vještine koje će im pomoći u razumijevanju i procjeni IKT rizika i njihova učinka na poslovanje financijskog subjekta.

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 koja je usklađena s njihovim poslovnim potrebama, veličinom i složenosti.

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 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.

5. Financijski subjekti, osim mikropoduzeća, dužni su na odgovarajući način razdvojiti 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.

7. 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 i istodobno vodeći računa o prirodi, opsegu i složenosti usluga i aktivnosti financijskih subjekata.

9. Okvir upravljanja IKT rizicima iz stavka 1. sadržava strategiju digitalne 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 poremećaja u radu IKT-a;

   (c) utvrditi jasne ciljeve informacijske sigurnosti;

   (d) objasniti referentnu 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) na razini subjekta utvrditi holističku strategiju nabave IKT-a od više dobavljača u kojoj se izlažu ključne ovisnosti o trećim stranama pružateljima IKT usluga i objašnjava razlog za mješovitu nabavu od različitih trećih strana pružatelja usluga;

   (h) uvesti testiranje digitalne operativne otpornosti;

   (i) u glavnim crtama izložiti komunikacijsku strategiju u slučaju IKT incidenata.

10. Po odobrenju nadležnih tijela financijski subjekti mogu delegirati zadaće provjere usklađenosti sa zahtjevima za upravljanje IKT rizicima poduzeću unutar grupe ili vanjskom poduzeću.

Članak 6.

Sustavi, protokoli i alati IKT-a

1. Financijski subjekti dužni su koristiti i održavati sustave, protokole i alate IKT-a koji ispunjavaju sljedeće uvjete:

   (a) sustavi i alati primjereni su prirodi, raznolikosti, složenosti i 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 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, 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 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 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 IKT imovine te veze i međusobnu ovisnost među različitom IKT imovinom.

5. Financijski subjekti dužni su utvrditi i dokumentirati sve procese koji ovise o trećim stranama pružateljima IKT usluga te utvrditi međusobnu povezanost s trećim stranama pružateljima IKT usluga.

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, posebno prije i nakon povezivanja starih i novih 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 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 najnoviju tehnologiju i procese u području IKT-a koji:

   (a) jamče 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 loše administracije ili rizika povezanih s obradom, uključujući neodgovarajuće vođenje evidencije.

4. Kao dio okvira upravljanja IKT rizicima iz članka 5. stavka 1. 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 i njihovih korisnika;

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

   (c) provoditi politike 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 te u tu svrhu uvesti politike, postupke i kontrole koje se odnose na ovlasti za pristup i njihovu pouzdanu administraciju;

   (d) provoditi politike i protokole za snažne mehanizme autentifikacije na temelju mjerodavnih standarda i namjenskih sustava kontrola kako bi se spriječio pristup kriptografskim ključevima, kojima se podaci šifriraju na temelju rezultata odobrenih procesa klasifikacije podataka i procjene rizika;

(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 odmah prekinuti 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 utvrditi 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. osigurava se više razina kontrole, utvrđuju pragovi upozorenja i kriteriji za otkrivanje IKT incidenata i primjenu procesa odgovora na IKT incidente te uspostavljaju automatski mehanizmi upozoravanja za relevantno osoblje nadležno za odgovor na IKT incidente.

3. Financijski subjekti dužni su izdvojiti dovoljno resursa i kapaciteta, vodeći računa o svojoj veličini, poslovnom profilu i profilu rizičnosti, za praćenje aktivnosti korisnika, neobičnih pojava u IKT-u i IKT incidenata, posebno kibernapada.

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 namjensku i sveobuhvatnu politiku kontinuiteta poslovanja u području IKT-a kao sastavni dio svoje politike za kontinuitet operativnog poslovanja.

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:

   (a) evidentiranje svih IKT incidenata;

(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 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 koja, 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 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 troškovima i gubicima uzrokovanima poremećajima u radu IKT-a i IKT incidentima.

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. 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 čije se operativno okruženje razlikuje od glavnog operativnog okruženja i nije povezano s glavnim okruženjem i zaštićeno je 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 osigurati da su njihovi redundantni kapaciteti IKT-a opremljeni resursima, kapacitetima i funkcijama koji su dostatni i primjereni poslovnim potrebama.

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 odmah 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 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 obaviti višestruke provjere, uključujući usklađivanje, kako bi osigurali najviši stupanj cjelovitosti podataka. Te 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 koji su primjereni njihovoj veličini, poslovnom profilu i profilu rizičnosti, 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 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 financijski subjekti, osim mikropoduzeća, obavješćuju nadležna tijela o tim promjenama.

   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, 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. Oni se primjenjuju na sve zaposlenike i više rukovodstvo.

Financijski subjekti 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 o IKT incidentima ili velikim ranjivostima za klijente i druge ugovorne strane te javnost, ovisno o slučaju.

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 za 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;

(b) propisati kako se politikama, postupcima i alatima za sigurnost IKT-a iz članka 8. stavka 2. sigurnosne kontrole uključuju u sustave od samog početka (integrirana sigurnost), omogućuju prilagodbe razvoju prijetnji i osigurava primjena tehnologije dubinske obrane;

(c) pobliže opisati odgovarajuće tehnike, metode i protokole iz članka 8. stavka 4. točke (b);

(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.

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 procese za osiguravanje dosljednog i integriranog praćenja, rješavanja IKT incidenata i praćenja mjera poduzetih nakon njih kako bi se osiguralo utvrđivanje i otklanjanje 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 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 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 te podatka je li IKT incident imao učinak na ugled;

(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 nakon savjetovanja 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 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 taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do [*Ured za publikacije: unijeti datum: godinu dana 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.

2. Kada značajni IKT incident utječe ili može utjecati na financijske interese korisnika usluge i klijenata, financijski subjekti dužni su bez odgode obavijestiti svoje korisnike usluga i klijente o značajnom IKT incidentu i što prije ih obavijestiti o svim mjerama koje su poduzete da bi se smanjili negativni učinci takvog incidenta.

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

   (a) početnu obavijest bez odgode, a najkasnije do kraja radnog dana ili, u slučaju značajnog IKT incidenta do kojeg je došlo manje od dva sata prije kraja radnog dana, najkasnije četiri sata od početka idućeg radnog dana ili, u slučaju nedostupnosti kanala za izvješćivanje, čim oni postanu dostupni;

   (b) privremeno izvješće najkasnije jedan tjedan od 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 trenutka slanja početnog izvješća.

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.

5. Po primitku izvješća iz stavka 1. nadležno tijelo bez nepotrebne odgode dostavlja pojedinosti o 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.

6. EBA, ESMA ili EIOPA i ESB 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;

(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 stavka 1. točke (a) i zajednički nacrt provedbenih tehničkih standarda iz stavka 1. točke (b) do xx 202x. dostavljaju Komisiji do [*Ured za publikacije: unijeti datum: jednu godinu od datuma stupanja na snagu*].

Komisiji se dodjeljuje ovlast za dopunu ove Uredbe donošenjem zajedničkih regulatornih tehničkih standarda iz stavka 1. točke (a) 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 stavka 1. točke (b) u skladu s člankom 15. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1095/2010 odnosno Uredbe (EU) br. 1094/2010.

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 takvog EU-ova čvorišta;

(b) prednosti, ograničenja i moguće rizike;

(c) elemente operativnog upravljanja;

(d) uvjete članstva;

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

(f) preliminarnu procjenu financijskih troškova koje iziskuje uspostavljanje operativne platforme koja podržava 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.

2. Europska nadzorna tijela, u okviru Zajedničkog odbora, svake godine sastavljaju anonimizirano i agregirano izvješće o obavijestima o 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, 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.

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 dužni su izraditi, provoditi i preispitivati, vodeći računa o svojoj veličini, poslovnom profilu i profilu rizičnosti, 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 pruženih usluga te druge čimbenike koje financijski subjekt smatra primjerenima.

4. Financijski subjekti osiguravaju da testove provode neovisne strane, unutarnje ili vanjske.

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

6. Financijski subjekti dužni su testirati sve ključne sustave i aplikacije 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, uključujući 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 sa stavkom 4. provode napredno testiranje u obliku penetracijskog testiranja vođenog prijetnjama barem svake tri godine.

2. Penetracijsko testiranje vođeno prijetnjama obuhvaća barem ključne funkcije i usluge financijskog subjekta i provodi se na sustavima trenutačno u produkciji koji podržavaju te funkcije. Točan opseg penetracijskog testiranja vođenog prijetnjama utvrđuju financijski subjekti na temelju procjene ključnih funkcija i usluga, a potvrđuju ga nadležna tijela.

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

   Ako su treće strane pružatelji IKT usluga obuhvaćene opsegom penetracijskog testiranja vođenog prijetnjama, financijski subjekt poduzima potrebne mjere kako bi osigurao sudjelovanje tih pružatelja.

   Financijski subjekti provode djelotvorne kontrole upravljanja rizicima kako bi smanjili rizik od mogućeg učinka na podatke, rizik oštećenja imovine i poremećaja u radu ključnih usluga 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 nadležnom tijelu dokumentaciju koja potvrđuje da je penetracijsko testiranje vođeno prijetnjama provedeno u skladu sa zahtjevima. Nadležna tijela potvrđuju dokumentaciju i izdaju potvrdu.

3. Za potrebe provedbe penetracijskog testiranja vođenog prijetnjama financijski subjekti angažiraju provoditelje testiranja u skladu s člankom 24.

Nadležna tijela utvrđuju financijske subjekte koji su dužni provesti penetracijsko testiranje vođeno prijetnjama proporcionalno veličini, opsegu, djelatnosti i općem profilu rizičnosti financijskog subjekta, 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.

4. EBA, ESMA i EIOPA, nakon savjetovanja s ESB-om i uzimajući u obzir relevantne Unijine okvire koji se primjenjuju na penetracijska testiranja vođena saznanjima, izrađuju nacrt regulatornih tehničkih standarda kojima se preciznije utvrđuju:

(a) kriteriji koji se primjenjuju za potrebe primjene stavka 3. ovog članka;

(b) zahtjevi povezani s:

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

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

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

(c) vrsta nadzorne suradnje koja je potrebna za provedbu penetracijskog testiranja vođenog prijetnjama u kontekstu financijskih subjekata koji posluju u više država članica 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: dva mjeseca 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 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;

(d) koji, ako su vanjski provoditelji testiranja, 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, ako su vanjski provoditelji testiranja, propisno i u cijelosti pokriveni odgovarajućim osiguranjem od profesionalne odgovornosti, uključujući rizike od namjernog i nemarnog postupanja.

2. Financijski subjekti 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) 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.

3. Kao dio okvira upravljanja IKT rizicima financijski subjekti donose i redovito preispituju strategiju za IKT rizik treće strane uzimajući u obzir strategiju nabave od

više dobavljača iz članka 5. stavka 9. točke (g). 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 trećih strana pružatelja IKT usluga.

Ugovori iz prvog podstavka na odgovarajući se način dokumentiraju tako da se ugovori koji obuhvaćaju ključne ili važne funkcije odvoje od onih koji ih ne obuhvaćaju.

Financijski subjekti dostavljaju nadležnim tijelima najmanje jednom godišnje informacije o broju novih ugovora o korištenju IKT usluga, 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 najnovije standarde informacijske sigurnosti.

7. Pri ostvarivanju prava pristupa, nadzora i revizije treće strane pružatelja IKT usluga 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 tehnološki vrlo 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 raskid ugovora o korištenju IKT usluga barem u sljedećim okolnostima:

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

(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 ukupnog upravljanja IKT rizicima na razini treće strane pružatelja IKT usluga te osobito načina na koji osigurava sigurnost i cjelovitost povjerljivih, osobnih ili drugih osjetljivih ili neosobnih podataka;

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

9. Financijski subjekti uvode izlazne strategije kako bi uzeli u obzir rizike koji bi se mogli pojaviti na razini treće strane pružatelja IKT usluga, osobito moguću 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.

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: unijeti datum: jednu godinu od 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 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 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 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, osobito ako podugovaratelj IKT usluga ima sjedište u trećoj zemlji.

Ako se ugovor u korištenju IKT usluga sklopi s trećom stranom pružateljem IKT usluga sa sjedištem u trećoj zemlji, financijski subjekti smatraju važnima barem sljedeće čimbenike:

(a) poštovanje zaštite osobnih podataka;

(b) djelotvorno izvršavanje zakonodavstva;

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

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

Financijski subjekti procjenjuju mogu li i u kojoj mjeri potencijalno dugi ili složeni lanci podugovaranja utjecati na njihov kapacitet cjelovitog praćenja 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 u jednom pisanom dokumentu koji je dostupan stranama u papirnatom obliku ili nekom pristupačnom formatu koji se može preuzeti.

2. 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 na kojima će se pružati ugovorene ili podugovorene funkcije i usluge i lokacije na kojima će se obrađivati podaci, uključujući lokaciju pohrane, te zahtjev da treća strana pružatelj IKT usluga obavijesti financijski subjekt ako planira mijenjati te lokacije;

(c) odredbe o pristupačnosti, dostupnosti, cjelovitosti, sigurnosti i zaštiti osobnih podataka te 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;

(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) 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;

(f) obvezu treće strane pružatelja IKT usluga da u slučaju IKT incidenta 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) 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, 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 potpune suradnje tijekom izravnog nadzora koji provodi financijski subjekt te pojedinosti o opsegu, modalitetima i učestalosti nadzora na daljinu;

(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 tijela;

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

(a) 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;

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

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

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).

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 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 foruma osnovanog u skladu s člankom 29. stavkom 1.:

(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.

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 oslanjanju 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 pružatelj 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.

3. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 50. radi dopune 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. Europska nadzorna tijela, u okviru Zajedničkog odbora, izrađuju, objavljuju i svake godine ažuriraju popis trećih strana pružatelja ključnih IKT usluga na razini Unije.

7. Za potrebe stavka 1. točke (a) nadležna tijela svake godine dostavljaju Nadzornom forumu osnovanom u skladu s člankom 29. agregirana izvješća iz članka 25. stavka 4. Nadzorni forum 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.

9. Financijski subjekti ne koriste usluge treće strane pružatelja IKT usluga sa sjedištem u trećoj zemlji čije bi usluge u skladu sa stavkom 1. točkom (a) bile određene kao ključne da ta treća strana ima sjedište u Uniji.

Članak 29.

Struktura nadzornog okvira

1. U skladu s člankom 57. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010 Zajednički odbor osniva Nadzorni forum kao pododbor za pružanje podrške radu Zajedničkog odbora i glavnog nadzornog tijela iz članka 28. stavka 1. točke (b) u području IKT rizika treće strane za sve financijske sektore. Nadzorni forum izrađuje nacrt zajedničkih stajališta i zajedničke akte Zajedničkog odbora u tom području.

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

2. Nadzorni odbor 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.

3. Nadzorni forum 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.

4. Nadzorni forum sastoji se od predsjednika europskih nadzornih tijela i jednog predstavnika na visokoj razini koji je sadašnji član osoblja relevantnog nadležnog tijela iz svake države članice. Izvršni direktor svakog europskog nadzornog tijela i jedan predstavnik Europske komisije, ESRB-a i ESB-a te ENISA-e sudjeluju u radu Nadzornog odbora kao promatrači.

5. U skladu s člankom 16. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010 europska nadzorna tijela izdaju smjernice o suradnji europskih nadzornih tijela i nadležnih tijela za potrebe ovog odjeljka u pogledu detaljnih postupaka i uvjeta koji se odnose na izvršenje zadaća nadležnih tijela i europskih nadzornih tijela te pojedinosti o razmjenama informacija koje su nadležnim tijelima potrebne za poduzimanje mjera na temelju preporuka koje glavna nadzorna tijela upute trećim stranama pružateljima ključnih IKT usluga u skladu s člankom 31. stavkom 1. točkom (d).

6. 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.

7. Europska nadzorna tijela, u okviru Zajedničkog odbora i na temelju pripremnog rada Nadzornog foruma, svake godine dostavljaju Europskom parlamentu, Vijeću i Komisiji izvješće o primjeni ovog odjeljka.

Članak 30.

Zadaće glavnog nadzornog tijela

1. 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.

2. Procjena iz stavka 1. 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 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. glavno nadzorno tijelo donosi jasan, detaljan i obrazložen individualni plan nadzora za svaku treću stranu pružatelja ključnih IKT usluga. O tom se planu svake godine obavješćuje treću stranu pružatelja ključnih IKT usluga.

4. Nakon što se usuglase 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 s glavnim nadzornim tijelom.

Članak 31.

Ovlasti glavnog nadzornog tijela

1. Za potrebe izvršavanja zadaća utvrđenih u ovom odjeljku glavno nadzorno tijelo ovlašteno je:

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

   (b) provoditi opće istrage i 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 točke (d) ovog stavka;

   (d) 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 glavno 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 glavno 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 glavno 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,

         – podugovara se ključna ili važna funkcija financijskog subjekta.

2. Glavno nadzorno tijelo savjetuje se s Nadzornim forumom prije izvršavanja ovlasti iz stavka 1.

3. Treće strane pružatelji ključnih IKT usluga surađuju u dobroj vjeri s glavnim nadzornim tijelom i pomažu glavnom nadzornom tijelu u obavljanju njegovih zadaća.

4. Glavno nadzorno tijelo može izreći periodičnu novčanu kaznu kako bi treću stranu pružatelja ključnih IKT usluga primorao na poštovanje stavka 1. točaka (a), (b) i (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, jednak je 1 % prosječnog dnevnog svjetskog prometa treće strane pružatelja ključnih IKT usluga 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 nalazim 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.

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

(a) upućuje na ovaj članak kao pravnu osnovu 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 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 rok za dostavu informacija;

(e) navodi periodične novčane kazne predviđene člankom 31. stavkom 4. ako su dostavljene tražene informacije nepotpune;

(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 34. stavka 1. može provoditi potrebne istrage trećih strana pružatelja ključnih IKT usluga.

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) izraditi ili pribaviti 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.

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 koji se koriste za pružanje usluga financijskim subjektima ili mu pridonose.

5. Prije planiranog terenskog posjeta 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 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, a nakon savjetovanja s Nadzornim forumom, glavno nadzorno tijelo donosi preporuke koje upućuje 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 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 glavnih nadzornih 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 su glavna nadzorna tijela izdala u skladu s člankom 31. stavkom 1. točkom (d) treće strane pružatelji ključnih IKT usluga dužne su obavijestiti glavno nadzorno tijelo o tome namjeravaju li slijediti te preporuke. Glavna nadzorna tijela odmah tu informaciju prosljeđuju nadležnim tijelima.

2. Nadležna tijela prate jesu li financijski subjekti uzeli u obzir rizike utvrđene u preporukama koje su glavna nadzorna tijela uputila trećim stranama pružateljima ključnih IKT usluga u skladu s člankom 31. stavkom 1. točkom (d).

3. Nadležna tijela mogu, u skladu s člankom 44., zahtijevati od financijskih subjekata da privremeno obustave, djelomično ili u cijelosti, korištenje ili uvođenje usluge koju im pruža treća strana pružatelj ključnih IKT usluga dok se ne uklone rizici utvrđeni u preporukama upućenima trećim stranama pružateljima ključnih IKT usluga. Ona prema potrebi mogu od financijskih subjekata zatražiti da raskinu, djelomično ili u cijelosti, relevantne ugovore sklopljene s trećim stranama pružateljima ključnih IKT usluga.

4. Pri donošenju odluka iz stavka 3. nadležna tijela uzimaju 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.

5. Nadležna tijela redovito informiraju glavna nadzorna tijela o pristupima i mjerama koje su poduzela u okviru svojih zadaća nadzora financijskih subjekata te o ugovornim mjerama koje su poduzeli financijski subjekti ako treća strana pružatelj ključnih IKT usluga nije djelomično ili u cijelosti prihvatila preporuke koje su joj uputila glavna nadzorna tijela.

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 administrativne troškove i razmjeran je prometu treće strane.

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 mogu međusobno 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, osobito informiranjem o kiberprijetnjama, ograničavanjem ili sprečavanjem širenja kiberprijetnji, podrškom obrambenim kapacitetima, tehnikama otkrivanja prijetnji, strategija ublažavanja učinka ili faza odgovora i oporavka financijskih subjekata;

(b) odvijaju se u pouzdanim zajednicama financijskih subjekata;

(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[48] i smjernice o politici tržišnog natjecanja[49].

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.

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 kriptoimovine, izdavatelje 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*];

48 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.).

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

(f) za središnje depozitorije 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 institucije 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 xx/202x*;

(r) za pružatelje usluga skupnog financiranja, nadležno tijelo određeno u skladu s *člankom x. Uredbe xx/202x*;

(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 mogu zatražiti da ih se pozove na sudjelovanje u radu skupine za suradnju.

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.

Članak 43.

Financijske međusektorske vježbe, komunikacija i suradnja

1. Europska nadzorna tijela, u okviru Zajedničkog odbora i u suradnji s nadležnim tijelima, ESB-om 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 povezane prijetnje 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 i ESB 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: unijeti datum: jednu godinu od 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, 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 pod 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].

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 dva 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 dva 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 preispituje kriterije za određivanje trećih strana pružatelja ključnih IKT usluga iz članka 28. stavka 2. te Europskom parlamentu i Vijeću dostavlja izvješće, prema potrebi zajedno s prijedlogom zakonodavnog akta.

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) briše se stavak 2.;

(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].”;

(4) u stavku 6. prvi podstavak zamjenjuje se sljedećim*:*

„CSD utvrđuje, prati i upravlja rizicima koje bi ključni sudionici u sustavima za namiru vrijednosnih papira kojima upravlja, kao i pružatelji usluga i službi te drugi CSD-ovi ili tržišne infrastrukture mogli predstavljati za njegove operacije. Nadležnim i relevantnim tijelima na zahtjev dostavlja informacije o svakom takvom utvrđenom riziku. Bez odgode obavješćuje nadležno tijelo i relevantna tijela i o svim operativnim incidentima koji proizlaze iz tih rizika, osim IKT rizika.”;

(5) u stavku 7. prvi podstavak zamjenjuje se sljedećim*:*

„ESMA u bliskoj suradnji s članovima ESSB-a izrađuje nacrt regulatornih tehničkih standarda kojima se preciznije utvrđuju operativni rizici iz stavaka od 1. do 6., osim IKT rizika, te metode testiranja, uklanjanja ili minimiziranja tih rizika, uključujući politike kontinuiteta poslovanja te planove oporavka u slučaju katastrofe iz stavaka 3. i 4. i metode njihove procjene.”

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) briše se stavak 4.;

(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) briše se stavak 5.;

(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) briše se stavak 3.;

(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: 12 mjeseci 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.

Sastavljeno u Bruxellesu,

Za Europski parlament
Predsjednik

Za Vijeće
Predsjednik

ZAKONODAVNI FINANCIJSKI IZVJEŠTAJ

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

1.2. Predmetna područja politike

1.3. Vrsta prijedloga/inicijative

1.4. Ciljevi

1.5. Osnova prijedloga/inicijative

1.6. Trajanje i financijski učinak prijedloga/inicijative

1.7. Predviđeni načini upravljanja

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

2.2. Sustavi upravljanja i kontrole

2.3. Mjere za sprečavanje prijevara i nepravilnosti

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslovi višegodišnjeg financijskog okvira i proračunske linije rashoda na koje prijedlog/inicijativa ima učinak

3.2. Procijenjeni učinak na rashode

3.2.1. Sažetak procijenjenog učinka na rashode

3.2.2. Procijenjeni učinak na odobrena sredstva

3.2.3. Procijenjeni učinak na ljudske resurse

3.2.4. Usklađenost s aktualnim višegodišnjim financijskim okvirom

3.2.5. Doprinos trećih strana

3.3. Procijenjeni učinak na prihode

Prilog

Opće pretpostavke

Nadzorne ovlasti

ZAKONODAVNI FINANCIJSKI IZVJEŠTAJ – „AGENCIJE”

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

Prijedlog uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti financijskog sektora.

1.2. Predmetna područja politike

Područje politike: financijska stabilnost, financijske usluge i unija tržišta kapitala Aktivnost: digitalna operativna otpornost

1.3. Prijedlog se odnosi na

☑ **novo djelovanje**

☐ **novo djelovanje nakon pilot-projekta/pripremnog djelovanja**[50]

☐ **produženje postojećeg djelovanja**

☐ **spajanje ili preusmjeravanje jednog ili više djelovanja u drugo/novo djelovanje**

1.4. Ciljevi

1.4.1. Opći ciljevi

Opći je cilj inicijative povećati digitalnu operativnu otpornost subjekata iz financijskog sektora EU-a pojednostavnjenjem i ažuriranjem postojećih pravila te uvođenjem novih zahtjeva u područjima u kojima postoje praznine. Time bi se unaprijedila i digitalna dimenzija jedinstvenih pravila. Ukupni cilj može se podijeliti na tri opća cilja: 1. smanjenje rizika od poremećaja i nestabilnosti u području financija, 2. smanjenje administrativnog opterećenja i povećanje djelotvornosti nadzora te 3. povećanje zaštite potrošača i ulagatelja.

1.4.2. Posebni ciljevi

Posebni su ciljevi prijedloga sljedeći: detaljnije obraditi probleme rizika informacijskih i komunikacijskih tehnologija („IKT”) i povećanje razine sveukupne digitalne otpornosti financijskog sektora pojednostavniti izvješćivanje o IKT incidentima i riješiti problem preklapanja zahtjeva za izvješćivanje omogućiti financijskim nadzornim tijelima pristup informacijama o IKT incidentima osigurati da financijski subjekti obuhvaćeni ovim prijedlogom provode procjenu djelotvornosti svojih preventivnih mjera i mjera za otpornost te utvrđuju ranjivosti u području IKT-a smanjiti rascjepkanost jedinstvenog tržišta i omogućiti prekogranično prihvaćanje rezultata testiranja

50 Kako je navedeno u članku 58. stavku 2. točkama (a) ili (b) Financijske uredbe.

jačati ugovorne zaštitne mjere za financijske subjekte kada koriste IKT usluge, među ostalim za pravila o eksternalizaciji poslova (upravljanje praćenjem trećih strana pružatelja IKT usluga) omogućiti nadzor aktivnosti trećih strana pružatelja ključnih IKT usluga poticati razmjenu saznanja o prijetnjama u financijskom sektoru.

1.4.3. Očekivani rezultati i učinak

Navesti očekivane učinke prijedloga/inicijative na ciljane korisnike/skupine.

Akt o digitalnoj operativnoj otpornosti za financijski sektor osigurao bi sveobuhvatan okvir kojim su obuhvaćeni svi aspekti digitalne operativne otpornosti i njime bi se djelotvorno poboljšala sveukupna operativna otpornost financijskog sektora. Njime bi se zaštitila jasnoća i koherentnost jedinstvenih pravila.

Njime bi se utvrdilo i međudjelovanje s Direktivom NIS i njezino bi preispitivanje bilo jasnije i koherentnije. Njime bi se financijskim subjektima pojasnila različita pravila o digitalnoj operativnoj otpornosti kojih se moraju pridržavati, osobito u slučaju financijskih subjekata s nekoliko odobrenja za rad koji posluju na različitim tržištima unutar EU-a.

1.4.4. Pokazatelji uspješnosti

Navesti pokazatelje za praćenje napretka i postignuća

Mogući pokazatelji:

broj IKT incidenata u financijskom sektoru EU-a i njihov učinak

broj značajnih IKT incidenata o kojima su obaviješteni bonitetni nadzornici

broj financijskih subjekata koji bi morali obavljati penetracijska testiranja vođena prijetnjama („TLPT”)

broj financijskih subjekata koji pri sklapanju ugovora s trećim stranama pružateljima IKT usluga primjenjuju standardne ugovorne klauzule

broj trećih strana pružatelja ključnih IKT usluga koje nadziru europska nadzorna tijela/bonitetni nadzornici

broj financijskih subjekata koji sudjeluju u rješenjima za razmjenu saznanja o prijetnjama

broj tijela koja primaju izvješća o istom IKT incidentu

broj prekograničnih TLPT-a.

1.5. Osnova prijedloga/inicijative

1.5.1. Zahtjevi koje treba ispuniti u kratkoročnom ili dugoročnom razdoblju, uključujući detaljan vremenski plan provedbe inicijative

Financijski sektor uvelike se oslanja na informacijske i komunikacijske tehnologije (IKT). Usprkos znatnom napretku ostvarenom u okviru nacionalnih i europskih ciljanih politika i zakonodavnih inicijativa, 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 usmjerena na zaštitu konkurentnosti i stabilnosti EU-a u kontekstu gospodarstva, boniteta i ponašanja na tržištu. Sigurnost IKT-a i sveukupna digitalna otpornost dio su operativnog rizika, ali 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. To znači da bi ovim prijedlogom trebalo odgovoriti na sljedeće izazove:

Pravni okvir EU-a kojim su obuhvaćeni IKT rizik i operativna otpornost u cijelom financijskom sektoru rascjepkan je i nije sasvim dosljedan.

Zbog nedosljednosti zahtjeva za izvješćivanje o IKT incidentima nadzorna tijela imaju nepotpun pregled prirode, učestalosti, važnosti i učinka incidenata.

Neki financijski subjekti izloženi su složenim, preklapajućim i potencijalno nedosljednim zahtjevima za izvješćivanje o istom IKT incidentu.

Nedostatna razmjena informacija i suradnja u području saznanja o kiberprijetnjama na strateškoj, taktičkoj i operativnoj razini sprečavaju pojedine financijske subjekte da primjereno procijene, prate i odgovore na kiberprijetnje i obrane se od njih.

U određenim financijskim podsektorima mogući sui višestruki i nekoordinirani okviri za penetracijsko testiranje i testiranje otpornosti, bez prekograničnog priznavanja rezultata, dok u drugim podsektorima takvih okvira za testiranje ni nema.

Budući da nadzorna tijela nemaju uvid u aktivnosti financijskih subjekata koje im pružaju treće strane pružatelji IKT usluga, financijski subjekti pojedinačno i financijski sustav u cjelini izloženi su operativnim rizicima.

Financijska nadzorna tijela nemaju dostatne ovlasti ni alate za praćenje i upravljanje koncentracijskim i sistemskim rizicima koji proizlaze iz oslanjanja financijskih subjekata na treće strane pružatelje IKT usluga.

1.5.2. Dodana vrijednost sudjelovanja Unije (može proizlaziti iz različitih čimbenika, npr. prednosti koordinacije, pravne sigurnosti, veće djelotvornosti ili komplementarnosti). Za potrebe ove točke „dodana vrijednost sudjelovanja Unije” vrijednost je koja proizlazi iz intervencije Unije i predstavlja dodatnu vrijednost u odnosu na vrijednost koju bi države članice inače ostvarile same.

Razlozi za djelovanje na europskoj razini (*ex ante*):

Digitalna operativna otpornost pitanje je od zajedničkog interesa za financijska tržišta EU-a. Djelovanje na razini EU-a donijelo bi više prednosti i veću vrijednost od pojedinačnog djelovanja na nacionalnoj razini. Bez dodavanja tih operativnih odredbi o IKT riziku, jedinstvenim bi se pravilima osigurali alati za suzbijanje svih drugih vrsta rizika na europskoj razini, ali bi se izostavili aspekti digitalne operativne otpornosti ili bi ih se prepustilo rascjepkanim i nekoordiniranim nacionalnim inicijativama. Prijedlog osigurava pravnu jasnoću o tome kada se i kako primjenjuju odredbe o digitalnoj operativnoj otpornosti, osobito na financijske subjekte koji posluju prekogranično, i države članice više ne bi trebale pojedinačno poboljšavati pravila, standarde i očekivanja o operativnoj otpornosti i kibersigurnosti zbog zasad ograničene obrade tih tema u propisima EU-a i opće prirode Direktive NIS.

Očekivana dodana vrijednost Unije (*ex post*):

Intervencijom Unije znatno bi se povećala djelotvornost politike uz istodobno pojednostavnjenje i smanjenje financijskog i administrativnog opterećenja za sve financijske subjekte. Uskladilo bi se područje gospodarstva koje je duboko povezano i integrirano i već ostvaruje koristi od jedinstvenog skupa pravila i nadzora. Kad je riječ o izvješćivanju o IKT incidentima, prijedlogom se smanjuju opterećenje i implicitni troškovi izvješćivanja o istom IKT incidentu, o kojem se sada obavješćuju razna tijela EU-a i/ili nacionalna tijela. Olakšalo bi se i uzajamno priznavanje/prihvaćanje rezultata testiranja subjekata s prekograničnim poslovanjem koji su obuhvaćeni višestrukim okvirima za testiranje u različitim državama članicama.

1.5.3. Pouke iz prijašnjih sličnih iskustava

Nova inicijativa

1.5.4. Usklađenost s višegodišnjim financijskim okvirom i moguće sinergije s drugim prikladnim instrumentima

Cilj ovog prijedloga u skladu je s nizom drugih politika i tekućih inicijativa EU-a, prvenstveno Direktivom o mrežnoj i informacijskog sigurnosti (NIS) i Direktivom o europskoj kritičnoj infrastrukturi (ECI). Prijedlogom se zadržavaju koristi horizontalnog okvira za kibersigurnost jer tri financijska podsektora ostaju obuhvaćena područjem primjene Direktive NIS. Zahvaljujući održavanju te veze s ekosustavom Direktive NIS, financijska nadzorna tijela mogla bi razmjenjivati relevantne informacije s nadležnim tijelima iz Direktive NIS i sudjelovati u radu Skupine za suradnju NIS. Prijedlog ne bi utjecao na Direktivu NIS nego bi je nadogradio i riješio bi se problem mogućih preklapanja putem izuzeća *lex specialis*. Međudjelovanje Uredbe o financijskim uslugama i Direktive NIS i dalje bi bilo uređeno klauzulom *lex specialis*, čime bi se financijske subjekte oslobodilo materijalnih zahtjeva iz Direktive NIS i izbjegla bi se preklapanja tih dvaju akata. Prijedlog je usto u skladu s Direktivom o europskoj kritičnoj infrastrukturi (ECI), koja se upravo preispituje kako bi se poboljšala zaštita kritičnih infrastruktura od prijetnji koje nisu povezane s kibersigurnosti te njihova otpornost na te prijetnje.

Ovaj prijedlog ne utječe na višegodišnji financijski okvir (VFO). Prvo, nadzorni okvir za treće strane pružatelje ključnih IKT usluga u potpunosti bi se financirao iz naknada naplaćenih od tih pružatelja; drugo, obavljanje dodatnih regulatornih zadaća povezanih s digitalnom operativnom otpornosti koje bi bile povjerene europskim nadzornim tijelima osigurat će se unutarnjim premještanjem postojećih zaposlenika.

To znači da će se u okviru budućeg godišnjeg proračunskog postupka predložiti povećanje broja ovlaštenog osoblja agencije. Agencija će i dalje raditi na povećanju sinergija i učinkovitosti (među ostalim s pomoću IT sustavâ) te pozorno pratiti dodatno radno opterećenje povezano s ovim prijedlogom, koje bi se moglo odraziti u broju članova ovlaštenog osoblja koji agencija zatraži u okviru godišnjeg proračunskog postupka.

1.5.5. Ocjena različitih dostupnih mogućnosti financiranja, uključujući mogućnost preraspodjele

Razmatrano je nekoliko mogućnosti financiranja:

Prvo, dodatni troškovi mogli bi se financirati iz uobičajenog mehanizma financiranja europskih nadzornih tijela. Međutim, to bi podrazumijevalo znatno povećanje doprinosa EU-a financijskim sredstvima europskih nadzornih tijela.

Ta je mogućnost odabrana za troškove koji se odnose na regulatorne zadaće povezane s ovim prijedlogom. Naime, od europskih nadzornih tijela zatražit će se preraspodjela postojećeg osoblja za izradu brojnih tehničkih standarda. Međutim, dodatni troškovi nadzora trećih strana pružatelja ključnih IKT usluga ne mogu se pokriti preraspodjelom resursa unutar europskih nadzornih tijela koja imaju i druge zadaće osim onih predviđenih ovim prijedlogom i onih predviđenih drugim zakonodavnim aktima Unije. Nadalje, za obavljanje nadzornih zadaća povezanih s digitalnom operativnom otpornosti potrebno je specifično tehničko znanje i stručnost. Budući da europska nadzorna tijela zasad nemaju dovoljno takvih resursa, potrebni su dodatni resursi.

Naposljetku, prema prijedlogu naknade će se naplaćivati od trećih strana pružatelja ključnih IKT usluga koje podliježu nadzoru. Predviđeno je da se njima pokriju svi dodatni resursi koje europska nadzorna tijela trebaju za izvršavanje svojih novih zadaća i ovlasti.

1.6. Trajanje i financijski učinak prijedloga/inicijative

☐ **Ograničeno trajanje**

☐ prijedlog/inicijativa na snazi od [DD/MM]GGGG do [DD/MM]GGGG

☐ financijski učinak od GGGG do GGGG

☑ **Neograničeno trajanje**

Provedba s početnim razdobljem od 2021.

nakon čega slijedi redovna provedba.

1.7. Predviđeni načini upravljanja[51]

Izravno upravljanje koje provodi Komisija

☐ putem izvršnih agencija

☐ **Podijeljeno upravljanje** s državama članicama

☑ **Neizravno upravljanje** povjeravanjem zadaća izvršenja proračuna:

☐ međunarodnim organizacijama i njihovim agencijama (navesti)

☐ EIB-u i Europskom investicijskom fondu

☑ tijelima iz članaka 70. i 71.

☐ tijelima javnog prava

☐ tijelima uređenima privatnim pravom koja pružaju javne usluge u mjeri u kojoj daju odgovarajuća financijska jamstva

☐ tijelima uređenima privatnim pravom države članice kojima je povjerena provedba javno-privatnog partnerstva i koja daju odgovarajuća financijska jamstva

☐ osobama kojima je povjerena provedba određenih djelovanja u području ZVSP-a u skladu s glavom V. UEU-a i koje su navedene u odgovarajućem temeljnom aktu.

Napomene

Nije primjenjivo

[51] Informacije o načinima upravljanja i upućivanja na Financijsku uredbu dostupni su na internetskim stranicama BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

Navesti učestalost i uvjete.

U skladu s već postojećim mehanizmima europska nadzorna tijela sastavljaju redovita izvješća o svojem radu (uključujući interno izvješćivanje višeg rukovodstva, izvješćivanje odbora i sastavljanje godišnjeg izvješća), a Revizorski sud i Služba Komisije za unutarnju reviziju provode reviziju njihova korištenja resursa i uspješnosti. Praćenje i izvješćivanje o mjerama uključenima u prijedlog bit će u skladu s već postojećim zahtjevima i s novim zahtjevima koji proizlaze iz ovog prijedloga.

2.2. Sustavi upravljanja i kontrole

2.2.1. Obrazloženje načina upravljanja, mehanizama provedbe financiranja, načina plaćanja i predložene strategije kontrole

Upravljanje će biti neizravno, a za njega će biti odgovorna europska nadzorna tijela. Mehanizam financiranja bile bi naknade naplaćene od predmetnih trećih strana pružatelja ključnih IKT usluga.

2.2.2. Informacije o utvrđenim rizicima i uspostavljenim sustavima unutarnje kontrole za ublažavanje rizika

Kada je riječ o zakonitom, ekonomičnom, učinkovitom i djelotvornom korištenju odobrenih sredstava na temelju prijedloga, očekuje se da prijedlog neće uzrokovati nove važne rizike koji ne bi bili obuhvaćeni postojećim okvirom za unutarnju kontrolu. Međutim, novi bi problem mogao nastati u pogledu osiguranja pravodobne naplate naknada od predmetnih trećih strana pružatelja ključnih IKT usluga.

2.2.3. Procjena i obrazloženje troškovne učinkovitosti kontrola (omjer troškova kontrole i vrijednosti sredstava kojima se upravlja) i procjena očekivane razine rizika od pogreške (pri plaćanju i pri zaključenju)

Već su uspostavljeni sustavi upravljanja i kontrole predviđeni uredbama o europskim nadzornim tijelima. Europska nadzorna tijela blisko surađuju sa Službom Komisije za unutarnju reviziju kako bi se osigurala primjena odgovarajućih standarda u svim područjima okvira za unutarnju kontrolu. Ti će se mehanizmi u skladu s ovim prijedlogom primjenjivati i na ulogu europskih nadzornih tijela. Nadalje, svake financijske godine Europski parlament, na temelju preporuke Vijeća, izdaje svakom europskom nadzornom tijelu razrješnicu za izvršenje njegova proračuna.

2.3. Mjere za sprečavanje prijevara i nepravilnosti

Navesti postojeće ili predviđene mjere za sprečavanje i zaštitu, npr. iz strategije za borbu protiv prijevara.

Za potrebe suzbijanja prijevare, korupcije i svih drugih nezakonitih radnji odredbe Uredbe (EU, Euratom) br. 883/2013 Europskog parlamenta i Vijeća od 11. rujna 2013. o istragama koje provodi Europski ured za borbu protiv prijevara (OLAF) primjenjuju se na europska nadzorna tijela bez ograničenja.

Europska nadzorna tijela imaju posebnu strategiju suzbijanja prijevara i pripadajući akcijski plan. Pojačana djelovanja europskih nadzornih tijela u području borbe protiv prijevara bit će u skladu s pravilima i smjernicama iz Financijske uredbe (mjere suzbijanja prijevara u okviru dobrog financijskog upravljanja), OLAF-ovim politikama za sprečavanje prijevara, odredbama iz Strategije Komisije za borbu protiv prijevara (COM(2011) 376) te s odredbama iz Zajedničkog pristupa decentraliziranim agencijama EU-a (srpanj 2012.) i pripadajućeg plana.

Nadalje, u uredbama o osnivanju europskih nadzornih tijela i u financijskim uredbama europskih nadzornih tijela utvrđene su odredbe o izvršenju i kontroli proračuna europskih nadzornih tijela te o primjenjivim financijskim propisima, uključujući propise o sprečavanju prijevara i nepravilnosti.

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslovi višegodišnjeg financijskog okvira i proračunske linije rashoda na koje prijedlog/inicijativa ima učinak

Postojeće proračunske linije

<u>Prema redoslijedu</u> naslova višegodišnjeg financijskog okvira i proračunskih linija.

Naslov višegodišnjeg financijskog okvira	Proračunska linija	Vrsta rashoda	Doprinos			
	Broj	dif./nedif.[52]	zemalja EFTA-e[53]	zemalja kandidatkinja[54]	trećih zemalja	u smislu članka 21. stavka 2. točke (b) Financijske uredbe

Zatražene nove proračunske linije

<u>Prema redoslijedu</u> naslova višegodišnjeg financijskog okvira i proračunskih linija.

Naslov višegodišnjeg financijskog okvira	Proračunska linija	Vrsta rashoda	Doprinos			
	Broj	dif./nedif.	zemalja EFTA-e	zemalja kandidatkinja	trećih zemalja	u smislu članka 21. stavka 2. točke (b) Financijske uredbe

[52] Dif. = diferencirana odobrena sredstva; nedif. = nediferencirana odobrena sredstva.
[53] EFTA: Europsko udruženje slobodne trgovine.
[54] Zemlje kandidatkinje i, ako je primjenjivo, potencijalni kandidati sa zapadnog Balkana.

3.2. Procijenjeni učinak na rashode

3.3. Sažetak procijenjenog učinka na rashode

U milijunima EUR (do 3 decimalna mjesta)

Naslov višegodišnjeg financijskog okvira	Broj	Naslov

Glavna uprava: <..>			2020.	2021.	2022.	2023.	2024.	2025.	2026.	2027.	**UKUPNO**
	Obveze	(1)									
	Plaćanja	(2)									
UKUPNA odobrena sredstva za Glavnu upravu <>	Obveze										
	Plaćanja										

Naslov višegodišnjeg financijskog okvira		

U milijunima EUR (do 3 decimalna mjesta)

		2022.	2023.	2024.	2025.	2026.	2027.	**UKUPNO**
Glavne uprave:								
• Ljudski resursi								
• Ostali administrativni rashodi <>								
GLAVNE UPRAVE UKUPNO	Odobrena sredstva							

UKUPNA odobrena sredstva iz NASLOVA višegodišnjeg financijskog okvira	(ukupne obveze = ukupna plaćanja)							

U milijunima EUR (do 3 decimalna mjesta) po stalnim cijenama

		2022.	**2023.**	**2024.**	**2025.**	**2026.**	**2027.**	**UKUPNO**
UKUPNA odobrena sredstva iz NASLOVA 1. višegodišnjeg financijskog okvira	Obveze							
	Plaćanja							

3.3.1. Procijenjeni učinak na odobrena sredstva

☑ Za prijedlog/inicijativu nisu potrebna odobrena sredstva za poslovanje.

☐ Za prijedlog/inicijativu potrebna su sljedeća odobrena sredstva za poslovanje:

Odobrena sredstva za preuzimanje obveza u milijunima EUR (do 3 decimalna mjesta) po stalnim cijenama

Navesti ciljeve i rezultate ⇩			2022.		2023.		2024.		2025.		2026.		2027.		**UKUPNO**	
	REZULTATI															
	Vrsta[55]	Prosječni trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Ukupni broj	Ukupni trošak
POSEBNI CILJ br. 1[56]…																
– Rezultat																
Međuzbroj za posebni cilj br. 1																
POSEBNI CILJ br. 2...																
– Rezultat																
Međuzbroj za posebni cilj br. 2																
UKUPNI TROŠAK																

55 Rezultati se odnose na proizvode i usluge koji se isporučuju (npr.: broj financiranih studentskih razmjena, kilometri izgrađenih prometnica itd.).

56 Kako je opisan u odjeljku 1.4.2. „Posebni ciljevi…”.

3.3.2. Procijenjeni učinak na ljudske resurse

3.3.2.1. Sažetak

☐ Za prijedlog/inicijativu nisu potrebna administrativna odobrena sredstva.

☑ Za prijedlog/inicijativu potrebna su sljedeća administrativna odobrena sredstva:

U milijunima EUR (do 3 decimalna mjesta) po stalnim cijenama

EBA, EIOPA, ESMA	2022.	2023.	2024.	2025.	2026.	2027.	**UKUPNO**
Privremeno osoblje (razredi AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Privremeno osoblje (razredi AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Ugovorno osoblje							
Upućeni nacionalni stručnjaci							
UKUPNO	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Potrebe u pogledu osoblja (u EPRV-u):

EBA, EIOPA, ESMA i EEA	2022.	2023.	2024.	2025.	2026.	2027.	**UKUPNO**
Privremeno osoblje (razredi AD) EBA = 5, EIOPA = 5, ESMA = 5	15	15	15	15	15	15	15
Privremeno osoblje (razredi AST) EBA = 1, EIOPA = 1, EEA = 1	3	3	3	3	3	3	3
Ugovorno osoblje							
Upućeni nacionalni stručnjaci							
UKUPNO	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Procijenjene potrebe u pogledu ljudskih resursa za (matične) glavne uprave

☑ Za prijedlog/inicijativu nisu potrebni ljudski resursi.

☐ Za prijedlog/inicijativu potrebni su sljedeći ljudski resursi:

Procjenu navesti u cijelom iznosu (ili najviše do jednog decimalnog mjesta)

<table>
<tr><th colspan="2"></th><th>2022.</th><th>2023.</th><th>2024.</th><th>2025.</th><th>2026.</th><th>2027.</th></tr>
<tr><td colspan="2">• Radna mjesta prema planu radnih mjesta (dužnosnici i privremeno osoblje)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">• Vanjsko osoblje (u ekvivalentu punog radnog vremena: EPRV)[57]</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">XX 01 02 01 (UO, UNS, UsO iz „globalne omotnice”)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">XX 01 02 02 (UO, LO, UNS, UsO i MSD u delegacijama)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">XX 01 04 yy[58]</td><td>– u sjedištima[59]</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>– u delegacijama</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">XX 01 05 02 (UO, UNS, UsO – neizravno istraživanje)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">10 01 05 02 (UO, UNS, UsO – izravno istraživanje)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Druge proračunske linije (navesti)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">UKUPNO</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

XX se odnosi na odgovarajuće područje politike ili glavu proračuna.

Potrebe za ljudskim resursima pokrit će se osobljem glavne uprave kojemu je već povjereno upravljanje djelovanjem i/ili koje je preraspoređeno unutar glavne uprave te, prema potrebi, resursima koji se mogu dodijeliti nadležnoj glavnoj upravi u okviru godišnjeg postupka dodjele sredstava uzimajući u obzir proračunska ograničenja.

Opis zadaća:

Dužnosnici i privremeno osoblje	
Vanjsko osoblje	

Opis izračuna troškova za ekvivalent punog radnog vremena trebao bi biti uključen u Prilog V. odjeljak 3.

[57] UO = ugovorno osoblje; LO = lokalno osoblje; UNS = upućeni nacionalni stručnjaci; UsO = ustupljeno osoblje; MSD = mladi stručnjaci u delegacijama.

[58] U okviru gornje granice za vanjsko osoblje iz odobrenih sredstava za poslovanje (prijašnje linije „BA”).

[59] Uglavnom za strukturne fondove, Europski poljoprivredni fond za ruralni razvoj (EPFRR) i Europski fond za ribarstvo (EFR).

3.3.3. Usklađenost s aktualnim višegodišnjim financijskim okvirom

☑ Prijedlog/inicijativa u skladu je s aktualnim višegodišnjim financijskim okvirom.

☐ Prijedlog/inicijativa iziskuje reprogramiranje relevantnog naslova višegodišnjeg financijskog okvira.

☐ Za prijedlog/inicijativu potrebna je primjena instrumenta fleksibilnosti ili revizija višegodišnjeg financijskog okvira[60].

Objasniti što je potrebno te navesti predmetne naslove i proračunske linije te odgovarajuće iznose.

[…]

3.3.4. Doprinos trećih strana

☐ Prijedlogom/inicijativom ne predviđa se sudjelovanje trećih strana u sufinanciranju.

☑ Prijedlogom/inicijativom predviđa se sufinanciranje prema sljedećoj procjeni:

U milijunima EUR (do 3 decimalna mjesta)

EBA

	2022.	2023.	2024.	2025.	2026.	2027.	Ukupno
Troškove u potpunosti pokrivaju naknade naplaćene od nadziranih subjekata[61].	1,373	1,948	1,748	1,748	1,748	1,748	10,313
UKUPNO sufinancirana odobrena sredstva	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022.	2023.	2024.	2025.	2026.	2027.	Ukupno
Troškove u potpunosti pokrivaju naknade naplaćene od nadziranih subjekata[62].	1,305	1,811	1,611	1,611	1,611	1,611	9,560
UKUPNO sufinancirana odobrena sredstva	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022.	2023.	2024.	2025.	2026.	2027.	Ukupno

60 Vidjeti članke 11. i 17. Uredbe Vijeća (EU, Euratom) br. 1311/2013 kojom se uspostavlja višegodišnji financijski okvir za razdoblje 2014.–2020.

61 100 % ukupnog procijenjenog troška plus ukupni mirovinski doprinosi poslodavca.

62 100 % ukupnog procijenjenog troška plus ukupni mirovinski doprinosi poslodavca.

Troškove u potpunosti pokrivaju naknade naplaćene od nadziranih subjekata[63].	1,373	1,948	1,748	1,748	1,748	1,748	10,313
UKUPNO sufinancirana odobrena sredstva	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Procijenjeni učinak na prihode

☑ Prijedlog/inicijativa nema financijski učinak na prihode.

☐ Prijedlog/inicijativa ima sljedeći financijski učinak:

☐ na vlastita sredstva

☐ na ostale prihode

☐ navesti jesu li prihodi namijenjeni proračunskim linijama rashoda

U milijunima EUR (do 3 decimalna mjesta)

Proračunska linija prihoda:	Odobrena sredstva dostupna za tekuću financijsku godinu	Učinak prijedloga/inicijative[64]						
		Godina **N**	Godina **N+1**	Godina **N+2**	Godina **N+3**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)		
Članak ………….								

Za razne namjenske prihode navesti odgovarajuće proračunske linije rashoda.

[…]

Navesti metodu izračuna učinka na prihode.

[…]

63 100 % ukupnog procijenjenog troška plus ukupni mirovinski doprinosi poslodavca.

64 Kad je riječ o tradicionalnim vlastitim sredstvima (carine, pristojbe na šećer) navedeni iznosi moraju biti neto iznosi, to jest bruto iznosi nakon odbitka od 20 % na ime troškova naplate.

PRILOG

Opće pretpostavke

Glava I. – Rashodi za osoblje

Sljedeće posebne pretpostavke primijenjene su pri izračunu rashoda za osoblje na temelju utvrđenih potreba za osobljem koje su objašnjene u nastavku:

- troškovi za dodatno osoblje zaposleno 2022. izračunani su za šest mjeseci s obzirom na predviđeno vrijeme potrebno za zapošljavanje dodatnog osoblja,
- prosječni godišnji trošak privremenog člana osoblja iznosi 150 000 EUR, što uključuje troškove od 25 000 EUR za „habillage” (zgrade, IT itd.),
- korekcijski koeficijent primjenjiv na plaće osoblja u Parizu (EBA i ESMA) iznosi 117,7 te 99,4 za plaće osoblja u Frankfurtu (EIOPA),
- iznos mirovinskih doprinosa poslodavca za privremeno osoblje dobiven je na temelju standardnih osnovnih plaća uključenih u standardne prosječne godišnje troškove, tj. 95 660 EUR,
- dodatno privremeno osoblje pripada razredima AD5 i AST.

Glava II. – Rashodi za infrastrukturu i poslovanje

Troškovi su dobiveni množenjem broja članova osoblja i udjela tjedana rada u godini zaposlenja standardnim troškom za „habillage”, tj. 25 000 EUR.

Glava III. – Rashodi poslovanja

Troškove se procjenjuje na temelju sljedećih pretpostavki:

- godišnji troškovi prevođenja iznosili bi 350 000 EUR za svako europsko nadzorno tijelo;
- pretpostavlja se da će se jednokratni IT trošak od 500 000 EUR za svako europsko nadzorno tijelo raspodijeliti na dvije godine, 2022. i 2023., u omjeru 50 : 50. Procjenjuje se da će godišnji troškovi održavanja od 2024. iznositi 50 000 EUR za svako europsko nadzorno tijelo;
- procjenjuje se da će godišnji troškovi izravnog nadzora iznositi 200 000 EUR za svako europsko nadzorno tijelo.

Prema prethodno navedenim procjenama godišnji troškovi iznosili bi:

Naslov višegodišnjeg financijskog okvira	Broj	

Stalne cijene

EBA:			2022.	2023.	2024.	2025.	2026.	2027.	**UKUPNO**
Glava 1.:	Obveze	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Plaćanja	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Glava 2.:	Obveze	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Plaćanja	(2 a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Glava 3.:	Obveze	(3 a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Plaćanja	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
UKUPNA odobrena sredstva za EBA-u	Obveze	=1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Plaćanja	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022.	2023.	2024.	2025.	2026.	2027.	**UKUPNO**
Glava 1.:	Obveze	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Plaćanja	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Glava 2.:	Obveze	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Plaćanja	(2 a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Glava 3.:	Obveze	(3 a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Plaćanja	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000

UKUPNA odobrena sredstva za EIOPA-u	Obveze	=1+1a+3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	Plaćanja	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022.	2023.	2024.	2025.	2026.	2027.	**UKUPNO**
Glava 1.:	Obveze	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Plaćanja	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Glava 2.:	Obveze	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Plaćanja	(2 a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Glava 3.:	Obveze	(3 a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Plaćanja	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
UKUPNA odobrena sredstva za ESMA-u	Obveze	=1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Plaćanja	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Za prijedlog su potrebna sljedeća odobrena sredstva za poslovanje:

Odobrena sredstva za preuzimanje obveza u milijunima EUR (do 3 decimalna mjesta) po stalnim cijenama

EBA

Navesti ciljeve i rezultate ⇩			2022.		2023.		2024.		2025.		2026.		2027.			
	REZULTATI															
	Vrsta[65]	Prosječni trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Ukupni broj	Ukupni trošak
POSEBNI CILJ br. 1[66] Izravni nadzor trećih strana pružatelja ključnih IKT usluga																
– Rezultat				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Međuzbroj za posebni cilj br. 1																
POSEBNI CILJ br. 2...																
– Rezultat																
Međuzbroj za posebni cilj br. 2																
UKUPNI TROŠAK				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Navesti ciljeve i rezultate ⇩			2022.		2023.		2024.		2025.		2026.		2027.			
	REZULTATI															
	Vrsta[67]	Prosječni trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Ukupni broj	Ukupni trošak
POSEBNI CILJ br. 1[68] Izravni nadzor trećih strana pružatelja ključnih IKT usluga																

---

65 Rezultati se odnose na proizvode i usluge koji se isporučuju (npr.: broj financiranih studentskih razmjena, kilometri izgrađenih prometnica itd.).

66 Kako je opisan u odjeljku 1.4.2. „Posebni ciljevi…”.

67 Rezultati se odnose na proizvode i usluge koji se isporučuju (npr.: broj financiranih studentskih razmjena, kilometri izgrađenih prometnica itd.).

68 Kako je opisan u odjeljku 1.4.2. „Posebni ciljevi…”.

– Rezultat				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Međuzbroj za posebni cilj br. 1																
POSEBNI CILJ br. 2...																
– Rezultat																
Međuzbroj za posebni cilj br. 2																
UKUPNI TROŠAK				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Navesti ciljeve i rezultate ⇩			2022.		2023.		2024.		2025.		2026.		2027.			
	REZULTATI															
	Vrsta[69]	Prosječni trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Ukupni broj	Ukupni trošak
POSEBNI CILJ br. 1[70] Izravni nadzor trećih strana pružatelja ključnih IKT usluga																
– Rezultat				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Međuzbroj za posebni cilj br. 1																
POSEBNI CILJ br. 2...																
– Rezultat																
Međuzbroj za posebni cilj br. 2																
UKUPNI TROŠAK				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Rezultati se odnose na proizvode i usluge koji se isporučuju (npr.: broj financiranih studentskih razmjena, kilometri izgrađenih prometnica itd.).

[70] Kako je opisan u odjeljku 1.4.2. „Posebni ciljevi…”.

Nadzorne aktivnosti u potpunosti će se financirati iz naknada naplaćenih od nadziranih subjekata na sljedeći način:

EBA

	2022.	2023.	2024.	2025.	2026.	2027.	Ukupno
Troškove u potpunosti pokrivaju naknade naplaćene od nadziranih subjekata[71].	1,373	1,948	1,748	1,748	1,748	1,748	10,313
UKUPNO sufinancirana odobrena sredstva	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022.	2023.	2024.	2025.	2026.	2027.	Ukupno
Troškove u potpunosti pokrivaju naknade naplaćene od nadziranih subjekata[72].	1,305	1,811	1,611	1,611	1,611	1,611	9,560
UKUPNO sufinancirana odobrena sredstva	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022.	2023.	2024.	2025.	2026.	2027.	Ukupno
Troškove u potpunosti pokrivaju naknade naplaćene od nadziranih subjekata[73].	1,373	1,948	1,748	1,748	1,748	1,748	10,313
UKUPNO sufinancirana odobrena sredstva	1,373	1,948	1,748	1,748	1,748	1,748	10,313

POSEBNE INFORMACIJE

Ovlasti za izravni nadzor

[71] 100 % ukupnog procijenjenog troška plus ukupni mirovinski doprinosi poslodavca.
[72] 100 % ukupnog procijenjenog troška plus ukupni mirovinski doprinosi poslodavca.
[73] 100 % ukupnog procijenjenog troška plus ukupni mirovinski doprinosi poslodavca.

Na početku treba podsjetiti da bi ESMA-i subjekti koji su pod njezinim izravnim nadzorom trebali plaćati naknade (jednokratni troškovi za registraciju i periodični troškovi za trajni nadzor). To vrijedi za agencije za kreditni rejting (vidjeti Delegiranu uredbu Komisije (EU) br. 272/2012) i trgovinske repozitorije (vidjeti Delegiranu uredbu Komisije (EU) br. 1003/2013).

Prema ovom zakonodavnom prijedlogu, europskim nadzornim tijelima povjerit će se nove zadaće čiji je cilj promicanje konvergencije pristupa nadzoru IKT rizika treće strane u financijskom sektoru tako da se treće strane pružatelje ključnih IKT usluga obuhvati nadzornim okvirom Unije.

Nadzorni okvir predviđen ovim Prijedlogom temelji se na postojećoj institucijskoj arhitekturi u području financijskih usluga, u okviru koje Zajednički odbor europskih nadzornih tijela osigurava međusektorsku koordinaciju svih pitanja povezanih s IKT rizicima u skladu sa svojim zadaćama u području kibersigurnosti, a u tome mu podršku pruža relevantni pododbor (Nadzorni forum) koji je odgovoran za svu pripremu pojedinačnih odluka i zajedničkih preporuka upućenih trećim stranama pružateljima ključnih IKT usluga.

U tom okviru europskim nadzornim tijelima koja su imenovana glavnim nadzornim tijelima za svaku treću stranu pružatelja ključnih IKT usluga dodjeljuju se ovlasti za primjereno paneuropsko praćenje pružatelja tehnoloških usluga koji imaju ključnu ulogu u funkcioniranju financijskog sektora. Nadzorne dužnosti utvrđene su u Prijedlogu i dodatno pojašnjene u Obrazloženju. One uključuju pravo na podnošenje zahtjeva za sve informacije i dokumentaciju bitne za provedbu općih istraga i nadzora, pravo na upućivanje preporuka te pravo da nakon toga podnesu izvješća o postupcima ili mjerama koje su treće strane pružatelji ključnih IKT usluga provele kako bi ispunile te preporuke.

Za obavljanje novih zadaća predviđenih ovim Prijedlogom, europska nadzorna tijela zapošljavaju dodatno osoblje specijalizirano za IKT rizik koje će se baviti procjenom ovisnosti o trećim stranama.

Procjenjuje se da će svakom tijelu trebati 6 zaposlenika u punom radnom vremenu (5 zaposlenika iz funkcijske skupine administratora (AD) i jedan iz funkcijske skupine asistenata (AST) kao podrška administratorima). Procjenjuje se da će europska nadzorna tijela imati i dodatne troškove za IT od 500 000 EUR (jednokratni troškovi) i da će svako od ta tri europska nadzorna tijela imati godišnje troškove održavanja od 50 000 EUR. Jedan važan element izvršenja novih zadaća misije su radi izravnog nadzora i revizija, što se procjenjuje na 200 000 EUR godišnje za svako europsko nadzorno tijelo. U stavku operativnih rashoda uključen je i godišnji iznos od 350 000 EUR za troškove prevođenja raznih dokumenata koje će europska nadzorna tijela primati od trećih strana pružatelja ključnih IKT usluga.

Svi prethodno navedeni administrativni troškovi u potpunosti će se financirati iz godišnjih pristojbi koje će europska nadzorna tijela naplaćivati od nadziranih trećih strana pružateljima ključnih IKT usluga (bez učinka na proračun EU-a).

EUROPSKA KOMISIJA

Bruxelles, 24.9.2020.
COM(2020) 596 final

2020/0268 (COD)

Prijedlog

DIREKTIVE EUROPSKOG PARLAMENTA I VIJEĆA

o izmjeni direktiva 2006/43/EZ, 2009/65/EZ, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 i EU/2016/2341

(Tekst značajan za EGP)

{SEC(2020) 309 final} - {SWD(2020) 203 final} - {SWD(2020) 204 final}

OBRAZLOŽENJE

1. KONTEKST PRIJEDLOGA

• Razlozi i ciljevi prijedloga

Ovaj Prijedlog dio je paketa mjera kojima se dodatno, uz istodobno ublažavanje rizika, omogućuje i podupire potencijal digitalnih financija u kontekstu inovacija i tržišnog natjecanja. U skladu je s Komisijinim prioritetima pripreme Europe za digitalno doba i izgradnje gospodarstva u interesu građana spremnog za budućnost. Paket o digitalnim financijama sadržava novu strategiju za digitalne financije za financijski sektor EU-a[1], s ciljem da EU prihvati digitalnu revoluciju te da ju pod vodstvom inovativnih europskih poduzeća potakne i tako svim europskim potrošačima i poduzećima omogući prednosti digitalnih financija. Osim ovog Prijedloga paket uključuje i Prijedlog uredbe o tržištima kriptoimovine[2], Prijedlog uredbe o pilot-režimu za tržišne infrastrukture koje se temelje na tehnologiji decentraliziranog vođenja evidencije transakcija (DLT)[3] i Prijedlog uredbe o digitalnoj operativnoj otpornosti za financijski sektor[4].

Razlozi i ciljevi tih dvaju skupova zakonodavnih mjera navedeni su u obrazloženju Prijedloga uredbe o pilot-režimu za tržišne infrastrukture koje se temelje na tehnologiji decentraliziranog vođenja evidencije transakcija, Prijedloga uredbe o tržištima kriptovimovine odnosno Prijedloga uredbe o digitalnoj operativnoj otpornosti te se i ovdje primjenjuju. Posebni razlozi za ovaj Prijedlog direktive odnose se na potrebu da se radi osiguranja pravne sigurnosti u pogledu kriptoimovine i postizanja ciljeva jačanja digitalne operativne otpornosti utvrdi privremeno izuzeće za multilateralne trgovinske platforme te izmijene ili pojasne određene odredbe u postojećim direktivama EU-a o financijskim uslugama.

• Dosljednost s postojećim odredbama politike u tom području

Ovaj Prijedlog, kao i prijedlozi uredbi iz istog paketa, dio je širih aktivnosti koje se provode na europskoj i međunarodnoj razni s ciljem i. jačanja kibersigurnosti u području financijskih usluga i uklanjanja većih operativnih rizika te ii. uvođenja jasnog, proporcionalnog i poticajnog pravnog okvira za pružatelje usluga povezanih s kriptoimovinom.

• Dosljednost u odnosu na druge politike Unije

Kako je predsjednica von der Leyen navela u svojim političkim smjernicama[5] i kako je navedeno u Komunikaciji „Izgradnja digitalne budućnosti Europe”[6], iznimno je važno da

---

[1] Komunikacija Komisije Europskom parlamentu, Europskom vijeću, Vijeću, Europskoj središnjoj banci, Europskom gospodarskom i socijalnom odboru i Odboru regija o strategiji za digitalne financije za EU, 23. rujna 2020., COM(2020) 591.

[2] Prijedlog uredbe Europskog parlamenta i Vijeća o tržištima kriptoimovine i izmjeni Direktive (EU) 2019/1937, COM(2020) 593.

[3] Prijedlog uredbe Europskog parlamenta i Vijeća o pilot-režimu za tržišne infrastrukture koje se temelje na tehnologiji decentraliziranog vođenja evidencije transakcija, COM(2020) 594.

[4] Prijedlog uredbe Europskog parlamenta i Vijeća o operativnoj otpornosti financijskog sektora i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014, COM(2020) 595.

[5] Predsjednica Ursula von Der Leyen, *Političke smjernice za sljedeću Europsku komisiju 2019.– 2024.*, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_hr.pdf.

Europa unutar sigurnih i etičkih granica iskoristi prednosti digitalnog doba i ojača svoj industrijski i inovacijski kapacitet.

Kad je riječ o kriptoimovini, ovaj je Prijedlog usko povezan sa širim politikama Komisije o tehnologiji lanaca blokova jer je kriptoimovina, kao glavna primjena tehnologije lanaca blokova, povezana s promicanjem te tehnologije u cijeloj Europi.

Kad je riječ o operativnoj otpornosti, u europskoj strategiji za podatke[7] navedena su četiri stupa – zaštita podataka, temeljna prava, sigurnost i kibersigurnost, kao ključni preduvjeti za društvo osnaženo upotrebom podataka. Pravni okvir za jačanje digitalne operativne otpornosti financijskih subjekata Unije dosljedan je s tim ciljevima politike. Prijedlogom bi se poduprle i politike oporavka od koronavirusa jer bi se osiguralo da sve veće oslanjanje na digitalne financije prati operativna otpornost. Oba prijedloga ujedno su i odgovor na pozive Foruma na visokoj razini o uniji tržišta kapitala da se utvrde jasna pravila za upotrebu kriptovaluta (preporuka br. 7.) te da se uspostave nova pravila o kiberotpornosti (preporuka br. 10.).[8]

2. PRAVNA OSNOVA, SUPSIDIJARNOST I PROPORCIONALNOST

- **Pravna osnova**

Ovaj Prijedlog direktive temelji se na članku 53. stavku 1. i članku 114. UFEU-a.

- **Supsidijarnost (za neisključivu nadležnost)**

Vidjeti obrazloženja prijedloga uredbi o tržištima kriptoimovine, privremenom režimu o tržišnim infrastrukturama DLT i digitalnoj operativnoj otpornosti.

- **Proporcionalnost**

Vidjeti obrazloženja prijedloga uredbi o tržištima kriptoimovine, privremenom režimu o tržišnim infrastrukturama DLT i digitalnoj operativnoj otpornosti.

- **Odabir instrumenta**

Ovaj Prijedlog direktive povezan je s prijedlozima uredbi o tržištima kriptoimovine, privremenom režimu o tržišnim infrastrukturama DLT i digitalnoj operativnoj otpornosti. U tim uredbama utvrđuju se ključna pravila kojima se uređuju i. pružatelji usluga povezanih s kriptoimovinom, ii. uvjeti za pilot-režim za tržišne infrastrukture DLT i iii. upravljanje IKT rizicima, izvješćivanje o incidentima, testiranje i nadzor. Kako bi se postigli ciljevi utvrđeni u tim uredbama, potrebno je utvrditi i privremeno izuzeće za multilateralne trgovinske platforme i izmijeniti nekoliko direktiva Europskog parlamenta i Vijeća donesenih na temelju članka 53. stavka 1. i članka 114. UFEU-a. Ovaj je Prijedlog direktive stoga potreban za izmjenu tih direktiva.

---

6 Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, Izgradnja digitalne budućnosti Europe, COM(2020)67 final.

7

8 Forum na visokoj razini o uniji tržišta kapitala (2020.). „Nova vizija za europska tržišta kapitala: završno izvješće, https://ec.europa.eu/info/sites/info/files/business_economy_euro/growth_and_investment/documents/200610-cmu-high-level-forum-final-report_en.pdf.

3. REZULTATI *EX POST* EVALUACIJA, SAVJETOVANJA S DIONICIMA I PROCJENA UČINKA

- ***Ex post* evaluacije/provjere primjerenosti postojećeg zakonodavstva**

Vidjeti obrazloženja prijedloga uredbi o tržištima kriptoimovine, privremenom režimu o tržišnim infrastrukturama DLT i digitalnoj operativnoj otpornosti.

- **Savjetovanja s dionicima**

Vidjeti obrazloženja prijedloga uredbi o tržištima kriptoimovine, privremenom režimu o tržišnim infrastrukturama DLT i digitalnoj operativnoj otpornosti.

- **Prikupljanje i primjena stručnog znanja**

Vidjeti obrazloženja prijedloga uredbi o tržištima kriptoimovine, privremenom režimu o tržišnim infrastrukturama DLT i digitalnoj operativnoj otpornosti.

- **Procjena učinka**

Vidjeti obrazloženja prijedloga uredbi o tržištima kriptoimovine, privremenom režimu o tržišnim infrastrukturama DLT i digitalnoj operativnoj otpornosti.

- **Primjerenost i pojednostavnjenje propisa**

Vidjeti obrazloženja prijedloga uredbi o tržištima kriptoimovine, privremenom režimu o tržišnim infrastrukturama DLT i digitalnoj operativnoj otpornosti.

- **Temeljna prava**

Vidjeti obrazloženja prijedloga uredbi o tržištima kriptoimovine, privremenom režimu o tržišnim infrastrukturama DLT i digitalnoj operativnoj otpornosti.

4. UTJECAJ NA PRORAČUN

Vidjeti obrazloženja prijedloga uredbi o tržištima kriptoimovine, privremenom režimu o tržišnim infrastrukturama DLT i digitalnoj operativnoj otpornosti.

5. DRUGI ELEMENTI

- **Planovi provedbe i mehanizmi praćenja, evaluacije i izvješćivanja**

Vidjeti obrazloženja prijedloga uredbi o tržištima kriptoimovine, privremenom režimu o tržišnim infrastrukturama DLT i digitalnoj operativnoj otpornosti.

- **Detaljno obrazloženje posebnih odredaba prijedloga**

Svi članci odnose se na Prijedlog uredbe o digitalnoj operativnoj otpornosti i dopunjuju ga. Sadržavaju izmjene raznih zahtjeva za upravljanje operativnim rizicima ili rizicima predviđenih u direktivama 2006/43/EZ, 2009/65/EZ, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 i EU/2016/2341 Europskog parlamenta i Vijeća tako što se u te odredbe uvode precizna upućivanja i time postiže pravna jasnoća. Konkretno:

– člancima od 2. do 4. te člancima 6. i 8. mijenjaju se Direktiva 2009/65/EZ o usklađivanju zakona i drugih propisa u odnosu na subjekte za zajednička ulaganja u prenosive vrijednosne papire (UCITS)[9], Direktiva 2009/138/EZ o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II),[10] Direktiva 2011/61/EU o upraviteljima alternativnih investicijskih fondova (Direktiva o UAIF-ima),[11] Direktiva 2014/56/EU o zakonskim revizijama godišnjih financijskih izvještaja i konsolidiranih financijskih izvještaja[12] i Direktiva EU/2016/2341 o djelatnostima i nadzoru institucija za strukovno mirovinsko osiguranje,[13] kako bi se za upravljanje tih financijskih subjekata njihovim sustavima i alatima IKT-a u svaku od tih direktiva uvela posebna upućivanja na Uredbu (EU) 2021/xx [DORA] jer bi ono trebalo biti u skladu s odredbama te uredbe,

– člankom 5. mijenjaju se zahtjevi iz Direktive 2013/36/EU (Direktiva o kapitalnim zahtjevima, CRD)[14] o planovima postupanja u kriznim situacijama i planovima kontinuiteta poslovanja kako bi se uvrstili planovi kontinuiteta poslovanja i planovi za oporavak od kriznih situacija u području informacijskih i komunikacijskih tehnologija u skladu s odredbama utvrđenima u Uredbi (EU) 2021/xx [DORA],

– člankom 6. mijenjaju se Direktiva 2014/65/EU o tržištima financijskih instrumenata (MIFID 2) dodavanjem upućivanja na Uredbu (EU) 2021/xx [DORA] te izmjenom odredbi koje se odnose na kontinuitet i redovitost investicijskih usluga i aktivnosti, otpornost i dostatan kapacitet sustava trgovanja, učinkovite mjere za kontinuitet poslovanja i upravljanje rizicima,

– člankom 7. mijenja se Direktiva (EU) 2015/2366 o platnim uslugama na unutarnjem tržištu (PSD2)[15], odnosno pravila o odobrenju uvođenjem upućivanja na Uredbu (EU) 2021/xx [DORA]. Osim toga, pravila o obavijesti o incidentima iz te direktive ne bi trebala uključivati obavijesti o IKT incidentima koje se Uredbom (EU) 2021/xx [DORA] u potpunosti usklađuju.

U članku 6. prvom stavku dodatno se objašnjava pravni tretman kriptoimovine koja se smatra financijskim instrumentom. To se postiže izmjenom definicije „financijskog instrumenta” u Direktivi 2014/65/EU o tržištima financijskih instrumenata kako bi se bez ikakve pravne

[9] Direktiva 2009/65/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o usklađivanju zakona i drugih propisa u odnosu na subjekte za zajednička ulaganja u prenosive vrijednosne papire (SL L 302, 17.11.2009., str. 32.).

[10] Direktiva 2009/138/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (SL L 335, 17.12.2009., str. 1.).

[11] Direktiva 2011/61/EU Europskog parlamenta i Vijeća od 8. lipnja 2011. o upraviteljima alternativnih investicijskih fondova i o izmjeni direktiva 2003/41/EZ i 2009/65/EZ te uredbi (EZ) br. 1060/2009 i (EU) br. 1095/2010 (SL L 174, 1.7.2011., str. 1.).

[12] Direktiva 2014/56/EU Europskog parlamenta i Vijeća od 16. travnja 2014. o izmjeni Direktive 2006/43/EZ o zakonskim revizijama godišnjih financijskih izvještaja i konsolidiranih financijskih izvještaja (SL L 158, 27.5.2014., str. 196.).

[13] Direktiva (EU) 2016/2341 Europskog parlamenta i Vijeća od 14. prosinca 2016. o djelatnostima i nadzoru institucija za strukovno mirovinsko osiguranje (SL L 354, 23.12.2016., str. 37.).

[14] Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ (SL L 176, 27.6.2013., str. 338.).

[15] Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ (SL L 337, 23.12.2015., str. 35.).

dvojbe pojasnilo da se ti instrumenti mogu izdavati primjenom tehnologije decentraliziranog vođenja evidencija transakcija.

Člankom 6. četvrtim stavkom dopunjuje se Prijedlog uredbe o pilot-režimu za tržišne infrastrukture tehnologije decentraliziranog vođenja evidencije transakcija privremenim izuzimanjem tržišnih infrastruktura koje se temelje na tehnologiji decentraliziranog vođenja transakcija od određenih odredbi Direktive 2014/65/EU kako bi im se omogućilo da razviju rješenja za trgovanje i namiru transakcija kriptoimovinom koja bi se smatrala financijskim instrumentima.

2020/0268 (COD)

Prijedlog

DIREKTIVE EUROPSKOG PARLAMENTA I VIJEĆA

o izmjeni direktiva 2006/43/EZ, 2009/65/EZ, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 i EU/2016/2341

(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 53. stavak 1. i članak 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europske središnje banke,[16]

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora,[17]

u skladu s redovnim zakonodavnim postupkom,

budući da:

(1) Unija treba primjereno i sveobuhvatno odgovoriti na digitalne rizike kojima su izloženi svi financijski subjekti, a koji proizlaze iz rastuće primjene informacijske i komunikacijske tehnologije (IKT) pri pružanju i korištenju financijskih usluga.

(2) Subjekti u financijskom sektoru u velikoj se mjeri oslanjaju na digitalne tehnologije u svakodnevnom poslovanju i stoga je iznimno važno zajamčiti operativnu otpornost njihovih digitalnih operacija na IKT rizike. To postaje sve važnije zbog rasta tržišta naprednih tehnologija, prvenstveno mogućnosti da se digitalni prikazi vrijednosti ili prava elektronički prenose i pohranjuju primjenom tehnologije decentraliziranog vođenja evidencije transakcija ili slične tehnologije („kriptoimovina”), te usluga povezanih s takvom imovinom.

(3) Na razini Unije zahtjevi koji se odnose na IKT rizik financijskog sektora trenutačno su sadržani u direktivama 2006/43/EZ,[18] 2009/66/EZ,[19] 2009/138/EZ,[20]

---

16 SL C ..., ..., str. 1....

17 SL C , , str. .

18 Direktiva 2006/43/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o zakonskim revizijama godišnjih financijskih izvještaja i konsolidiranih financijskih izvještaja, kojom se mijenjaju direktive Vijeća 78/660/EEZ i 83/349/EEZ i stavlja izvan snage Direktiva Vijeća 84/253/EEZ (SL L 157, 9.6.2006., str. 87).

19 Direktiva 2009/65/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o usklađivanju zakona i drugih propisa u odnosu na subjekte za zajednička ulaganja u prenosive vrijednosne papire (UCITS)(SL L 302, 17.11.2009., str. 32.).

20 Direktiva 2009/138/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II) (SL L 335, 17.12.2009., str. 1.).

2011/61/EZ,[21] EU/2013/36,[22] 2014/65/EU,[23] (EU) 2015/2366,[24] (EU) 2016/2341[25] Europskog parlamenta i Vijeća, različiti su i ponekad nepotpuni. U nekim je slučajevima IKT rizik samo implicitno naveden kao dio operativnog rizika, dok u drugima uopće nije naveden. To bi trebalo ispraviti usklađivanjem Uredbe (EU) xx/20xx Europskog parlamenta i Vijeća[26] [DORA] i tih akata. U ovoj se Direktivi predlaže niz izmjena koje se smatraju potrebnima radi pravne jasnoće i dosljednosti u vezi s raznim zahtjevima za digitalnu operativnu otpornost koji se primjenjuju na financijske subjekte koji imaju odobrenje za rad i nad kojima se provodi nadzor u skladu s tim direktivama, a koji su potrebni za obavljanje njihovih djelatnosti, čime se jamči neometano funkcioniranje unutarnjeg tržišta.

(4) U području bankarskih usluga, u Direktivi 2013/36/EU o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima utvrđuju se samo opća pravila o internom upravljanju i odredbe o operativnom riziku koje sadržavaju zahtjeve za planove postupanja u kriznim situacijama i planove kontinuiteta poslovanja koji implicitno služe kao osnova za razmatranje upravljanja IKT rizikom. Međutim, kako bi se osiguralo eksplicitno razmatranje IKT rizika, zahtjeve za planove postupanja u kriznim situacijama i planove kontinuiteta poslovanja trebalo bi izmijeniti da se uvrste planovi kontinuiteta poslovanja i planovi za oporavak od kriznih situacija i za IKT rizik, u skladu sa zahtjevima utvrđenima u Uredbi (EU) 2021/xx [DORA].

(5) U Direktivi 2014/65/EU o tržištu financijskih instrumenata utvrđuju se stroža pravila o IKT-u za investicijska društva i mjesta trgovanja samo ako se bave algoritamskim trgovanjem. Manje detaljni zahtjevi primjenjuju se na usluge dostave podataka i na trgovinske repozitorije. Osim toga, ta direktiva sadržava samo ograničene odredbe o mjerama nadzora i zaštite sustava za obradu podataka te o korištenju odgovarajućih sustava, sredstava i postupaka kojima se osigurava kontinuitet i redovitost poslovnih usluga. Tu bi direktivu trebalo uskladiti s Uredbom (EU) 2021/xx [DORA] u pogledu kontinuiteta i redovitosti investicijskih usluga i aktivnosti, operativne otpornosti, kapaciteta sustava trgovanja i učinkovitosti mjera za kontinuitet poslovanja i upravljanje rizicima.

(6) Trenutačno definicija „financijskog instrumenta” u Direktivi 2014/65/EU ne obuhvaća eksplicitno financijske instrumente koji se izdaju primjenom kategorije tehnologija koje podržavaju decentraliziranu evidenciju šifriranih podataka (tehnologija decentraliziranog vođenja evidencije transakcija, „DLT”). Kako bi se takvim financijskim instrumentima moglo trgovati na tržištu u skladu s postojećim

---

21 Direktiva 2011/61/EU Europskog parlamenta i Vijeća od 8. lipnja 2011. o upraviteljima alternativnih investicijskih fondova i o izmjeni direktiva 2003/41/EZ i 2009/65/EZ te uredbi (EZ) br. 1060/2009 i (EU) br. 1095/2010 (SL L 174, 1.7.2011., str. 1.).

22 Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ (SL L 176, 27.6.2013., str. 338.).

23 Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU (SL L 173, 12.6.2014., str. 349.).

24 Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ (SL L 337, 23.12.2015., str. 35.).

25 Direktiva (EU) 2016/2341 Europskog parlamenta i Vijeća od 14. prosinca 2016. o djelatnostima i nadzoru institucija za strukovno mirovinsko osiguranje (SL L 354, 23.12.2016., str. 37.).

26 SL L […], […], str. […].

pravnim okvirom, trebalo bi izmijeniti definiciju iz Direktive 2014/65/EU da ih se obuhvati.

(7) Osobito, kako bi se omogućio razvoj kriptoimovine koja bi se smatrala financijskim instrumentom i DLT-a, uz istovremenu visoku razinu financijske stabilnosti, integriteta tržišta, transparentnosti i zaštite ulagatelja, bilo bi korisno uspostaviti privremeni režim za tržišne infrastrukture DLT. Taj bi privremeni pravni okvir nadležnim tijelima trebao omogućiti da privremeno dopuste da tržišne infrastrukture DLT funkcioniraju na temelju alternativnog skupa zahtjeva o pristupu tim infrastrukturama, a ne onih koji se inače primjenjuju na temelju propisa Unije o financijskim uslugama koji bi ih mogli spriječiti u razvoju rješenja za trgovanje i namiru transakcija kriptoimovinom koja bi se smatrala financijskim instrumentom. Taj bi pravni okvir trebao biti privremen kako bi se europskim nadzornim tijelima i nacionalnim nadležnim tijelima omogućilo stjecanje iskustva o mogućnostima i posebnim rizicima koje donosi kriptoimovina kojom se trguje na tim infrastrukturama. Ova je Direktiva stoga povezana s Uredbom [o pilot-režimu za tržišne infrastrukture koje se temelje na tehnologiji decentraliziranog vođenja evidencije transakcija] i podržava taj novi regulatorni okvir Unije o tržišnim infrastrukturama DLT ciljanim izuzećem od određenih odredbi Unijinih propisa o financijskim uslugama koji se primjenjuju na aktivnosti i usluge u vezi s financijskim instrumentima kako su definirani u članku 4. stavku 1. točki 15. Direktive 2014/65/EU, a koji inače ne bi potpunu fleksibilnost koja je potrebna pri uvođenju rješenja u fazama transakcija trgovanja i nakon trgovanja koje uključuju kriptoimovinu.

(8) Multilateralna trgovinska platforma DLT trebala bi biti multilateralni sustav kojim upravlja investicijsko društvo ili tržišni operater koji ima odobrenje za rad u skladu s Direktivom 2014/65/EU, koji je dobio posebno odobrenje na temelju Uredbe (EU) xx/20xx Europskog parlamenta i Vijeća[27] [Prijedlog uredbe o pilot-režimu za tržišne infrastrukture DLT]. Na multilateralne trgovinske platforme DLT trebali bi se primjenjivati svi zahtjevi koji se primjenjuju na multilateralnu trgovinsku platformu na temelju te direktive, osim ako im nacionalno nadležno tijelo odobri izuzeće u skladu s ovom Direktivom. Jedna od mogućih regulatornih prepreka razvoju multilateralne trgovinske platforme za prenosive vrijednosne papire izdane na DLT-u mogla bi biti obveza posredovanja utvrđena Direktivom 2014/65/EU. Tradicionalna multilateralna trgovinska platforma može kao članove i sudionike prihvatiti samo investicijska društva, kreditne institucije i druge osobe koje imaju dovoljno stručnog znanja i kompetencija za trgovanje te odgovarajuću organizacijsku strukturu i sredstva. Multilateralnoj trgovinskoj platformi DLT trebalo bi omogućiti da zatraži izuzeće od takve obveze kako bi se malim ulagateljima omogućio jednostavan pristup mjestu trgovanja, pod uvjetom da postoje odgovarajuće zaštitne mjere za zaštitu ulagatelja.

(9) U Direktivi (EU) 2015/2366 o platnim uslugama propisana su posebna pravila o kontrolama sigurnosti informacijskih i komunikacijskih tehnologija te mjere ublažavanja za potrebe izdavanja odobrenja za obavljanje platnih usluga. Ta bi pravila o odobrenju trebalo izmijeniti radi njihova usklađenja s Uredbom (EU) 2021/xx [DORA]. Nadalje, pravila o obavijesti o incidentima iz te direktive ne bi se

[27] [puni naslov] (SL L […], […], str. […]).

trebala primjenjivati na obavijesti o IKT incidentima koje se Uredbom (EU) 2021/xx [DORA] u potpunosti usklađuju.

(10) Direktiva 2009/138/EZ o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja i Direktiva EU/2016/2341 o djelatnostima i nadzoru institucija za strukovno mirovinsko osiguranje djelomično pokrivaju IKT rizik u svojim općim odredbama o sustavu upravljanja te upravljanju rizicima, te bi neke zahtjeve trebalo detaljno urediti delegiranim uredbama s mogućim posebnim upućivanjima na IKT rizik. Neke još općenitije odredbe primjenjuju se na ovlaštene revizore i revizijska poduzeća jer Direktiva 2014/56/EU Europskog parlamenta i Vijeća[28] sadržava samo opće odredbe o unutarnjoj organizaciji. Slično tome, samo se vrlo općenita pravila primjenjuju na upravitelje alternativnih investicijskih fondova i društva za upravljanje na koje se primjenjuju direktive 2011/61/EU i 2009/65/EZ. Te bi direktive stoga trebalo uskladiti sa zahtjevima iz Uredbe (EU) 2021/xx [DORA] u pogledu upravljanja sustavima i alatima informacijske i komunikacijske tehnologije.

(11) U mnogim slučajevima dodatni zahtjevi o IKT-u već su utvrđeni u delegiranim i provedbenim aktima koji su doneseni na temelju nacrta tehničkih regulatornih i provedbenih tehničkih standarda koje je izradilo nadležno europsko nadzorno tijelo. Radi pravne jasnoće u pogledu činjenice da pravna osnova za odredbe o IKT riziku odsad proizlazi isključivo iz Uredbe (EU) 2021/xx [DORA], trebalo bi izmijeniti ovlasti iz tih direktiva uz objašnjenje da su odredbe o IKT riziku izvan opsega tih ovlasti.

(12) Kako bi se osigurala dosljedna i istovremena primjena Uredbe xx/20xx [DORA] i ove Direktive, koje zajedno čine novi okvir za digitalnu operativnu otpornost financijskog sektora, države članice trebale bi početi primjenjivati odredbe nacionalnog prava kojima se prenosi ova Direktiva od datuma primjene navedene uredbe.

(13) Direktive 2006/43/EZ, 2009/66/EZ, 2009/138/EZ, 2011/61/EZ, EU/2013/36, 2014/65/EU, (EU) 2015/2366 i (EU) 2016/2341 donesene su na temelju članka 53. stavka 1. i članka 114. Ugovora o funkcioniranju Europske unije. Izmjene iz ove Direktive trebale bi zbog međusobne povezanosti predmeta i ciljeva tih izmjena biti uključene u jedan akt, a taj jedan akt trebalo bi donijeti na temelju članka 53. stavka 1. i članka 114. Ugovora o funkcioniranju Europske unije.

(14) S obzirom na to da ciljeve ove Direktive ne mogu dostatno ostvariti države članice jer podrazumijevaju usklađivanja u obliku ažuriranja i izmjena zahtjeva koji su već navedeni u direktivama, nego se zbog njezina opsega i učinaka djelovanja oni na bolji način mogu ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim 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.

(15) U skladu sa Zajedničkom političkom izjavom država članica i Komisije od 28. rujna 2011. o dokumentima s objašnjenjima[29], države članice obvezale su se da će u opravdanim slučajevima uz obavijest o svojim mjerama za prenošenje priložiti jedan ili više dokumenata u kojima se objašnjava veza između sastavnih

---

28 Direktiva 2014/56/EU Europskog parlamenta i Vijeća od 16. travnja 2014. o izmjeni Direktive 2006/43/EZ o zakonskim revizijama godišnjih financijskih izvještaja i konsolidiranih financijskih izvještaja (SL L 158, 27.5.2014., str. 196.).

29 SL C 369, 17.12.2011., str. 14.

dijelova direktive i odgovarajućih dijelova nacionalnih instrumenata za prenošenje. U pogledu ove Direktive, zakonodavac smatra opravdanim dostavljanje takvih dokumenata,

DONIJELI SU OVU DIREKTIVU:

Članak 1.

Izmjene Direktive 2006/43/EZ

U članku 24.a stavku 1. Direktive 2006/43/EZ točka (b) zamjenjuje se sljedećim:

„(b) ovlašteni revizor ili revizorsko društvo dužni su raspolagati odgovarajućim administrativnim i računovodstvenim postupcima, mehanizmima unutarnje kontrole kvalitete, djelotvornim postupcima procjene rizika te djelotvornim mjerama nadzora i zaštite za upravljanje svojim sustavima i alatima informacijske i komunikacijske tehnologije u skladu s člankom 6. Uredbe (EU) 2021/xx [DORA] Europskog parlamenta i Vijeća*.

---

* [*puni naslov*] (SL L […], […], str. […]).”.

Članak 2.

Izmjene Direktive 2009/65/EZ

Članak 12. Direktive 2009/65/EZ mijenja se kako slijedi:

(1) u stavku 1. drugom podstavku točka (a) zamjenjuje se sljedećim:

„(a) da ima odgovarajuće administrativne i računovodstvene postupke, mjere nadzora i zaštite elektroničke obrade podataka, među ostalim sustave informacijske i komunikacijske tehnologije koji su uspostavljeni i kojima se upravlja u skladu s člankom 6. Uredbe (EU) 2021/xx Europskog parlamenta i Vijeća* [DORA], kao i odgovarajuće mehanizme unutarnjeg nadzora uključujući pravila za osobne transakcije svojih zaposlenika ili za posjedovanje ili upravljanje ulaganjima u financijske instrumente u svrhu ulaganja za vlastiti račun, kojima se barem osigurava da se svaka transakcija koja uključuje UCITS može rekonstruirati prema svojem porijeklu, uključenim stranama, vrsti te vremenu i mjestu na kojem je izvršena, te da se imovina UCITS-a kojom upravlja društvo za upravljanje ulaže u skladu s pravilima fonda ili dokumentima o osnivanju, te važećim zakonskim odredbama;

---

* [*puni naslov*] (SL L […], […], str. […]).”;

(2) stavak 3. zamjenjuje se sljedećim:

„3. Ne dovodeći u pitanje članak 116., Komisija donosi, putem delegiranih akata u skladu s člankom 112.a, mjere kojima se definira sljedeće:

(a) postupci i mjere iz stavka 1. drugog podstavka točke (a), osim onih koji se odnose na upravljanje rizicima informacijske i komunikacijske tehnologije;

(b) strukture i organizacijske zahtjeve za smanjenje sukoba interesa na najmanju moguću mjeru navedene u stavku 1. drugom podstavku točki (b). ”;

Članak 3.

Izmjena Direktive 2009/138/EZ

Direktiva 2009/138/EZ mijenja se kako slijedi:

(1) u članku 41. stavak 4. zamjenjuje se sljedećim:

„4. Društva za osiguranje i društva za reosiguranje dužna su poduzeti razumne mjere kako bi osigurala kontinuitet i redovitost svojih djelatnosti, uključujući i izradu planova postupanja u kriznim situacijama. U tu svrhu društvo koristi primjerene i proporcionalne sustave, resurse i postupke i uspostavlja sustave informacijske i komunikacijske tehnologije te njima upravlja u skladu s člankom 6. Uredbe (EU) 2021/xx Europskog parlamenta i Vijeća* [DORA].”;

---

* [*puni naslov*] (SL L […], […], str. […]).

(2) u članku 50. stavku 1. točke (a) i (b) zamjenjuju se sljedećim:

„(a) elemente sustava iz članaka 41., 44., 46. i 47., osim elemenata koji se odnose na upravljanje rizikom informacijske i komunikacijske tehnologije, i područja navedenih u članku 44. stavku 2.;”;

(b) funkcije iz članaka 44., 46., 47. i 48., osim funkcija koje se odnose na upravljanje rizikom informacijske i komunikacijske tehnologije.”.

Članak 4.

Izmjene Direktive 2011/61/EZ

Članak 18. Direktive 2011/61/EZ zamjenjuje se sljedećim:

„*Članak 18.*

Opća načela

1. Države članice zahtijevaju da UAIF-i u svakom trenutku koriste odgovarajuće i primjerene ljudske i tehničke resurse koji su nužni za pravilno upravljanje AIF-ima.

Nadležna tijela matične države članice UAIF-a, uzimajući u obzir i vrstu AIF-ova kojima upravlja UAIF, posebno zahtijevaju da UAIF-i imaju odgovarajuće administrativne i računovodstvene postupke, mjere nadzora i zaštite za upravljanje sustavima informacijske i komunikacijske tehnologije propisane člankom 6. [Uredba(EU) 2021/xx Europskog parlamenta i Vijeća* [DORA]], kao i primjerene mehanizme unutarnje kontrole uključujući, posebno, pravila za osobne transakcije svojih zaposlenika ili za posjedovanje ili upravljanje ulaganjima u financijske instrumente u svrhu ulaganja za vlastiti račun, kojima se barem osigurava da se svaka transakcija koja uključuje AIF-e može rekonstruirati prema svojem porijeklu, uključenim stranama, vrsti te vremenu i mjestu na kojem je izvršena, te da se imovina AIF-ova kojima upravlja UAIF ulaže u skladu s pravilima AIF-a ili osnivačkim aktom te važećim zakonskim odredbama.

2. Komisija putem delegiranih akata u skladu s člankom 56. te ovisno o uvjetima iz članaka 57. i 58. donosi mjere kojima se pobliže određuju postupci i mjere iz stavka 1., osim za sustave informacijske i komunikacijske tehnologije.

---

* [*puni naslov*] (SL L […], […], str. […]).”.

Članak 5.

Izmjena Direktive 2013/36/EU

U članku 85. Direktive 2013/36/EU stavak 2. zamjenjuje se sljedećim:

„2. Nadležna tijela osiguravaju da institucije imaju odgovarajuće planove postupanja u kriznim situacijama i planove kontinuiteta poslovanja, uključujući planove kontinuiteta poslovanja i planove za oporavak od kriznih situacija za tehnologiju koju koriste za komunikaciju informacija („informacijska i komunikacijska tehnologija”) izrađene u skladu s člankom 6. Uredbe (EU) 2021/xx Europskog parlamenta i Vijeća *[DORA], da mogu nastaviti s radom u slučaju ozbiljnih poremećaja u poslovanju i ograničiti gubitke nastale zbog takvog poremećaja.

---

* [*puni naslov*] (SL L […], […], str. […]).”

Članak 6.

Izmjene Direktive 2014/65/EU

Direktiva 2014/65/EU mijenja se kako slijedi:

(1) u članku 4. stavku 1. točka 15. zamjenjuje se sljedećim:

„financijski instrument” znači instrumenti utvrđeni u odjeljku C Priloga I., među ostalim instrumenti izdani primjenom tehnologije decentraliziranog vođenja evidencije transakcija;”;

(2) Članak 16. mijenja se kako slijedi:

(a) stavak 4. zamjenjuje se sljedećim:

„4. Investicijsko društvo poduzima odgovarajuće korake da bi osiguralo kontinuitet i redovitost investicijskih usluga i aktivnosti. U tu svrhu investicijsko društvo koristi primjerene i razmjerne sustave, uključujući sustave informacijske i komunikacijske tehnologije („IKT”) koji su uspostavljeni i kojima se upravlja u skladu s člankom 6. Uredbe (EU) 2021/xx Europskog parlamenta i Vijeća* [DORA] te primjerene i razmjerne resurse i postupke.”;

(b) u stavku 5. drugi i treći podstavak zamjenjuju se sljedećim:

„Investicijsko društvo dužno je imati odgovarajuće administrativne i računovodstvene postupke, mehanizme unutarnje kontrole i djelotvorne postupke procjene rizika.

Ne dovodeći u pitanje mogućnost da nadležna tijela zatraže pristup komunikaciji u skladu s ovom Direktivom i Uredbom (EU) br. 600/2014, investicijsko društvo dužno je imati dobre sigurnosne mehanizme kojima se jamči, u skladu sa zahtjevima iz Uredbe (EU) 2021/xx Europskog parlamenta i Vijeća* [DORA], sigurnost i autentikacija sredstava za prijenos podataka, smanjuje rizik oštećenja podataka i neovlaštenog pristupa te sprečava odavanje informacija neprekidnom zaštitom povjerljivosti podataka.”;

(3) Članak 17. mijenja se kako slijedi:

(a) stavak 1. zamjenjuje se sljedećim:

„1. Investicijsko društvo koje se bavi algoritamskim trgovanjem uspostavlja djelotvorne sustave i kontrolu rizika primjerene svojem poslovanju kako bi osiguralo da njegovi sustavi trgovanja budu otporni i imaju dovoljno kapaciteta u skladu sa zahtjevima utvrđenima u poglavlju II. Uredbe (EU) 2021/xx [DORA], da podliježu odgovarajućim pragovima i ograničenjima trgovanja te da spriječe slanje neispravnih naloga ili općenito rad sustava kojim se stvara ili doprinosi neurednosti tržišta.

Takvo društvo uspostavlja i djelotvorne sustave i kontrole rizika kako bi osiguralo da se sustavi za trgovanje ne koriste u svrhu koja je suprotna Uredbi (EU) br. 596/2014 ili pravilima mjesta trgovanja s kojim je povezano.

Investicijsko društvo uspostavlja djelotvorne mehanizme kontinuiteta poslovanja kako bi moglo riješiti svaki problem prekida sustava za trgovanje, uključujući planove za kontinuitet poslovanja i planove za oporavak od kriznih situacija za informacijsku i komunikacijsku tehnologiju utvrđene u skladu s člankom 6. Uredbe (EU) 2021/xx [DORA], i osigurava potpuno testiranje i pravilan nadzor kako bi se osiguralo da ispunjavaju opće zahtjeve iz ovog stavka i sve posebne zahtjeve iz poglavlja II. i IV. Uredbe (EU) 2021/xx [DORA].”;

(b) u stavku 7. točka (a) zamjenjuje se sljedećim:

„(a) pojedinosti organizacijskih zahtjeva navedenih u stavcima od 1. do 6., osim onih koji se odnose na upravljanje IKT rizikom, koje treba uvesti za investicijska društva koja pružaju razne investicijske usluge, investicijske aktivnosti, pomoćne usluge ili kombinaciju istih, pri čemu pojedinosti u vezi s organizacijskim zahtjevima iz stavka 5. utvrđuju posebne zahtjeve za izravan pristup tržištu i sponzorirani pristup tako da se osigura da kontrole koje se primjenjuju na sponzorirani pristup budu najmanje istovjetne onima koje se primjenjuju na izravan pristup tržištu;”;

(4) U članku 19. dodaje se sljedeći stavak:

„3. Međutim, ako investicijsko društvo ili tržišni operater upravlja multilateralnom trgovinskom platformom koja se temelji na tehnologiji decentraliziranog vođenja evidencije transakcija (multilateralna trgovinska platforma DLT) kako je definirana u članku 2. stavku 3. Uredbe xx/20xx [Prijedlog uredbe o pilot-režimu za tržišnu infrastrukturu DLT], nadležno tijelo može prema svojim pravilima kojima se uređuje pristup iz članka 18. stavka 3. na najviše na četiri godine dopustiti da investicijsko društvo ili tržišni operater prihvati fizičke osobe u multilateralnu trgovinsku platformu DLT kao članove ili sudionike, pod uvjetom da te osobe ispunjavaju sljedeće zahtjeve:

(a) moraju imati dovoljno dobar poslovni ugled i iskustvo; i

(b) moraju imati dovoljno stručnog znanja, osposobljenosti i iskustva za trgovanje, među ostalim znanja o trgovanju i funkcioniranju tehnologije decentraliziranog vođenja evidencija transakcija („DLT”).

Ako odobri izuzeće iz prvog podstavka, nadležno tijelo može odrediti dodatne mjere zaštite ulagatelja radi zaštite fizičkih osoba koje su prihvaćene u multilateralnu trgovinsku platformu DLT kao članovi ili sudionici. Te će mjere biti razmjerne profilu rizičnosti sudionika ili članova.”;

(5) u članku 47. stavak 1. mijenja se kako slijedi:

(a) točka (b) zamjenjuje se sljedećim:

„(b) budu primjereno opremljena za upravljanje rizicima kojima su izložena, uključujući upravljanje rizicima za sustave i alate IKT-a u skladu s člankom 6. Uredbe (EU) 2021/xx [DORA]*, kako bi uvela primjerene mjere i sustave za utvrđivanje svih značajnih rizika u poslovanju i uspostavila djelotvorne mjere za ublažavanje tih rizika.”;

(b) točka (c) briše se;

(6) članak 48. mijenja se kako slijedi:

(a) stavak 1. zamjenjuje se sljedećim:

„1. Države članice zahtijevaju da uređeno tržište izgradi svoju operativnu otpornost u skladu sa zahtjevima iz poglavlja II. Uredbe (EU) 2021/xx [DORA] kako bi se osiguralo da njegovi sustavi trgovanja budu otporni, da imaju dovoljno kapaciteta za obradu velikog broja naloga i poruka, da mogu osigurati uredno trgovanje u uvjetima tržišnog stresa, da budu u potpunosti testirani kako bi se osiguralo da ti uvjeti budu ispunjeni te da podliježu djelotvornim mehanizmima kontinuiteta poslovanja kako bi se osigurao kontinuitet njegovih usluga u slučaju prekida njegova sustava za trgovanje.].”;

(b) stavak 6. zamjenjuje se sljedećim:

„6. Države članice zahtijevaju da uređeno tržište ima uspostavljene učinkovite sustave, postupke i mehanizme, uključujući zahtjev da članovi ili sudionici provode odgovarajuća testiranja algoritama i omoguće okruženje kojima se olakšavaju takva testiranja u skladu sa zahtjevima iz poglavlja II. i IV. Uredbe (EU) 2021/xx [DORA], kako bi osiguralo da algoritamski sustavi trgovanja ne mogu prouzročiti ili doprinijeti neurednim uvjetima trgovanja na tržištu i kako bi se upravljalo neurednim tržišnim uvjetima koji se pojave u takvim algoritamskim sustavima trgovanja, uključujući sustave kojima se ograničava omjer neizvršenih naloga i transakcija koje je član ili sudionik mogao unijeti u sustav, koji bi mogli usporiti tok naloga ako se pojavi rizik dosezanja maksimalnog kapaciteta sustava te utvrditi i provoditi minimalni pomak cijene koji je dopušten na tržištu.”;

(c) stavak 12. mijenja se kako slijedi:

i. točka (a) zamjenjuje se sljedećim:

„(a) zahtjeva koji osiguravaju da sustavi uređenih tržišta budu otporni i da imaju dovoljan kapacitet, osim zahtjeva koji se odnose na digitalnu operativnu otpornost;”;

ii. točka (g) zamjenjuje se sljedećim:

zahtjeva koji osiguravaju odgovarajuće testiranje algoritama, osim testiranja digitalne operativne otpornosti, kako bi se osiguralo da sustavi algoritamskog trgovanja, uključujući visokofrekventno algoritamsko trgovanje, ne mogu prouzročiti ili doprinijeti neurednim uvjetima trgovanja na tržištu.”;

Članak 7.

Izmjene Direktive (EU) 2015/2366

Direktiva (EU) 2015/2366 mijenja se kako slijedi:

(7) u članku 5. stavku 1. trećem podstavku prva rečenica zamjenjuje se sljedećim:

„U kontroli sigurnosti i mjerama ublažavanja iz prvog podstavka točke (j) navodi se na koji način osigurava visoku razinu tehničke sigurnosti i zaštitu podataka, među ostalim za softver i IT sustave koje upotrebljava podnositelj zahtjeva ili društva kojima eksternalizira svoje cjelokupne operacije ili dio svojih operacija, u skladu s poglavljem II. Uredbe (EU) 2021/xx Europskog parlamenta i Vijeća * [DORA]. Te mjere uključuju i sigurnosne mjere utvrđene u članku 95. stavku 1. Tim mjerama uzimaju se u obzir smjernice EBA-e o sigurnosnim mjerama iz članka 95. stavka 3. kada se donesu.”; ___________________________

* [puni naslov] (SL L […], […], str. […]).

(8) članak 95. mijenja se kako slijedi:

(a) stavak 1. zamjenjuje se sljedećim:

„1. Države članice osiguravaju da pružatelji platnih usluga uspostave okvir s prikladnim mjerama ublažavanja i kontrolnim mehanizmima za upravljanje operativnim i sigurnosnim rizicima koji se odnose na platne usluge koje pružaju te da u tom okviru pružatelji platnih usluga utvrde i imaju djelotvorne postupke upravljanja incidentima, uključujući otkrivanje i klasifikaciju značajnih operativnih i sigurnosnih incidenata, razmatrajući pritom rizike za informacijsku i komunikacijsku tehnologiju u skladu s poglavljem II. Uredbe (EU) 2021/xx [DORA].”;

(b) stavak 4. briše se;

(c) stavak 5. zamjenjuje se sljedećim:

„5. EBA promiče suradnju, uključujući razmjenu informacija, između nadležnih tijela te između nadležnih tijela i ESB-a, u području operativnih rizika povezanih s platnim uslugama.”;

(9) članak 96. mijenja se kako slijedi:

(a) stavak 1. zamjenjuje se sljedećim:

„1. U slučaju značajnog operativnog ili sigurnosnog incidenta koji nije IKT incident kako je definiran u članku 3. stavku 6. Uredbe (EU) xx/20xx [DORA], pružatelj platnih usluga bez nepotrebne odgode obavješćuje nadležno tijelo u svojoj matičnoj državi članici.”;

(b) stavak 5. briše se;

(10) U članku 98. stavak 5. zamjenjuje se sljedećim:

„5. U skladu s člankom 10. Uredbe (EU) br. 1093/2010 EBA preispituje i, prema potrebi, redovito ažurira regulatorne tehničke standarde kako bi se, među ostalim, uzeli u obzir inovacije i tehnološki razvoj te odredbe poglavlja II. Uredbe (EU) 2021/xx [DORA].”.

Članak 8.

Izmjena Direktive (EU) 2016/2341

U članku 21. stavku 5. Direktive (EU) 2016/2341 druga rečenica zamjenjuje se sljedećim:

„U tu svrhu institucije za strukovno i mirovinsko osiguranje koriste primjerene i razmjerne sustave, resurse i postupke i uspostavljaju sustave i alate IKT-a te njima upravljaju u skladu s člankom 6. Uredbe (EU) 2021/xx Europskog parlamenta i Vijeća* [DORA].

---

* [*puni naslov*] (SL L […], […], str. […]).”.

Članak 9.

Prenošenje

1. Države članice najkasnije do [godina dana nakon donošenja] donose i objavljuju zakone i druge propise koji su potrebni radi usklađivanja s ovom Direktivom. One Komisiji odmah dostavljaju tekst tih odredaba.

   One primjenjuju te odredbe od [datum stupanja na snagu Uredbe DORA/njezin datum početka primjene, ako je različit].

   Kada države članice donose te odredbe, one sadržavaju upućivanje na ovu Direktivu ili se na nju upućuje prilikom njihove službene objave. Države članice određuju načine tog upućivanja.

2. Države članice Komisiji dostavljaju tekst glavnih odredaba nacionalnog prava koje donesu u području na koje se odnosi ova Direktiva.

Članak 10.

Stupanje na snagu

Ova Direktiva stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Članak 11.

Adresati

Ova je Direktiva upućena državama članicama.

Sastavljeno u Bruxellesu,

Za Europski parlament
Predsjednik

Za Vijeće
Predsjednik